ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Π.Μ.Σ. ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ:

ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ - ΖΗΤΗΜΑΤΑ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΗΝ ΕΞΥΠΝΗ ΠΟΛΗ (SMART CITY)

ΓΚΛΕΖΑΚΟΥ ΕΙΡΗΝΗ (ΜΔ2011)

Επιβλέπουσα Καθηγήτρια: κα Λίλιαν Μήτρου

Πειραιάς, Ιούνιος 2022

Θερμές ευχαριστίες στην επιβλέπουσα καθηγήτρια μου κα Λίλιαν Μήτρου για την υποστήριξή της στην εκπόνηση της παρούσης εργασίας.

Πίνακας περιεχομένων

ΠΕΡΙΛΗΨΗ

Η παρούσα εργασία έχει ως θέμα ζητήματα προστασίας προσωπικών δεδομένων που προκύπτουν εντός του πλαισίου μιας έξυπνης πόλης. Για να κατανοηθεί το φαινόμενο της έξυπνης πόλης εξετάζονται αρχικώς ο ορισμός αυτής και η αρχιτεκτονική της δομή. Εν συνέχεια αναφερόμαστε στο βασικό ρόλο που διαδραματίζει το Διαδίκτυο των Πραγμάτων καθώς και στους κινδύνους ασφαλείας που ενδέχεται να προκύψουν. Η απανταχού παρουσία του Διαδικτύου των Πραγμάτων μας κάνει στην πορεία να αναρωτιόμαστε για το κατά πόσο επηρεάζεται η ιδιωτικότητα του ατόμου εντός του περιβάλλοντος της έξυπνης πόλης. Περαιτέρω, εξαιτίας της σύνθεσης αυτής και υπό το πρίσμα του ΓΚΠΔ προβαίνουμε στην εξέταση ειδικότερων θεμάτων προστασίας προσωπικών δεδομένων με κύρια αναφορά στο ρόλο των εμπλεκόμενων μερών, στη νομιμότητα της επεξεργασίας , στη διενέργεια εκτίμησης αντικτύπου και στο σκοπό επεξεργασίας. Εν συνεχεία, δεδομένης της στενής σχέσης με το Διαδίκτυο των Πραγμάτων θίγονται ορισμένα ζητήματα αναφορικά με τα Μεγάλα Δεδομένα και την Τεχνητή Νοημοσύνη, σχετικά με την εφαρμογή αυτών στην έξυπνη πόλη και τους κινδύνους που ενέχουν έναντι της προστασίας των προσωπικών δεδομένων. Πριν ολοκληρώσουμε εξετάζουμε τη λειτουργία των ανοιχτών δεδομένων για τις έξυπνες πόλεις και το κατά πόσο ενδέχεται να επέμβουν στην προστασία του απορρήτου και τέλος αναφερόμαστε μέσα από παραδείγματα έξυπνων πόλεων στα μέτρα που μπορούν να ληφθούν από τις ‘’έξυπνες πόλεις’’ για την προστασία των προσωπικών δεδομένων.

ΕΙΣΑΓΩΓΗ

Οι Τεχνολογίες Πληροφορικής και Επικοινωνιών (ΤΠΕ), οι οποίες αναμφίβολα έχουν εισβάλλει και εκσυγχρονίσει σχεδόν όλους τους τομείς της σύγχρονης ζωής, δεν θα μπορούσαν σε καμία περίπτωση να αφήσουν ανεπηρέαστο το ''οικοσύστημα'' μιας πόλης. Η ενσωμάτωση νέων τεχνολογιών στις δομές μιας πόλης της προσέδωσε τον χαρακτηρισμό '"Έξυπνη Πόλη''. Η εξελισσόμενη επίσης παρουσία του Διαδικτύου των Πραγμάτων (ΔτΠ) κατέστησε οποιαδήποτε λειτουργία της πόλης ''συνδεδεμένη''.

Η αδιάλειπτη παραγωγή δεδομένων μέσα στον περιβάλλον της έξυπνης πόλης αποτελεί και την κινητήρια δύναμη για την περαιτέρω εξέλιξή της. Το σύνολο σχεδόν των αποφάσεων που λαμβάνονται κα αφορούν τις δράσεις που πρέπει να πραγματοποιηθούν για την εύρυθμη λειτουργία αυτής προσδιορίζεται πλέον από την ανάλυση των σχετικών δεδομένων. Ένας από τους βασικούς στόχους της έξυπνης πόλης, παραμένει ωστόσο η προστασία από την επεξεργασία των προσωπικών δεδομένων των υποκειμένων αυτής.

Με αφορμή την τελευταία αυτή διαπίστωση, επιχειρείται με την παρούσα να αναδειχθούν ορισμένοι βασικοί προβληματισμοί αναφορικά με την επεξεργασία των προσωπικών δεδομένων που λαμβάνει χώρα στο πλαίσιο των λειτουργιών μιας έξυπνης πόλης. Προς τούτο, στο πρώτο κεφάλαιο της παρούσας εξετάζεται αρχικά η έννοια και η αρχιτεκτονική δομή της έξυπνης πόλης, ο ρόλος του Διαδικτύου των Πραγμάτων στις λειτουργίες της, ενώ αναδεικνύονται και ορισμένα ζητήματα ασφάλειας αυτής. Στο δεύτερο κεφάλαιο εξετάζονται ζητήματα που σχετίζονται με την ιδιωτικότητα των κατοίκων μιας πόλης, ειδικότερα ζητήματα που προκύπτουν ως προς την επεξεργασία των προσωπικών αναφορικά με τον Γενικό Κανονισμό Προστασίας Δεδομένων ΕΕ 679/2016 (ΓΚΠΔ), ζητήματα σχετικά με την εφαρμογή των Μεγάλων Δεδομένων (Big Data) και της Τεχνητής Νοημοσύνης στο περιβάλλον της έξυπνης πόλης. Τέλος, γίνεται αναφορά στο ρόλο των ανοιχτών δεδομένων (open

data) και επισημαίνονται ορισμένοι κίνδυνοι από την αποανωνυμοποίηση των open data.

1. ΕΞΥΠΝΗ ΠΟΛΗ

1.1 ΟΡΙΣΜΟΣ

Στην βιβλιογραφία δεν υφίσταται ακόμη ένας ενιαίος ορισμός για την έννοια της έξυπνης πόλης, αλλά ποικίλοι ορισμοί, περίπου τριάντα έξι στον αριθμό, οι οποίοι διαμορφώνονται αναλόγως σε ποιο στοιχείο ή πτυχή αυτής δίνεται έμφαση[1]. Έτσι, μερικοί ορισμοί της ΕΠ επικεντρώνονται στις ΤΠΕ ως κινητήρια δύναμη και διευκόλυνση της τεχνολογίας, ενώ ευρύτεροι ορισμοί περιλαμβάνουν τις κοινωνικοοικονομικές διαστάσεις, το στοιχείο της διακυβέρνησης και τη συμμετοχή πολλών κατηγοριών ενδιαφερομένων, τη βελτίωση της βιωσιμότητας, της ποιότητας ζωής και της αστικής ευημερίας[2][1].

Σίγουρα όμως στην έννοια αυτής περιλαμβάνεται πρωτίστως η εφαρμογή Τεχνολογιών Πληροφορικής κι Επικοινωνιών, η οποία αφενός αποτελεί την ειδοποιό διαφορά μεταξύ της κλασικής έννοιας της πόλης και της ΕΠ, καθώς της παρέχει τη δυνατότητα να παρακολουθεί, να ελέγχει και να αξιοποιεί με το μέγιστο δυνατό τρόπο τις υπηρεσίες της (όπως είναι οι μεταφορές, ο ηλεκτρισμός, η προστασία του φυσικού περιβάλλοντος, η πρόληψη και καταστολή εγκλήματος, η υγεία των πολιτών, η παροχή κοινωνικών υπηρεσιών, η διαχείριση έκτακτων αναγκών και πολλοί άλλοι τομείς) και αφετέρου η ικανότητα να διαχειρίζεται τις πληροφορίες και τα δεδομένα που παράγονται σε αυτήν και τους πόρους που η ΕΠ διαθέτει με απώτερο σκοπό τη βελτίωση της ποιότητας ζωής των ανθρώπων της.

Ακολουθούν μερικές έννοιες της ΕΠ σε καθεμιά από τις οποίες δίνεται έμφαση σε συγκεκριμένο στοιχείο αυτής ή σε συγκεκριμένο σκοπό που η ΕΠ επιδιώκει[2]:

«Η χρήση των ΤΠΕ καθιστά τα κρίσιμα στοιχεία υποδομής και τις υπηρεσίες μιας πόλης – τα οποία περιλαμβάνουν τη διοίκηση της πόλης, την εκπαίδευση, την υγειονομική περίθαλψη,

[1] Mapping Smart Cities in the EU [2] Υπάρχουν βέβαια και εκείνοι[1] οι οποίοι έχουν προειδοποιήσει ότι ενδεχομένως οι πόλεις, που βιάζονται να χαρακτηριστούν ως ΄΄έξυπνες΄΄, μπορεί να αγνοήσουν τη σημασία του να καταστούν και βιώσιμες, με συνέπεια, εάν επικεντρωθούν αποκλειστικά στη βελτίωση των τεχνολογικών συστημάτων εύκολα να καταστούν ΄΄απαρχαιωμένες΄΄.

τη δημόσια ασφάλεια, τα κτίρια, τις μεταφορές και τις υπηρεσίες κοινής ωφέλειας – πιο έξυπνα, διασυνδεδεμένα και αποτελεσματικά» [2].

«Μια πόλη μπορεί να ονομάζεται ''Έξυπνη'' όταν οι επενδύσεις σε ανθρώπινο και κοινωνικό κεφάλαιο και οι παραδοσιακές και σύγχρονες επικοινωνιακές υποδομές, τροφοδοτούν βιώσιμη οικονομική ανάπτυξη και υψηλή ποιότητα ζωής, με συνετή διαχείριση των φυσικών πόρων, μέσω συμμετοχικής διακυβέρνησης[2][2]».

«Μια πόλη θεωρείται ''έξυπνη'' όταν υιοθετεί ψηφιακές τεχνολογίες που βασίζονται σε δεδομένα για το σχεδιασμό, τη διαχείριση και την παροχή δημοτικών υπηρεσιών. Οι τεχνολογίες πληροφοριών και επικοινωνιών (ΤΠΕ), η ανάλυση δεδομένων και το Διαδίκτυο των πραγμάτων (ΔτΠ) είναι μερικά από τα κύρια συστατικά αυτών των τεχνολογιών, σε συνδυασμό με το σχεδιασμό ιστοσελίδων, τις διαδικτυακές καμπάνιες μάρκετινγκ και τις ψηφιακές υπηρεσίες. Τέτοιες τεχνολογίες μπορεί να περιλαμβάνουν έξυπνες υποδομές κοινής ωφέλειας και μεταφορών, έξυπνες κάρτες, έξυπνες συγκοινωνίες, δίκτυα καμερών και αισθητήρων ή συλλογή δεδομένων από επιχειρήσεις για την παροχή προσαρμοσμένων διαφημίσεων ή άλλων υπηρεσιών»[3].

Από τους παραπάνω ορισμούς μπορεί κανείς να διακρίνει επίσης και την αναγκαιότητα στη σημερινή εποχή της ύπαρξης της ΕΠ. Το Μάϊο του 2018, σύμφωνα με στοιχεία του τμήματος Οικονομικών και Κοινωνικών Θεμάτων των Ηνωμένων Εθνών, το 55% του παγκόσμιου πληθυσμού ζούσε σε αστικές περιοχές, ποσοστό που αναμένεται να αυξηθεί στο 68% έως το 2050, ενώ σχετικές προβλέψεις δείχνουν ότι η αστικοποίηση, η σταδιακή μετατόπιση της κατοικίας του ανθρώπινου πληθυσμού από αγροτικές σε αστικές περιοχές, σε συνδυασμό με την αύξηση του παγκόσμιου πληθυσμού θα μπορούσε να προσθέσει άλλα 2,5 δισεκατομμύρια ανθρώπους στις αστικές περιοχές έως το 2050, με σχεδόν το 90% αυτής της αύξησης να λαμβάνει χώρα στην Ασία και την Αφρική[3][3]. Λαμβάνοντας υπόψη το γεγονός, ειδικοί τόσο στη βιομηχανία όσο και στον ακαδημαϊκό χώρο συμφώνησαν στην έξυπνη πόλη ως την ιδανική λύση για την αντιμετώπιση των προκλήσεων που προκύπτουν από τη δραστική αστικοποίηση, την αύξηση του πληθυσμού, την υποβάθμιση των πηγών ενέργειας, την περιβαλλοντική ρύπανση κ.λπ.[5] [9] Σε ευρωπαϊκό επίπεδο, οι

[2] Mapping Smart Cities in the EU, [2]

[3]https://www.un.org/development/desa/en/news/population/2018-revision-of-world-urbanization-prospects.html

πρωτοβουλίες για τις έξυπνες πόλεις μπορούν να θεωρηθούν χρήσιμο μέσο για την επίτευξη των στόχων τους στο πρόγραμμα Ευρώπη 2020[4]. Οι πόλεις είναι αστικά κέντρα που φιλοξενούν σημαντικό αριθμό ανθρώπων, συχνά σε πυκνοκατοικημένες περιοχές[2]. Για το λόγο αυτό, οι πόλεις ως έξυπνες οντότητες μπορεί να είναι ιδιαίτερα κατάλληλες για την ανάπτυξη πρωτοβουλιών προς αντιμετώπιση κρίσιμων προβλημάτων, όπως η ενέργεια και η κλιματική αλλαγή [2]. Η πυκνότητα και η ποικιλομορφία των κατοίκων (πληθυσμός και επιχειρήσεις) διευκολύνει την αμοιβαία αναγνώριση των προβλημάτων, την κινητοποίηση της κρίσιμης μάζας και την αποτελεσματική ανακατανομή και παρακολούθηση των ρόλων και των ευθυνών[2].

Σύμφωνα με έρευνα του 2020 από την εταιρεία συμβούλων Frost & Sullivan, οι επενδύσεις σε τεχνολογίες έξυπνων πόλεων αναμένεται να φτάσουν τα 327 δισεκατομμύρια δολάρια έως το 2025 (από 96 δισεκατομμύρια δολάρια το 2019)[7].

1.2 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΩΝ ΕΞΥΠΝΩΝ ΠΟΛΕΩΝ

Μια πόλη θα πρέπει να διαθέτει τα παρακάτω χαρακτηριστικά για να μπορεί να χαρακτηριστεί έξυπνη [2]:

Έξυπνη Διακυβέρνηση (smart governance) : Με τον όρο αυτό νοείται συνδυασμένη διακυβέρνηση εντός και εκτός των ορίων της πόλης, συμπεριλαμβανομένων υπηρεσιών και αλληλεπιδράσεων που συνδέουν και, όπου χρειάζεται, ενσωματώνουν δημόσιους, ιδιωτικούς, ευρωπαϊκούς και διεθνείς οργανισμούς, ώστε η πόλη να μπορεί να λειτουργεί αποδοτικά ως ένας οργανισμός. Η αλληλεπίδραση αυτή μπορεί να επιτευχθεί με τις ΤΠΕ, οι οποίες επιτρέπουν την εφαρμογή έξυπνων διαδικασιών και τη διαλειτουργικότητα και τροφοδοτούνται από δεδομένα. Η έξυπνη διακυβέρνηση συνίσταται επίσης στις συμπράξεις δημόσιου και ιδιωτικού τομέα και συνεργασία με διαφορετικούς για την επιδίωξη ''έξυπνων'' στόχων, όπως είναι η διαφάνεια, τα ανοιχτά δεδομένα με τη χρήση ΤΠΕ, η ηλεκτρονική διακυβέρνηση με τη συμμετοχική στη λήψη αποφάσεων και η παροχή ηλεκτρονικών υπηρεσιών. Μια έξυπνη διακυβέρνηση θα αλληλοεπιδράσει δυναμικά με τους πολίτες, την κοινότητα και τις επιχειρήσεις σε πραγματικό χρόνο για να πυροδοτήσει την ανάπτυξη, την καινοτομία και την πρόοδο[8].

[4] Η Ευρώπη 2020 είναι η στρατηγική της ΕΕ για την τόνωση της ανάπτυξης και των θέσεων εργασίας σε ολόκληρη την περιοχή, προκειμένου να δημιουργηθεί μια έξυπνη, βιώσιμη και χωρίς αποκλεισμούς οικονομία, https://www.eea.europa.eu/policy-documents/com-2010-2020-europe-2020

Έξυπνη οικονομία (smart economy): Με τον όρο Έξυπνη Οικονομία εννοούμε το ηλεκτρονικό επιχειρείν, το ηλεκτρονικό εμπόριο, την αυξημένη παραγωγικότητα, τη δυνατότητα παραγωγής ή παροχής υπηρεσιών και την καινοτομία με τη δυνατότητα ΤΠΕ. Η Έξυπνη Οικονομία σημαίνει επίσης τοπική και παγκόσμια διασύνδεση και διεθνή ενσωμάτωση με φυσικές και εικονικές ροές αγαθών, υπηρεσιών και γνώσεων.

Έξυπνη κινητικότητα (**smart mobility):** Ο όρος αυτός δηλώνει βιώσιμα, διασυνδεδεμένα και ολοκληρωμένα συστήματα μεταφορών και logistics, η λειτουργία των οποίων υποστηρίζεται από ΤΠΕ και τα οποία ενδεικτικά περιλαμβάνουν τραμ, λεωφορεία, τρένα, μετρό, αυτοκίνητα, ποδήλατα και πεζούς. Ειδικά για μια βιώσιμη κινητικότητα δίνεται προτεραιότητα σε καθαρές και συχνά μη μηχανοκίνητες επιλογές. Η χρήση ΤΠΕ στις μετακινήσεις παρέχει αφενός στο κοινό τη δυνατότητα να έχει πρόσβαση σε σχετικές πληροφορίες σε πραγματικό χρόνο, με σκοπό την εξοικονόμηση χρόνου και κόστους, τη βελτίωση της αποτελεσματικότητας των μετακινήσεων, τη μείωση των εκπομπών CO2, και αφετέρου, δίνει τη δυνατότητα στους διαχειριστές του δικτύου μεταφορών, σε συνδυασμό με την παροχή από τους χρήστες των δικών τους δεδομένων σε πραγματικό χρόνο, να βελτιώσουν τις παρεχόμενες υπηρεσίες τους και να παρέχουν εξίσου χρήσιμες πληροφορίες στους πολίτες. Οι μετακινήσεις αυτές, γνωστές και ως ευφυείς, Intelligent Transport Systems (ITS), περιλαμβάνουν επίσης διάφορους τύπους συστημάτων επικοινωνίας και πλοήγησης, μεταξύ οχημάτων (π.χ. car-to-car) και μεταξύ οχημάτων και σταθερών τοποθεσιών (π.χ. car-to-infrastructure)[9]. Τα ITS καλύπτουν επίσης συστήματα σιδηροδρομικών, υδάτινων και αεροπορικών μεταφορών, ακόμη και τις αλληλεπιδράσεις τους. Ως αποτέλεσμα, ανόμοια μέσα μεταφοράς διασυνδέονται μεταξύ τους για να προσφέρουν ένα παγκόσμιο σύστημα μεταφορών. Τα δίκτυα ad hoc οχημάτων (VANET) κέρδισαν μεγάλη προσοχή με την έννοια των ευφυών συστημάτων μεταφορών[10].

Έξυπνο περιβάλλον (smart environment): Στο έξυπνο περιβάλλον μιας πόλης περιλαμβάνονται οι ανανεώσιμες πηγές ενέργειας, τα ενεργειακά δίκτυα με τη χρήση ΤΠΕ, οι έξυπνοι μετρητές, ο έλεγχος και η παρακολούθηση της ρύπανσης, η ''πράσινη'' ανακαίνιση και ανέγερση κτιρίων, ο ''πράσινος'' αστικός σχεδιασμός, καθώς και η αποδοτικότητα, η επαναχρησιμοποίηση και η υποκατάσταση των φυσικών πόρων[9].

Σημαντικό παράδειγμα αποτελεί η ικανότητα λήψης αποφάσεων βάσει δεδομένων που ''παράγονται'' από τα έξυπνα κτίρια, έτσι ώστε να μεγιστοποιηθεί η ενεργειακή τους απόδοση, να ελαχιστοποιηθεί το λειτουργικό τους κόστος και να ενώ παράλληλα

συνδέονται περαιτέρω με άλλα συστήματα για τη διαχείριση της ασφάλειας, της επιτήρησης, του ελέγχου φωτισμού κ.λπ.[9] Επιπλέον, η αξιοποίηση της γνώσης μέσω των διαθέσιμων δικτύων επιτρέπει στα έξυπνα κτίρια να βελτιώσουν την ποιότητα των υπηρεσιών που προσφέρονται στους ενοίκους αυτών.

Η έξυπνη ενέργεια, ως μέρος του έξυπνου περιβάλλοντος, προωθεί μια ολιστική προσέγγιση καθώς συμπεριλαμβάνει την πράσινη ενέργεια, τη βιώσιμη ενέργεια και τις ανανεώσιμες πηγές ενέργειας. Στοχεύει στην εξυπηρέτηση των ενεργειακών απαιτήσεων μιας κοινότητας, ενσωματώνοντας τις ανανεώσιμες πηγές ενέργειας για τη διατήρηση της βιωσιμότητας των μη ανανεώσιμων πηγών ενέργειας, ελαχιστοποιώντας παράλληλα τις αρνητικές επιπτώσεις στο περιβάλλον, όπως τη μείωση του αποτυπώματος άνθρακα[11].

Ένα έξυπνο δίκτυο ενέργειας ενσωματώνει αποτελεσματικά τις δράσεις και τις συμπεριφορές όλων των συνδεδεμένων χρηστών, δηλαδή των καταναλωτών και των παραγωγών. Η αποτελεσματική διανομή ενέργειας στο έξυπνο ενεργειακό σύστημα καθίσταται δυνατή με τη χρήση έξυπνων υποδομών, έξυπνων δικτύων, έξυπνων μετρητών καθώς και κατάλληλου επιπέδου αξιοποίησης της τεχνολογίας πληροφοριών και επικοινωνιών (ΤΠΕ) [9]. Ο πυρήνας ενός έξυπνου ενεργειακού συστήματος είναι η πληροφοριακή υποδομή που είναι υπεύθυνη για τη συλλογή των πληροφοριών κατανάλωσης ενέργειας καθώς και για την κοινή χρήση των πληροφοριών σχετικά με την τιμή του παρόχου ενέργειας [9].

Έξυπνοι άνθρωποι (smart people): Στον όρο Έξυπνοι Άνθρωποι περιλαμβάνονται εκείνοι που διαθέτουν ηλεκτρονικές δεξιότητες, εκείνοι που δύνανται να εργαστούν με τη χρήση ΤΠΕ, έχουν πρόσβαση στην εκπαίδευση και στην κατάρτιση, στη διαχείριση ανθρώπινων πόρων, και τοποθετούνται σε μια κοινωνία που βελτιώνει τη δημιουργικότητα και προωθεί την καινοτομία, δίχως αποκλεισμούς. Αυτό το χαρακτηριστικό της ΕΠ επιτρέπει σε άτομα και κοινότητες να εισάγουν, να χρησιμοποιούν και να διαχειρίζονται δεδομένα, μέσω κατάλληλων εργαλείων ανάλυσης, να λαμβάνουν αποφάσεις και να δημιουργούν προϊόντα και υπηρεσίες.

Έξυπνος τρόπος ζωής (smart living): Με αυτόν τον όρο νοούνται οι τρόποι συμπεριφοράς και κατανάλωσης που υποστηρίζονται από ΤΠΕ. Το Smart Living δηλώνει επίσης μια υγιή και ασφαλή διαβίωση σε μια πολιτιστικά ζωντανή πόλη με ποικίλες πολιτιστικές εγκαταστάσεις,. Το Smart Living συνδέεται επίσης με υψηλά επίπεδα κοινωνικής συνοχής και κοινωνικού κεφαλαίου.

Μέρος της έξυπνης διαβίωσης θεωρείται η έξυπνη υγειονομική περίθαλψη, η οποία αποτελεί συνδυασμό στοιχείων, όπως της παραδοσιακής υγειονομικής περίθαλψης, των έξυπνων βιοαισθητήρων, των φορητών συσκευών, των ΤΠΕ και των έξυπνων συστημάτων ασθενοφόρων [9]. Η τηλεϊατρική μπορεί να θεωρηθεί ως συγκεκριμένο παράδειγμα έξυπνης υγειονομικής περίθαλψης, δυνάμει της οποίας παρέχεται κλινική υγειονομική περίθαλψη σε απομακρυσμένες τοποθεσίες. Μέσω των εφαρμογών smart health care, παρέχονται δεδομένα υγείας ασθενών σε εξουσιοδοτημένους χρήστες, όπως ιατροί, νοσηλευτές και τεχνικοί εργαστηρίων, μέσω ασφαλούς δικτύου νοσοκομειακών συστημάτων, με σκοπό τη λήψη αποφάσεων σε πραγματικό χρόνο για την κατάσταση της υγείας των ασθενών [10]. Έτσι, η ενσωμάτωση της έξυπνης υγειονομικής περίθαλψης στις έξυπνες πόλεις αποτελεί καίριο χαρακτηριστικό στην παγκόσμια υλοποίηση της έννοιας της έξυπνης πόλης.

Όπως έγινε φανερό από τα παραπάνω, οι τεχνολογίες πληροφορικής κι επικοινωνιών είναι το κλειδί για το σχεδιασμό, την υλοποίηση και τη λειτουργία έξυπνων πόλεων. Διαφορετικού είδους στοιχεία, όπως υποδομές, κτίρια, φυσικές κατασκευές, ηλεκτρική υποδομή, υποδομές επικοινωνιών, συμβάλλουν στην πραγματοποίηση των ΕΠ [9]. Ωστόσο, η ενσωμάτωση έξυπνων και ασφαλών τεχνολογιών, ώστε οι πόλεις να είναι όχι μόνο έξυπνες αλλά και βιώσιμες, η δε εγκατάσταση τέτοιων σύγχρονων τεχνολογιών να μην είναι οικονομικά δυσβάσταχτη για την πόλη και τους κατοίκους αυτής, αποτελεί μεγάλη πρόκληση.

1.3 ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΗΣ ΕΞΥΠΝΗΣ ΠΟΛΗΣ

Οι ερευνητές εργάζονται ένθερμα για τον καθορισμό της αρχιτεκτονικής ΕΠ με σκοπό την ανάπτυξη έξυπνων πόλεων στον πραγματικό κόσμο. Ωστόσο, η σκοπιμότητα καθορισμού μιας καθολικής αρχιτεκτονικής έξυπνων πόλεων για ανάπτυξη σε πραγματικό κόσμο απέχει πολύ από την πραγματικότητα, αν και θεωρητικά εφικτή. Μια τυπική αρχιτεκτονική δομή της ΕΠ έχει ως εξής:

ΕΠΙΠΕΔΟ ΣΥΛΛΟΓΗΣ: Στο επίπεδο αυτό περιλαμβάνονται οι υποδομές της ΕΠ, όπως αυτές των μεταφορών, της υγείας, της μέτρησης της ποιότητας του αέρα και του νερού, στις οποίες είναι εγκατεστημένοι αισθητήρες, ενεργοποιητές, αναγνώστες και άλλες συσκευές

ανίχνευσης. Η συλλογή των δεδομένων που απαρτίζουν και ταυτόχρονα παράγονται στο περιβάλλον μιας ΕΠ αποτελούν το σημαντικότερο ρόλο για τη λειτουργία των υπολοίπων υπηρεσιών αυτής, ενώ παράλληλα η συλλογή και η επεξεργασία τους αποδεικνύεται μια ιδιαίτερα απαιτητική διαδικασία εξαιτίας της ετερογένειας και της πολυπλοκότητας αυτών [11]. Έτσι, το επίπεδο ανίχνευσης και συλλογής δεδομένων, αποτελεί το πρώτο επίπεδο της ΕΠ, το οποίο απαρτίζεται από έξυπνες συσκευές και διαφόρων ειδών συσκευές καταγραφής διαφόρων τύπων δεδομένων και παραμέτρους δεδομένων (π.χ. υγρασία, θερμοκρασία, πίεση, φως, κ.λπ.) [11]. Το επίπεδο ανίχνευσης προσφέρει διάφορες τεχνικές για τη βελτίωση της απόδοσης λήψης δεδομένων σε διαφορετικά περιβάλλοντα, μεταξύ των οποίων αισθητήρες Zigbee, Bluetooth και αναγνώρισης ραδιοσυχνοτήτων (RFID), ενεργοποιητές, κάμερες και συσκευές με ενσωματωμένο σύστημα εντοπισμού θέσης (GPS). Ωστόσο μια ευρεία κάλυψη, η οποία επιτυγχάνεται από τον αυξανόμενο των συνδεδεμένων στο δίκτυο συσκευών, δεν συνεπάγεται αυτόματα και την αξιόπιστη μετάδοση των δεδομένων [11].

ΕΠΙΠΕΔΟ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΩΝ

Η σύνδεση των δεδομένων που παράγονται στο πρώτο επίπεδο, με τους σταθμούς διαχείρισης, πραγματοποιείται στο δεύτερο επίπεδο, αυτό της μετάδοσης, το οποίο είναι και η ραχοκοκαλιά της ΕΠ, αποτελείται δε από διάφορους τύπους ενσύρματων και ασύρματων δικτύων και δορυφορικών τεχνολογιών. Αναλόγως το πεδίο κάλυψης, το επίπεδο μετάδοσης χωρίζεται περαιτέρω σε δύο υποεπίπεδα, δίκτυο πρόσβασης και δίκτυο μετάδοσης[11]. Τεχνολογίες όπως Bluetooth[5], Zigbee[6], επικοινωνία κοντινού πεδίου (NFC)[7],Machine to machine (M2M), RFID[8] είναι γνωστές ως τεχνολογίες δικτύου πρόσβασης που παρέχουν συγκριτικά μικρής εμβέλειας κάλυψη. Τεχνολογίες που προσφέρουν

[5] Το Bluetooth είναι μια άλλη δημοφιλής τεχνολογία δικτύου πρόσβασης που μειώνει σημαντικά την κατανάλωση ενέργειας στην επικοινωνία, λόγω των ραδιοφωνικών σημάτων μικρού μήκους κύματος.

[6] Το ZigBee προσφέρει επικοινωνία χαμηλής ισχύος μεταξύ συσκευών με δυνατότητα ZigBee εντός εμβέλειας 10 μέτρων. Το πιο σημαντικό, το ZigBee αξιοποιεί την αυτοοργανωμένη, αξιόπιστη και πολλαπλή δικτύωση πλέγματος μαζί με μεγάλη διάρκεια ζωής της μπαταρίας

[7] Το NFC είναι μια τεχνολογία δικτύου πρόσβασης που διευκολύνει την επικοινωνία μεταξύ δύο συσκευών σε απόσταση 10 εκατοστών. Το NFC εκτελεί αναγνώριση, ενώ μοιράζεται πληροφορίες μεταξύ συσκευών με δυνατότητα NFC.

[8] Η τεχνολογία RFID έχει τμήμα ραδιοσυχνοτήτων (RF) του ηλεκτρομαγνητικού φάσματος για να αναγνωρίσει ένα μοναδικό αντικείμενο, ένα άτομο, ένα όχημα ή ένα ζωο. Στην πραγματικότητα, το RFID έχει κοινές ομοιότητες με τα συστήματα barcode. Ωστόσο, αποδίδει καλά στην αναγνώριση πραγμάτων από απόσταση σε σύγκριση με τα συστήματα barcode.

ευρύτερη κάλυψη, όπως 3G, 4G, 5G[9] και δίκτυα ευρείας περιοχής χαμηλής κατανάλωσης (LP-WAN) είναι γνωστές ως τεχνολογίες δικτύου μετάδοσης . Ο συνεχώς αυξανόμενος αριθμός έξυπνων συσκευών, η κινητικότητα και οι πτυχές ευρείας περιοχής έχουν προωθήσει τη ζήτηση για ασύρματα δίκτυα ευρείας εμβέλειας σε εργασίες σχεδιασμού και υλοποίησης των ΕΠ. Για τη λειτουργία της ΕΠ απαιτείται μια υποδομή δικτύου υψηλής ταχύτητας που θα συνδυαστεί με τα δίκτυα αισθητήρων για να υποστηρίξει την αναμενόμενη αύξηση του αριθμού των συνδεδεμένων συσκευών και να διευκολύνει την κινητικότητα, τη σύνδεση και την κοινή χρήση των πληροφοριών [8].

ΕΠΙΠΕΔΟ ΔΙΑΧΕΙΡΙΣΗΣ ΔΕΔΟΜΕΝΩΝ [11] Το τρίτο επίπεδο διαχείρισης δεδομένων, στο οποίο λαμβάνουν χώρα εργασίες διαχείρισης δεδομένων, οργάνωσης, ανάλυσης, αποθήκευσης και λήψης αποφάσεων, αποτελεί το πιο σημαντικό μεταξύ όλων των επιπέδων που συνθέτουν την ΕΠ και για το λόγο αυτό χαρακτηρίζεται και ως ο ''εγκέφαλος'' κάθε ΕΠ. Η αποτελεσματικότητα αυτού του επιπέδου διαχείρισης είναι ζωτικής σημασίας για μια βιώσιμη ΕΠ, καθώς η απόδοση υπηρεσιών των λειτουργιών των ΕΠ βασίζεται στη διαχείριση δεδομένων. Οι έξυπνες λειτουργίες της ΕΠ εκτελούνται από στοιχεία διαχείρισης συμβάντων και διαχείρισης αποφάσεων. Το τμήμα διαχείρισης αποφάσεων προβαίνει στη λήψη των κατάλληλων αποφάσεων σύμφωνα με τα δεδομένα που συγκεντρώθηκαν από ετερογενείς πηγές δεδομένων, τα δεδομένα που ανακτήθηκαν από τα συστήματα αποθήκευσης δεδομένων, και την επεξεργασία αυτών, πολλές φορές με τη χρήση αλγόριθμων, με απώτερο σκοπό τη μεταφορά αυτών στο αμέσως επόμενο επίπεδο, αυτό της εφαρμογής, για να εκτελεστούν ανάλογα.

ΕΠΙΠΕΔΟ ΕΦΑΡΜΟΓΗΣ Πρόκειται για το ανώτερο επίπεδο της αρχιτεκτονικής μιας ΕΠ, η αποτελεσματική απόδοση του οποίου επηρεάζει άμεσα και σημαντικά τις προσδοκίες των κατοίκων και την ικανοποίηση τους από τις λειτουργίες της ΕΠ, καθώς αλληλεπιδρά άμεσα με αυτούς [11]. Στις υπηρεσίες του επιπέδου αυτού περιλαμβάνονται τα στοιχεία που απαρτίζουν την ΕΠ και αναφέρονται ανωτέρω υπό 1.2[10]. Αυτό το τελευταίο επίπεδο κλιμακώνει την απόδοση της πόλης μέσω πολυάριθμων εφαρμογών που χρησιμοποιούν επεξεργασμένα και αποθηκευμένα δεδομένα. Για το λόγο αυτό, η ενεργοποίηση της

[9] Το κυψελοειδές δίκτυο πέμπτης γενιάς (5G) είναι το τσιτάτο στις σύγχρονες τηλεπικοινωνίες. Στα δίκτυα 5G, μεγάλος αριθμός τεράστιων κεραιών πολλαπλών εισόδων πολλαπλών εξόδων, είναι ενσωματωμένος σε σταθμούς βάσης για τη μεταφορά ασύρματης κίνησης σε επίπεδο gigabit.

[10] Βλ. κεφάλαιο 1.2.

ανταλλαγής πληροφοριών μεταξύ διαφορετικών εφαρμογών φαίνεται ως μια πολλά υποσχόμενη προσέγγιση για την εξέλιξη των ΕΠ.

1.4 ΠΑΡΑΔΕΙΓΜΑΤΑ ΕΞΥΠΝΩΝ ΠΟΛΕΩΝ

Η πόλη της Σιγκαπούρης [12]

Η Σιγκαπούρη παραμένει εδώ και τρία χρόνια στην πρώτη θέση στην κατάταξη των ΕΠ. Από τα πιο χαρακτηριστικά στοιχεία της Σιγκαπούρης ως έξυπνης πόλης είναι η βελτιστοποίηση της αποδοτικότητας των μεταφορών για όλους τους κατοίκους. Η Υπηρεσία Επιστήμης, Τεχνολογίας και Έρευνας δημιούργησε έναν αυτόνομο στόλο για να βοηθήσει τους ηλικιωμένους και τους κατοίκους με ειδικές ανάγκες της πόλης να παραμείνουν κινητικοί. Οι φοιτητές στο Εθνικό Πανεπιστήμιο της Σιγκαπούρης μπορούν να μεταφερθούν γύρω από την πανεπιστημιούπολη με αυτοοδηγούμενο λεωφορείο. Δεδομένα από κάρτες εισιτηρίων, από αισθητήρες σε περισσότερα από 5.000 οχήματα και από την παρακολούθηση των λεωφορείων σε πραγματικό χρόνο, αναλύονται για τη βελτιστοποίηση των μεταφορών.

Ένας άλλος τομέας στον οποίο ξεχωρίζει η Σιγκαπούρη είναι αυτός της υγείας. Δεδομένου ότι μέχρι το 2050, το 47% του πληθυσμού της Σιγκαπούρης θα είναι 65 ετών και άνω, για να μειώσει την πίεση του γηράσκοντος πληθυσμού στις υπηρεσίες περίθαλψης των κατοίκων της πόλης, η Σιγκαπούρη έχει ψηφιοποιήσει το σύστημα υγειονομικής περίθαλψής της. Οι συμβουλές μέσω του βίντεο TeleHealth αντικαθιστούν τις φυσικές επισκέψεις όταν αυτές δεν είναι εφικτές, ενώ το σύστημα TeleRehab επιτρέπει στους ασθενείς να κάνουν ασκήσεις στο σπίτι τους. Φορητές συσκευές παρακολουθούν την πρόοδο των ασθενών και μεταδίδουν τα δεδομένα στον θεραπευτή τους μέσω ασύρματου δικτύου. «Chatbot» που υποστηρίζονται από τεχνητή νοημοσύνη (AI) μιλούν με ηλικιωμένους, τους ενημερώνουν για δραστηριότητες της κοινότητας και ενσωματώνουν μηνύματα που προάγουν την υγιεινή ζωή. Το έξυπνο σύστημα προειδοποίησης ηλικιωμένων που λειτουργεί με ΤΝ παρακολουθεί και μαθαίνει τις τακτικές κινήσεις των ανθρώπων, ειδοποιώντας τον φροντιστή όταν συμβαίνει κάτι ασυνήθιστο και μπορεί να απαιτείται επείγουσα φροντίδα.

Η πόλη της Βαρκελώνης

Η Βαρκελώνη, δεύτερη μεγαλύτερη πόλη στην Ισπανία, βρίσκεται στην κορυφή μεταξύ των καλύτερων έξυπνων πόλεων στην Ευρώπη. Στη διαδικασία μετασχηματισμού της Βαρκελώνης, ο απώτατος στόχος ήταν να χρησιμοποιηθούν οι ΤΠΕ στις επιχειρηματικές διαδικασίες και στη δημόσια διοίκηση για τη βελτίωση της προσβασιμότητας, της διαφάνειας και της αποτελεσματικότητας των υπηρεσιών. Η υποδομή, οι πληροφορίες και το ανθρώπινο κεφάλαιο προσδιορίζονται ως τα κύρια πλεονεκτήματα της έξυπνης πόλης της Βαρκελώνης [11].

Η έξυπνη πόλη της Βαρκελώνης περιλαμβάνει διάφορες νέες υπηρεσίες, όπως εσωτερικές διοικητικές υπηρεσίες, υπηρεσίες βελτίωσης της καθημερινής ζωής των πολιτών και υπηρεσίες από πολίτη σε πολίτη. Οι εσωτερικές κυβερνητικές υπηρεσίες βοηθούν τους δημοτικούς συμβούλους να λαμβάνουν καλύτερες αποφάσεις και να σχεδιάζουν πολιτικές με τη βοήθεια χρήσιμων πληροφοριών που παρέχονται μέσω των δημοσίων υπαλλήλων[11]. Το μοντέλο της πόλης διανέμει ενημερωμένες πληροφορίες για να προσφέρει καλύτερες υπηρεσίες που κάνουν την καθημερινή ζωή των πολιτών πιο άνετη. Προκειμένου να ανταποκριθεί σε αυτές τις πράξεις, η πόλη της Βαρκελώνης είναι εξοπλισμένη με ένα εταιρικό δίκτυο οπτικών ινών, δίκτυο Wi-Fi mesh, δίκτυο αισθητήρων πολλαπλών χρήσεων και πολλαπλών πωλητών και ένα δημόσιο δίκτυο Wi-Fi. Το εξαιρετικά πυκνό δίκτυο αισθητήρων της Βαρκελώνης ενισχύει περαιτέρω τη δημιουργία δεδομένων που υποστηρίζουν τη διαχείριση των υπηρεσιών της πόλης σε πραγματικό χρόνο [11].

Η εγκατάσταση αισθητήρων κενής θέσης σε πολυώροφους χώρους στάθμευσης έχει αυξήσει την αποτελεσματικότητα της εύρεσης θέσης στάθμευσης όπως και τα έσοδα από αυτήν. Η έξυπνη πόλη της Βαρκελώνης είναι μια ταχέως εξελισσόμενη για να εξυπηρετεί τους πολίτες με τις πιο καινοτόμες έξυπνες λύσεις σε όλους τους τομείς της ζωής.

Η πόλη της Νέας Υόρκης [13]

Με πληθυσμό πάνω από 8,5 εκατομμύρια, η Νέα Υόρκη χρησιμοποιεί 1 δισεκατομμύριο γαλόνια νερού κάθε μέρα. Το Τμήμα Περιβαλλοντικής Προστασίας της Νέας Υόρκης έχει αναπτύξει ένα μεγάλης κλίμακας σύστημα αυτόματης ανάγνωσης μετρητών (AMR) προκειμένου να λαμβάνει μια καλύτερη εικόνα της κατανάλωσης νερού, ενώ παρέχει στους πελάτες ένα χρήσιμο εργαλείο για να ελέγχουν καθημερινά τη χρήση νερού. Οι μονάδες AMR έχουν εγκατασταθεί σε περισσότερες από 800.000 ιδιοκτησίες, και

επιτρέπουν στο Τμήμα Περιβαλλοντικής Προστασίας να τιμολογεί τους πελάτες με μεγαλύτερη ακρίβεια. Το έξυπνο σύστημα μέτρησης ωφελεί επίσης τους τελικούς χρήστες: οι ''μικροί χρήστες'' ενημερώνονται για την κατανάλωση νερού τέσσερις φορές την ημέρα, ενώ οι ''μεγάλοι χρήστες'' μπορούν να παρακολουθούν ανά μία ώρα τα σχετικά δεδομένα. Οι μονάδες AMR ενσωματώνονται επίσης με μια εφαρμογή smartphone που προειδοποιεί τους πελάτες για πιθανές διαρροές νερού όταν εντοπίζονται μη φυσιολογικές τιμές στην κατανάλωση νερού. Το πρόγραμμα ειδοποίησης διαρροής ήταν εξαιρετικά επιτυχημένο, εξοικονομώντας περισσότερα από 73 εκατομμύρια δολάρια.

Το τμήμα υγιεινής της Νέας Υόρκης επίσης είναι το μεγαλύτερο στον κόσμο, συλλέγοντας περισσότερους από 10.500 τόνους απορριμμάτων την ημέρα. Η συλλογή απορριμμάτων από χιλιάδες κάδους είναι μια αρκετά υλικοτεχνική πρόκληση: οι κάδοι απορριμμάτων μπορεί να ξεχειλίσουν αν αφεθούν χωρίς επίβλεψη, ενώ και η συλλογή των απορριμμάτων αποτελεί πολύ συχνά σπατάλη καυσίμου και εργασίας.

Το BigBelly είναι ένας έξυπνος κάδος απορριμμάτων που αναπτύσσεται σε όλη τη Νέα Υόρκη και προσφέρει σημαντικά πλεονεκτήματα σε σύγκριση με τους παραδοσιακούς κάδους απορριμμάτων, καθώς είναι εξοπλισμένο με έναν ασύρματο αισθητήρα που παρακολουθεί τη στάθμη των απορριμμάτων, επιτρέποντας τον πιο αποτελεσματικό προγραμματισμό των διαδρομών που απαιτούνται για την παραλαβή τους. Το σύστημα περιλαμβάνει έναν συμπιεστή απορριμμάτων που λειτουργεί με ηλιακή ενέργεια, επιτρέποντας στον κάδο απορριμμάτων να χωράει πέντε φορές περισσότερα απόβλητα από έναν συμβατικό. Το BigBelly βελτιώνει την απόδοση συλλογής απορριμμάτων κατά 50% έως 80%, και συμβάλλει επίσης στον έλεγχο των εκπομπών αερίων μειώνοντας τον χρόνο που περνούν τα απορριμματοφόρα στο δρόμο.

Η Νέα Υόρκη ξεχωρίζει επίσης και για το ''Πρόγραμμα Ψηφιακής Πόλης της Νέας Υόρκης'', το οποίο περιλαμβάνει πρωτοβουλίες όπως [14]: Το πρόγραμμα *ACRIS (Automated City Register Information System)* για έρευνα στο αρχείο των ιδιοκτησιών, το *Business Express*, μια υπηρεσία μιας στάσης για πρόσβαση σε όλες τις επιτρεπόμενες λειτουργίες νέων επιχειρήσεων σε ένα μέρος, το *NYC Service*, μια βάση δεδομένων στην οποία καταχωρούνται οι εθελοντικές δράσεις και οργανώσεις, το *Bill Payments*, μια πλατφόρμα πληρωμών για τους κατοίκους της Νέας Υόρκης προκειμένου να πληρώνουν τους δημοτικούς λογαριασμούς τους, το σύστημα *Permits & Applications*, μέσω του οποίου οι κάτοικοι μπορούν να καταχωρούν αιτήσεις για τη διενέργεια δραστηριοτήτων μέσα στην

πόλη, όπως φεστιβάλ δρόμου και αθλητικές εκδηλώσεις καθώς και το *NY Culture Calendar*, του οποίου τη διαχείριση έχει αναλάβει το Τμήμα Πολιτιστικών Υποθέσεων, παρέχοντας το πρόγραμμα των πολιτιστικών εκδηλώσεων της πόλης.

2. INTERNET OF THINGS ΚΑΙ ΕΞΥΠΝΕΣ ΠΟΛΕΙΣ

2.1 Ο ΡΟΛΟΣ ΤΟΥ INTERNET OF THINGS (IOT) ΣΤΗ ΛΕΙΤΟΥΡΓΙΑ ΤΩΝ ΕΞΥΠΝΩΝ ΠΟΛΕΩΝ

Η αλματώδης αύξηση του αστικού πληθυσμού τις τελευταίες δεκαετίες επηρεάζει πολλές φορές αρνητικά την ποιότητα των υπηρεσιών που μια πόλη επιδιώκει να παρέχει στους κατοίκους αυτής. Η αύξηση του πληθυσμού που συγκεντρώνεται σε αυτές συνάγεται και τη μεγέθυνση ορισμένων προβλημάτων που έτσι κι αλλιώς ''βασανίζουν'' κρίσιμους τομείς μια πόλης, όπως είναι η εκπαίδευση, η υγεία, οι μεταφορές, η ενέργεια, η ανεργία και η δημόσια ασφάλεια. Στο μετριασμό αυτών των προκλήσεων και την εξεύρεση βιώσιμων αποδοτικών και αποτελεσματικών λύσεων προσπαθεί να συνεισφέρει η ενσωμάτωση των ΤΠΕ στον παραδοσιακό τρόπο παροχής υπηρεσιών, μέρος των οποίων αποτελεί το Διαδίκτυο των Πραγμάτων-ΔτΠ (Internet of Things-IoT). Ένας από τους πιο δημοφιλείς και ευρέως χρησιμοποιούμενους ορισμούς του IoT είναι ότι επιτρέπει σε ανθρώπους και πράγματα να συνδέονται ανά πάσα στιγμή, οπουδήποτε, με οτιδήποτε και οποιονδήποτε, ιδανικά χρησιμοποιώντας οποιοδήποτε δίκτυο και οποιαδήποτε υπηρεσία.

Η αρχιτεκτονική του IoT [15] αποτελείται από τα παρακάτω μέρη, τα οποία προσιδιάζουν με την αρχιτεκτονική της ΕΠ:

Επίπεδο έξυπνων συσκευών / αισθητήρων: Επιτρέπουν τη διασύνδεση του φυσικού και ψηφιακού κόσμου, με σκοπό τη συλλογή και την επεξεργασία πληροφοριών σε πραγματικό χρόνο.

Επίπεδο πυλών και δικτύων: Η υποδομή ενσύρματου ή ασύρματου δικτύου λειτουργεί ως μέσο μεταφοράς των παραγόμενων από τους αισθητήρες δεδομένων.

Επίπεδο διαχείρισης υπηρεσιών: Στο επίπεδο αυτό είναι δυνατή η επεξεργασία πληροφοριών, μέσω μεθόδων ανάλυσης, ελέγχων ασφαλείας, μοντελοποίησης διαδικασιών και διαχείρισης συσκευών.

Επίπεδο εφαρμογής: Ευρεία εφαρμογή σε ποικίλους τομείς της οικονομίας για τη μετατροπή τους σε «έξυπνα περιβάλλοντα» (ενδεικτικά: πόλεις, μεταφορές, κτήρια,

λιανική πώληση, εφοδιαστική αλυσίδα, γεωργία, βιομηχανία, υγεία, αλληλεπίδραση χρηστών, πολιτισμό και τουρισμό, περιβάλλον και ενέργεια).

Η εξέλιξη στις ΤΠΕ και η τεχνολογία ανταλλαγής πληροφοριών είναι οι οδηγοί της εμβέλειας και της κλίμακας της ΕΠ [8]. Αυτή η ταχεία εξέλιξη φέρνει επανάσταση στην κατασκευή ΕΠ με την άνοδο του IoT. Λόγω της προόδου στην τεχνολογία αισθητήρων και του μειωμένου κόστους παραγωγής τους, της ανάπτυξης των εφαρμογών cloud, των τεχνολογιών επεξεργασίας και αποθήκευσης, η ανάπτυξη των αισθητήρων, οι οποίοι αποτελούν μέρος του IoT [8], έχει αυξηθεί τα τελευταία χρόνια, και ως εκ τούτου είναι ιδιαίτερα διαδεδομένη η εγκατάσταση τους στο περιβάλλον των ΕΠ. Τα συστήματα IoT είναι ευέλικτα και αξιόπιστα ώστε να υποστηρίζουν ένα ευρύ φάσμα στόχων που θέτει μια ΕΠ. Με αισθητήρες συνδεδεμένους σε κάθε όχημα, συσκευή ή εξοπλισμό στον οποίο βασίζεται καθημερινά μια πόλη, το IoT μπορεί να οδηγήσει σε μια πιο εξελιγμένη προσέγγιση στη διαχείριση πληροφοριών αναφορικά με διάφορους τομείς μιας πόλης, παρέχοντας μεγαλύτερη αξιοπιστία και με σημαντικά μικρότερο κόστος[16].
Το IoT μπορεί να ενσωματώνει μεγάλο αριθμό διαφορετικών και ετερογενών συσκευών, παρέχοντας παράλληλα ανοιχτή πρόσβαση σε επιλεγμένα υποσύνολα δεδομένων για την ανάπτυξη μιας πληθώρας ψηφιακών υπηρεσιών [17]. Ωστόσο, η οικοδόμηση μιας γενικής αρχιτεκτονικής δομής για το IoT είναι μια πολύ περίπλοκη εργασία, κυρίως λόγω της εξαιρετικά μεγάλης ποικιλίας συσκευών, των τεχνολογιών του επιπέδου σύνδεσης και των υπηρεσιών που μπορεί να εμπλέκονται σε ένα τέτοιο σύστημα [17]. Προς τούτο, έχει δημιουργηθεί μια ειδική υποκατηγορία του IoT, το Urban IoT, που έχει σχεδιαστεί για να υποστηρίξει το όραμα της ΕΠ, το οποίο στοχεύει στην εκμετάλλευση των πιο προηγμένων τεχνολογιών επικοινωνίας για την υποστήριξη σημαντικών και αναγκαίων υπηρεσιών τόσο για τη διοίκηση της πόλης και για τους κατοίκους αυτής [17]. Επιτρέποντας την εύκολη πρόσβαση και αλληλεπίδραση με μια μεγάλη ποικιλία συσκευών όπως, οικιακές συσκευές, κάμερες παρακολούθησης, αισθητήρες παρακολούθησης, ενεργοποιητές, οθόνες, οχήματα κ.λπ., το IoT προωθεί την ανάπτυξη μιας σειράς εφαρμογών που χρησιμοποιούν τον τεράστιο όγκο και τα διάφορα είδη δεδομένων που παράγονται σε μια ΕΠ, για την παροχή νέων υπηρεσιών σε πολίτες, εταιρείες και δημόσιες διοικήσεις. Οι υπηρεσίες μιας ΕΠ βασίζονται σε αυτήν την αρχιτεκτονική, όπου ένα πυκνό και ετερογενές σύνολο περιφερειακών συσκευών που αναπτύσσονται στην αστική περιοχή, δημιουργούν

διαφορετικούς τύπους δεδομένων οι οποίοι στη συνέχεια μεταφέρονται μέσω κατάλληλων τεχνολογιών επικοινωνίας σε ένα κέντρο ελέγχου, όπου πραγματοποιείται αποθήκευση και επεξεργασία δεδομένων [17]. Η ανάπτυξη του urban IoT, μπορεί να αποφέρει πολλά οφέλη στη διαχείριση και τη βελτιστοποίηση των παραδοσιακών δημόσιων υπηρεσιών, όπως οι μεταφορές και η στάθμευση, ο φωτισμός της πόλης, η επιτήρηση και η συντήρηση των δημόσιων χώρων [17].

Βέβαια πρέπει να σημειωθεί πως για μια ΕΠ δεν αρκεί μόνο η εφαρμογή του IoT, αλλά πρέπει να ληφθεί υπόψη και η κοινωνική πτυχή αυτής, στην οποία συμπεριλαμβάνονται ο θεμελιώδης ρόλος των πολιτών που ζουν και εργάζονται σε αυτήν και ο τρόπος διακυβέρνησής της [1]. Οι ανάγκες, η ιδιωτικότητα, η ασφάλεια και η αποδοχή των πολιτών θεωρούνται σημαντικές προκλήσεις για κάθε ΕΠ, συνεπώς, θα πρέπει να αναπτυχθεί μια στρατηγική που να περιλαμβάνει πολίτες, επιχειρήσεις και να είναι προσαρμόσιμη στις ανάγκες αυτών και στους στόχους που επιδιώκει να ικανοποιήσει μια πόλη[1].

2.2 ΕΦΑΡΜΟΓΕΣ ΤΟΥ IOT ΣΤΗΝ ΕΞΥΠΝΗ ΠΟΛΗ

Έξυπνοι χώροι στάθμευσης

Σε ένα σύστημα έξυπνης στάθμευσης, με την τοποθέτηση αισθητήρων στους δρόμους και την εγκατάσταση έξυπνων οθονών, παρακολουθείται η άφιξη και η αναχώρηση οχημάτων με σκοπό τη ΄΄διανομή΄΄χώρων στάθμευσης μέσα στην πόλη και τη δημιουργία νέοι χώρων στάθμευσης, όπου είναι υπαρκτός μεγάλος όγκος οχημάτων [18]. Επιπλέον, μέσω τεχνολογιών επικοινωνίας μικρής εμβέλειας όπως το RFID και το NFC, είναι δυνατό να πραγματοποιηθεί ηλεκτρονική επαλήθευση των αδειών στάθμευσης, επιτρέποντας έτσι την προσφορά καλύτερων υπηρεσιών στους κατοίκους και εμπόρους μιας πόλης [19].

Εφαρμογές για έξυπνη υγεία [19]

Στον τομέα της υγειονομικής περίθαλψης, εφαρμογές IoT συνίστανται ενδεικτικά στις παρακάτω λειτουργίες, προσφέροντας εξαιρετικά πλεονεκτήματα στις ΕΠ: παροχή πληροφοριών σε πραγματικό χρόνο σχετικά με τους δείκτες υγείας των ασθενών με τη χρήση φορητών συσκευών υγείας ακόμη και απομακρυσμένα, πρόληψη λήψης λανθασμένων φαρμάκων και δόσεων, παρακολούθηση θέσης των ασθενοφόρων, on-line

έλεγχος διαθεσιμότητας προϊόντων αίματος και οργάνων μεταμόσχευσης. Επίσης, ο έλεγχος ταυτότητας προσωπικού στοχεύει στη βελτίωση της συμπεριφοράς του υπαλλήλου προς τους ασθενείς. Η συλλογή και η ανίχνευση δεδομένων κατά τα ανωτέρω συμβάλλει στην εξοικονόμηση χρόνου για την επεξεργασία δεδομένων, στην πρόληψη ανθρώπινων λαθών και στην αποτελεσματικότερη ροή εργασιών μιας μονάδας υγείας.

Εφαρμογές στις μετακινήσεις και στην κυκλοφορία των οχημάτων

Προς επίλυση προβλημάτων, όπως η κυκλοφοριακή συμφόρηση, η ρύπανση, ο προγραμματισμός και η μείωση κόστους των δημόσιων συγκοινωνιών, συγκεκριμένες ΤΠΕ, όπως οι Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I), Vehicle to Pedestrian (V2P) or Pedestrian to Infrastructure (P2I), έχουν κάνει εφικτό το σχεδιασμό έξυπνων συστημάτων μεταφοράς [20] Με τα αυτοκίνητα να διαθέτουν συσκευές GPS και στο οδικό δίκτυο να έχουν εγκατασταθεί κάμερες, ακουστικοί αισθητήρες και αισθητήρες ποιότητας αέρα, παράγουν δεδομένα σε πραγματικό χρόνο τα οποία χρησιμοποιούνται ήδη για τη χαρτογράφηση διαδρομής σε εφαρμογές όπως το Waze και το Google Maps και για τον προγραμματισμό ταξιδιών στα μέσα μαζικής μεταφοράς, ενώ παράλληλα αξιοποιούνται τόσο από τις αρχές διαχείρισης της κυκλοφορίας όσο και από τους κατοίκους [19].

Μείωση της περιβαλλοντικής μόλυνσης

Μαζί με την υπηρεσία παρακολούθησης ποιότητας του αέρα, μια εφαρμογή IoT με χρήση αισθητήρων στα αστικά κέντρα ή σε κάποιο πάρκο της πόλης, μπορεί να επιτρέπει την κατανάλωση ενέργειας ολόκληρης της πόλης, επιτρέποντας έτσι στις αρμόδιες υπηρεσίες και τους κατοίκους να έχουν μια σαφή και λεπτομερή εικόνα της ποσότητας ενέργειας που απαιτείται από τις διάφορες λειτουργίες (δημόσιος φωτισμός, μεταφορές, φανάρια, κάμερες ελέγχου, θέρμανση/ψύξη δημόσιων κτιρίων κλπ) [17]. Έτσι είναι δυνατό να εντοπιστούν οι κύριες πηγές κατανάλωσης ενέργειας και να τεθούν προτεραιότητες προκειμένου να βελτιστοποιηθεί η συμπεριφορά τους ως προς την κατανάλωση ενέργειας, κατεύθυνση που υποδεικνύεται και από σχετική ευρωπαϊκή οδηγία για τη βελτίωση της ενεργειακής απόδοσης τα επόμενα χρόνια.

Το urban IoT μπορεί να παρακολουθήσει τα επίπεδα θορύβου σε διαφορετικά σημεία και να παρέχει δεδομένα στο δήμο ώστε να λάβει τα κατάλληλα μέτρα για τη μείωσή του[17]. Επιπλέον η κατασκευή ενός χωροχρονικού χάρτη της ηχορύπανσης σε μια ΕΠ,

συμβάλλει στην ενίσχυση της δημόσιας ασφάλειας μέσω ανιχνευτή ήχου για τον εντοπισμό π.χ. σπάσιμο γυαλιών, παρέχοντας εμπιστοσύνη στους ιδιοκτήτες εγκαταστάσεων [17].

Διαχείριση των αποβλήτων [17]

Η διαχείριση των απορριμμάτων μιας πόλης, εξαιτίας του κόστους της αυτής υπηρεσίας και του περιορισμένου χώρου για την απόθεση αυτών σε ειδικούς χώρους, αποτελεί πρωταρχικό ζήτημα για κάθε ΕΠ. Ωστόσο, η χρήση έξυπνων δοχείων απορριμμάτων, τα οποία ανιχνεύουν το επίπεδο φορτίου, επιτρέπουν τη βελτιστοποίηση της διαδρομής των φορτηγών συλλογής, τη μείωση του κόστος συλλογής απορριμμάτων και την ποιότητα της ανακύκλωσης. Σε μια τέτοια έξυπνη υπηρεσία διαχείρισης απορριμμάτων, έξυπνα δοχεία απορριμμάτων συνδέονται σε ένα κέντρο ελέγχου όπου ένα λογισμικό βελτιστοποίησης επεξεργάζεται τα δεδομένα και καθορίζει τη βέλτιστη διαχείριση του στόλου των φορτηγών συλλογής.

Έξυπνα κτίρια [17]

Τα διατηρητέα με ιστορική αξία κτίρια μιας πόλης απαιτούν τη συνεχή παρακολούθηση των πραγματικών συνθηκών τους και τον προσδιορισμό εκείνων των περιοχών της ΕΠ που υπόκεινται περισσότερο στην επίδραση εξωτερικών παραγόντων. Το IoT μπορεί να παρέχει μια κατανεμημένη βάση δεδομένων μετρήσεων δομικής ακεραιότητας του κτιρίου, τα οποία συλλέγονται από κατάλληλους αισθητήρες που έχουν τοποθετηθεί στα κτίρια, όπως αισθητήρες δόνησης και παραμόρφωσης, αισθητήρες ατμοσφαιρικών παραγόντων στις γύρω περιοχές για την παρακολούθηση των επιπέδων ρύπανσης, και αισθητήρες θερμοκρασίας και υγρασίας για πλήρη χαρακτηρισμό των περιβαλλοντικών συνθηκών. Αυτή η βάση δεδομένων μπορεί να μειώσει την ανάγκη για δαπανηρούς ελέγχους και να επιτρέψει τη στοχευμένη και προληπτική συντήρηση. Τα ανωτέρω δεδομένα μπορούν να είναι δημόσια προσβάσιμα προκειμένου να ευαισθητοποιηθούν οι πολίτες ως προς τη διατήρηση της ιστορικής κληρονομιάς της πόλης. Περαιτέρω, αισθητήρες πραγματοποιούν μετρήσεις και συλλέγουν δεδομένα από όλα τα τεχνικά συστήματα του κτιρίου εξ αποστάσεως και αυτόματα. Στη συνέχεια, αυτές οι πληροφορίες μπορούν να αποθηκευτούν σε μια βάση δεδομένων χρησιμοποιώντας τεχνολογία cloud και να είναι προσβάσιμες σε τρίτους για την παρακολούθηση της κατανάλωσης ενέργειας του κτιρίου,

την παρατήρηση πιθανής σπατάλης ενέργειας και την εξαγωγή συμπερασμάτων σχετικά με την ενεργειακή απόδοση [21].

2.3. ΠΡΟΚΛΗΣΕΙΣ ΣΤΗΝ ΕΦΑΡΜΟΓΗ ΤΩΝ IoT ΣΤΙΣ ΕΞΥΠΝΕΣ ΠΟΛΕΙΣ

Το IoT αποτελεί ένα από τα πιο πολύτιμα τεχνολογικά εργαλεία για την ψηφιοποίηση κάθε πτυχής της καθημερινής μας ζωής. Ειδικότερα στο περιβάλλον των ΕΠ το στοιχείο της ψηφιοποίησης συνεπάγεται τον ταχύτατο πολλαπλασιασμό αισθητήρων σε κάθε τομέα λειτουργίας μιας πόλης. Ωστόσο, μια τέτοια ευρεία χρήση συστημάτων IoT στις ΕΠ έχει ως αποτέλεσμα τη δημιουργία, σημαντικών προκλήσεων που είναι αναγκαίο να ληφθούν υπόψη και για τις οποίες γίνεται λόγος αμέσως παρακάτω.

Ετερογένεια συσκευών

Οι έξυπνοι αισθητήρες, μέρος του συστήματος IoT, κατασκευάζονται από πολλούς διαφορετικούς προμηθευτές οι οποίοι ακολουθούν διαφορετικούς μηχανισμούς, πρότυπα μέτρησης, μορφές δεδομένων και πρωτόκολλα συνδεσιμότητας[20]. Η εγκατάσταση αισθητήρων και συσκευών στην ΕΠ για να είναι αποδοτική θα πρέπει να επιτρέπει την απρόσκοπτη ανταλλαγή δεδομένων μεταξύ τους, τον προγραμματισμό εργασιών μεταξύ τους και την συγκέντρωση των δεδομένων με τέτοιο τρόπο ώστε να είναι δυνατή η εξαγωγή συμπερασμάτων[20]. Πρόκειται για μια σημαντική πρόκληση που δύσκολα θα μπορεί να ξεπεραστεί χωρίς την ανάπτυξη και χρήση ανοιχτών πρωτοκόλλων και μορφών δεδομένων που θα παρέχουν τη δυνατότητα στους κατασκευαστές να δημιουργούν εξοπλισμό, ο οποίος θα μπορεί να επικοινωνεί μεταξύ τους, δίνοντας έτσι περαιτέρω ώθηση στην ανάπτυξη του συστήματος IoT[20].

Χαμηλή κατανάλωση ενέργειας

Συνήθως, οι συσκευές IoT, μικρές σε μέγεθος, για να λειτουργήσουν απαιτούν μια συνεχή πηγή ενέργειας, η οποία αποτελεί σημαντική πρόκληση όσον αφορά τη διάρκεια ζωής της μπαταρίας και το κόστος. Για την αντιμετώπιση αυτού του ζητήματος στις ΕΠ, οι συσκευές πρέπει να διαθέτουν χαμηλή κατανάλωση ενέργειας, ώστε να εξασφαλίζεται παράλληλα και χαμηλό κόστος, ένα πρόβλημα το οποίο θα μπορούσε να επιλυθεί μέσω των εξελίξεων

στον τομέα της ασύρματης τεχνολογίας [22]. Επιπλέον, επειδή οι συγκεκριμένες συσκευές χρειάζεται να μετρούν, μεταφέρουν και αποθηκεύουν δεδομένα που έχουν συλλέξει, απαιτείται επίσης ανάπτυξη νέων τεχνολογιών μνήμης και αποθήκευσης καθώς και συσκευών χαμηλής ισχύος που παρατείνουν τη διάρκεια ζωής της μπαταρίας όσο το δυνατόν περισσότερο. Η αποθήκευση αυτού του μεγάλου όγκου δεδομένων καθιστά αναγκαία την ανάπτυξη αλγορίθμων συμπίεσης και ειδικότερων σχημάτων βάσεων δεδομένων[20].

Δικτύωση[22]

Μια ΕΠ που βασίζεται στο IoT και περιλαμβάνει δισεκατομμύρια συσκευές στο δίκτυο της, για να είναι σε θέση να πετύχει πρέπει να έχει την ικανότητα να παρέχει σύνδεση με κάθε διαθέσιμη συσκευή IoT, η οποία διαθέτει ανιχνευτικές ικανότητες και παράγει σημαντικές πληροφορίες. Στην ΕΠ, οι συσκευές IoT μπορούν να χρησιμοποιήσουν οποιαδήποτε διαθέσιμα δίκτυα επικοινωνίας όπως δημόσια Wi-Fi, Bluetooth, δίκτυα κινητής τηλεφωνίας και δορυφόρους για να επικοινωνούν με το κέντρο εφαρμογών που βρίσκεται στο cloud. Πολλές συσκευές ωστόσο απαιτούν κινητικότητα και διεκπεραίωση δεδομένων για την παροχή αποδεκτής ποιότητας υπηρεσίας.

Τεχνικές ανάλυσης δεδομένων

Το πολυπληθές δίκτυο αισθητήρων που είναι εγκατεστημένοι στην ΕΠ παράγει τεράστιο όγκο δεδομένων, τα οποία είτε αφορούν μετρήσεις στοιχείων του περιβάλλοντος είτε προσωπικά δεδομένα των ίδιων των κατοίκων της πόλης.

Για την ανάλυση αυτών των δεδομένων, χρησιμοποιούνται έξυπνες τεχνικές και αλγόριθμοι. Για παράδειγμα, μπορούν να εφαρμόζονται αλγόριθμοι deep learning για την αποτελεσματική ανάλυση τεράστιων πληροφοριών που παράγονται από τοπικά συνδεδεμένες συσκευές [22]. Τα σημαντικότερα ζητήματα που πρέπει να αντιμετωπιστούν σε αυτήν την περίπτωση είναι ο σεβασμός του απορρήτου των χρηστών κατά την ανάλυση δεδομένων, η ανωνυμοποίηση ευαίσθητων δεδομένων, η παροχή υποδομής για συλλογή, αποθήκευση και ανάλυση των δεδομένων καθώς και η παροχή της απαιτούμενης υπολογιστικής ισχύος για την εξαγωγή συμπερασμάτων από την επεξεργασία των δεδομένων [22].

3.ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΕΞΥΠΝΗ ΠΟΛΗ

Οι ΕΠ υπόσχονται πολλά οφέλη, με αισθητήρες να παρακολουθούν τη ρύπανση ή να προσφέρουν πληροφορίες σε πραγματικό χρόνο για τη στάθμευση αυτοκινήτων, με κάμερες να παρακολουθούν τη συμφόρηση και να διαχειρίζονται τη ροή της κυκλοφορίας. Ωστόσο, ειδικοί, προειδοποιούν ότι κρίσιμες δημόσιες υπηρεσίες θα πρέπει να θωρακιστούν για να αποτραπούν τυχόν δυσλειτουργίες και τα κάθε είδους δεδομένα πρέπει επίσης να προστατευτούν από αλλοίωση, απώλεια, κλοπή σε μεγάλους όγκους [23]. Όταν η ΕΠ δεν είναι ασφαλής, αυτό σημαίνει ότι δεν διασφαλίζονται βασικές υπηρεσίες όπως η δημόσια ασφάλεια, η διακυβέρνηση, η υγειονομική περίθαλψη, η παροχή ενέργειας και οι κάθε είδους (κρίσιμες ή μη) υποδομές. Η έλλειψη ασφάλειας μπορεί να οδηγήσει ακόμη και σοβαρό ζήτημα εθνικής ασφάλειας, σε χώρα της οποίας κρίσιμες υποδομές μιας ΕΠ παραβιάζονται.

Οι έξυπνες πόλεις μπορούν να αυξήσουν την παραγωγικότητα και την αποδοτικότητα τους για τους πολίτες, αλλά αντιμετωπίζουν σοβαρό πρόβλημα όταν υποτιμάται η ασφάλεια που πρέπει να διαθέτουν. Καθώς οι τοπικές κυβερνήσεις επιδιώκουν έξυπνες πρωτοβουλίες, η αξιοποίηση του πλήρους δυναμικού αυτών των ψηφιακά συνδεδεμένων κοινοτήτων πρέπει να ξεκινά με την εφαρμογή βέλτιστων πρακτικών για προστασία από κυβερνοεπιθέσεις [24].

Ερευνητές από το Πανεπιστήμιο της Καλιφόρνιας στο Berkley, ζήτησαν από 76 ειδικούς στον τομέα της κυβερνοασφάλειας να ταξινομήσουν διαφορετικές τεχνολογίες σύμφωνα με τις τεχνικές ευπάθειας τους, την ελκυστικότητά τους στους επιτιθέμενους και τον πιθανό αντίκτυπο μιας σοβαρής κυβερνοεπίθεσης [25][11]. Στις πρώτες τρεις τεχνολογίες συγκαταλέγονταν οι ειδοποιήσεις έκτακτης ανάγκης, η βιντεοεπιτήρηση δρόμου και τα έξυπνα σήματα κυκλοφορίας.

[11] https://www.smartcitiesworld.net/news/news/which-smart-city-tech-poses-the-greatest-risk-for-cyber-attacks-6249, Τις υπόλοιπες πιο πιθανές τεχνολογίες για κυβερνοεπίθεση αποτελούσαν η παρακολούθηση κατανάλωσης νερού, τα έξυπνη διόδια, τα ανοικτά δεδομένα δημόσιας συγκοινωνίας, η ανίχνευση πυροβολισμού, οι έξυπνοι κάδοι απορριμμάτων ή ανακύκλωσης και η δορυφορική ανίχνευση διαρροής νερού. βλ. εδώ συνολικά τα αποτελέσματα της έρευνας https://cltc.berkeley.edu/2021/03/16/smart-cities/

3.1.Η ΣΗΜΑΣΙΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΓΙΑ ΤΗ ΛΕΙΤΟΥΡΓΙΑ ΤΗΣ ΕΞΥΠΝΗΣ ΠΟΛΗΣ

Μια έξυπνη πόλη είναι προϊόν μιας έξυπνης αρχιτεκτονικής όπου παρέχονται προηγμένες υπηρεσίες μέσω εφαρμογών που είναι συμβατές με έξυπνες εφαρμογές ασφάλειας και απορρήτου[26]. Βασικά στοιχεία μιας ΕΠ, όπως η έξυπνη διακυβέρνηση, η έξυπνη επικοινωνία, το έξυπνο περιβάλλον, οι έξυπνες μεταφορές, οι έξυπνες εφαρμογές διαχείρισης ενέργειας, απορριμμάτων και υδάτων υπόσχονται την έξυπνη ανάπτυξη της πόλης. Ταυτόχρονα ωστόσο πρωταρχικός στόχος μιας ΕΠ πρέπει να είναι η επιβολή μέγιστης ασφάλειας και προστασίας του απορρήτου του μεγάλου όγκου δεδομένων που σχετίζονται με αυτές τις έξυπνες τεχνολογίες.

Κατά κύριο λόγο, ο κύριος στόχος της ασφάλειας πληροφοριών είναι η προστασία των δεδομένων ή των πληροφοριών από κακόβουλες επιθέσεις, ιούς, απάτες και διάφορες άλλες κακόβουλες δράσεις που μπορεί να βλάψουν είτε τις πληροφορίες αυτοτελώς, είτε την απαίτηση των πληροφοριών για τις ενσωματωμένες στην ΕΠ τεχνολογίες[26]. Προβλήματα ασφάλειας και απορρήτου δημιουργούνται λόγω των τρωτών σημείων που υπάρχουν συνήθως σε κάθε επίπεδο ενός έξυπνου συστήματος. Επιθέσεις, όπως η μη εξουσιοδοτημένη πρόσβαση, η άρνηση υπηρεσίας (DoS) καθώς και η υπερβολική συλλογή δεδομένων από παρόχους υπηρεσιών και τρίτους μπορούν να υποβαθμίσουν την ποιότητα των έξυπνων υπηρεσιών και να εκθέσουν τους κατοίκους σε παραβίαση του απορρήτου[136], αντίστοιχα. Για παράδειγμα, το 2015, σχεδόν 230.000 πολίτες που ζούσαν στην Ουκρανία υπέστησαν μια μακρά περίοδο αποσύνδεσης ηλεκτρικού ρεύματος επειδή το σύστημα του δικτύου ηλεκτρικής ενέργειας δέχθηκε επίθεση από χάκερ. Οι αρνητικές επιπτώσεις της ασφάλειας των πληροφοριών δεν περιορίζονται μόνο στην τεχνική πλευρά, αλλά μπορούν επίσης να έχουν αρνητικές επιπτώσεις στις οικονομικές πτυχές μιας κοινωνίας.

Εκτός από την επιδίωξη για παροχή έξυπνων εφαρμογών στον ιστό της ΕΠ, με στόχο τη βιωσιμότητα της και το ευ ζην των κατοίκων της, οι υπεύθυνοι χάραξης πολιτικής μιας ΕΠ και ιδίως όσοι ασχολούνται με την ασφάλεια των συστημάτων αυτής, πρέπει να φροντίσουν το στοιχείο «έξυπνο» στις ΕΠ να μπορεί να αναγνωσθεί με πολλούς τρόπους. Ενώ η λέξη «έξυπνο» περιλαμβάνει την έννοια της βελτιστοποίησης των λειτουργιών που

βασίζονται στα διαθέσιμα δεδομένα, μπορεί, και πρέπει επίσης να περιλαμβάνει και την έννοια του απαραβίαστου[27]. Οι ΕΠ προσφέρουν αισθητήρες, μεγάλα δεδομένα και προηγμένους υπολογιστές ως απαντήσεις σε αυτές τις προκλήσεις, αλλά συχνά έχουν δεχτεί κριτική επειδή ασχολούνται πολύ με το υλικό παρά με τους ανθρώπους[28].

Το θέμα της ασφάλειας είναι εξαιρετικά σημαντικό και αποτελεί απαραίτητη προϋπόθεση για την αποδοχή των υποδομών των έξυπνων πόλεων από τους κατοίκους και χρήστες αυτών, επειδή τα δίκτυα είναι επιρρεπή σε ένα μεγάλο εύρος κακόβουλων επιθέσεων, ενώ διάφορα εσωτερικά και εξωτερικά μέρη μιας ΕΠ δεν είναι απολύτως αξιόπιστα [29].

Η πρόκληση για τις ΕΠ που χρησιμοποιούν πολύπλοκα ψηφιακά δίκτυα για τη διαχείριση χιλιάδων συστημάτων και υπηρεσιών αυτών, είναι ότι κάθε συσκευή που βασίζεται σε συγκεκριμένο λογισμικό για τη λειτουργία της, αποτελεί από μόνη της πιθανό θύμα κυβερνοεπίθεσης. Εξαιτίας αυτής της αδυναμίας, αρκετές πρωτοβουλίες ΕΠ έχουν επικριθεί από ειδικούς, οι οποίοι υποστήριξαν ότι διάφορα συστήματα που οι ΕΠ προμηθεύτηκαν, αναπτύχθηκαν με ελάχιστα συντονισμένη εξέταση των πιθανών κινδύνων στο απόρρητο και την ασφάλεια αυτών [30]. Σε μια ΕΠ, τυχόν απερίσκεπτη και μη ασφαλής δράση ενός ατόμου ή ενός οργανισμού μπορεί να θέσει ολόκληρη την πόλη σε κίνδυνο. Λόγω της εξάρτησης διαφόρων στοιχείων των έξυπνων πόλεων στις ΤΠΕ, προκλήσεις στον κυβερνοχώρο (όπως διαρροή πληροφοριών και κακόβουλες επιθέσεις στον κυβερνοχώρο) μπορούν να επηρεάσουν τη συμπεριφορά των λειτουργιών των ΕΠ [31].

Οι υπεύθυνοι ασφαλείας και λήψης αποφάσεων θα μπορούσαν να χωρίσουν τις επιπτώσεις στην ασφάλεια των συστημάτων μιας ΕΠ χρησιμοποιώντας ως κριτήριο τις βασικές απαιτήσεις που επιδιώκει η ασφάλεια των πληροφοριακών συστημάτων, δηλαδή την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα, όπως όμως αυτές διαμορφώνονται στο περιβάλλον των ΕΠ [32].

Εμπιστευτικότητα: Μόνο εγκεκριμένο και ειδικά εξουσιοδοτημένο προσωπικό θα πρέπει να έχει πρόσβαση στα συστήματα της ΕΠ και μόνο στο βαθμό που απαιτείται για τον ρόλο του. Οποιαδήποτε μη εξουσιοδοτημένη πρόσβαση θα πρέπει να αντιμετωπίζεται ως παραβίαση και οποιαδήποτε τέτοια παραβίαση θα μπορούσε να έχει ως αποτέλεσμα την παραβίαση του απορρήτου των δεδομένων των πολιτών. Αυτό από μόνο του θα μπορούσε να οδηγήσει σε απώλεια εμπιστοσύνης, φήμης και μπορεί να επιφέρει οικονομικές κυρώσεις για μη συμμόρφωση σύμφωνα και με τον ΓΚΠΔ [33].

Ακεραιότητα: Τα δεδομένα που συλλέγονται από την ΕΠ πρέπει να είναι ακριβή και να χρησιμοποιούνται για τον σκοπό για τον οποίο συλλέγονται. Αυτό απαιτεί ισχυρούς ελέγχους γνησιότητας για να αποτραπεί η αλλοίωση ή η καταστροφή δεδομένων. Οποιαδήποτε τέτοια παραβίαση θα μπορούσε να έχει συνέπειες που οδηγούν σε μείωση της αποτελεσματικότητας των λειτουργιών της ΕΠ. Επιπλέον, θα πρέπει να λαμβάνεται υπόψη η ακεραιότητα των πηγών δεδομένων. Θα πρέπει να ληφθούν περαιτέρω υπόψη τα χαρακτηριστικά των πηγών δεδομένων της ΕΠ, ώστε να μπορούν να διαμορφωθούν ως προς την ακρίβεια, την πληρότητα και την εγκυρότητα για τον εντοπισμό και την ειδοποίηση τυχόν ύποπτων μετρήσεων και παραβιάσεων ακεραιότητας.

Διαθεσιμότητα: Τα συστήματα μιας ΕΠ πρέπει να διασφαλίζουν έγκαιρη και αξιόπιστη πρόσβαση στις πληροφορίες και χρήση αυτών. Μια παραβίαση θα μπορούσε να έχει συνέπειες που θα μπορούσαν να οδηγήσουν σε διακοπή της καθημερινής λειτουργίας. Για παράδειγμα, εάν το σύστημα ήταν εκτός σύνδεσης για περισσότερο από μισή ημέρα, θα μπορούσε να δημιουργήσει τεράστια απογοήτευση στους πολίτες που δεν μπορούν να χρησιμοποιήσουν υπηρεσίες που είναι ενσωματωμένες στην ΕΠ (όπως πληρωμές στάθμευσης). Η λειτουργία κρίσιμων υποδομών που βασίζεται σε δεδομένα πραγματικού χρόνου θα πρέπει να μπορεί να συνεχίσει να λειτουργεί έστω και στοιχειωδώς, ακόμη και σε περίπτωση έλλειψης ή απώλειας δεδομένων πραγματικού χρόνου.

3.2 ΕΥΠΑΘΕΙΕΣ ΠΟΥ ΑΥΞΑΝΟΥΝ ΤΟΝ ΚΙΝΔΥΝΟ ΤΩΝ ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΩΝ ΣΤΗΝ ΕΞΥΠΝΗ ΠΟΛΗ

Οι ΕΠ διαθέτουν ορισμένα εγγενή χαρακτηριστικά τα οποία τις καθιστούν πιο ευάλωτες στον κίνδυνο κυβερνοεπιθέσεων. Στην ενότητα αυτή παρουσιάζονται τα πιο σημαντικά από αυτά.

ΑΛΛΗΛΕΞΑΡΤΗΣΗ ΚΑΙ ΠΟΛΥΠΛΟΚΟΤΗΤΑ

Δεδομένα που συλλέγονται για παράδειγμα από τοποθετημένους αισθητήρες σε μια πόλη, μεταφέρονται μέσω της υποδομής της ΕΠ συνήθως σε μια πλατφόρμα για την παροχή υπηρεσιών υψηλού επιπέδου. Η έννοια της πλατφόρμας IoT χαρακτηρίζει συνήθως ένα σύνολο στοιχείων υποδομής για την κοινή χρήση των πληροφοριών που παράγονται από

συσκευές και συστήματα IoT [34]. Σε αυτό το πλαίσιο, μια βασική πτυχή είναι η διασφάλιση της διαλειτουργικότητας σχετικά με την παρουσίαση ακατέργαστων δεδομένων και πληροφοριών που προέρχονται από διαφορετικές πηγές, ενώ παράλληλα αυτά προστατεύονται κατάλληλα [34].

Για το λόγο αυτό, τα συστήματα των ΕΠ είναι συνήθως μεγάλα και πολύπλοκα, με πολλές αλληλεξαρτήσεις, μεγάλες και σύνθετες επιφάνειες, ευάλωτες προς επίθεση. Αυτή η πολυπλοκότητα σημαίνει ότι μπορεί να είναι δύσκολο να γνωρίζουμε σε τι κινδύνους εκτίθενται όλα τα μέρη, να μετρήσουμε και να μετριάσουμε τους κινδύνους και να διασφαλίσουμε την ασφάλεια απ' άκρη σε άκρη[35]. Ακόμα κι αν τα ανεξάρτητα μέρη είναι ασφαλή, η σύνδεσή τους με άλλα συστήματα μπορεί ενδεχομένως να τα θέσει σε κίνδυνο με το επίπεδο ασφάλειας να είναι εγγυημένο μόνο από το λιγότερο ασφαλές μέρος [36]. Επιπλέον, οι αλληλεξαρτήσεις μεταξύ τεχνολογιών και συστημάτων σημαίνουν ότι είναι πιο δύσκολο να διατηρηθούν και να αναβαθμιστούν[36].

Η ασφάλεια του IoT είναι εξαιρετικά μεταβλητή**,** με ορισμένα συστήματα να στερούνται κρυπτογράφησης ή ονομάτων χρήστη και κωδικών πρόσβασης, ενώ άλλα είναι ανοιχτά σε επίθεση από κακόβουλο λογισμικό ή τροποποίηση υλικολογισμικού[36].

Οι ανωτέρω αλληλεξαρτήσεις των συστημάτων έχουν ως αποτέλεσμα, σε περίπτωση κυβερνοεπίθεσης να επηρεαστεί όχι μόνο ένα μέρος της αλυσίδας αλλά περισσότερα, δηλαδή να προκληθεί μια αλληλουχία παραβιάσεων. Για παράδειγμα, εξαιτίας μιας κυβερνοεπίθεσης σε μια υποδομή ηλεκτρικής ενέργειας, η οποία τροφοδοτεί κατοικίες, βιομηχανικούς χώρους, μέσα μαζικής μεταφοράς, θα μπορούσε να καταρρεύσει ένα αστικό λειτουργικό σύστημα και στη συνέχεια να καταρρεύσουν άλλα συστήματα, όπως η διαχείριση της κυκλοφορίας, οι υπηρεσίες έκτακτης ανάγκης και οι υπηρεσίες παροχής νερού[12]. Δεδομένου ότι οι ευπάθειες του απορρήτου και της ασφάλειας ενισχύονται από τη διασυνδεσιμότητα της ΕΠ, η εμπιστοσύνη των χρηστών στο σύστημα μπορεί να κλονιστεί πιο εύκολα [37]. Μια διαδοχική αστοχία στην υποδομή ως η περίπτωση κατά την οποία «μια διακοπή σε μια υποδομή προκαλεί την αποτυχία ενός μέρους μιας δεύτερης υποδομής, η οποία στη συνέχεια προκαλεί διακοπή στη δεύτερη υποδομή» [38]. Το 2001, διακοπές ηλεκτρικής ενέργειας στην Καλιφόρνια προκάλεσαν κλιμακωτές βλάβες σε

[12] Για παράδειγμα, μια εξελιγμένη κυβερνοεπίθεση στο λογισμικό που ελέγχει τμήματα του δικτύου ηλεκτρικής ενέργειας της Ουκρανίας απενεργοποίησε την τροφοδοσία σε περίπου ένα τέταρτο εκατομμυρίου καταναλωτών για αρκετές ώρες τον Δεκέμβριο του 2015.

πολλές βιομηχανίες που εξαρτώνται από την άμεσα διαθέσιμη ηλεκτρική ενέργεια, όπως την εξόρυξη, τη μεταφορά και τη διύλιση πετρελαίου, φυσικού αερίου, νερού και γεωργικών καλλιεργειών [39].

Ο προσδιορισμός της σοβαρότητας, της διάρκειας και του μεγέθους διαδοχικών δυσλειτουργιών σε ένα εξαιρετικά διασυνδεδεμένο δίκτυο είναι ένα σημαντικό βήμα για τον μετριασμό των διαταραχών. Οι υπεύθυνοι διαχείρισης τέτοιων κρίσεων τείνουν να εστιάζουν στον μετριασμό της διαδοχικής αποτυχίας από τις επί μέρους παραβιάσεις της ασφάλειας στον κυβερνοχώρο, σε βάρος της ολιστικής κατανόησης των διαδοχικών αποτυχιών. Οι υπεύθυνοι για την ασφάλεια της ΕΠ πρέπει επίσης να κατανοήσουν πώς οι φυσικές απειλές μπορούν να επηρεάσουν την υποδομή στον κυβερνοχώρο, όπως για παράδειγμα, σε περιοχές επιρρεπείς σε σεισμούς θα πρέπει να λάβουν υπόψη πώς οι φυσικές καταστροφές μπορούν να διαταράξουν μια ψηφιακά διασυνδεδεμένη ΕΠ και για το λόγο αυτό να αναπτύξουν συγκεκριμένα σχέδια έκτακτης ανάγκης για την ελαχιστοποίηση των ζημιών. Προκειμένου να ελαχιστοποιηθούν οι διαδοχικές επιπτώσεις, οι κίνδυνοι και η αλληλεξάρτηση πρέπει να μοντελοποιηθούν και να κατηγοριοποιηθούν, αναλόγως με τη συγκεκριμένο τομέα κάθε φορά που υφίσταται βλάβη, όπως οι μονάδες ηλεκτρισμού, οι αγωγοί που παρέχουν ηλεκτρική ενέργεια, τα νοσοκομεία ή οι σταθμοί φιλτραρίσματος νερού.

Ειδικότερα, στο πεδίο του IoT, μία και μόνο ευάλωτη συσκευή θα μπορούσε να δημιουργήσει ζητήματα χαμηλής ασφάλειας και στις υπόλοιπες συσκευές IoT που είναι συνδεδεμένες μέσω του ίδιου δικτύου [40]. Συγκεκριμένα, ένα πλήθος συσκευών IoT συνδέονται μέσω οικιακών δικτύων Wi-Fi, τα οποία είναι αρκετά εύκολο να παραβιαστούν, με αποτέλεσμα, εάν μια συσκευή που είναι συνδεδεμένη σε οικιακό δίκτυο δεν προστατεύεται επαρκώς, ένας χάκερ θα μπορούσε να χρησιμοποιήσει αυτήν τη συσκευή για να παραβιάσει ολόκληρο το οικιακό δίκτυο και, ως εκ τούτου, να θέσει σε κίνδυνο άλλες συσκευές που είναι συνδεδεμένες σε αυτό, όπως φορητούς υπολογιστές και κινητά τηλέφωνα [40]. Επιπλέον, η υποδομή IoT μπορεί να χρησιμοποιηθεί για την εκτέλεση άλλων ειδών επιθέσεων, όπως επιθέσεις άρνησης υπηρεσίας (DoS) που συνέβησαν το φθινόπωρο του 2016, όπου πολλοί σημαντικοί ιστότοποι διαταράχθηκαν από το botnet Mirai που επιτέθηκε σε μη ασφαλείς συσκευές IoT και τις χρησιμοποίησε για να ‘’βομβαρδίσει΄΄ άλλους διακομιστές [36].

ΑΔΥΝΑΜΗ ΑΣΦΑΛΕΙΑ ΛΟΓΙΣΜΙΚΟΥ-ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΔΕΔΟΜΕΝΩΝ

Μία από τις ευπάθειες είναι η αδύναμη ασφάλεια λογισμικού και η κρυπτογράφηση δεδομένων [36]. Σε μεγάλα συστήματα που αναπτύσσονται στις πόλεις, υπάρχουν εκατομμύρια γραμμές κώδικα που αποτελούν χιλιάδες πιθανά σημεία εκμετάλλευσης για ιούς δικτύου, κακόβουλο λογισμικό και κατευθυνόμενες εισβολές. Πολλοί προμηθευτές εφαρμόζουν προσαρμοσμένα πρωτόκολλα ασύρματης και ενσύρματης επικοινωνίας είτε με πολύ χαμηλή ασφάλεια είτε χωρίς ασφάλεια[42]. Ακόμη και όταν η κρυπτογράφηση εφαρμόζεται σε ασύρματες και ενσύρματες επικοινωνίες, είτε οι προμηθευτές εφαρμόζουν σωστά την κρυπτογράφηση, είτε εφαρμόζουν απαρχαιωμένους και αδύναμους αλγόριθμους κρυπτογράφησης, είτε εφαρμόζουν γνωστή κρυπτογράφηση, η οποία εξακολουθεί να διαθέτει αδύναμη διαχείριση κλειδιών κρυπτογράφησης. Επιπλέον, οι διοικήσεις των πόλεων και οι πωλητές τεχνολογιών για τις ΕΠ, συχνά τις χρησιμοποιούν χωρίς να πραγματοποιούν δοκιμές κυβερνοασφάλειας [42]. Για παράδειγμα, σήμερα, οι περισσότεροι αισθητήρες δεν είναι σε θέση να δημιουργήσουν μια κρυπτογραφημένη σύνδεση λόγω της προτεραιότητας που δίνεται στη φυσική αυτονομία της συσκευής ή στον περιορισμό του κόστους κατασκευής [43]. Επίσης είναι δύσκολο να διασφαλιστεί η ασφάλεια από άκρη σε άκρη, επειδή οι περισσότεροι αισθητήρες και συσκευές χαμηλής κατανάλωσης στην αγορά δεν έχουν επαρκή υπολογιστική ισχύ για να υποστηρίξουν κρυπτογραφημένη σύνδεση δικτύου [43].

ΠΑΛΑΙΑ ΣΥΣΤΗΜΑΤΑ – ΚΑΚΗ ΣΥΝΤΗΡΗΣΗ- ΑΞΙΟΛΟΓΗΣΗ ΑΣΦΑΛΕΙΑΣ

Ένας άλλος τομέας ευπάθειας αφορά τη χρήση μη ασφαλών παλαιών συστημάτων και την ανεπαρκή συντήρηση. Πολλές τεχνολογίες ΕΠ τοποθετούνται σε πολύ παλαιότερη υποδομή που βασίζεται σε λογισμικό και τεχνολογία που δημιουργήθηκε πριν αρκετά χρόνια, η οποία δεν έχει αναβαθμιστεί εδώ και αρκετό καιρό. Αυτές οι τεχνολογίες μπορούν να δημιουργήσουν εγγενείς ευπάθειες σε νεότερα συστήματα παρέχοντας τα λεγόμενα «forever-day exploits» (‘’τρύπες’’ σε προϊόντα λογισμικού παλαιού τύπου που οι πωλητές δεν υποστηρίζουν πλέον και επομένως δεν θα διορθωθούν ποτέ) [36]. Ακόμη και στην περίπτωση των νεότερων τεχνολογιών, μπορεί να είναι δύσκολο να δοκιμαστούν και να διατεθούν ενημερώσεις κώδικα σε κρίσιμα λειτουργικά συστήματα που πρέπει να είναι πάντα ενεργοποιημένα [42].

Καθώς μαζί με την εξέλιξη των τεχνολογιών εμφανίζονται νέες μορφές επιθέσεων και ανακαλύπτονται τρωτά σημεία, είναι φυσικό επακόλουθο ότι θα μεταβληθούν και τα επίπεδα ασφάλειας των συσκευών και της υποδομής IoT καθ' όλη τη διάρκεια του κύκλου ζωής τους. Ως εκ τούτου, η χρήση αυτοματοποιημένης παρακολούθησης, δοκιμής και εργαλείων μετριασμού είναι απαραίτητη για την αντιμετώπιση των κινδύνων που προκύπτουν από τέτοιες απειλές ή πιθανές αστοχίες κατασκευής ή διαμόρφωσης[34]. Αν και η χρήση εργαλείων ανίχνευσης εισβολών έχει εξεταστεί ευρέως, η διαδικασία της αξιολόγησης ασφάλειας στις ΕΠ που βασίζονται στο IoT απαιτεί πρόσθετα μέτρα λόγω των πιθανών επιπτώσεων που προκύπτουν από απειλές ασφάλειας.

ΑΝΘΡΩΠΙΝΟ ΛΑΘΟΣ

Η ασφάλεια μιας ΕΠ κινδυνεύει επίσης κι από ένα τυχαίο ή σκοπούμενο ανθρώπινο λάθος, από την πλευρά των ανθρώπων που εργάζονται για την παροχή υπηρεσιών σε μια ΕΠ. Τα συστήματα των ΕΠ δεν λειτουργούν πλήρως αυτόνομα, και ο άνθρωπος σχεδόν πάντα βρίσκεται στο κέντρο λήψης αποφάσεων ως μέρος της αλληλεπίδρασης με τα συστήματα αυτά, με αποτέλεσμα, ένα ανθρώπινο λάθος είτε τυχαίο, είτε εσκεμμένο να οδηγήσει σε διαρροή δεδομένων ή στη δυσλειτουργία του συστήματος[44]. Υπάρχουν πολλοί τρόποι που ένας χρήστης ΕΠ με εξουσία π.χ. υπάλληλος του δήμου μπορεί να σαμποτάρει το σύστημα. Για παράδειγμα, υπάλληλοι ανοίγουν μηνύματα ηλεκτρονικού ψαρέματος και εγκαθιστούν ιούς ή κακόβουλο λογισμικό ή εισάγουν αφελώς μολυσμένα στικ δεδομένων σε υπολογιστές [36]. Σε άλλες περιπτώσεις, το κατάλληλο λογισμικό ασφαλείας δεν είναι εγκατεστημένο ή έχει ρυθμιστεί εσφαλμένα ή οι εγκατεστημένοι κωδικοί του κατασκευαστή δεν αλλάζουν ή η ασφάλεια του συστήματος δεν διατηρείται ενημερωμένη[42]. Επιπλέον, οι χάκερς είναι έμπειροι στην εκμετάλλευση της ελλειπούς γνώσης στοιχειωδών μέτρων ασφαλείας, και με τη μέθοδο phishing μπορούν να αποδεσμεύσουν από τους χρήστες βασικές πληροφορίες (π.χ. ονόματα χρήστη και κωδικούς πρόσβασης) που διευκολύνουν την πρόσβαση[36]. Δεδομένου ότι υπάρχουν περιπτώσεις κατά τις οποίες υπηρεσίες επιτρέπουν στο προσωπικό τους να φέρει και να χρησιμοποιεί τις προσωπικές του συσκευές για να συνδεθεί με συσκευές και πληροφορίες σχετικές με την εργασία που οφείλουν να παρέχουν, είναι απίθανο να αποφευχθούν κίνδυνοι ασφάλειας, εξαιτίας κακόβουλων εφαρμογών (κακόβουλο λογισμικό) ή εγγενών ευπάθειών των εφαρμογών [29]. Μια άλλη πρόκληση που αντιμετωπίζουν επίσης οι

έξυπνες πόλεις είναι ότι το προσωπικό που είναι υπεύθυνο για την ανάλυση δεδομένων συχνά δεν έχει τις απαιτούμενες γνώσεις για να ανταποκριθεί αποτελεσματικά σε τυχόν πιθανές απειλές που μπορεί να προκύψουν 45. Καθώς οι ΕΠ μπορεί να λειτουργούν πάνω σε τεράστιο αριθμό συστημάτων και συσκευών που διαχειρίζονται κρίσιμες υπηρεσίες, ένα μικρό σφάλμα μπορεί να επιδεινώσει την απόδοσή τους, όπως για παράδειγμα, τον Νοέμβριο του 2013, η υπηρεσία Bay Area Rapid Transit (BART) στην Καλιφόρνια των ΗΠΑ, τερματίστηκε λόγω τεχνικού προβλήματος που αφορούσε την εναλλαγή τροχιάς, επηρεάζοντας 19 τρένα με περίπου 500–1000 επιβάτες[29]. Ακόμη, μια απειλή εκ των έσω, μπορεί να υπάρχει σε κάθε εταιρεία ή οργανισμό, όπως είναι και η ΕΠ. Οποιοσδήποτε νυν ή πρώην υπάλληλος, συνεργάτης ή ανάδοχος που έχει ή είχε πρόσβαση στα ψηφιακά στοιχεία του οργανισμού, ενδέχεται να καταχραστεί ηθελημένα ή ακούσια αυτήν την πρόσβαση [21].

Προς την κατεύθυνση ευαισθητοποίησης των χρηστών σχετικά με τους κινδύνους της κυβερνοασφάλειας που σχετίζονται και με το IoT, το άρθρο 10 του κανονισμού ΕΕ 881/2019 [46] για την κυβερνοασφάλεια υποστηρίζει την ανάγκη προώθησης συγκεκριμένων δράσεων μέσω καλών πρακτικών για πολίτες, οργανισμούς και επιχειρήσεις σε θέματα πρακτικών ασφαλείας στον κυβερνοχώρο. Επιπλέον, μια πρόσφατη έκθεση του ENISA τονίζει την ανάγκη για πρωτοβουλίες ευαισθητοποίησης για την ενθάρρυνση της ανάπτυξης αξιόπιστων σεναρίων IoT [34]. Θα πρέπει να σημειωθεί ότι η αύξηση των πρωτοβουλιών ευαισθητοποίησης θα είναι ζωτικής σημασίας για την ασφαλή ανάπτυξη έξυπνων πόλεων με δυνατότητα IoT, καθώς οι πολίτες διαδραματίζουν ενεργό ρόλο στην παροχή δεδομένων μέσω των συσκευών τους. Όπως αποδεικνύεται από γνωστές επιθέσεις (π.χ. το botnet Mirai), οι συσκευές IoT που έχουν παραβιαστεί μπορούν να χρησιμοποιηθούν για την πραγματοποίηση επιθέσεων εναντίον συστημάτων ΤΠΕ και κρίσιμων υποδομών, συνεπώς, η έλλειψη ευαισθητοποίησης θα μπορούσε να αντιπροσωπεύει κινδύνους ασφάλειας και ιδιωτικότητας που επηρεάζουν άλλα συστήματα και πολίτες σε μια ΕΠ[34].

3.3 ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΣΤΑ ΕΠΙΠΕΔΟ ΤΟΥ IoT

Κάθε συσκευή IoT φιλοξενεί τεχνολογίες στις οποίες οποιοσδήποτε παράγοντας απειλής θα μπορούσε να στοχεύσει προκειμένου να αποκτήσει πρόσβαση στο δίκτυο ενός

οργανισμού. Η εταιρία Gartner ανέφερε ότι το 20% των οργανισμών παρατήρησε τουλάχιστον μία επίθεση βασισμένη στο IoT από το 2015 έως το 2018, ενώ μέχρι το 2020 περισσότερο από το 25% των επιθέσεων έναντι επιχειρήσεων θα αφορούν συσκευές IoT[47]. Ωστόσο, μια έρευνα του 2018 σε 950 εταιρείες που κατασκευάζουν και χρησιμοποιούν τεχνολογία IoT, διαπίστωσε ότι λίγο λιγότερο από το μισό, συγκεκριμένα ποσοστό 48%, δεν διαθέτει μηχανισμούς ανίχνευσης για προστασία από επιθέσεις στον κυβερνοχώρο[48].

Σύμφωνα με στατιστικά στοιχεία επιθέσεων που βασίζονται στο IoT για το 2019, η μέση συσκευή IoT δέχεται επίθεση μόλις πέντε λεπτά μετά την ενεργοποίησή της [49]. Η έκρηξη στη δημοτικότητα των έξυπνων συσκευών αναμενόταν να οδηγήσει σε αύξηση των κυβερνοεπιθέσεων και δυστυχώς αυτό έχει αποδειχθεί αληθινό.

ΦΥΣΙΚΟ ΕΠΙΠΕΔΟ

Το φυσικό επίπεδο των ΕΠ περιλαμβάνει χιλιάδες διαφορετικούς αισθητήρες και ενεργοποιητές που αλληλεπιδρούν άμεσα με το περιβάλλον. Αυτή η ετερογένεια μαζί με τη διαρκώς μεταβαλλόμενη φύση του φυσικού επιπέδου, η οποία προκαλείται από τη δυναμική φύση των σύγχρονων πόλεων, θέτει ένα μεγάλο αριθμό ζητημάτων ασφάλειας και απορρήτου[27].

Ο κ. Cerrudo, ένας Αργεντινός ερευνητής ασφάλειας στο IOActive Labs (μια εταιρεία ασφάλειας Διαδικτύου), ανακάλυψε ότι λόγω ελλιπών μέτρων ασφαλείας μπορούσε να χακάρει το σύστημα κυκλοφορίας της περιοχής Capitol Hill της Ουάσιγκτον, μετατρέποντας τα κόκκινα φανάρια σε πράσινα και τα πράσινα σε κόκκινα[50].

Η ασφάλεια σε επίπεδο υλικολογισμικού πρέπει να παρέχει προστασία από σχετικές επιθέσεις, καθώς ένας παραβιασμένος κόμβος μετατρέπεται άνετα σε επιφάνεια εκκίνησης για διαρροή δεδομένων και διάφορες επιθέσεις δικτύου[27]. Τα smartphones και τα λειτουργικά τους συστήματα, που αποτελούν αναπόσπαστο κόμβο για πολλές υπηρεσίες IoT, υπόκεινται σε επιπλοκές ασφάλειας, με αποτέλεσμα, για καθεμία από τις υπηρεσίες IoT που φιλοξενεί ένα smartphone να απαιτούνται μοναδικές υπηρεσίες ασφαλείας[27].

Ακόμη, απαιτούνται συμπληρωματικά μέτρα για την ασφάλιση των συσκευών και την προστασία τους από σκόπιμη παραβίαση ή ακούσιες ζημιές, όπως με την κάλυψη αυτών σε ασφαλείς θήκες που περιορίζουν τη μη εξουσιοδοτημένη πρόσβαση. Πρόκειται για μια

απλή και αποτελεσματική (αλλά δαπανηρή) προσέγγιση που ενισχύει σημαντικά την ασφάλεια σε επίπεδο συσκευής[27]. Μια άλλη διάσταση της ασφάλειας της συσκευής περιλαμβάνει αποδεδειγμένη διαγραφή δεδομένων, έναν μηχανισμό που εγγυάται ότι τα ευαίσθητα δεδομένα πράγματι διαγράφονται και ως εκ τούτου δεν είναι προσβάσιμα στη μνήμη ενός κόμβου[27].

Σημαντικές απειλές για την ασφάλεια που μπορούν που έχουν ως στόχο το φυσικό επίπεδο, το οποίο αποτελείται από αισθητήρες και ενεργοποιητές, είναι οι ακόλουθες[51]:

Κατάληψη κόμβων (node capturing): Οι επιτιθέμενοι μπορούν να εντοπίσουν τις συσκευές που αποτελούν μέρος της εφαρμογής IoT και να τις αντικαταστήσουν, από άλλες κακόβουλες, οι οποίες αν και θα φαίνονται μέρος του συστήματος θα ελέγχονται από τον εισβολέα, με αποτέλεσμα ολόκληρη η ασφάλεια της εφαρμογής να τίθεται σε κίνδυνο.

Επίθεση με εγκατάσταση κακόβουλου κώδικα (malicious code injection attack): Η επίθεση περιλαμβάνει την εισαγωγή κάποιου κακόβουλου κώδικα στη μνήμη της συσκευής ή του ενεργοποιητή, εξαναγκάζοντας αυτές είτε να εκτελέσουν ακούσιες λειτουργίες είτε να διευκολύνουν την πρόσβαση του επιτιθέμενου στο πλήρες σύστημα IoT.

Επίθεση με εγκατάσταση ψευδών δεδομένων (false data injection attack): Ο εισβολέας, μόλις καταλάβει τη συσκευή μπορεί να τη χρησιμοποιήσει για να εισάγει λανθασμένα στοιχεία, οδηγώντας έτσι σε ψευδή αποτελέσματα και σε δυσλειτουργία της εφαρμογής IoT. Ο εισβολέας μπορεί επίσης να χρησιμοποιήσει αυτήν τη μέθοδο για να προκαλέσει και επίθεση άρνησης εξυπηρέτησης (DoS attack).

Side-Channel Attacks (SCA): Εκτός από άμεσες επιθέσεις στις συσκευές, ‘’έμμεσες’’ επιθέσεις σε αυτές μπορεί να οδηγήσουν σε διαρροή ευαίσθητων δεδομένων. Πληροφορίες όπως η μικροαρχιτεκτονική δομή των επεξεργαστών, η ηλεκτρομαγνητική εκπομπή και η κατανάλωση ενέργειας αποκαλύπτουν ευαίσθητες πληροφορίες στους επιτέθεμενους.

Υποκλοπή και παρεμβολές (eavesdropping and interference): Εφαρμογές IoT οι οποίες περιλαμβάνουν συχνά διάφορους κόμβους που λειτουργούν σε ανοιχτά περιβάλλοντα είναι ιδιαίτερα εκτεθιμένες σε κινδύνους, καθώς οι επιτιθέμενοι μπορούν να υποκλέψουν δεδομένα κατά τη διάρκεια διαφορετικών φάσεων, όπως κατά τη μετάδοση δεδομένων ή κατά τη διαδικασία ελέγχου ταυτότητας.

Επιθέσεις «Drain of Battery» (DoB): Λαμβάνοντας υπόψη τον ζωτικό ρόλο των μονάδων αποθήκευσης ενέργειας στο IoT, οι επιτιθέμενοι χρησιμοποιούν την εξάντληση ενέργειας

της μπαταρίας για να παύσουν τη λειτουργία μιας συσκευής ή ακόμη κι ενός ολόκληρου δικτύου. Οι επιθέσεις εξάντλησης ενέργειας παρεμποδίζουν τις επικοινωνίες της συσκευής για να αυξήσουν σκόπιμα το κόστος κατανάλωσης ενέργειας[27].

Επιθέσεις εκκίνησης (booting attacks)[51]: Οι συσκευές είναι ευάλωτες σε διάφορες επιθέσεις κατά τη διαδικασία εκκίνησης, γιατί οι ενσωματωμένες διαδικασίες ασφαλείας δεν είναι ενεργοποιημένες σε αυτό σημείο. Έτσι οι εισβολείς ενδέχεται να εκμεταλλευτούν αυτήν την ευπάθεια και να προσπαθήσουν να επιτεθούν στις συσκευές όταν αυτές επανεκκινούνται.

Botnet: Διάφορες ευάλωτες συσκευές IoT που χρησιμοποιούνται ευρέως στις ΕΠ, στα έξυπνα κτίρια και στα έξυπνα σπίτια είναι ιδιαίτερα ελκυστικές για την εγκατάσταση ισχυρού κακόβουλου λογισμικού, όπως οι παραλλαγές του botnet Mirai. Μια έκθεση της εταιρίας Kaspersky που δημοσιεύθηκε τον Οκτώβριο του 2019 χαρακτήρισε το Mirai και τις παραλλαγές του ως τις κορυφαίες απειλές έναντι συσκευών IoT το πρώτο εξάμηνο του 2019. Το Mirai και τα παράγωγά του παραμένουν το πιο κοινό κακόβουλο λογισμικό IoT[47]. Το Mirai ανακαλύφθηκε για πρώτη φορά τον Αύγουστο του 2016, γρήγορα εξαπλώθηκε σε δρομολογητές και και ήταν υπεύθυνο για σημαντικές επιθέσεις DDoS εκείνη τη χρονιά[47].

ΕΠΙΠΕΔΟ ΕΠΙΚΟΙΝΩΝΙΑΣ-ΜΕΤΑΔΟΣΗΣ ΔΕΔΟΜΕΝΩΝ

Στο επίπεδο επικοινωνίας συγκαταλέγεται το δίκτυο μικρής και μεσαίας εμβέλειας που επιτρέπει στους αισθητήρες να μεταδίδουν τα δεδομένα που συλλέγουν σε μια πύλη, όπως ηλεκτρονικοί υπολογιστές με πρόσβαση στο διαδίκτυο, μέσω των οποίων τα δεδομένα μεταφέρονται από και προς το cloud [27].

Μερικές από τις πιο συνηθισμένες επιθέσεις στο επίπεδο αυτό είναι οι εξής[20] :

Man in the Middle: Πρόκειται για επίθεση που αναφέρεται στην υποκλοπή δεδομένων στο δίκτυο με την παραποίηση της ταυτότητας μιας συσκευής δικτύου. Η επίθεση αυτή πραγματοποιείται με την εμφάνιση του προοριζόμενου παραλήπτη στον αποστολέα και του αρχικού αποστολέα στον παραλήπτη από μη εξουσιοδοτημένα πρόσωπα. Οι επιτιθέμενοι θα μπορούσαν να στοχεύσουν εταιρείες ανάπτυξης εφαρμογών για κινητά ή απλώς να στοχεύσουν τα δεδομένα που τροφοδοτούν τις εφαρμογές, βάσει των οποίων οι κάτοικοι των πόλεων λαμβάνουν αποφάσεις[42]. Για παράδειγμα, εάν η εφαρμογή δημόσιας συγκοινωνίας εμφανίζει καθυστέρηση σε ένα λεωφορείο, ένας πολίτης θα

μπορούσε να επιλέξει να ταξιδέψει στη δουλειά του με αυτοκίνητο[42]. Εάν ληφθεί η ίδια απόφαση από εκατοντάδες άτομα σε περιοχές υψηλής πυκνότητας, το αποτέλεσμα είναι μια κυκλοφοριακή συμφόρηση, την οποία μπορούμε να θεωρήσουμε ως DoS attack.

Spoofing Attack: Σε τέτοιου είδους επίθεση, ένας εισβολέας προστίθεται ως μια νόμιμη συσκευή στο δίκτυο, επιτρέποντάς του έτσι να στέλνουν ακανόνιστα ή ανώμαλα δεδομένα για να διαταραχθεί η κανονική λειτουργία του συστήματος μιας ΕΠ. Λόγω της διαφορετικής φύσης των συσκευών IoT που έχουν διαφορετικά επίπεδα ενσωματωμένης ασφάλειας, το spoofing attack αποτελεί ιδιαίτερα επικίνδυνη επίθεση για συστήματα IoT.

Επιθέσεις Διακοπής Υπηρεσιών- Denial of Service (DoS) ή Distributed DOS (DDoS): Πρόκειται για επιθέσεις κατά τις οποίες μια οντότητα αποκτά πρόσβαση στο δίκτυο και χρησιμοποιώντας νόμιμους κόμβους μέσα σε αυτό ''πλημμυρίζει'' τον στόχο με περιττά αιτήματα για την εξάντληση του εύρους της ζώνης δικτύου και την υποβάθμιση της ποιότητας των υπηρεσιών. Στην ΕΠ, η οποία εξαρτάται από τους αισθητήρες για να έχει μια ολοκληρωμένη εικόνα στο τι συμβαίνει εντός αυτής, οι επιθέσεις DOS μπορούν να βλάψουν το σύστημα της ΕΠ, γεγονός που μπορεί να οδηγήσει σε απώλεια περιουσίας και ζωής.

Eavesdropping /Sniffing attack: Στην υποκλοπή μια μη εξουσιοδοτημένη οντότητα εντάσσεται στο δίκτυο και μπορεί να υποκλέψει τα δεδομένα που ανταλλάσσονται μεταξύ των συσκευών στο δίκτυο.

Side channel attack: Σε αυτές τις περιπτώσεις είναι δυνατή η εξαγωγή πληροφοριών με την παρατήρηση της λειτουργίας των ενσωματωμένων χαρακτηριστικών, όπως η ισχύς που καταναλώνεται, ο χρόνος, η ανάλυση κυκλοφορίας, η ανάλυση σφαλμάτων. Αν και σε αυτού του είδους τις επιθέσεις, δεν παρέχεται πρόσβαση σε μη εξουσιοδοτημένα μέρη, οι επιτιθέμενοι μπορούν να προσδιορίσουν σημαντικές πληροφορίες σχετικά με το σύστημα, όπως το πρωτόκολλο που χρησιμοποιείται ή να τους επιτραπεί η αποστολή πακέτων δεδομένων έτσι ώστε να υποβαθμιστεί η απόδοση του δικτύου.

ΕΠΙΠΕΔΟ ΕΠΕΞΕΡΓΑΣΙΑΣ ΣΤΟ IoT

Πολλές υπηρεσίες έξυπνων πόλεων βασίζονται σε τεχνολογίες cloud, πράγμα που σημαίνει ότι τα δεδομένα που συλλέγονται από τους αισθητήρες μεταφέρονται τελικώς σε έναν κεντρικό διακομιστή[27]. Οι διακομιστές που βασίζονται στο cloud προτιμώνται επειδή είναι ισχυροί και μπορούν να εκτελούν περίπλοκους αλγόριθμους, μπορούν να

κλιμακωθούν ώστε να ανταποκρίνονται στις διαρκώς μεταβαλλόμενες απαιτήσεις μιας έξυπνης πόλης, ενώ το cloud είναι πάντα διαθέσιμο και έχει τη δυνατότητα να παρέχει υπηρεσίες σε πραγματικό χρόνο και σε μεγάλο αριθμό πελατών ταυτόχρονα[27]. Οι διακομιστές που βασίζονται στο cloud είναι το σημείο σύγκλισης όλων των δεδομένων που συλλέγονται σε μια εφαρμογή έξυπνης πόλης. Επομένως, οποιαδήποτε παραβίαση ασφάλειας μπορεί να θέσει σε κίνδυνο το απόρρητο και την ασφάλεια μεγάλου αριθμού χρηστών και μπορεί στη συνέχεια να οδηγήσει σε σοβαρότερες και μεγαλύτερης κλίμακας συνέπειες[27].

Αναφέρονται μερικά από τα κύρια ζητήματα ασφάλειας που εντοπίζονται σε αυτό το επίπεδο[51]:

Κλοπή δεδομένων (data thefts): Οι εφαρμογές IoT συγκεντρώνουν πολλά κρίσιμα και προσωπικά δεδομένα. Εφόσον οι εφαρμογές είναι ευάλωτες σε αυτές τις επιθέσεις, τότε και οι χρήστες θα είναι απρόθυμοι να καταχωρήσουν τα προσωπικά τους δεδομένα. Δεδομένου ότι μια υπηρεσία cloud θα χρησιμοποιείται από πολλές οντότητες με διαφορετικά πρωτόκολλα και πρακτικές ασφαλείας, είναι εξαιρετικά σημαντικό τα δεδομένα που αποθηκεύονται σε αυτό να είναι κρυπτογραφημένα έτσι ώστε να μην επιτρέπεται η έκθεσή του σε ανεπιθύμητες οντότητες, με κίνδυνο την παραβίαση του απορρήτου των χρηστών[20].

Επιθέσεις ελέγχου πρόσβασης (Access control attacks): Ο έλεγχος της πρόσβασης είναι ένας μηχανισμός που επιτρέπει μόνο στους νόμιμους χρήστες μέσω ασφαλών διαδικασιών να έχουν πρόσβαση στα δεδομένα ή στον λογαριασμό. Καθώς οι περισσότερες εφαρμογές των ΕΠ βασίζονται στη χρήση δεδομένων από διαφορετικές εφαρμογές για την παροχή έξυπνων υπηρεσιών, αυτό έχει ως αποτέλεσμα τα δεδομένα που έχουν συλλεχθεί να χρησιμοποιηθούν από πολλές διαφορετικές επιχειρήσεις [20]. Περιλαμβάνεται επίσης η μη εξουσιοδοτημένη σύνδεση σε δίκτυο, οι διαρροές δεδομένων, η περιήγηση σε αρχεία, η απόκτηση προσωπικών δεδομένων και η εκμετάλλευση πόρων για προσωπική χρήση[52]. Επιπλέον, η μη εξουσιοδοτημένη χρήση και πρόσβαση μπορεί να επηρεάσει την ακεραιότητα, την εμπιστευτικότητα και την αυθεντικότητα, καθώς οι επιτιθέμενοι ενδέχεται να έχουν αποκτήσει ολοκληρωμένες δυνατότητες[52].

Επιθέσεις διακοπής υπηρεσιών (Denial of Services): Τέτοιες επιθέσεις στερούν από τους νόμιμους χρήστες τη χρήση των υπηρεσιών των εφαρμογών IoT, καθώς καθιστούν το δίκτυο και τους διακομιστές υπερφορτωμένο από τις επιθέσεις αιτημάτων με αποτέλεσμα

να μην μπορούν να ανταποκριθούν. Αυτού του είδους οι επιθέσεις στοχεύουν τη διαθεσιμότητα των εφαρμογών. Η αύξηση του αριθμού των συνδεδεμένων υπηρεσιών παγκοσμίως και η εξάρτησή τους από το IoT για την εκτέλεση και τη διευκόλυνση τέτοιων υπηρεσιών προκαλεί ανησυχίες σχετικά με επιθέσεις DoS που ενδέχεται να προκαλέσουν αστοχίες σε ολόκληρη τη χώρα, τόσο σε επιχειρήσεις όσο και σε κρίσιμα συστήματα[21].

Malicious Code injection Attacks: Οι επιτιθέμενοι προσπαθούν με την ευκολότερη και απλούστερη μέθοδο να εισέλθουν σε ένα σύστημα ή ένα δίκτυο. Εάν το σύστημα είναι ευάλωτο σε κακόβουλα λογισμικά λόγω ανεπαρκών και ανίσχυρων κωδικών, τότε αυτό θα ήταν το πρώτο σημείο εισόδου που θα επέλεγε ένας εισβολέας.

4. ΖΗΤΗΜΑΤΑ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΤΗΝ ΕΞΥΠΝΗ ΠΟΛΗ

4.1. Η ΙΔΙΩΤΙΚΟΤΗΤΑ ΤΟΥ ΚΑΤΟΙΚΟΥ ΜΙΑ ΕΞΥΠΝΗΣ ΠΟΛΗΣ

Παλαιότερα, στο περιβάλλον μιας -συνήθως- μεγάλης πόλης, ένα πρόσωπο θα μπορούσε να θεωρήσει ότι όταν κινείται σε αυτή χάνει για λίγο την ‘’ταυτότητά’’ του, δρα μέσα στο πλήθος και περνάει απαρατήρητος, στοιχείο το οποίο δεν θεωρείτο απαραίτητα αρνητικό, αλλά αντιθέτως προσέδιδε ίσως μια μεγαλύτερη ελευθερία κινήσεων. Υπό το πρίσμα των σύγχρονων τεχνολογικών εξελίξεων, οι οποίες έχουν διεισδύσει στη λειτουργία των έξυπνων πόλεων, οι κάτοικοι μιας πόλης μπορούν να χαρακτηριστούν ως ‘’ψηφιακοί πολίτες’’, όχι μόνο εξαιτίας της ψηφιοποίησης και των πιο απλών καθημερινών συναλλαγών αλλά και επειδή ζουν και λειτουργούν όλο και περισσότερο σε ένα περιβάλλον, στο οποίο οποιαδήποτε δραστηριότητα λαμβάνει χώρα ‘’αφήνει πίσω της ίχνη’’[53]. Πολλές από τις δραστηριότητές, εντός του διαδικτύου ή ακόμη και εκτός σύνδεσης, παράγουν δεδομένα (δεδομένα γεωγραφικής τοποθεσίας που αποκαλύπτει η χρήση κινητού τηλεφώνου, μεταδεδομένα της διαδικτυακής επικοινωνίας, δεδομένα σχετικά με τις προτιμήσεις, δεδομένα για τις κινήσεις και τις συνήθειες στα έξυπνα σπίτια, δεδομένα που παράγονται από δίκτυο αισθητήρων).

Στο πλαίσιο της βιβλιογραφίας για την επέμβαση των ΤΠΕ στην ιδιωτικότητα των κατοίκων μιας ΕΠ, έχει γίνει προσπάθεια να προσδιορισθεί αυτή υπό το πρίσμα πέντε κατηγοριών στις οποίες θίγεται ,και το οποίο έχει ως εξής [54]:

Το *απόρρητο της ταυτότητας,* το οποίο σχετίζεται με την αποκάλυψη αυτής κάθε φορά που ένας χρήστης αποκτά πρόσβαση σε μια υπηρεσία έξυπνης πόλης. Εάν οι χρήστες προσδιορίσουν την ταυτότητά τους, οι πάροχοι υπηρεσιών και άλλα τρίτα μέρη θα μπορούν να συσχετίσουν τους χρήστες και τις δραστηριότητές τους.

Το *απόρρητο ερωτημάτων* που υποβάλλονται από τους χρήστες στις παρεχόμενες υπηρεσίες. Μετά τη συλλογή των ερωτημάτων που υποβάλλονται από τους χρήστες, οι πάροχοι υπηρεσιών μπορούν να σκιαγραφήσουν το προφίλ των χρηστών και να λάβουν πληροφορίες σχετικά με τις συνήθειες τους.

Το *απόρρητο τοποθεσίας* αφορά τη διασφάλιση ότι διατηρείται το απόρρητο της φυσικής τοποθεσίας του χρήστη.

Το *απόρρητο του αποτυπώματος* σχετίζεται με τον έλεγχο των πληροφοριών που μπορούν να ανακτηθούν ή να συναχθούν από σύνολα μικροδεδομένων. Στην πραγματικότητα, οι δραστηριότητες σε μια έξυπνη πόλη περιλαμβάνουν την απόκτηση, συλλογή και αποθήκευση μεγάλων ποσοτήτων μικροδεδομένων, δηλαδή των πληροφοριών σε επίπεδο ερωτηθέντων. Αυτά τα μικροδεδομένα λαμβάνονται από διάφορες πηγές, όπως δίκτυα αισθητήρων, συσκευές ανάγνωσης RFID, κ.λπ. Ως εκ τούτου, μια υπηρεσία σχετίζεται με ένα σύνολο μικροδεδομένων που καταγράφει τις πληροφορίες σχετικά με τη χρήση μιας υπηρεσίας. Τα σύνολα μικροδεδομένων μπορούν να κοινοποιηθούν σε τρίτους, οι οποίοι θα λάβουν ποικίλες πληροφορίες.

Το *απόρρητο του κατόχου* σχετίζεται με την επίγνωση του απορρήτου των ερωτημάτων στις βάσεις δεδομένων από διαφορετικές αυτόνομες οντότητες, για παράδειγμα ο συσχετισμός της χρήσης ηλεκτρικής ενέργειας με τη χρήση άλλων υπηρεσιών, όπως τηλεπικοινωνιών, για εμπορικούς σκοπούς.

4.2.ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ – ΣΥΓΧΡΟΝΟ ΕΡΓΑΛΕΙΟ ΕΠΙΤΗΡΗΣΗΣ?

Το Διαδίκτυο των Πραγμάτων (IoT) αποτελεί τη ραχοκοκαλιά της ΕΠ. Αισθητήρες, συνδεδεμένοι σε δημόσια ή ιδιωτικά δίκτυα είναι παντού εγκατεστημένοι, σε κάθε καίριο σημείο της πόλης και συγκεντρώνουν δεδομένα.

Σε άρθρο στην εφημερίδα ‘’The Guardian’’ αναφέρεται ότι ‘’*Μπορεί να βρεθούμε να αλληλεπιδρούμε με χιλιάδες μικρά αντικείμενα γύρω μας σε καθημερινή βάση, το καθένα*

συλλέγοντας φαινομενικά αβλαβή δεδομένα 24/7, πληροφορίες που αυτά τα πράγματα θα μεταφέρουν στο cloud, όπου θα υποβληθούν σε επεξεργασία, συσχέτιση και αναθεώρηση. Το έξυπνο ρολόι σας θα αποκαλύψει την έλλειψη άσκησης στην ασφαλιστική εταιρεία υγείας σας, το αυτοκίνητό σας θα ενημερώσει τον ασφαλιστή σας για τη συχνή υπερβολική ταχύτητα και ο κάδος απορριμμάτων θα ενημερώσει τον τοπικό σας δήμο ότι δεν ακολουθείτε τους τοπικούς κανονισμούς ανακύκλωσης. Αυτό είναι το IoT, και αν και μπορεί να ακούγεται τραβηγμένο, συμβαίνει ήδη [55]''. Παρακολουθώντας τον κόσμο με εντατικούς και παρεμβατικούς τρόπους – όχι μόνο στις κατοικίες και τα οχήματα αλλά ακόμη και στο ίδιο τους το σώμα– οι συσκευές που βασίζονται σε δεδομένα μπορούν να ωθήσουν, να χειραγωγήσουν και να διαμορφώσουν τις συμπεριφορές, τις συνήθειες και τις προτιμήσεις, να περιορίσουν την αυτονομία και να επιφέρουν ποσοτικοποίηση, διαχωρισμό και διακρίσεις [56]. Το βασικό πρόβλημα του IoT, είναι ότι οι συσκευές του έχουν σχεδιαστεί με τέτοιο τρόπο, ώστε να είναι διακριτικές και απρόσκοπτες στη λειτουργία τους από το χρήστη, και όπως έχει αναφερθεί κατορθώνουν να διεισδύουν σε κάθε πτυχή της καθημερινής ζωής ,μέχρι να μην ξεχωρίζουν καθόλου [57].

Σε συνδυασμό με τεχνολογίες προσδιορισμού θέσης τα αντικείμενα με ενσωματωμένους αισθητήρες (sensors) αποκτούν πρωτόγνωρες ιδιότητες , καθώς μπορούν να γνωρίζουν που βρίσκονται τα ίδια ή ποια άλλα αντικείμενα και πρόσωπα βρίσκονται στο κοντινό περιβάλλον[58]. Στο ubiquitous computing η ηλεκτρονική επεξεργασία πληροφορίας δεν διαχωρίζεται από τις άλλες καθημερινές δραστηριότητες, δεν γίνεται καν αντιληπτή ως τέτοια ενώ προσαρμόζεται στο εκάστοτε περιβάλλον[58].

Στην πόλη Eindhoven της Δανίας η αστυνομία, οι ιδιοκτήτες παμπ, ο δήμος και οι επιχειρηματίες συνεργάζονται για να βελτιώσουν την ατμόσφαιρα στην οδό αυτής Stratumseind, προς ενίσχυση της ασφάλεια και της οικονομίας, δοκιμάζοντας καινοτόμες ιδέες για την αντιμετώπιση περιστατικών βίας. Βασικός στόχος είναι επίσης και η βελτίωση των συνθηκών διαβίωσης και στέγασης στην πόλη. Για τους λόγους αυτούς δημιουργήθηκε το εργαστήριο της οδού Stratumseind (SLL) στην πόλη Eindhoven της Δανίας, ένα περιβάλλον ανάπτυξης και δοκιμής στο οποίο συνεργάζονται εταιρείες, πανεπιστήμια, κυβερνήσεις, κάτοικοι και επιχειρηματίες του Stratumseind[59]. Νέα προϊόντα και υπηρεσίες αναπτύσσονται από κοινού, εστιάζοντας στην τεχνολογία, την κοινωνιολογία, τη διαχείριση της βίας και τη διαχείριση του πλήθους. Αυτό απαιτεί τη συλλογή και ανάλυση όλων των ειδών δεδομένων. Για παράδειγμα στο χώρο της νυχτερινής διασκέδασης έχουν

τοποθετηθεί κάμερες, αισθητήρες και όργανα μέτρησης. Όλα τα δεδομένα παρακολουθούνται σε πραγματικό χρόνο στο κέντρο πληροφοριών αυτού του εργαστηρίου.

Η επιτήρηση εντός του SLL [60] αφορά κυρίως την παρακολούθηση του φυσικού δημόσιου χώρου, και περιορίζεται στην οδό Stratumseind. Ωστόσο, καθώς εκτελείται μέσω διαφόρων ψηφιακών τεχνολογιών που λειτουργούν ως αισθητήρες (βιντεοκάμερες, κάμερες ήχου και τεχνολογίες δυναμικού φωτισμού), πιθανώς να εξαπλωθεί σε άλλους δρόμους της πόλης, να βασίζεται στη συλλογή και ανάλυση δεδομένων, και ως εκ τούτου να καθίσταται περισσότερο δικτυωμένη και ''αόρατη''. Η αδιαφάνεια μιας τέτοιας επιτήρησης ενισχύεται καθώς οι αισθητήρες και τα συστήματα ηλεκτρονικών επικοινωνιών που την υποστηρίζουν ενσωματώνονται στο αστικό περιβάλλον και είναι επομένως λιγότερο αισθητά για τον διερχόμενο [60].

Οι κάμερες ήχου και οι τεχνολογίες παρακολούθησης WIFI, συχνά σε σχήμα μικρών μαύρων κουτιών που τοποθετούνται στον κλασικό φωτισμό του δρόμου, δεν είναι ιδιαίτερα διακριτές , ενώ δεν απουσίαζαν και πινακίδες που γνωστοποιούσαν την επιτήρηση στις εισόδους της οδού Stratumseind. Πολλοί αισθητήρες είναι ενσωματωμένοι στο φάσμα της οδού Stratumseind (π.χ. προσαρτημένοι σε κτίρια ή σε υπάρχοντες στύλους φωτισμού) με σκοπό την άμεση ανίχνευση, συμπεριλαμβανομένων «έξυπνων» βιντεοκάμερων, αισθητήρων ήχου και καμερών ήχου, μετεωρολογικού σταθμού και τεχνολογίας iBeacon. Υπό αυτή την έννοια, το έξυπνο τηλέφωνο (με τεχνολογία GPS) μπορεί να λειτουργήσει ως συσκευή παρακολούθησης. Στην πραγματικότητα, οποιαδήποτε δικτυωμένη διαδραστική συσκευή μπορεί να λειτουργήσει ως αισθητήρας στο βαθμό που συλλέγει και μοιράζεται δεδομένα σχετικά με τη χρήση της. Αυτά τα δεδομένα μπορούν στη συνέχεια να χρησιμοποιηθούν για την εξαγωγή πληροφοριών σχετικά με τον χρήστη και το περιβάλλον του χρήστη. Στην περίπτωση του SLL, τα έξυπνα τηλέφωνα χρησιμοποιούνται για τον προσδιορισμό της κατοικίας και της εθνικότητας (όπως διακρίνεται από τη διαμονή και τη συνδρομή κινητής τηλεφωνίας) των επισκεπτών του Stratumseind. Τα μοναδικά αναγνωριστικά του smartphone τους, αν και ψευδώνυμα, συλλαμβάνονται επίσης από την παρακολούθηση WIFI που εκτελείται από την SLL. Η επιτήρηση εντός του SLL είναι επομένως κατά κύριο λόγο «εποπτεία αισθητήρα», που αντιπροσωπεύει έναν διάχυτο, πάντα ενεργό και παθητικό τύπο συλλογής δεδομένων .

Το SLL όχι μόνο παρακολουθεί τον φυσικό δημόσιο χώρο της οδού Stratumseind και των περιχώρων της, αλλά παρακολουθεί επίσης –αν και σε πολύ μικρότερο βαθμό– ορισμένα μέσα κοινωνικής δικτύωσης, όπως το Twitter. Πραγματοποιεί έναν απλό τύπο ανάλυσης συναισθήματος αναλύοντας tweets που συνδέονται με κάποιο τρόπο με το Stratumseind (π.χ. ονοματίζοντας τον δρόμο, ένα συγκεκριμένο μπαρ στο δρόμο ή έναν συγκεκριμένο γνωστό μπάρμαν) και ταξινομώντας τα ως θετικά, αρνητικά και ουδέτερα. Υπό αυτή την έννοια, το κοινό – επισκέπτες του Stratumseind – εκτίθεται πρόθυμα και συμμετέχει έτσι στη δική του επιτήρηση.

4.3 ΑΥΤΟΕΠΙΤΗΡΗΣΗ ΜΕ ΧΡΗΣΗ ΣΥΣΚΕΥΩΝ IOT

Μία από τις βασικότερες συνέπειες των συσκευών IoT είναι ότι παρέχουν τη δυνατότητα για μια μαζική επιτήρηση αλλά και τη δυνατότητα για αυτοεπιτήρηση [61]. Αυτά τα συστήματα αυτοεπιτήρησης έχουν διαφορετικά επίπεδα- ορισμένα συστήματα βασίζονται σε μικροσκοπικά συστήματα, όπως το πόσο δραστήριο είναι ένα άτομο που φοράει μια συσκευή FitBit, και ορισμένα βασίζονται σε μακροεντολές, όπως η παρακολούθηση μιας πόλης για την κατανάλωση ηλεκτρικής ενέργειας, την κυκλοφοριακή κίνηση και τις εγκληματικές δραστηριότητες [61]. Η μικρο-προσανατολισμένη επιτήρηση γίνεται συχνά στοιχείο μεγαλύτερων συστημάτων, όπως για παράδειγμα η παρακολούθηση των χτύπων της καρδιάς, η οποία, σε συνδυασμό με μια αξιολόγηση της αρτηριακής πίεσης, έναν αξιολογητή ύπνου και έναν μετρητή βημάτων, μπορεί να δημιουργήσει έναν καλύτερο δείκτη προσωπικής υγείας. Οι πληροφορίες ενός μεμονωμένου ατόμου, με τη σειρά τους, μπορούν να προσπελαστούν, να συγκεντρωθούν, ακόμα και να ανωνυμοποιηθούν, και να ταξινομηθούν από εταιρείες υγείας ή ασφαλιστές για να προβλέψουν τις τάσεις της υγείας και να δημιουργήσουν μεγαλύτερη αποτελεσματικότητα στις επιχειρήσεις τους.

Οι πληροφορίες που δημιουργούνται από τις συσκευές μετάδοσης μπορούν εύκολα να κοινοποιηθούν σε προγραμματιστές εφαρμογών, κατασκευαστές και άλλα ενδιαφερόμενα τρίτα μέρη. Αξιοσημείωτο είναι ότι αυτού του είδους η επιτήρηση από τις συσκευές IoT φαίνεται πολύ λιγότερο επεμβατική, ενώ η μεταβίβαση των δεδομένων προκαλεί ελάχιστο φόβο, ακριβώς επειδή τυχόν αρνητικές επιπτώσεις από το διαμοιρασμό των δεδομένων καθίστανται λιγότερο ορατές [61]. Ένα άλλο σημαντικό χαρακτηριστικό των IoT είναι ότι συνήθως η επιτήρηση πραγματοποιείται με τη συναίνεση των υποκειμένων, εν συνεχεία

τα δεδομένα ενδέχεται να μεταβιβάζονται στον κατασκευαστή κι από εκεί σε άλλα τρίτα μέρη. Αντίθετα, όταν μοιραζόμαστε προσωπικά δεδομένα στον διαδικτυακό ψηφιακό κόσμο – για παράδειγμα στο Facebook, το Google, το Amazon ή το eBay – γνωρίζουμε, έστω και αμυδρά ότι έχουμε την ευκαιρία, τουλάχιστον μία φορά, να δώσουμε ή να αρνηθούμε τη συγκατάθεσή μας για τη συλλογή δεδομένων, προτού αρχίσουμε να χρησιμοποιούμε την υπηρεσία (ακόμα και αν στην πραγματικότητα η κύρια επιλογή μας είναι είτε να λάβουμε είτε να απορρίψουμε πλήρως την υπηρεσία)[28]. Στο IoT, τέτοιες ειδοποιήσεις και ευκαιρίες απουσιάζουν κατά κύριο λόγο από το σχεδιασμό. Ακόμη και όπου η διακριτικότητα δεν αποτελεί προδιαγραφή λειτουργίας, οι συσκευές IoT απλώς δεν διαθέτουν συνήθως μέσα για να εμφανίζουν ειδοποιήσεις απορρήτου ή/και να παρέχουν ακριβή συναίνεση σύμφωνα με τις προτιμήσεις που εκφράζουν τα άτομα, καθώς οι συσκευές είναι συνήθως μικρές, χωρίς οθόνη ή πληκτρολόγιο[28].

4.4.Η ΤΕΧΝΟΛΟΓΙΑ ΕΓΚΑΤΑΣΤΑΣΗΣ ΕΞΥΠΝΩΝ ΜΕΤΡΗΤΩΝ, ΠΑΡΑΔΕΙΓΜΑ ΠΡΟΣΒΟΛΗΣ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ?

Μία από τις βασικότερες εφαρμογές των ΤΠΕ στις έξυπνες πόλεις είναι η έξυπνη ενέργεια, με σκοπό την αξιοποίηση των ανανεώσιμων πηγών ενέργειας καθώς και την ανακύκλωση της παραγόμενης ενέργειας προκειμένου, τεχνικών φιλικών προς το περιβάλλον. Για την επίτευξη αυτού μπορούν να χρησιμοποιηθούν έξυπνοι μετρητές, οι οποίοι εγκαθίστανται στα κτίρια, βιομηχανικά ή οικιακά. Η άμεση επαφή με τις αγορές ηλεκτρικής ενέργειας επιτρέπει στον έξυπνο μετρητή να προγραμματίζει τους βέλτιστους χρόνους λειτουργίας συσκευών όπως ψυγεία ή πλυντήρια ρούχων ή να ‘’παραγγείλει’’ ηλεκτρική ενέργεια, με βάση τις τρέχουσες τιμές και τη διαθεσιμότητα[62]. Μπορεί επίσης να κοινοποιήσει πληροφορίες της τρέχουσας και μελλοντικής κατανάλωσης στον ιδιοκτήτη του σπιτιού και να προτείνει ή να ενθαρρύνει την εξοικονόμηση ενέργειας ή να στείλει αυτές τις πληροφορίες σε παρόχους ενέργειας προκειμένου να τους επιτρέψει να προβλέψουν καλύτερα τη μελλοντική ζήτηση και να αποφύγουν την πλεονάζουσα παραγωγική ικανότητα[62].

Αυτή η καινοτομία, ωστόσο αν και αρχικά δείχνει εξαιρετικά αποτελεσματική προς τη μείωση εκπομπών άνθρακα, απαραίτητη για την εν γένει προστασία του περιβάλλοντος

και χαρακτηριστικό μιας έξυπνης πόλης, ενέχει εντούτοις κινδύνους για την ιδιωτικότητα των ατόμων και την εμπιστοσύνη των καταναλωτών.

Αυτό σημαίνει ότι μια συστηματική παρακολούθηση της ενέργειας θα μπορούσε να αποκαλύψει πληροφορίες σχετικά με τις δραστηριότητες των κατοίκων. Οι αλγόριθμοι εξόρυξης δεδομένων μπορεί να είναι ικανοί όχι μόνο να συνάγουν τις τρέχουσες και προηγούμενες δραστηριότητες του καταναλωτή από τέτοια δεδομένα, αλλά και να ανιχνεύουν συνήθειες και συγκεκριμένα γεγονότα (π.χ. αν στο χώρο βρίσκονται επιπλέον άτομα από τους συνήθεις ενοίκους) [62]. Μια σημαντική παράμετρος στο σχεδιασμού του συστήματος, επομένως, είναι σε ποιο βαθμό λεπτομέρειας αποθηκεύονται και/ή μεταδίδονται οι επιμέρους τοπικές μετρήσεις ενέργειας προς τον πάροχο ενέργειας. Αυτό οδηγεί άμεσα στο ερώτημα ποιος φορέας επιτρέπεται να συλλέγει, να αναλύει και να συγκεντρώνει δεδομένα κατανάλωσης ενέργειας σε ένα σύστημα που συνήθως κυριαρχείται από λίγους οιονεί μονοπωλητές.

Στην προσπάθεια της Ολλανδίας να εφαρμόσει το σύστημα των έξυπνων μετρητών κατά τη μεταφορά της οδηγίας 2006/32/EC εντοπίστηκαν δύο προβλήματα[63]. Το πρώτο πρόβλημα ήταν η υποτίμηση της σημασίας της ιδιωτικής ζωής. Οι συντάκτες των αρχικών νομοσχεδίων για τις έξυπνες μετρήσεις εστίασαν σχεδόν αποκλειστικά στις οικονομικές και περιβαλλοντικές πτυχές των έξυπνων δικτύων και των έξυπνων μετρητών. Όταν αναγκάστηκαν να προβούν σε εκτίμηση επιπτώσεων στο απόρρητο της ιδιωτικής ζωής, τότε έγινε αντιληπτό ότι οι έξυπνοι μετρητές έχουν την ικανότητα να αποκαλύπτουν αρκετά ευαίσθητες πληροφορίες για το απόρρητο, επηρεάζοντας έτσι όχι μόνο το απόρρητο πληροφοριών αλλά και το απόρρητο της κατοικίας και της οικογενειακής ζωής, γεγονός που αρχικώς φάνηκε να αγνοήθηκε. Το δεύτερο πρόβλημα ήταν η επέκταση της λειτουργικότητας πέρα από τον αρχικό σκοπό[63]. Ενώ η ευρωπαϊκή νομοθεσία απαιτούσε από τους έξυπνους μετρητές να παρέχουν ανατροφοδότηση στους τελικούς χρήστες, βοηθώντας τους έτσι να εξοικονομήσουν ενέργεια, οι ολλανδικοί λογαριασμοί πρόσθεσαν αρκετές λειτουργίες στον προτεινόμενο έξυπνο μετρητή, όπως ο μετρητής να είναι ελεγχόμενος σε απόσταση για τη ρύθμιση της παροχής ενέργειας, τόσο για σκοπούς καταπολέμησης απάτης όσο και για σκοπούς διαχείρισης βλαβών. Ο συνδυασμός όλων αυτών των λειτουργιών οδήγησε σε έναν έξυπνο μετρητή με δυνατότητα πολύ υψηλής συχνότητας αμφίδρομης κυκλοφορίας μεταξύ του μετρητή και του δικτύου, αγνοώντας λιγότερο επεμβατικές εναλλακτικές, όπως οι οθόνες στο σπίτι ή η συγκέντρωση

μεμονωμένων δεδομένων μετρητών στο δίκτυο, τα οποία πιθανότατα θα μπορούσαν εξίσου να εξυπηρετήσουν τους σκοπούς της εξοικονόμησης ενέργειας ή της διαχείρισης του δικτύου.

Ειδικότερα στην Ευρώπη, με αφορμή την ανάπτυξη έξυπνων συστημάτων μέτρησης, ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων εξέδωσε το 2012 σύσταση στα κράτη μέλη **[64]**, προειδοποιώντας ότι: *. . . η πανευρωπαϊκή ανάπτυξη έξυπνων συστημάτων μέτρησης επιτρέπει τη μαζική συλλογή προσωπικών πληροφοριών από τα νοικοκυριά, πρωτοφανές στον ενεργειακό τομέα. Η πιθανή παρεμβατικότητα της συλλογής αυξάνεται από το γεγονός ότι συλλέγονται δεδομένα, τα οποία ενδέχεται να συνάγουν πληροφορίες σχετικά με οικιακές δραστηριότητες: τα δεδομένα μπορούν να παρακολουθούν τι κάνουν τα μέλη ενός νοικοκυριού στον προσωπικό και ιδιωτικό χώρο της κατοικίας τους. Αυτό εγείρει ανησυχίες όσον αφορά την ασφάλεια, τα δικαιώματα στην ιδιωτική ζωή και την προστασία των προσωπικών δεδομένων.*

Η σύσταση ανέφερε επίσης ότι: *Οι κίνδυνοι για την προστασία των δεδομένων, ωστόσο, προχωρούν περισσότερο από αυτούς πιο άμεσες ανησυχίες. Πράγματι, εάν δεν υπάρχουν επαρκείς διασφαλίσεις για να διασφαλίζουν ότι μόνο εξουσιοδοτημένα μέρη μπορεί να έχουν πρόσβαση και να επεξεργάζονται δεδομένα για σαφώς καθορισμένους σκοπούς και σε συμμόρφωση με την ισχύουσα νομοθεσία περί προστασίας δεδομένων, η ανάπτυξη της έξυπνης μέτρησης μπορεί να οδηγήσει στη λεπτομερή παρακολούθηση της καθημερινότητας των ανθρώπων και στη δημιουργία προφίλ αυτών με βάση τις οικιακές τους δραστηριότητες.*

Η κατανόηση των έξυπνων τεχνολογιών ως τεχνολογιών με δυνατότητα επιτήρησης, επομένως, θέτει τη συζήτηση σε διαφορετική θέση. Από θέματα που σχετίζονται με τη συμμετοχή και την καινοτομία μέχρι την ιδιωτικότητα, τα θεμελιώδη δικαιώματα, την ηθική και την ευθύνη στην τεχνολογική καινοτομία [65].

Η επέμβαση και ο περιορισμός στην ιδιωτικότητα που μπορεί να επιφέρει η εγκατάσταση των έξυπνων μετρητών διαφαίνεται μέσα από το άρθρο 8 της Ευρωπαϊκής Σύμβασης Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ)[66]. Το άρθρο 8 παρ. 1 της ΕΣΔΑ[13] – με τις τέσσερις συνιστώσες του - σεβασμός της ιδιωτικής ζωής, της οικογενειακής ζωής, της κατοικίας και

[13] Αρ. 8 παρ. 1 της ΕΣΔΑ ''Παν πρόσωπον δικαιούται εις τον σεβασμόν της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και της αλληλογραφίας του''.

της αλληλογραφίας- μπορεί να καλύψει ένα ευρύ φάσμα θεμάτων, όπως ενδεικτικά η ακεραιότητα, η πρόσβαση σε πληροφορίες και δημόσια έγγραφα, το απόρρητο της αλληλογραφίας και της επικοινωνίας, η προστασία της κατοικία, προστασία προσωπικών δεδομένων, υποκλοπές επικοινωνιών, φύλο, υγεία, ταυτότητα (δηλαδή δικαίωμα να έχει κάποιος έλεγχο σε δείκτες ταυτότητας όπως το όνομά κάποιου), σεξουαλικό προσανατολισμό, προστασία από περιβαλλοντικές οχλήσεις και ούτω καθεξής[66]. Λαμβανομένου υπόψη η έξυπνη μέτρηση, συμβάλει στην πανταχού παρούσα επιτήρηση των καταναλωτών ενέργειας με τη συλλογή στοιχείων και λεπτομερειών που προκύπτουν από την κατανάλωση ηλεκτρικής ενέργειας, χρειάζονται ακριβή κριτήρια για τη ρύθμισή του[66], όπως αυτά ρυθμίζονται στο α. 8 παρ. 2 της ΕΣΔΑ[14]. Ειδικότερα, οποιοσδήποτε περιορισμός στην άσκηση αυτών των δικαιωμάτων πρέπει να προβλέπεται από το νόμο (κριτήριο νομιμότητας), να είναι αναγκαίος στη δημοκρατική κοινωνία (αναγκαιότητα) και να εξυπηρετεί τουλάχιστον ένα από τα συγκεκριμένα δημόσια συμφέροντα: την εθνική ασφάλεια, δημόσια ασφάλεια ή οικονομική ευημερία της χώρας, την προάσπιση της τάξης και την πρόληψη ποινικών παραβάσεων εγκληματικότητας, την προστασία της υγείας ή της ηθικής, την προστασία των δικαιωμάτων και ελευθεριών των άλλων. Επιπλέον, οποιαδήποτε παρέμβαση πρέπει να είναι ανάλογη προς τον επιδιωκόμενο θεμιτό σκοπό και να ανταποκρίνεται σε μια επιτακτική κοινωνική ανάγκη (αναλογικότητα). Ορισμένες μέθοδοι για να αξιολογήσουμε την έλλειψης αναλογικότητας περιλαμβάνουν την έκδηλη δυσαναλογία ή την ύπαρξη εναλλακτικής και λιγότερο παρεμβατικής λύσης.

Με βάση τα παραπάνω είναι αρκετά εύκολο να θεσπιστεί το νομικό πλαίσιο για τα έξυπνα δίκτυα (δηλαδή να εκπληρωθεί το κριτήριο της νομιμότητας), είναι πολύ πιο δύσκολο όμως να εκτιμηθεί εάν μπορεί να δικαιολογηθεί ο βαθμός παρέμβασής του(δηλαδή αναγκαιότητα, νομιμότητα και αναλογικότητα). Για το λόγο αυτό γεννιώνται ορισμένα ερωτήματα[66]: Συμβάλλει η έξυπνη μέτρηση στην «οικονομική ευημερία της χώρας»; Συμβάλλει στην ενεργειακή απόδοση και σε μια πιο ανταγωνιστική αγορά ενέργειας; Είναι αυτή η παρέμβαση ανάλογη με τον επιδιωκόμενο στόχο; Υπάρχουν λιγότερο επεμβατικές

[14] Αρ. 8 παρ. 2 της ΕΣΔΑ ''Δεν επιτρέπεται να υπάρξη επέμβασις δημοσίας αρχής εν τη ασκήσει του δικαιώματος τούτου, εκτός εάν η επέμβασις αύτη προβλέπεται υπό του νόμου και αποτελεί μέτρον το οποίον, εις μίαν δημοκρατικήν κοινωνίαν, είναι αναγκαίον δια την εθνικήν ασφάλειαν, την δημοσίαν ασφάλειαν, την οικονομικήν ευημερίαν της χώρας, την προάσπισιν της τάξεως και την πρόληψιν ποινικών παραβάσεων, την προστασίαν της υγείας ή της ηθικής, ή την προστασίαν των δικαιωμάτων και ελευθεριών άλλων.''

εναλλακτικές; Υπάρχει ένας καλός «αναλογικός» λόγος για την αποστολή λεπτομερών δεδομένων μέτρησης έξω από το σπίτι του καταναλωτή; Η απάντηση σε αυτές τις ερωτήσεις εξαρτάται από τις λειτουργίες που επιλέγουν οι φορείς εκμετάλλευσης έξυπνων δικτύων. Η επιβολή ενός συστήματος, το οποίο υποτίθεται ότι υποστηρίζει το συμφέρον του καταναλωτή, ενώ σε αυτό ενσωματώνονται λειτουργίες που δεν μπορούν να ελεγχθούν από τον καταναλωτή και εξυπηρετούν συμφέροντα τρίτων μερών, αποτελεί μια ευθεία αμφισβήτηση του δικαιώματος της ιδιωτικής ζωής[66].

4.5. Η ΙΔΙΩΤΙΚΟΤΗΤΑ ΤΗΣ ΤΟΠΟΘΕΣΙΑΣ ΣΤΗΝ ΕΞΥΠΝΗ ΠΟΛΗ

Ενώ παλαιότερα η παρακολούθηση ήταν μια χρονοβόρα διαδικασία, που απαιτούσε τη σπατάλη αρκετών ωρών και δεν διευκόλυνε την καταγραφή και το συσχετισμό των αποτελεσμάτων της, σήμερα αντιθέτως, μια σειρά έξυπνων τεχνολογιών έχει μετατρέψει την παρακολούθηση γεωγραφικής τοποθεσίας σε μια διάχυτη, συνεχή, αυτόματη και σχετικά φθηνή διαδικασία που επιτρέπει την επεξεργασία και αποθήκευση δεδομένων και τη δημιουργία προφίλ κινήσεων των ανθρώπων [67]. Η τοποθεσία είναι ένα κρίσιμο και συχνά κεντρικό στοιχείο στην έννοια έννοιες του απανταχού υπολογίζειν[68]. Η παραβίαση του απορρήτου της τοποθεσίας ανέκαθεν προκαλούσε στο άτομο μια αίσθηση ανησυχίας, η οποία πήγαζε από την υποψία παρακολούθησής του, ωστόσο η αίσθηση αυτή έχει σήμερα πολλαπλασιαστεί, καθώς οι πληροφορίες τοποθεσίας είναι διάχυτες και συνεχώς διαθέσιμες. Τώρα που η τεχνολογία έχει αλλάξει ριζικά τη διαθεσιμότητα πληροφοριών, το απόρρητο της τοποθεσίας είναι στενά συνδεδεμένο με τον έλεγχο της πρόσβασης σε αυτές τις πληροφορίες και οι άνθρωποι θέλουν να έχουν τον έλεγχο της διαθεσιμότητας των πληροφοριών[69]. Αν και οι επιλογές ρύθμισης του απορρήτου της τοποθεσίας έχουν πλέον μελετηθεί αρκετά καλά στο πλαίσιο των κινητών συσκευών που φέρουν οι χρήστες, αυτές δεν έχουν επεκταθεί ιδιαίτερα στο πλαίσιο του IoT, όπου η επικοινωνία μεταξύ συσκευών μπορεί να μεταφέρει πληροφορίες τοποθεσίας δίχως την επίγνωση των χρηστών[68].

Πολύ συχνές είναι πλέον οι υπηρεσίες που βασίζονται στη δημόσια διαθεσιμότητα τεχνολογιών εντοπισμού τοποθεσίας και οι οποίες πρέπει να πληρούν τρία κριτήρια για το σκοπό αυτό: να ορίζουν τη θέση με υψηλή ακρίβεια, να μεταδίδουν την τρέχουσα

τοποθεσία σε έναν πάροχο υπηρεσιών και να το κάνουν σε πραγματικό χρόνο[62]. Από τις πιο δημοφιλείς ιδέες αυτών των υπηρεσιών είναι η διαφήμιση βάσει τοποθεσίας. Ένας προμηθευτής διαφημιστικών πινακίδων εξωτερικού χώρου, η εταιρία Clear Channel Outdoor ανακοίνωσε τη δημιουργία έξυπνων πινακίδων, χρησιμοποιώντας ένα πρόγραμμα που ονομάζεται Radar[137]. Αυτές οι διαφημιστικές πινακίδες μπορούν να εντοπίσουν τα κινητά τηλέφωνα των οδηγών και των επιβατών κοντά σε αυτές και στη συνέχεια να προσδιορίσουν εάν αυτά τα άτομα έχουν πρόσβαση στον ιστότοπο της εταιρείας για την οποία είχε τοποθετηθεί η διαφημιστική πινακίδα. Τέτοιου είδους υπηρεσίες όμως, προκαλούν ορισμένους προβληματισμούς, όπως κατά πόσο οι καταναλωτές είναι επαρκώς ενημερωμένοι όταν η διαδικτυακή τους συμπεριφορά παρακολουθείται, εάν έχουν τη δυνατότητα να δηλώσουν ρητά την εξαίρεσή τους ή τη συμμετοχή τους σε τέτοιες υπηρεσίες.

Λόγω της ποικιλίας και της αυξανόμενης διάδοσης των συνδεδεμένων συσκευών μέσω RFID ή Wi-Fi [62], ο προσδιορισμός θέσης φαίνεται να υπόκειται λιγότερο στον έλεγχο του χρήστη, ενώ οι ίδιοι, λόγω έλλειψης του τρόπου λειτουργίας και του αντικτύπου αυτής της τεχνολογίας φαίνεται να μην γνωρίζουν ότι τα συστήματα αυτά όχι μόνο παρέχουν πληροφορίες, αλλά επίσης είναι σε θέση να στέλνουν πληροφορίες και να λαμβάνουν απαντήσεις. Σε ορισμένες πόλεις έχει εγκατασταθεί ένα πλέγμα wifi, για την παροχή δημόσιου wifi, για τη δημιουργία ενός συστήματος απόκρισης έκτακτης ανάγκης και επικοινωνίας , για βοήθεια σε περίπτωση αστικής καταστροφής και για γενική επιτήρηση [67]. Στην περίπτωση του δημόσιου wifi, τα αναγνωριστικά των συσκευών που έχουν πρόσβαση στο δίκτυο καταγράφονται και μπορούν να εντοπιστούν μεταξύ σημείων του δικτύου wifi. Ένα τέτοιο δίκτυο, με 160 κόμβους, εγκαταστάθηκε από το αστυνομικό τμήμα του Σιάτλ το 2013. Το ιστορικό τοποθεσίας μέσω των προηγούμενων σημείων πρόσβασης Wi-Fi μπορούσε να αποκαλυφθεί επειδή μια συσκευή με δυνατότητα σύνδεσης σε Wi-Fi μεταδίδει το όνομα κάθε δικτύου στο οποίο έχει συνδεθεί προηγουμένως, προκειμένου να προσπαθήσει να βρει ένα για να συνδεθεί αυτόματα.

Οι πληροφορίες που αναφέρονται σε μια τοποθεσία, λόγω των σύγχρονων τεχνολογιών και της εξάπλωσης του IoT χαρακτηρίζονται από υψηλή ακρίβεια του προσδιορισμού της τοποθεσίας. Δυνατότητες ανίχνευσης, όπως το iBeacon της Apple μπορούν να ενεργοποιηθούν στα μοντέλα iPhone χωρίς πρόσθετο υλικό και να εντοπίσουν τους χρήστες συμβατών συσκευών μέσα σε μια στενή περίμετρο, χρησιμοποιώντας τεχνολογία

Bluetooth. Ομοίως, έξυπνες οικιακές συσκευές, εφόσον συνδεθούν σε δίκτυο Wi-Fi, είναι εφικτό να συναχθεί η τοποθεσία τους από τη θέση του σημείου ασύρματης πρόσβασης. Επιπλέον, η τοποθεσία των συσκευών, όπως τα smartphone με τα οποία αλληλεπιδρούν, μπορεί να είναι ενήμερη για την τοποθεσία αυτών και η σύνδεση μεταξύ τους μπορεί να αξιοποιηθεί σε εφαρμογές με επίγνωση τοποθεσίας[15]. Σε πολλές πόλεις, δίκτυα αισθητήρων έχουν αναπτυχθεί σε όλη την υποδομή των δρόμων, όπως σε κάδους και φανοστάτες για τη λήψη και παρακολούθηση αναγνωριστικών τηλεφώνου, όπως διευθύνσεις MAC. Στο Λονδίνο, η Renew εγκατέστησε τέτοιους αισθητήρες σε 200 κάδους, καταγράφοντας μέσα σε μία εβδομάδα το 2014 αναγνωριστικά από 4.009.676 συσκευές και παρακολουθώντας τα καθώς μετακινούνταν από κάδο σε κάδο [70]. Η εταιρεία ανέφερε ότι μπορούσαν να μετρήσουν την εγγύτητα, την ταχύτητα και τον κατασκευαστή των συσκευών, να παρακολουθήσουν τα καταστήματα που επισκέφτηκαν τα άτομα, να προσδιορίσουν το χρόνο που ξόδεψαν εκεί και το πόσο συχνοί πελάτες είναι, χρησιμοποιώντας αυτές τις πληροφορίες για να εμφανίσουν διαφημίσεις παρόμοιου περιεχομένου στις οθόνες που ήταν εγκατεστημένες στους κάδους.

Επίσης, η ταχύτητα [68] με την οποία παράγονται τα δεδομένα τοποθεσίας από τις συσκευές ποικίλλει σημαντικά ανάλογα με τον τύπο και την ακρίβεια των πληροφοριών που χρησιμοποιούνται, ακόμη και από σχετικά απλά συστήματα GPS αυτοκινήτου παρέχεται συνεχής ενημέρωση τοποθεσίας πολλές φορές ανά δευτερόλεπτο. Η παρακολούθηση της κίνησης είναι ένα παράδειγμα του τρόπου με τον οποίο μια ακολουθία τοποθεσίας μπορεί να οδηγήσει σε ροές πληροφοριών υψηλής ταχύτητας, όπως και οι μεταβαλλόμενες τοποθεσίες μπορούν επίσης να οδηγήσουν στην ενημέρωση των χαρτών και άλλων πληροφοριών στο τοπικό πλαίσιο.

Η κοινοποίηση των δεδομένων που αποκαλύπτουν την τοποθεσία των ατόμων δημιουργεί ορισμένους προβληματισμούς. Αποτελεί προσιτή διαδικασία η εκπαίδευση των χρηστών ώστε να γνωρίζουν πως να επιλέξουν αν θέλουν να αποκαλύψουν ή να μοιραστούν αυτήν την πληροφορία? Μπορούν επίσης να διαμορφώσουν οι ίδιοι την πολιτική απορρήτου για την τεχνολογία εντοπισμού θέσης, ειδικότερα στις συσκευές IoT, όπου δεν γίνεται ιδιαίτερα αντιληπτό ότι μεταξύ των δεδομένων που συλλέγονται περιλαμβάνονται και

[15] Για παράδειγμα, το iOS 8 και το HomeKit μπορούν να επωφεληθούν από το "geofencing" για να ρυθμίσουν έναν θερμοστάτη σε λειτουργία "home" όταν ένας ιδιοκτήτης σπιτιού βρίσκεται εντός μιας συγκεκριμένης περιμέτρου του σπιτιού και σε λειτουργία "μακριά" όταν βρίσκεται εκτός αυτής της περιμέτρου. Έτσι δημιουργείται μια αλυσίδα πολλών συνδέσμων, που μεταβιβάζουν πληροφορίες τοποθεσίας μεταξύ συσκευών, χρηστών και εφαρμογών.

στοιχεία της τοποθεσίας; Ποιες νομικές απαιτήσεις πρέπει να υπάρχουν σχετικά με τη διαδικασία συγχώνευσης πολλαπλών αναφορών θέσης, από διαφορετικές συσκευές προκειμένου να εξαχθούν λεπτομερή προφίλ κίνησης;

4.6 ΣΥΝΕΡΓΑΣΙΑ ΜΕΤΑΞΥ ΔΗΜΟΣΙΟΥ ΚΑΙ ΙΔΙΩΤΙΚΟΥ ΤΟΜΕΑ ΣΤΗΝ ΕΞΥΠΝΗ ΠΟΛΗ, ΑΠΕΙΛΗ ΓΙΑ ΤΗΝ ΙΔΙΩΤΙΚΟΤΗΤΑ?

Όπως έχει ήδη αναφερθεί στον πυρήνα της έξυπνης πόλης βρίσκεται η ενσωμάτωση των ΤΠΕ. Προκειμένου να επιτευχθεί η ψηφιοποίηση τόσο των καίριων υποδομών της ΕΠ, όπως είναι οι δημόσιες μεταφορές, η διανομή ενέργειας, η βελτίωση των περιβαλλοντικών συνθήκων καθώς και οι παρεχόμενες υπηρεσίες προς τους κατοίκους αυτής, είτε αυτές μπορούν να αφορούν για παράδειγμα την παροχή δεδομένων για την κυκλοφορία στους δρόμους, προκειμένου να καθορίσει ένα πρόσωπο τη διαδρομή που θα ακολουθήσει για να φτάσει στο χώρο εργασίας του, είτε προκειμένου ένας ηλικιωμένος να λάβει άμεση βοήθεια στην περίπτωση που χρειαστεί, απαιτούνται μεγάλου είδους επενδύσεις σε νέες τεχνολογίες και υποδομές. Αυτές οι επενδύσεις ωστόσο σημαίνουν και την καταβολή μεγάλων χρηματικών ποσών, και ειδικότερα τέτοιων επενδύσεων που ο οικονομικός προϋπολογισμός μιας πόλης πιθανόν να μην αντέχει. Την αδυναμία αυτή έρχονται να καλύψουν τεχνολογικές εταιρίες, πολλές φορές κολοσσοί στο είδος τους, προκειμένου να προσφέρουν στις πόλεις την ψηφιακή αναβάθμιση. Και κάπως έτσι δημιουργούνται συμπράξεις μεταξύ δημόσιου και ιδιωτικού τομέα, οι οποίες αποτελούν βασικό χαρακτηριστικό για να χαρακτηρισθεί μια πόλη ΄έξυπνη΄΄ και προϋπόθεση για την ανάπτυξη αυτών. Η ανάπτυξη του αστικού πληθυσμού, η οποία είναι δυσανάλογη της ανάπτυξης των αστικών υποδομών, σε συνδυασμό με τον υποχρηματοδοτούμενο προϋπολογισμό και το απαραίτητο μέλημα της βιωσιμότητας, καθιστούν τη συμμετοχή του ιδιωτικού τομέα ελκυστική επιλογή[71].

Δεδομένου ωστόσο ότι πρόκειται για ιδιωτικές εταιρίες, οι οποίες έχουν ως γνώμονα το εμπορικό κέρδος, δημιουργούνται προβληματισμοί σχετικά με το βαθμό και την έκταση επέμβασης αυτών των εταιριών αυτών στη λειτουργία μιας ΕΠ.

Μία από τις πρώτες πρωτοβουλίες για έξυπνες πόλεις εμφανίστηκε από πολυεθνική εταιρεία τεχνολογίας, την IBM, η οποία έκανε ιδιαίτερα δημοφιλή τον όρο «έξυπνη πόλη» και τον χρησιμοποίησε ως μια προσεκτική επένδυση για να αντιμετωπίσει την ύφεση του

2008 [71]. Η πρωτοβουλία αυτής «Εξυπνότερες Πόλεις» δημιούργησε μια αγορά νέων τεχνολογιών και συμβουλευτικών υπηρεσιών που απευθύνονται ειδικά στις τοπικές διοικήσεις πόλεων, όπως το «IBM Intelligent Operations Center». Παράδειγμα αυτού αποτελεί το Επιχειρησιακό Κέντρο του Ρίο, ένα δωμάτιο ελέγχου, όπου οι υπάλληλοι της πόλης έχουν πρόσβαση σε πλάνα από κλειστό κύκλωμα CCTV και σε χάρτες που δημιουργούνται από τα δεδομένα που συλλέγονται μέσα στην πόλη, καθώς και από πολλαπλούς αισθητήρες που είναι τοποθετημένοι στο οδικό δίκτυο[16] [73].

Οι συμπράξεις δημοσίου και ιδιωτικού τομέα σε μια πρώτη ανάγνωση φαίνονται ιδιαίτερα θετικές για τη δημιουργία και προώθηση καινοτόμων υπηρεσιών από τις ΕΠ προς τους κατοίκους της και για την ενίσχυση της βιωσιμότητας αυτών, η οποία τίθεται σε κίνδυνο από διάφορους παράγοντες. Οι διάφορες τεχνολογίες που χρησιμοποιούνται για την επίτευξη των ανωτέρω στόχων, όπως η χρήση της επιστήμης δεδομένων, των μεγάλων δεδομένων και της προγνωστικής ανάλυσης για ρύθμιση και τη διακυβέρνηση των πόλεων, σπάνια αποτελούν αποτέλεσμα παραγωγής της δημόσιας διοίκησης, αλλά προϊόν ιδιωτικών εταιρειών όπως η IBM, η Google και η Cisco [74]. Αυτές οι εταιρείες παρέχουν στις πόλεις τεχνολογίες που τους επιτρέπουν να συλλέγουν όσο το δυνατόν περισσότερα δεδομένα προκειμένου να εντοπίζουν, να κατανοούν και να λύνουν καλύτερα τα κοινωνικά προβλήματα. Οι συνέπειες αυτής της ιδιωτικοποίησης μέσω της τεχνολογίας στις δημόσιες αξίες εμφαίνονται κυρίως σε δύο επίπεδα [74]: Πρώτον, οι ιδιωτικοί φορείς παρέχουν τεχνολογία μέσω της οποίας μπορούν να συλλεχθούν και να αναλυθούν δεδομένα πολιτών. Δεύτερον, η ιδιωτική τεχνολογία αναδιαμορφώνει το περιεχόμενο, το είδος των υπηρεσιών και την πρόσβαση των πολιτών σε αυτές. Και στις δύο περιπτώσεις, οι ιδιωτικές πρωτοβουλίες και η τεχνολογία επανασχεδιάζουν τη σχέση μεταξύ πολιτών και δημοσίων φορέων.

Στην ιστοσελίδα www.extremetech.com, σε άρθρο του έτους 2012, αναφέρεται ότι στο άμεσο μέλλον οποιαδήποτε υποδομή της πόλης θα είναι συνδεδεμένη στο διαδίκτυο, προτρέποντας στο να φανταστεί ο αναγνώστης τι δυνατότητες δημιουργούνται από το

[16] Αντίστοιχα επιχειρησιακά κέντρα υπάρχουν και σε άλλες πόλεις, κατασκευασμένα από άλλες εταιρίες, όπως το Smart City Lounge στην Τζακάρτα, J''akarta Smart City Lounge opens doors to public," The Jakarta Post, 11 January 2016, http://www.thejakartapost.com/news/2016/01/11/jakarta-smart-city-lounge-opens-doors-public.html

Άλλα παραδείγματα εταιρειών περιλαμβάνουν το «City Intelligence Platform» της Siemens, το «Future» της Nokia X», το «Smart City Solution» της Huawei, το «CityNext» της Microsoft και το «Internet of Everything» της Cisco.

συνδυασμό όλων των δεδομένων που συλλέγονται από κάθε γωνιά της πόλης. Εύστοχα λοιπόν στο εν λόγω άρθρο ο τίτλος του έχει ως εξής *«Το Διαδίκτυο των πραγμάτων και οι έξυπνες πόλεις: ένας υπολογιστής IBM θα είναι ο επόμενος δήμαρχος σας;».*

Η διαπίστωση αυτή δηλώνει μια άμεση ή έμμεση μορφή ιδιωτικοποίησης μέσω της τεχνολογίας που δημιουργεί περίπλοκα προβλήματα διαφάνειας και λογοδοσίας. Η έλλειψη διαφάνειας επηρεάζει άλλους μακροχρόνιους νομικούς θεσμούς και δικαιώματα των πολιτών, όπως η δίκαιη διαδικασία, η ελευθερία ενημέρωσης, η απαγόρευση διάκρισης και η αμερόληπτη δικαιοσύνη [74].

Περαιτέρω, υποτίθεται ότι σε μια πόλη, οι δημόσιοι φορείς ενεργούν ακολουθώντας μακροπρόθεσμους στόχους και λιγότερο οικονομικά αποτελέσματα, όπως προσιτές, δίκαιες και βιώσιμες δημόσιες υπηρεσίες, ενώ οι ιδιωτικοί φορείς, από την άλλη πλευρά, εξυπηρετούν εμπορικά συμφέροντα που επικεντρώνονται σε βραχυπρόθεσμα αποτελέσματα, οικονομικά οφέλη και διαχείριση περιουσιακών στοιχείων με γνώμονα το κέρδος [71]. Στην περίπτωση κατά την οποία η διοίκηση μιας πόλης, είτε δεν είναι σε θέση να παρακολουθήσει και να επανεξετάσει τις δραστηριότητες και τις επιδόσεις που αναλαμβάνει να εκτελέσει ένας ιδιωτικός φορέας, είτε δεν μπορεί να διατηρήσει την πρόσβαση σε πληροφορίες, είτε δεν διαθέτει επαρκή τεχνογνωσία για να ελέγξει τη δράση των ιδιωτικών φορέων, είναι πολύ πιθανό να καμφθούν οι μηχανισμοί διαφάνειας ως προς τη δράση των τρίτων μερών [71]. Οι ιδιωτικοί φορείς πρέπει να είναι σε θέση να λογοδοτούν για τον τρόπο με τον οποίο λειτουργούν και επεμβαίνουν, στο βαθμό που τους έχει επιτραπεί, στο σχεδιασμό των προϊόντων που παρέχουν στις έξυπνες πόλεις. Χαρακτηριστικό παράδειγμα αυτού, αποτελεί η χρήση ιδιόκτητων αλγορίθμων που προστατεύονται από το επιχειρηματικό απόρρητο, η οποία παρεμποδίζει έντονα την ανάγκη για διαφάνεια και, επομένως, τη δυνατότητα να λογοδοτούν οι ιδιώτες εταίροι για την τεχνολογία τους.

Ένα ακόμη γεγονός στο οποίο πρέπει να δοθεί ιδιαίτερη προσοχή, είναι η περαιτέρω αύξηση της ανισότητας και των διακρίσεων που μπορεί να επιφέρει η στενή εμπλοκή του ιδιωτικού τομέα στις δραστηριότητες της πόλης. Χαρακτηριστικό και ταυτόχρονα ακραίο παράδειγμα αποτελεί η πόλη Gurgaon στην Ινδία [75], μια πόλη 32 χιλιόμετρα έξω από το Νέο Δελχί, η οποία αναδύθηκε από μια πρώην αγροτική περιοχή, της οποίας τα κτίρια και όλες οι δομές δεν χτίστηκαν από κρατικές δράσεις, αλλά σχεδόν εξ ολοκλήρου από ιδιωτικές εταιρείες. Οι εταιρείες δημιούργησαν μια πόλη που ταιριάζει στις ανάγκες τους.

Μεγάλες πολυεθνικές εταιρείες, συμπεριλαμβανομένων των εταιριών Google, HSBC, Nokia και Intel, διαθέτουν γραφεία εκεί, ενώ νεοφυείς επιχειρήσεις θέλουν να μεταφέρουν την έδρα τους στο Gurgaon, ώστε να μπορούν να βρίσκονται κοντά στο τεράστιο δίκτυο εταιρειών. Παρά ταύτα, πρόκειται για μια πόλη στην οποία κυριαρχεί η ανισότητα, αν λάβει κανείς υπόψη τις δύο κατηγορίες κατοίκων που υπάρχουν σε αυτή, αφενός οι μορφωμένοι και οι ευκατάστατοι που εργάζονται σε μεγάλες εταιρίες και αφετέρου οι αρχικοί κάτοικοι αυτής, οι οποίοι μετατοπίστηκαν στα κοντινά και υποβαθμισμένα προάστια, και οι οποίοι ζουν στα όρια της ανέχειας[17].

Περαιτέρω, η διάδοση των τεχνολογιών επιτήρησης και η ανάπτυξη των τεχνολογικών εταιρειών που δουλεύουν πάνω σε αυτές και τις εξελίσσουν έχουν προσφέρει στις κυβερνήσεις μια πληθώρα ευκαιριών ώστε να συνεργάζονται, με ιδιωτικούς φορείς. Η εξωτερική ανάθεση εποπτείας συχνά επιδιώκει να επιδεινώσει τις ήδη περιττές επεμβάσεις των κυβερνήσεων στην καθημερινή μας ζωή και να υπονομεύσει τις θεμελιώδεις ελευθερίες μας, θολώνοντας τα όρια μεταξύ ιδιωτικών και δημόσιων χώρων και ομαλοποιώντας την επιτήρηση [77]. Σύγχρονο παράδειγμα αποτελεί το Ring bell της Amazon, μία έξυπνη συσκευή που επιτρέπει στους χρήστες του Ring να βλέπουν, να συνομιλούν και να καταγράφουν τα άτομα που φτάνουν στην είσοδο του σπιτιού τους. Η σχετική εφαρμογή Neighbors επιτρέπει στους χρήστες να μοιράζονται τις υποψίες τους για υποτιθέμενη εγκληματική δραστηριότητα έως και 5 μίλια γύρω από το σπίτι τους. Οι αναρτήσεις στην πλατφόρμα μπορούν να εμπίπτουν σε μία από τις πέντε κατηγορίες: Ασφάλεια, Έγκλημα, Απώλεια κατοικίδιου ζώου, Ύποπτος και Άγνωστος Επισκέπτης [78]. Η αστυνομία έχει πρόσβαση σε μια πλατφόρμα που έχει δημιουργηθεί με την ονομασία “Law Enforcement Neighbourhoods Portal” [78], η οποία δείχνει πού υφίστανται κάμερες Ring σε μια δεδομένη τοποθεσία και επιτρέπει στις αρχές να αλληλεπιδρούν απευθείας με τους ιδιοκτήτες των καμερών Ring bell και να ζητούν ανεπίσημα πλάνα για έρευνες, χωρίς ένταλμα. Εάν οι χρήστες αρνηθούν να μοιραστούν το υλικό τους, η αστυνομία μπορεί να το πάρει από την Amazon μέσω κλήτευσης. Εν τω μεταξύ, η Ring προσφέρει εκπαίδευση

17 Κάτι παρόμοιο, όχι τόσο ακραίο, έχει συμβεί στο Ρίο της Βραζιλίας. Η τεχνολογία έξυπνης πόλης – συμπεριλαμβανομένου του δικτύου κυκλοφορίας CCTV – είναι συγκεντρωμένη στις πλουσιότερες περιοχές της πόλης. Κατά συνέπεια, οι διαχειριστές πόλεων παρεμβαίνουν περισσότερο στις πλουσιότερες περιοχές – από όπου λαμβάνουν δεδομένα– παρά στις λιγότερο ανεπτυγμένες, επιδεινώνοντας έτσι τις ήδη υπάρχουσες ανισότητες. Smarter than Smart: Rio de Janeiro's Flawed Emergence as a Smart City,” Christopher Gaffney and Cerianne Robertson, 29 April 2016, available at: http://www.tandfonline.com/doi/abs/10.1080/10630732.2015.1102423?journalCode=cjut20

στην αστυνομία σχετικά με το πώς να λαμβάνει αποτελεσματικά τη συγκατάθεση των χρηστών του Ring όταν ζητούν το βίντεο τους.

Από τα παραπάνω παραδείγματα προκύπτει ότι ιδιωτικές εταιρίες που δημιουργούν και διαχειρίζονται αυτές τις τεχνολογίες διαθέτουν μια τεράστια ποσότητα εξαιρετικά λεπτομερών δεδομένων σχετικά με την τοποθεσία και τις κινήσεις των προσώπων στο φυσικό χώρο, από τα οποία μπορούν να συναχθούν πολλές άλλες πληροφορίες (όπως ο τρόπος μετακίνησης, οι δραστηριότητες ή ακόμα και ο τρόπος ζωής), στις οποίες μπορεί να αποκτήσουν πρόσβαση οι αρχές επιβολής του νόμου ή τρίτοι συνεργάτες για εμπορικούς σκοπούς. Η κύρια συνέπεια είναι ότι τα άτομα ''δεν χάνονται πλέον στο πλήθος'', αλλά πολύ περισσότερο παρακολουθούνται και ανιχνεύονται με βάση πληροφορίες που φανερώνουν το χώρο στον οποίο βρίσκονται οποιαδήποτε στιγμή, παράλληλα δε, εκτίθενται σε γεωγραφικά στοχευμένα προφίλ για διαφήμιση και κοινωνική ταξινόμηση[67].

4.7 ΠΕΡΑΙΤΕΡΩ ΠΡΟΒΛΗΜΑΤΙΣΜΟΙ

Τα δεδομένα μιας ΕΠ συλλέγονται, αποθηκεύονται, παρακολουθούνται, μοιράζονται και πωλούνται από υπηρεσίες μέσων κοινωνικής δικτύωσης, άλλες διαδικτυακές πλατφόρμες, μεσίτες δεδομένων, υπηρεσίες πληροφοριών και από τη δημόσια διοίκηση. Η απεριόριστη συλλογή δεδομένων, η οποία καθίσταται εφικτή από τον τεράστιο αριθμό των συνδεδεμένων συσκευών IoT στην έξυπνη πόλη, οδηγεί στη δημιουργία συνόλου δεδομένων, τα οποία μπορούν να διαμοιραστούν και να συνδυαστούν με άλλα σύνολα δεδομένων για την εξαγωγή πρόσθετων πληροφοριών [67]. Όπως αναφέρει ο Kitchin [67], η αδιάκοπη συγκέντρωση και επεξεργασία συνόλου δεδομένων, μπορεί να επιφέρει τις εξής συνέπειες όσον αφορά το απόρρητο: Πρώτον, οι άνθρωποι υπόκεινται πλέον σε πολύ μεγαλύτερα επίπεδα εντατικού ελέγχου και επιτήρησης από ποτέ άλλοτε, με τις τεχνολογίες των έξυπνων πόλεων να αναδεικνύουν πτυχές της ατομικής ζωής, ειδικά όταν συνδυάζονται με άλλα σύνολα δεδομένων. Δεύτερον, η διάχυση των ψηφιακών συναλλαγών και η επιτήρηση, καθώς και η αυξανόμενη χρήση μοναδικών αναγνωριστικών για πρόσβαση σε υπηρεσίες (π.χ. ονόματα χρήστη, κωδικοί πρόσβασης, αριθμοί λογαριασμών, διευθύνσεις, email, στοιχεία τηλεφώνου, αριθμοί πιστωτικών καρτών, αναγνωριστικό έξυπνης κάρτας, πινακίδες κυκλοφορίας), σημαίνει ότι είναι εντελώς

αδύνατο να διάγει κάποιος την καθημερινή του ζωή χωρίς να αφήσει ψηφιακά αποτυπώματα. Τρίτον, η μαζική καταγραφή, οργάνωση, αποθήκευση και κοινή χρήση μεγάλων δεδομένων για ένα φαινόμενο αλλάζει τις χρήσεις για τις οποίες μπορούν να χρησιμοποιηθούν αυτά τα δεδομένα. Τέταρτον, η επεξεργασία αυτών των δεδομένων επιτρέπει την εξαγωγή συμπερασμάτων, για τα οποία δεν υπήρχε αρχικώς πρόβλεψη να αποκαλυφθούν.

Μια ακόμη αρνητική συνέπεια της αδιάκοπης συλλογής δεδομένων που αφορούν τους κατοίκους μιας πόλης είναι το κοινώς λεγόμενο ''chilling effect''. Ενώ πολλές πόλεις διαθέτουν ήδη κάμερες παρακολούθησης σε κυκλοφοριακές διασταυρώσεις και κοινόχρηστους χώρους, σε πιο καινοτόμα έργα πόλης, στα στοιχεία που καταγράφει μια κάμερα προστίθενται δεδομένα από δελτία καιρού, από συσκευές αναγνώρισης πινακίδων αυτοκινήτων, μικρόφωνα ανίχνευσης πυροβολισμών και λογισμικό αναγνώρισης προσώπου [79]. Σε άλλες περιπτώσεις, στις πόλεις έχουν εγκατασταθεί αισθητήρες κάτω από δρόμους για να παρακολουθούν πώς οι άνθρωποι πλοηγούνται και αλληλεπιδρούν με ορισμένα σημεία αυτής, καθώς και συστήματα για το φωτισμό των δρόμων με ενσωματωμένους αισθητήρες κίνησης και κάμερες που εντοπίζουν πεζούς και σβήνουν όταν δεν είναι κανείς τριγύρω [79] . Αυτοί οι μη παρεμβατικοί αισθητήρες δόνησης μπορούν να παρακολουθούν τα βήματα για να ανιχνεύουν μεμονωμένους ενοίκους σε δημόσιους χώρους και να αναλύουν τα μοτίβα βάδισης για να λάβουν πληροφορίες για την υγεία των πεζών. Με τον τεράστιο όγκο δεδομένων να συλλέγονται από νέους αισθητήρες, μια μη εξουσιοδοτημένη ή χωρίς εχέγγυα πρόσβαση σε δεδομένα έξυπνων πόλεων τόσο από τις αρμόδιες διοικητικές αρχές όσο και από τους ιδιωτικούς φορείς μπορεί να έχουν έως επικίνδυνα αποτελέσματα για την ελευθερία του λόγου, της κίνησης και του συνεταιρίζεσθαι, προκαλώντας έτσι το κοινώς λεγόμενο chilling effect στους κατοίκους αυτής. Ακόμη κι αν εκ πρώτης όψεως η συλλογή των δεδομένων με τη χρήση τέτοιων αισθητήρων θα μπορούσε να φανεί αποτελεσματική, για τη μείωση της εγκληματικότητας ή την αύξηση της αποτελεσματικότητας των λειτουργιών μιας ΕΠ, αυτές οι πληροφορίες μπορούν να χρησιμοποιηθούν για τη δημιουργία βάσεων δεδομένων στις οποίες θα συμπεριλαμβάνονται οι δραστηριότητες των ατόμων, με ενδεχόμενο να αποκαλυφθούν ευαίσθητες πληροφορίες για τις διαπροσωπικές σχέσεις ενός προσώπου, τις αξίες του,

ακόμη και την κατάσταση της υγείας του[18]. Έτσι όμως υπάρχει ο κίνδυνος οι κάτοικοι μιας πόλης να προσαρμόζουν και να παρακολουθούν τη συμπεριφορά τους υπό το φόβο της απομόνωσης ή της πρόκλησης υποψιών[19].

5. ΟΙ ''ΥΠΟΣΤΗΡΙΚΤΕΣ'' ΤΗΣ ΕΞΥΠΝΗΣ ΠΟΛΗΣ: BIG DATA, ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΚΑΙ ΑΝΟΙΧΤΑ ΔΕΔΟΜΕΝΑ (OPEN DATA)

5.1 Η ΕΦΑΡΜΟΓΗ ΤΩΝ BIG DATA ΣΤΟ ΠΛΑΙΣΙΟ ΤΗΣ ΕΞΥΠΝΗ ΠΟΛΗΣ

Τα μεγάλα δεδομένα είναι ένας όρος που χρησιμοποιείται για να χαρακτηρίσει πολύ μεγάλα σύνολα δεδομένων που έχουν πολύπλοκη δομή και συνήθως συσχετίζονται με πρόσθετες δυσκολίες στην ανάλυση και εφαρμογή περαιτέρω διαδικασιών ή εξαγωγής αποτελεσμάτων. Η ανάλυση μεγάλων δεδομένων είναι ο όρος που χρησιμοποιείται για να περιγράψει τη διαδικασία έρευνας τεράστιων ποσοτήτων σύνθετων δεδομένων προκειμένου να αποκαλυφθούν κρυφά μοτίβα και συσχετισμοί [104].

Τα βασικότερα χαρακτηριστικά των Big Data (γνωστά και ως Vs) είναι τα εξής [105]:

1. ο όγκος: αναφέρεται στο μέγεθος των δεδομένων που έχουν δημιουργηθεί από όλες τις πηγές.
2. η ταχύτητα: αναφέρεται στην ταχύτητα με την οποία παράγονται, αποθηκεύονται, αναλύονται και επεξεργάζονται τα δεδομένα, ενώ δίνεται και έμφαση στην υποστήριξη της ανάλυσης μεγάλων δεδομένων σε πραγματικό χρόνο.
3. η ποικιλία: αναφέρεται στους διαφορετικούς τύπους δεδομένων που παράγονται. Τα περισσότερα δεδομένα είναι αδόμητα και δεν μπορούν εύκολα να κατηγοριοποιηθούν ή να ταξινομηθούν.
4. η μεταβλητότητα: αναφέρεται στον τρόπο με τον οποίο η δομή και η σημασία των δεδομένων αλλάζει συνεχώς.
5. η αξία: αναφέρεται στο πλεονέκτημα που μπορεί να προσφέρουν τα μεγάλα δεδομένα σε έναν οργανισμό, με βάση τη χρηστή συλλογή, διαχείριση και ανάλυση αυτών.

[18] Smart Cities: Utopian Vision, Dystopian Reality, 2017, οπ.π.
[19] οπ.π.

Το Διαδίκτυο των Πραγμάτων (IoT), με το οποίο επιτυγχάνεται η σύνδεση όλων των πραγμάτων για τα οποία ενδιαφέρονται οι άνθρωποι στον κόσμο και το οποίο αποτελεί ίσως το σπουδαιότερο εργαλείο για την ανάπτυξη της έξυπνης πόλης, προσθέτει στην παραγωγή πολύ περισσότερων δεδομένων και θεωρείται μια από τις κύριες κινητήριες δυνάμεις για την ανάλυση μεγάλων δεδομένων.

Μια ιδέα που φέρνει σε επαφή τα μεγάλα δεδομένα και τις έξυπνες συσκευές είναι η έννοια της «έξυπνης πόλης». Οι υπηρεσίες που θα μπορούσαν να βελτιωθούν σε έξυπνες πόλεις, συνήθως από συστήματα που βασίζονται σε δεδομένα, περιλαμβάνουν τη διαχείριση των μεταφορών και της κυκλοφορίας, την ενέργεια, την υγειονομική περίθαλψη, τη διαχείριση νερού ή απορριμμάτων, αλλά και την επιβολή του νόμου [106].

Μέσα από το φακό των Big Data, οι έξυπνες συσκευές ξεχωρίζουν για την ικανότητά τους να επεκτείνουν περαιτέρω τις πρακτικές εξόρυξης δεδομένων. Η παραγωγή δεδομένων από έξυπνες συσκευές μπορεί να ποικίλλει αρκετά, ενώ η διάχυτη και εκτεταμένη τακτική παραγωγή δεδομένων έξυπνων συσκευών ενδέχεται να μην είναι πλήρως αντιληπτή από τα άτομα που μπορεί να αγνοούν την παρουσία αισθητήρων (που συχνά είναι χαμηλού κόστους και μικροσκοπικά) και το πλήρες φάσμα των δεδομένων που παράγουν, καθώς και διαδικασίες επεξεργασίας δεδομένων που επεξεργάζονται αυτά τα διαφορετικά δεδομένα. [106].

5.2 ΠΡΟΚΛΗΣΕΙΣ ΣΤΗΝ ΕΦΑΡΜΟΓΗ ΤΩΝ ΜΕΓΑΛΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΗΝ ΕΞΥΠΝΗ ΠΟΛΗ

Στο [107] περιγράφονται μερικές προκλήσεις που αντιμετωπίζουν ο σχεδιασμός, και η ανάπτυξη εφαρμογών μεγάλων δεδομένων στις έξυπνες πόλεις, οι οποίες από τη φύση τους θεωρούνται πολύ δυναμικά και εξελισσόμενα περιβάλλοντα. Οι βασικότερες εξ΄αυτών είναι οι εξής:

Πηγές και χαρακτηριστικά δεδομένων: Τα δεδομένα παράγονται από πολλές διαφορετικές πηγές σε πολλές διαφορετικές μορφές, (π.χ. εικόνες, ήχος, tweets, βίντεο, αρχεία καταγραφής διακομιστή κ.λπ.), τα οποία ωστόσο πρέπει να ταξινομούνται σε δομημένη μορφή χρησιμοποιώντας κάποια μορφή προηγμένων συστημάτων βάσεων δεδομένων. Τα δεδομένα μπορούν να προέρχονται από όλους

τους ενδιαφερόμενους φορείς μιας Έξυπνης Πόλης όπως την κοινωνία που εκπροσωπείται από πολίτες και επιχειρήσεις και τις κυβερνήσεις που εκπροσωπούνται από φορείς χάραξης πολιτικής και διοικήσεις. Από τη μια πλευρά, οι πηγές δεδομένων μπορεί να περιλαμβάνουν παραδοσιακές πληροφορίες που κατέχονται από δημόσιους φορείς συμπεριλαμβανομένων ανώνυμων δεδομένων καθώς και προσωπικά δεδομένα, π.χ. από δημόσια μητρώα, εσωτερικά έσοδα, υγειονομική περίθαλψη, κοινωνικές υπηρεσίες κ.λπ. [108]. Από την άλλη πλευρά, οι ίδιοι οι πολίτες δημιουργούν μια συνεχή ροή δεδομένων μέσα και για τις πόλεις χρησιμοποιώντας τα smartphone τους, μέσων κοινωνικής δικτύωσης ή εφαρμογές που παρέχονται από τη διοίκηση της πόλης, αφήνουν ψηφιακά ίχνη που σχετίζονται με τις δραστηριότητές τους στη φυσική πόλη και δημιουργούν με αυτόν τον τρόπο πολύτιμες πληροφορίες [108].

Κοινή χρήση δεδομένων και πληροφοριών: Η κοινή χρήση δεδομένων και πληροφοριών μεταξύ διαφορετικών τμημάτων της πόλης είναι μια άλλη πρόκληση. Κάθε κρατική και δημοτική υπηρεσία έχει συνήθως τη δική της βάση δεδομένων με εμπιστευτικές ή δημόσιες πληροφορίες, τις περισσότερες από τις οποίες συχνά διστάζουν να μοιραστούν, ειδικά στην περίπτωση που πρόκειται για ειδικές κατηγορίες δεδομένων, οι οποίες διέπονται από ορισμένες προϋποθέσεις απορρήτου. Η πρόκληση εδώ είναι να διασφαλίσουμε ότι δεν θα ξεπεράσουμε τη λεπτή γραμμή μεταξύ της συλλογής και της χρήσης μεγάλων δεδομένων και της διασφάλισης των δικαιωμάτων ιδιωτικής ζωής των πολιτών. Αυτό ισχύει σε κάθε έξυπνη πόλη, καθώς εμπλέκονται πολλοί τομείς και βιομηχανίες έξυπνων πόλεων και θα πρέπει να βρουν τρόπους για να αποτρέψουν ή να μειώσουν τα εμπόδια για να επιτύχουν απρόσκοπτη ανταλλαγή και ανταλλαγή πληροφοριών μεταξύ διαφορετικών οντοτήτων. Επιπλέον, αν λάβει κανείς υπόψη και τις διαφορετικές πηγές δεδομένων, ορισμένοι τύποι δεδομένων όπως τα χωροχρονικά δεδομένα ανανεώνονται ιδιαίτερα γρήγορα . Ως εκ τούτου, είναι δύσκολο να δημιουργηθεί μια ενοποιημένη κατανόηση της σημασιολογίας δεδομένων και να εξαχθεί νέα γνώση με βάση συγκεκριμένα δεδομένα σε πραγματικό χρόνο.

Ενοποίηση δεδομένων: Τα δεδομένα έξυπνης πόλης περιλαμβάνουν διάφορες μορφές δεδομένων χρησιμοποιώντας μια μεγάλη ποικιλία έξυπνων αντικειμένων που είναι ενσωματωμένα σε όλη την πόλη. Ωστόσο, το όραμα της έξυπνης πόλης είναι να ενσωματώσει τόσο μεγάλο όγκο δεδομένων από πολλαπλές πηγές. Η ενοποίηση δεδομένων εντός της έξυπνης πόλης είναι μία από τις σημαντικές προκλήσεις που πρέπει να αντιμετωπιστούν. Τα τελευταία χρόνια, πολλές τεχνολογίες έχουν ενσωματωθεί σε έξυπνες πόλεις, οι οποίες μειώνουν τα τεχνικά εμπόδια στην αντιμετώπιση των δεδομένων. Ωστόσο, η ποιότητα των δεδομένων είναι ένα από τα απαιτητικά προβλήματα σε κάθε μηχανισμό ενοποίησης δεδομένων, ειδικά εάν τα δεδομένα είναι λανθασμένα ή ελλιπή [109].

Ποιότητα δεδομένων: Εξετάζοντας τις πιο θεμελιώδεις πτυχές των μεγάλων δεδομένων, υπάρχουν ορισμένες προκλήσεις που σχετίζονται με την ποιότητα των δεδομένων. Η ποιότητα των δεδομένων είναι ένα βασικό ζήτημα για οργανισμούς, όπως οι έξυπνες πόλεις, που χρησιμοποιούν αναλυτικά στοιχεία μεγάλων δεδομένων. Αυτό συνδέεται με αυτό που συχνά θεωρείται ως το «τέταρτο V», των Big Data, δηλαδή την ακρίβεια, ή με άλλα λόγια την αξιοπιστία των δεδομένων. Τα ανώτερα στελέχη σε οργανισμούς μεγάλων δεδομένων πρέπει να γνωρίζουν εάν μπορούν να εμπιστεύονται αυτό που προφανώς τους λένε τα δεδομένα. Αυτό μπορεί να περιλαμβάνει την εξέταση, για παράδειγμα, των πηγών των δεδομένων, πόσο ακριβή είναι, εάν είναι επαρκώς ενημερωμένα, πόσο ασφαλή διατηρούνται και εάν υπάρχουν περιορισμοί στον τρόπο χρήσης τους [110]. Η στήριξη σε πλήθος προμηθειών και η συνεργασία πολλών παρόχων θα έχει ως αποτέλεσμα δεδομένα που υποφέρουν από έλλειψη δομής και, κατά συνέπεια, προβλήματα συνέπειας, ετερογένειας και ανισότητας θα έχουν περισσότερες πιθανότητες να εμφανιστούν. Αυτό θα προκαλέσει περισσότερες προκλήσεις όπως η αβεβαιότητα και η αξιοπιστία των δεδομένων. Για παράδειγμα, δεδομένα αισθητήρων που συλλέγονται μέσω τρίτου μέρους χωρίς κεντρικό έλεγχο θα μπορούσαν να έχουν παραχθεί από αισθητήρες που είναι ελαττωματικοί, λανθασμένα βαθμονομημένοι ή πέραν της διάρκειας ζωής τους. Ως εκ τούτου, η συνεχής ενημέρωση των πολιτικών συλλογής και χρήσης δεδομένων, η κοινή χρήση και η συζήτησή τους μεταξύ όλων των οντοτήτων σε μια έξυπνη πόλη, η διασφάλιση ότι οι πολίτες κατανοούν και

εφαρμόζουν σωστά τις πολιτικές είναι ζωτικής σημασίας και ταυτόχρονα αποτελεί πρόκληση. Περαιτέρω, η κατανεμημένη και αυτόνομη υποδομή πληροφοριών που προσδιορίζει τις έξυπνες πόλεις επηρεάζει επίσης την ποιότητα των δεδομένων. Τα δεδομένα σε πραγματικό χρόνο που παράγονται σε αυτήν την υποδομή μπορεί να περιέχουν κάθε είδους ατέλειες, όπως ανακρίβεια, αβεβαιότητα, άγνοια, ασάφεια [111]. Οποιαδήποτε ατέλεια στα δεδομένα εντός της έξυπνης πόλης μπορεί να έχει αρνητικές επιπτώσεις στην απόδοση των αστικών υπηρεσιών και στη λήψη αποφάσεων [K111].

Ασφάλεια και απόρρητο: Μια άλλη από τις σημαντικότερες προκλήσεις σε μια έξυπνη πόλη και με τη χρήση μεγάλων δεδομένων είναι τα ζητήματα ασφάλειας και απορρήτου. Με βασικούς όρους, αυτό σημαίνει ότι οι βάσεις δεδομένων ενδέχεται να περιλαμβάνουν εμπιστευτικές πληροφορίες που σχετίζονται με τις διοικητικές αρχές και τους ανθρώπους, επομένως χρειάζονται υψηλά επίπεδα πολιτικών και μηχανισμών ασφαλείας για την προστασία αυτών των δεδομένων από μη εξουσιοδοτημένη χρήση και κακόβουλες επιθέσεις. Για παράδειγμα, πολλά προσωπικά δεδομένα ταυτοποίησης σχετικά με πολίτες, όπως κοινωνικές δραστηριότητες και τοποθεσίες, συλλέγονται καθημερινά. Αν και έχουν γίνει πολλές προσπάθειες για να αντιμετωπιστεί αυτή η ανησυχία, η διασφάλιση του τεράστιου όγκου ιδιωτικών δεδομένων που συλλέγονται από τεχνολογίες έξυπνων πόλεων από χάκερ και κλοπές γίνεται ένα δύσκολο πρόβλημα. Επιπλέον, αν και οι επιτυχημένες επιθέσεις στον κυβερνοχώρο σε πόλεις παραμένουν σχετικά σπάνιες, οι τεχνολογίες έξυπνων πόλεων εγείρουν μια σειρά από ανησυχίες για την ασφάλεια στον κυβερνοχώρο που απαιτούν προσοχή [109]. Εκτός από την ανάγκη να ασφαλιστούν τα δεδομένα καθώς ταξιδεύουν και καθώς χρησιμοποιούνται από τα διάφορα στοιχεία των εφαρμογών έξυπνων πόλεων, υπάρχει επίσης η ανάγκη σαφούς προσδιορισμού και προστασίας των δικαιωμάτων απορρήτου των οργανισμών και των ατόμων που αντιπροσωπεύουν αυτά τα δεδομένα. Τα δεδομένα υγείας, τα οικονομικά και τραπεζικά αρχεία, το ιστορικό αγορών και πολλά άλλα παρέχουν προσωπικές απόψεις των ανθρώπων που εκπροσωπούν. Πολλοί θεωρούν την πρόσβαση σε αυτό το είδος δεδομένων ως παραβίαση των νόμιμων δικαιωμάτων ενός ατόμου για την ιδιωτική ζωή. Η διασφάλιση της θέσπισης αυστηρών πολιτικών

απορρήτου και της σωστής εφαρμογής τους αντιπροσωπεύει μια μεγάλη πρόκληση εφαρμογών έξυπνων πόλεων μεγάλων δεδομένων και τους χρήστες[20].

5.3 ΕΦΑΡΜΟΓΕΣ ΤΩΝ ΜΕΓΑΛΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΗΝ ΕΞΥΠΝΗ ΠΟΛΗ

Η εφαρμογή των τεχνολογιών μεγάλων δεδομένων για την έξυπνη πόλη επιτρέπει την αποτελεσματική αποθήκευση και επεξεργασία δεδομένων για την παραγωγή πληροφοριών που μπορούν να βελτιώσουν διαφορετικές υπηρεσίες έξυπνων πόλεων και να βοηθήσουν τους υπεύθυνους λήψης αποφάσεων στο να σχεδιάσουν οποιαδήποτε επέκταση σε υπηρεσίες και πόρους έξυπνων πόλεων [109]. Επίσης, Οι εφαρμογές μεγάλων δεδομένων έχουν τη δυνατότητα να εξυπηρετήσουν πολλούς τομείς σε μια έξυπνη πόλη, βοηθώντας στην παροχή καλύτερων εμπειριών και υπηρεσιών στους κατοίκους, την απόδοση καλύτερων οικονομικών αποδόσεων στις εταιρίες, τη βελτίωση της υγειονομικής περίθαλψης με υπηρεσίες προληπτικής φροντίδας, εργαλείων διάγνωσης και θεραπείας, τη διαχείριση αρχείων υγειονομικής περίθαλψης και τη φροντίδα των ασθενών. Τα συστήματα των αστικών μεταφορών μπορούν να επωφεληθούν πολύ από τα μεγάλα δεδομένα για να βελτιστοποιήσουν τις διαδρομές και τα χρονοδιαγράμματα που ακολουθούν, ανταποκρινόμενα στις ποικίλες απαιτήσεις ώστε να είναι και πιο φιλικά προς το περιβάλλον [107]. Η ανάλυση μεγάλων δεδομένων μπορεί να διαδραματίσει σημαντικό ρόλο και στην ενεργοποίηση της έξυπνης διακυβέρνησης, καθώς οι οργανισμοί ή οι φορείς με κοινά ενδιαφέροντα μπορούν εύκολα να εντοπιστούν

[20] Άλλοι δύο παράγοντες που θέτουν προκλήσεις στην εφαρμογή των μεγάλων δεδομένων είναι το κόστος και ο πληθυσμός των έξυπνων πόλεων. Το κόστος είναι ένα ευαίσθητο θέμα που περιλαμβάνει τους τρόπους με τους οποίους οι δημόσιες αρχές μπορούν να επηρεάσουν τους ανθρώπους όταν χρησιμοποιούν λύσεις ΤΠΕ. Για παράδειγμα, χρησιμοποιώντας ένα σύστημα μείωσης της χρήσης ενέργειας, το οποίο αναγκάζει την κυβέρνηση να χρησιμοποιήσει νέα συστήματα, εξαρτήματα ή χαρακτηριστικά για την παρακολούθηση της κατανάλωσης και την καταγραφή πληροφοριών. Αυτό οδηγεί στη δημιουργία ενός έξυπνου συστήματος διαχείρισης ενέργειας. Ωστόσο, είναι επίσης πολύ ακριβό στην εφαρμογή. Πληθυσμός Έξυπνης Πόλης: Οι άνθρωποι επηρεάζουν και επηρεάζονται από τις έξυπνες εφαρμογές. Ιδιαίτερα το μέγεθος του πληθυσμού της πόλης έχει μεγάλη επίδραση στο μέγεθος των μεγάλων δεδομένων. Καθώς ο πληθυσμός αυξάνεται, το μέγεθος των παραγόμενων δεδομένων αυξάνεται επίσης γρήγορα και μπορεί να γίνει τεράστιο. Ως αποτέλεσμα, οι εφαρμογές έξυπνων πόλεων πρέπει να εξελίσσονται γρήγορα και να επεκτείνονται αποτελεσματικά για να χειρίζονται τον αυξανόμενο όγκο και την ποικιλία μεγάλων δεδομένων.

μέσω της ανάλυσης δεδομένων που και να προχωρήσουν σε συνεργασία μεταξύ τους [109].

Παράδειγμα έξυπνης πόλης όπου έχει εγκατασταθεί ένας μεγάλος αριθμός αισθητήρων αποτελεί το λιμάνι του Σανταντέρ στη βόρεια ακτή της Ισπανίας, η πόλη με τη μεγαλύτερη ένταση δεδομένων στην Ευρώπη [112]. Με επιχορήγηση 8 εκατομμυρίων ευρώ (10,6 εκατομμύρια δολάρια) από την Ευρωπαϊκή Επιτροπή πριν από τρία χρόνια, μια κοινοπραξία ευρωπαϊκών πανεπιστημίων και εταιρειών τηλεπικοινωνιών εγκατέστησε περίπου 18.000 σταθερούς και κινητούς αισθητήρες διαφόρων τύπων σε ολόκληρο τον δήμο με περίπου 180.000 κατοίκους. Εκτός από την παρακολούθηση της ατμοσφαιρικής ρύπανσης, του θορύβου και άλλων περιβαλλοντικών συνθηκών, οι αισθητήρες υποδεικνύουν πότε οι κάδοι απορριμμάτων χρειάζονται άδειασμα και πότε τα φώτα του δρόμου έχουν καεί ή μπορούν να σβήσουν επειδή δεν υπάρχει κανένας. Οι αισθητήρες που είναι θαμμένοι στο πεζοδρόμιο ανιχνεύουν ανοιχτούς και μεταδίδουν αυτές τις πληροφορίες σε ψηφιακές οθόνες που είναι τοποθετημένες σε μεγάλες διασταυρώσεις για να βοηθήσουν τους οδηγούς να καθοδηγούν. Το SmartSantander διαθέτει επίσης μια εφαρμογή smartphone που επιτρέπει στους κατοίκους να αναφέρουν προβλήματα όπως λακκούβες και να παρακολουθούν την απόκριση της πόλης. Χρησιμοποιώντας τα smartphone τους, οι κάτοικοι μπορούν να χρησιμοποιήσουν ένα σύστημα «επαυξημένης πραγματικότητας» που περιλαμβάνει 2600 οπτικές και ασύρματες ετικέτες σε τουριστικά αξιοθέατα, καταστήματα, στάσεις λεωφορείων και άλλες τοποθεσίες σε όλη την πόλη για να λάβουν εύκολα διαδικτυακές πληροφορίες για αυτές τις τοποθεσίες.

5.4. Η ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΣΤΙΣ ΕΞΥΠΝΕΣ ΠΟΛΕΙΣ

Τα συστήματα τεχνητής νοημοσύνης (ΤΝ) είναι συστήματα λογισμικού (ή ενδεχομένως και υλισμικού) που σχεδιάζονται από ανθρώπους και, βάσει ενός δεδομένου σύνθετου στόχου, ενεργούν στην υλική ή ψηφιακή διάσταση με το να αντιλαμβάνονται το περιβάλλον τους μέσω της απόκτησης δεδομένων, να ερμηνεύουν τα δομημένα ή αδόμητα δεδομένα που έχουν συλλεχθεί, να προβαίνουν σε συλλογισμούς με βάση τις γνώσεις ή να επεξεργάζονται τις πληροφορίες, που

εξάγονται από αυτά τα δεδομένα, και να αποφασίζουν ποια είναι η βέλτιστη ενέργεια (ή οι βέλτιστες ενέργειες) που θα πρέπει να εκτελέσουν για να επιτύχουν τον δεδομένο στόχο. Τα συστήματα ΤΝ μπορούν είτε να χρησιμοποιούν συμβολικούς κανόνες, είτε να μαθαίνουν ένα αριθμητικό μοντέλο, είτε να προσαρμόζουν τη συμπεριφορά τους με το να αναλύουν πώς επηρεάζεται το περιβάλλον από τις προηγούμενες ενέργειές τους [115].

Λαμβανομένης υπόψη της πληθώρας των τομέων μιας έξυπνης πόλης, στην οποία έχουν εφαρμογή όλα τα προηγμένα συστήματα της ΤΝ, μπορούμε να μιλάμε επίσης για αστική τεχνητή νοημοσύνη, η οποία μπορεί να οριστεί ως εξής: «Τα τεχνουργήματα που λειτουργούν σε πόλεις, τα οποία είναι ικανά να αποκτήσουν και να κατανοήσουν πληροφορίες για το αστικό περιβάλλον, χρησιμοποιώντας τελικά την αποκτηθείσα γνώση για να ενεργήσουν ορθολογικά σύμφωνα με προκαθορισμένους στόχους, σε περίπλοκες αστικές καταστάσεις όπου οι πληροφορίες ενδέχεται να λείπουν ή να είναι ελλιπείς» [116]. Μέχρι το 2025, η τεχνητή νοημοσύνη αναμένεται να ενεργοποιήσει πάνω από το 30% των εφαρμογών έξυπνων πόλεων, μεταξύ των οποίων και λύσεις αστικής μετακίνησης, συμβάλλοντας σημαντικά στην ανθεκτικότητα, τη βιωσιμότητα, την κοινωνική ευημερία και τη ζωτικότητα της αστικής ζωής [116].

Αποφασιστικός παράγοντας για την ανάπτυξη της ΤΝ είναι η εκθετική αύξηση και διαθεσιμότητα δεδομένων, συμπεριλαμβανομένων των δεδομένων που συλλέγονται και παράγονται από το Διαδίκτυο των Πραγμάτων. Το Διαδίκτυο των Πραγμάτων (IoT) που συνδέεται στενά με την έννοια της «πανταχού παρουσίας υπολογιστών», βασίζεται στην εκτεταμένη επεξεργασία δεδομένων μέσω του δικτύου αισθητήρων που επικοινωνούν και ανταλλάσσουν δεδομένα με ανεπιτήδευτο και απρόσκοπτο τρόπο [113]. Φαίνεται ότι και σε αυτή την περίπτωση υπάρχει ένα είδος αμφίδρομης σχέσης: Για να επιτευχθεί το πλήρες δυναμικό του, το IoT πρέπει να συνδυαστεί με την Τεχνητή Νοημοσύνη (AI) και ταυτόχρονα ο αντίκτυπος του AI σε κάθε πτυχή της ζωής θα πολλαπλασιάζεται και γίνεται πιο εξελιγμένο από τον συνδυασμό του με το Διαδίκτυο των Πραγμάτων [113].

5.5. ΑΝΟΙΧΤΑ ΔΕΔΟΜΕΝΑ (OPEN DATA) ΚΑΙ ΕΞΥΠΝΕΣ ΠΟΛΕΙΣ

Τα Open Data είναι ένα σημαντικό μέσο το οποίο διευκολύνει την πρόσβαση σε δεδομένα στους πολίτες, σε εταιρείες στην κοινωνία, προωθώντας την οικονομική ανάπτυξη, την επιστημονική έρευνα, την πολιτική και εταιρική ευθύνη [122].

Ως Open Data ορίζονται τα δεδομένα εκείνα που είναι ''ανοιχτά'' για χρήση χωρίς περιορισμούς, νομικούς ή τεχνολογικούς. Για το σκοπό αυτό, συνήθως θεωρείται ότι τα Open Data[122]:

1. Είναι διαθέσιμα στο Διαδίκτυο, ώστε να είναι προσβάσιμα και να καθίσταται δυνατή και εύκολη η λήψη αυτών.

2.Αναγνώσιμα από μηχανή. Η ανάλυση και η συγχώνευση δεδομένων πρέπει να είναι αυτοματοποιημένες έτσι ώστε να είναι εφικτά σε μεγάλα σύνολα δεδομένων ή σε μεγάλο αριθμό συνόλων δεδομένων.

3. Παρέχονται με ανοιχτή άδεια, η οποία θέτει ελάχιστους περιορισμούς για τον χρήστη[21].

5.6. ΧΡΗΣΙΜΟΤΗΤΑ ΤΩΝ OPEN DATA ΣΤΗΝ ΕΞΥΠΝΗ ΠΟΛΗ

Τα Open Data αποτελούν ακρογωνιαίο λίθο της ΕΠ τόσο εξαιτίας του ότι οι τεχνολογίες της ΕΠ, προκειμένου να λειτουργήσουν, εξαρτώνται από ανοιχτά δεδομένα τα οποία προέρχονται από τις διοικητικές αρχές αυτής και τις αστικές υπηρεσίες, όσο και γιατί τα Open Data εκτείνονται πέρα από τη λειτουργικότητα, στο ίδιο το περιβάλλον της διακυβέρνησης [123].

Πολλές τοπικές και εθνικές κυβερνήσεις έχουν υιοθετήσει πολιτικές ανοικτών δεδομένων οι οποίες κυμαίνονται από γενικές δηλώσεις αρχών (π.χ. Χάρτης Ανοιχτών Δεδομένων) έως συγκεκριμένες εντολές για τον τρόπο με τον οποίο θα αντιμετωπίζονται τα δεδομένα από την πόλη (π.χ. Ντουμπάι, Βιέννη, Σιάτλ) [**123]**

Τα Open Data καλύπτουν την ανάγκη για υψηλότερα επίπεδα διαφάνειας, για καλύτερη διαχείριση και έλεγχο των διαφορετικών πτυχών και εφαρμογών της ΕΠ και

[21] Παραδείγματα ανοιχτών αδειών είναι οι Creative Commons (ιδίως, CC ή CC-BY 4.0) ή πιο συγκεκριμένα, η Άδεια Ανοιχτής Κυβέρνησης του Ηνωμένου Βασιλείου στο http://www.nationalarchives.gov.uk/doc

της σχέσης των ΕΠ με τα μεγάλα δεδομένα, για διαφάνεια των πληροφοριών για όλους τους εμπλεκόμενους, και παράλληλα ενθαρρύνουν τη συνεργασία και την επικοινωνία μεταξύ οντοτήτων και τη δημιουργία περισσότερων υπηρεσιών και εφαρμογών που ενισχύουν περαιτέρω την έξυπνη πόλη [107]. Για τους σκοπούς αυτούς, κυβερνήσεις και δήμοι επιδιώκουν να προωθήσουν πρωτοβουλίες open data, όπου οι πληροφορίες που είναι ''κλειδωμένες'' στις πόλεις διατίθενται σε πολίτες, επιχειρήσεις και άλλους φορείς για κοινή χρήση, επαναχρησιμοποίηση και διανομή γύρω από πολιτιστικά, επιστημονικά, οικονομικά, περιβαλλοντικά θέματα [124].

Η τρέχουσα ψηφιακή οικονομία ενθαρρύνει τη συλλογή και χρήση δεδομένων με τρόπους που δημιουργούν έντονες ανισορροπίες ισχύος. Η τρέχουσα διαδικτυακή οικονομία έχει επιτρέψει στις ψηφιακές επιχειρήσεις, μέσω της συσσώρευσης τεράστιων βάσεων δεδομένων προσωπικών δεδομένων και δεδομένων συμπεριφοράς, να γίνουν πολύ πιο ισχυρές από ό,τι ανέμεναν οι ρυθμιστικές αρχές [K344]. Για το λόγο αυτό οι πόλεις θα πρέπει να διαδραματίσουν πιο ενεργό ρόλο στην αξιοποίηση πιο υπεύθυνης καινοτομίας με δεδομένα στην τοπική οικονομία, γεγονός το οποίο απαιτεί επίσης μια αλλαγή νοοτροπίας για να δούμε τα δεδομένα όχι ως εμπόρευμα προς πώληση, αλλά περισσότερο ως κοινό αγαθό [125].

Με τη χρήση των open data γίνεται προσπάθεια να δημιουργηθεί αξία μέσω της εκμετάλλευσης πληροφοριών, είτε πρόκειται για δεδομένα που ήδη κατέχει ο δημόσιος τομέας είτε για δεδομένα που συλλέγονται μέσω του δικτύου κατανεμημένων αισθητήρων που χαρακτηρίζουν τις υποδομές έξυπνων πόλεων [126]. Πρόκειται για ένα είδος ανατροφοδότησης, στο οποίο οι πληροφορίες που συλλέγονται από τους δημόσιους φορείς ή τις συμπράξεις δημόσιου-ιδιωτικού τομέα που διαχειρίζονται την υποδομή της έξυπνης πόλης απελευθερώνονται ως ανοιχτά δεδομένα και χρησιμοποιούνται ως βάση για την ανάπτυξη περαιτέρω δραστηριοτήτων στην ΕΠ [126.]

Οι πόλεις σήμερα συλλέγουν και αποθηκεύουν ένα ευρύ φάσμα δεδομένων που μπορεί να περιέχουν ευαίσθητες πληροφορίες για τους κατοίκους. Καθώς οι πόλεις αγκαλιάζουν πρωτοβουλίες ανοιχτών δεδομένων, περισσότερες από αυτές τις πληροφορίες γνωστοποιούνται στο κοινό. Ενώ το άνοιγμα δεδομένων έχει πολλά σημαντικά οφέλη, η κοινή χρήση δεδομένων ενέχει εγγενείς κινδύνους για το ατομικό

απόρρητο: τα δημοσιευμένα δεδομένα μπορούν να αποκαλύψουν πληροφορίες για άτομα που διαφορετικά δεν θα ήταν δημόσια [127].

6. ΖΗΤΗΜΑΤΑ ΕΦΑΡΜΟΓΗΣ ΤΟΥ ΓΕΝΙΚΟΥ ΚΑΝΟΝΙΣΜΟΥ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΣΤΗΝ ΕΞΥΠΝΗ ΠΟΛΗ

Η ιδέα της ΕΠ προέκυψε ως απάντηση στις προκλήσεις της αστικοποίησης του 21ου αιώνα, με σκοπό την αναζήτηση λύσεων για αποτελεσματικότητα, άνεση και ασφάλεια στην ΕΠ μέσω της τεχνολογίας. Παρά την ύπαρξη των διευκολύνσεων που προσφέρει μια ΕΠ, η ιδιωτικότητα και η προστασία των προσωπικών δεδομένων των κατοίκων της πρέπει επίσης να είναι συνυφασμένη με τα οφέλη αυτής.

Το οικοσύστημα της ΕΠ αποτελείται τα εξής στοιχεία: α) Από τη Διοίκηση της πόλης και τις επιμέρους διευθύνσεις αυτής, β) Από τις εταιρίες, κυρίως, τεχνολογικών υπηρεσιών, οι οποίες προσβλέπουν στις ΕΠ ως ένα πρόσφορο έδαφος για την παροχή των σύγχρονων υπηρεσιών τους, καλύπτοντας ένα ευρύ πεδίο δραστηριοτήτων, όπως της δημόσιας μετακίνησης, της ενέργειας, της υγείας της εκπαίδευσης κλπ. και γ) από τους κατοίκους της ΕΠ, οι οποίοι αποτελούν το επίκεντρο αυτής. Ωστόσο το καθένα από παραπάνω μέρη έχει διαφορετικές απόψεις για τον τρόπο συλλογής, επεξεργασίας και προστασίας των δεδομένων που συλλέγονται στα έργα των ΕΠ. Στην περίπτωση μάλιστα που τα δεδομένα που συλλέγονται είναι προσωπικά, η επεξεργασία και η προστασία αυτών ορίζονται στο Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR) 679/2016 της Ευρωπαϊκής Ένωσης.

Περαιτέρω, το Internet of Things, ως δίκτυο φυσικών αντικειμένων τα οποία είναι ενσωματωμένα με αισθητήρες, λογισμικό και άλλες τεχνολογίες, για τη σύνδεση και την ανταλλαγή δεδομένων με άλλες συσκευές και συστήματα μέσω του διαδικτύου, αποτελεί ακρογωνιαίο λίθο για τη λειτουργία της ΕΠ και συνεπάγεται ένα οικοσύστημα αλληλοεξαρτώμενων παραγόντων που πρέπει να αλληλεπιδράσουν μεταξύ τους, όπως ενδεικτικά οι αρχές μιας πόλης, οι πάροχοι δικτύων, οι πάροχοι αισθητήρων, οι κατασκευαστές έξυπνων συσκευών.

Σε έρευνα που έγινε σε κατοίκους της Φλάνδρας και των Βρυξελλών, διαπιστώθηκε ότι οι κάτοικοι επιθυμούν κατηγορηματικά οι διοικήσεις των πόλεων να είναι αυτές που θα δίνουν τις κατευθύνσεις και θα αποφασίζουν για τις ‘’έξυπνες’’ δράσεις σε

μια ΕΠ και ιδίως για αυτές που λαμβάνουν χώρα σε δημόσιο, παρά η σχετική διαχείριση να γίνεται μόνο από ιδιωτικούς οργανισμούς. Λαμβανομένου υπόψη ότι ένα μεγάλο σύνολο των παρεχόμενων υπηρεσιών εντός της ΕΠ απαιτεί την επεξεργασία προσωπικών δεδομένων των κατοίκων αυτής, είναι επακόλουθο να γεννώνται βασικοί προβληματισμοί αναφορικά με την εφαρμογή του ΓΚΠΔ, οι βασικότεροι εκ των οποίων είναι οι εξής:

6.1. Ο ΡΟΛΟΣ ΤΩΝ ΕΜΠΛΕΚΟΜΕΝΩΝ ΜΕΡΩΝ ΣΤΗΝ ΕΞΥΠΝΗ ΠΟΛΗ

Όπως αναφέρθηκε και ανωτέρω τα εμπλεκόμενα μέρη για την παροχή υπηρεσιών προς τους κατοίκους της ΕΠ είναι κυρίως οι αρχές αυτής και οι εταιρίες παροχής τεχνολογικών υπηρεσιών, με το καθένα από αυτά να έχει συγκεκριμένο ρόλο, ο οποίος περιγράφει ένα σύνολο ευθυνών, ενεργειών ή εξουσιοδοτήσεων. Έτσι και στο πλαίσιο του ΓΚΠΔ οι ρόλοι των ανωτέρω μερών ορίζονται γύρω από νομικές έννοιες όπως είναι η ευθύνη και η λογοδοσία. Δεδομένου ότι για τη λειτουργία της ΕΠ η σχέση μεταξύ των αρχών αυτής και του ιδιωτικού τομέα (κυρίως τεχνολογικών εταιριών) είναι σχεδόν απαραίτητη αλλά και εξαιρετικά στενή, αυτό έχει ως αποτέλεσμα σε πολλές δραστηριότητες επεξεργασίας δεδομένων, ο διαχωρισμός των υπευθύνων επεξεργασίας και των εκτελούντων την επεξεργασία μεταξύ τους με ακρίβεια να αποτελεί ένα δύσκολο πρόβλημα [81].

Στο α. 4 του ΓΚΠΔ ορίζονται τα μέρη που εμπλέκονται στην επεξεργασία των προσωπικών δεδομένων ως εξής:

υπεύθυνος επεξεργασίας: 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,

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,

αποδέκτης: 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 της Ένωσης ή κράτους μέλους δεν θεωρούνται ως αποδέκτες. Ο όρος αυτός εισήχθη τόσο για να ενισχυθεί η διαφάνεια της επεξεργασίας έναντι των υποκειμένων των δεδομένων, καθώς η πληροφόρηση για τους αποδέκτες των δεδομένων αποτελεί μέρος του δικαιώματος ενημέρωσης[22] και του δικαιώματος πρόσβασης[23], όσο και για την αποτελεσματική άσκηση των δικαιωμάτων που των υποκειμένων των δεδομένων όπως αυτά προβλέπονται στον ΓΚΠΔ[24] [82].

τρίτος: 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. Τρίτο μέρος δηλαδή θα μπορούσε να θεωρηθεί κάθε μέρος που δεν αποτελεί μέρος του «εσωτερικού κύκλου» μιας συγκεκριμένης επεξεργασίας δεδομένων [82]. Στο πλαίσιο της ΕΠ για παράδειγμα, εάν ο υπεύθυνος επεξεργασίας (η πόλη) κοινοποιήσει νομίμως ορισμένα δεδομένα από ένα έργο που σχετίζεται με την κινητικότητα σε μια οντότητα όπως το υπουργείο Μεταφορών, η οποία είναι εξωτερική στη συγκεκριμένη επεξεργασία δεδομένων που αναλαμβάνει η πόλη, το τελευταίο θα θεωρείτο τρίτο μέρος, με αποτέλεσμα στη συνέχεια το τρίτο μέρος να καθίσταται υπεύθυνος επεξεργασίας για την επεξεργασία που αναλαμβάνει μόλις λάβει τα δεδομένα [82].

Στον ΓΚΠΔ η αρχή της λογοδοσίας για τους υπεύθυνους επεξεργασίας συνίσταται αφενός στην ευθύνη και τη δικαιολόγηση των αποφάσεων που λαμβάνουν και αφετέρου στην ευθύνη να διασφαλίζουν και να είναι σε θέση να αποδείξουν τη συμμόρφωση με τον ΓΚΠΔ, με αποτέλεσμα η αρχή της λογοδοσίας να μεταφέρει την προστασία δεδομένων από τη θεωρία στην πράξη [WP29, 2010]. Επειδή ο ΓΚΠΔ λειτουργεί με βάση ανοιχτούς κανόνες (τις αρχές που σχετίζονται με την επεξεργασία δεδομένων προσωπικού χαρακτήρα) και την εξίσου ευρεία έννοια του κινδύνου, οι

---

[22] (άρθρα 13 & 14)

[23] (άρθρο 15)

[24] διόρθωσης (άρθρο 16). διαγραφή (άρθρο 17). και περιορισμός της επεξεργασίας (άρθρο 18): όταν λάβει ένα αίτημα για το υποκείμενο των δεδομένων σχετικά με οποιοδήποτε από αυτά τα δικαιώματα, ο υπεύθυνος επεξεργασίας πρέπει κατ' αρχήν να το κοινοποιεί σε κάθε αποδέκτη (άρθρο 19).

υπεύθυνοι επεξεργασίας έχουν σημαντικές εξουσίες λήψης αποφάσεων: για τον εντοπισμό και την αξιολόγηση των κινδύνων, τον προβληματισμό σχετικά με τα επιθυμητά αποτελέσματα και τα μέτρα που πρέπει να ληφθούν για να εξασφαλιστεί η συμμόρφωση με τις αρχές προστασίας δεδομένων και, γενικά, να εξασφαλιστεί δίκαιη εξισορρόπηση των συμφερόντων τους και των συμφερόντων των ατόμων των οποίων τα δεδομένα υπόκεινται σε επεξεργασία [82].

Παράλληλα και οι εκτελούντες την επεξεργασία καθίστανται υπεύθυνοι για μη συμμόρφωση με τις διατάξεις του ΓΚΠΔ που αναφέρονται σε αυτούς (όπως η τήρηση αρχείων δραστηριοτήτων επεξεργασίας[25], η ασφάλεια της επεξεργασίας[26], η ενημέρωση του υπεύθυνου επεξεργασίας σε περίπτωση παραβίασης δεδομένων[27], ο ορισμός Υπεύθυνου Προστασίας Δεδομένων (DPO) όπου προβλέπεται, η απαγόρευση πρόσληψης άλλων υποεκτελούντων χωρίς εξουσιοδότηση από τον υπεύθυνο επεξεργασίας[28], η συμμόρφωση με τις οδηγίες του υπεύθυνου επεξεργασίας[29]).

Στο περιβάλλον της ΕΠ η διάκριση των ανωτέρω ρόλων μπορεί πραγματικά να αποδειχθεί μια πολύ δύσκολη διαδικασία, γεγονός που αναφέρθηκε επανειλημμένα σε συζήτηση εκπροσώπων από διαφορετικές ομάδες ενδιαφερομένων για την προστασία των προσωπικών δεδομένων στην έξυπνη πόλη[30]. Μια πρόκληση που αναφέρθηκε επανειλημμένα ήταν το πρόβλημα της απόφασης ποιος είναι υπεύθυνος επεξεργασίας και ποιος εκτελών την επεξεργασία για μια συγκεκριμένη δραστηριότητα επεξεργασίας δεδομένων καθώς και ότι σε πολλές περιπτώσεις, οι έξυπνες πόλεις και οι προμηθευτές τεχνολογίας είναι και οι δύο υπεύθυνοι επεξεργασίας, δεδομένου ότι επεξεργάζονται δεδομένα για κοινούς σκοπούς ή ο καθένας για δικούς του σκοπούς [84]. Ένα συγκεκριμένο παράδειγμα που συζητήθηκε ήταν ο από κοινού έλεγχος σε συμπράξεις δημόσιου και ιδιωτικού τομέα.

---

[25] Α. 30 ΓΚΠΔ
[26] Α. 32 ΓΚΠΔ
[27] Α. 33 ΓΚΠΔ
[28] Α. 28 παρ.2 ΓΚΠΔ
[29] Α.29 ΓΚΠΔ
[30] Πρόκειται για συνεδρίας στρογγυλής τραπέζης που έλαβε χώρα στις 24 Ιουνίου 2019 στις Βρυξέλλες, η οποία συγκέντρωσε διάφορους ενδιαφερόμενους για να συζητήσουν προκλήσεις και λύσεις για την προστασία (προσωπικών) δεδομένων σε έξυπνες πόλεις.

Στον ΓΚΠΔ ορίζεται ότι *σε περίπτωση που δύο ή περισσότεροι υπεύθυνοι επεξεργασίας καθορίζουν από κοινού τους σκοπούς και τα μέσα της επεξεργασίας, αποτελούν από κοινού υπευθύνους επεξεργασίας*[31]. Η αξιολόγηση της ύπαρξης από κοινού υπευθύνων επεξεργασίας θα πρέπει να διενεργείται βάσει μιας πραγματικής και όχι τυπικής ανάλυσης της επιρροής στους σκοπούς και τα μέσα της επεξεργασίας, καθώς ελλοχεύει ο κίνδυνος σε ορισμένες περιπτώσεις να μην προβλέπεται για παράδειγμα στο νόμο ή στη σύμβαση είτε ο ορισμός των από κοινού υπευθύνων επεξεργασίας είτε ο ρόλος του υπεύθυνου επεξεργασίας να ανατίθεται σε μια οντότητα που στην πραγματικότητα δεν είναι σε θέση να «προσδιορίσει» τους σκοπούς και τα μέσα της επεξεργασίας [85]. Πρέπει να σημειωθεί ότι όλες οι επεξεργασίες που αφορούν πολλές οντότητες δεν οδηγούν σε από κοινού έλεγχο. Το πρωταρχικό κριτήριο για την ύπαρξη από κοινού ελέγχου είναι η από κοινού συμμετοχή δύο ή περισσότερων φορέων αφενός στον καθορισμό των σκοπών και αφετέρου στον καθορισμό των μέσων μιας επεξεργασίας. Εάν καθένα από αυτά τα στοιχεία καθορίζεται από όλες τις ενδιαφερόμενες οντότητες, θα πρέπει να θεωρούνται ως από κοινού ελεγκτές της εν λόγω επεξεργασίας [85].

Σύμφωνα με τον ΓΚΠΔ οι δύο βασικές προϋποθέσεις για να χαρακτηρισθεί μία οντότητα ως εκτελών την επεξεργασία είναι να είναι ξεχωριστή οντότητα σε σχέση με τον υπεύθυνο επεξεργασίας και η επεξεργασία προσωπικών δεδομένων να πραγματοποιείται για λογαριασμό και προς όφελος του υπεύθυνου επεξεργασίας. Μια χωριστή οντότητα σημαίνει ότι ο υπεύθυνος επεξεργασίας αποφασίζει να αναθέσει το σύνολο ή μέρος των δραστηριοτήτων επεξεργασίας (η επεξεργασία μπορεί να περιλαμβάνει ένα ευρύ φάσμα εργασιών που κυμαίνονται από τη συλλογή, την αποθήκευση και τη διαβούλευση έως τη χρήση, τη διάδοση ή με άλλο τρόπο διάθεση και την καταστροφή) [32]σε εξωτερικό οργανισμό, ακόμη κι αν αυτός ανήκει στον ίδιο όμιλο εταιρειών [85]. Δεύτερον, η επεξεργασία πρέπει να πραγματοποιείται για λογαριασμό του υπεύθυνου επεξεργασίας, αλλά υπό την άμεση εξουσία ή τον έλεγχό του, έτσι ώστε ο εκτελών την επεξεργασία να εφαρμόζει

[31] Αρ. 24ΓΚΠΔ
[32] Αρ.4 παρ. 2 ΓΚΠΔ

τις οδηγίες που του δίνει ο υπεύθυνος επεξεργασίας τουλάχιστον όσον αφορά τον σκοπό της επεξεργασίας και τα ουσιώδη στοιχεία των μέσων[33] [85].

Σε περιβάλλοντα όπου δρουν πολλαπλοί παράγοντες, όπως στις έξυπνες πόλεις, οι οποίοι περιλαμβάνουν πολύπλοκες λειτουργίες επεξεργασίας δεδομένων, είναι δύσκολο να διακριθεί η πραγματική επιρροή κάθε παράγοντα και το αν αυτή οδηγεί σε πρόσωπο που δρα ως υπεύθυνος ή ως εκτελών την επεξεργασία. Μπορεί να προκύψει πρόσθετος κίνδυνος για προσωπικά δεδομένα όταν πολλοί αποκεντρωμένοι υπεύθυνοι επεξεργασίας μοιράζονται τον ίδιο εκτελούντα την επεξεργασία για διαφορετικές δραστηριότητες επεξεργασίας δεδομένων [84]. Προγραμματιστές λογισμικού ή προγραμματιστές αισθητήρων μπορεί να μην εμπίπτουν στην κατηγορία του υπεύθυνου ή του εκτελούντος την επεξεργασία, αλλά ενδέχεται να επηρεάζουν την επεξεργασία δεδομένων και την προστασία που παρέχεται στα υποκείμενα των δεδομένων, με αποτέλεσμα, οι υπεύθυνοι επεξεργασίας, ως υπόλογοι σε λογοδοσία να καθίστανται ουσιαστικά υπεύθυνοι και για τις ενέργειες ή παραλείψεις άλλων [82]. Στην πράξη μπορεί να είναι ιδιαίτερα δύσκολο για τους υπεύθυνους επεξεργασίας να ασκούν έναντι των προγραμματιστών και των επεξεργαστών τον έλεγχο και την παρακολούθηση που απαιτούνται για τη διασφάλιση της συμμόρφωσης [82].

Στην ΕΠ το ρόλο εκτελούντων την επεξεργασία έχουν συνήθως εταιρίες παροχής τεχνολογικών προϊόντων οι οποίοι επεξεργάζονται προσωπικά δεδομένα ακολουθώντας συγκεκριμένες οδηγίες από έναν υπεύθυνο επεξεργασίας. Παραδείγματα εκτελούντων την επεξεργασία μπορούν να περιλαμβάνουν χειριστές δεδομένων, παρόχους συστημάτων λογισμικού, παρόχους που προσφέρουν υπηρεσίες αποθήκευσης. Ωστόσο ενδέχεται ανάλογα τέτοιου είδους εμπλεκόμενα πρόσωπα να μην καλύπτονται από τον ΓΚΠΔ, παρόλο που διαδραματίζουν κι αυτοί κάποιο ρόλο, επειδή δεν ταξινομούνται ούτε ως υπεύθυνοι επεξεργασίας ούτε ως εκτελούντες επεξεργασίας. Παραδείγματα εδώ θα μπορούσαν να είναι πάροχοι λογισμικού που απλώς αναπτύσσουν ένα λογισμικό χωρίς στη συνέχεια να

[33] Η νομιμότητα δε της επεξεργασίας σύμφωνα με το άρθρο 6 του ΓΚΠΔ και, κατά περίπτωση, το άρθρο 9 του ΓΚΠΔ θα απορρέει από τη δραστηριότητα του υπεύθυνου επεξεργασίας και ο εκτελών την επεξεργασία δεν πρέπει επεξεργάζεται τα δεδομένα με άλλο τρόπο παρά σύμφωνα με τις οδηγίες του υπεύθυνου επεξεργασίας.

συμμετέχουν στην ανάπτυξή του ή πάροχοι που αναπτύσσουν αισθητήρες ή ενεργοποιητές [K82].

Ένα ακόμη χαρακτηριστικό που συνήθως επηρεάζει τη σχέση μεταξύ υπευθύνου και εκτελούντος την επεξεργασία είναι η οικονομική ισχύς αυτών των δύο μερών, ειδικά αν λάβει κανείς υπόψη του ότι εκτελούντες την επεξεργασία ενδέχεται να είναι τεχνολογικές εταιρίες κολοσσοί στο είδος τους, έχοντας την ισχύ να επιβάλλουν τις δικές τους απαιτήσεις και όρους στη μεταξύ τους συνεργασία με τις αρχές μιας ΕΠ. Για παράδειγμα, οι τεχνολογικές εταιρίες μπορούν να χρησιμοποιήσουν αυτήν την εξουσία για να υποβάλουν αιτήματα σχετικά με το δικαίωμά τους να επεξεργάζονται και να επαναχρησιμοποιούν δεδομένα και οι πόλεις μπορεί να μην έχουν άλλη επιλογή από το να συναινέσουν σε αυτό [84]. Οι ΕΠ μπορούν να συνδεθούν με έναν συγκεκριμένο προμηθευτή, για παράδειγμα, όταν υπάρχει μόνο μία εταιρεία για μια συγκεκριμένη τεχνολογία ή όταν η αλλαγή προμηθευτή είναι πολύ δαπανηρή ή ανέφικτη [84]. Παρά ταύτα, η ανισορροπία στη συμβατική ισχύ ενός ‘’μικρότερου’’ υπεύθυνου επεξεργασίας σε σχέση με μεγάλους παρόχους υπηρεσιών δεν θα πρέπει να αποτελεί δικαιολογία για τον υπεύθυνο επεξεργασίας να αποδεχθεί ρήτρες και όρους συμβάσεων που δεν συμμορφώνονται με τη νομοθεσία περί προστασίας δεδομένων, ούτε μπορεί να απαλλάξει τον εκτελούντα την επεξεργασία από τις υποχρεώσεις προστασίας δεδομένων [85]. Οποιαδήποτε προτεινόμενη τροποποίηση, από τον εκτελούντα την επεξεργασία, των συμφωνιών επεξεργασίας δεδομένων που περιλαμβάνονται σε τυπικούς όρους και προϋποθέσεις θα πρέπει να κοινοποιείται απευθείας στον υπεύθυνο επεξεργασίας και να εγκρίνεται από αυτόν, λαμβάνοντας υπόψη το περιθώριο δράσης που διαθέτει ο εκτελών την επεξεργασία σε σχέση με μη ουσιώδη στοιχεία των μέσων επεξεργασίας [85].

Τον πρωταρχικό ρόλο έχουν όμως στο περιβάλλον των ΕΠ έχουν εντέλει οι ίδιοι οι κάτοικοι αυτής στην πλειοψηφία των περιπτώσεων, οι οποίοι στο πλαίσιο του ΓΚΠΔ έχουν την ιδιότητα των υποκειμένων των δεδομένων. Όπως επισημάνθηκε σχετικά, οι πολίτες μπορούν να έχουν τον έλεγχο των δεδομένων τους εφόσον τους παρέχονται επαρκείς πληροφορίες, σε διαφορετική περίπτωση, εφόσον οι ίδιοι δεν δείχνουν να ενδιαφέρονται, είναι φυσικό επακόλουθο ούτε οι τεχνολογικές εταιρίες-εκτελούντες την επεξεργασία να επιδείξουν ανάλογη ενδιαφέρον [84]. Σήμερα ωστόσο, κυριαρχεί η άποψη ότι, παρόλο που οι πολίτες ενδιαφέρονται για τα

προσωπικά τους δεδομένα, αισθάνονται αδύναμοι να ελέγξουν τον τρόπο με τον οποίο επεξεργάζονται από τρίτους, μια κατάσταση η οποία στη βιβλιογραφία αναφέρεται ως παραίτηση από την ιδιωτικότητα (privacy resignation) [86].

Οι κάτοικοι μιας πόλης πρέπει να είναι σε θέση να εξασκούν τα δικαιώματα που τους παρέχονται από τον ΓΚΠΔ και τα οποία προβλέπονται στα άρθρα 12 έως 22[34]. Ωστόσο, όπως αναφέρθηκε και ανωτέρω, από κοινού υπεύθυνοι επεξεργασίας δεδομένων αυξάνουν τον αριθμό των σημείων επαφής που απαιτούνται για την άσκηση των δικαιωμάτων των υποκειμένων των δεδομένων, ενώ τυχόν ρόλοι τρίτων μερών στον ''κύκλο'' επεξεργασίας προσωπικών δεδομένων, οι οποίοι είτε δεν καταγράφονται, είτε καταγράφονται περιορισμένα και δίχως σαφήνεια έχουν αρνητικό αντίκτυπο στην κατανομή των ευθυνών και στον μετριασμό των κινδύνων [82].

Ένα σχετικά απλό αλλά σημαντικό παράδειγμα [82] για την άσκηση των δικαιωμάτων του υποκειμένου μπορεί να καταδείξει τη σημασία που έχει το υποκείμενο των δεδομένων να εξασκεί αποτελεσματικά τα δικαιώματά του. Σε ένα έργο για παροχή μιας υπηρεσίας η διοίκηση της πόλης και μια ιδιωτική εταιρία συμπράττουν και λειτουργούν ως από κοινού υπεύθυνοι επεξεργασίας, εκτελώντας από κοινού τις υποχρεώσεις συμμόρφωσης με τον ΓΚΠΔ, όπως για παράδειγμα να γνωστοποιήσουν τα στοιχεία επικοινωνίας τους. Εν συνεχεία, η υποδομή του πρώτου έργου επαναχρησιμοποιείται για ένα άλλο αρκετά περεμφερές έργο, αλλά εδώ η πόλη δεν είναι πλέον υπεύθυνος επεξεργασίας. Τον ρόλο αυτόν έχει μια ιδιωτική εταιρία που χρησιμοποιεί την υποδομή του πρώτου έργου, η οποία οφείλει να δημιουργήσει ένα νέο σημείο επαφής για δικαιώματα υποκειμένου των δεδομένων. Από τη σκοπιά του ΓΚΠΔ οι ευθύνες για την τήρηση των διατάξεων του σχετικά με τα δικαιώματα των υποκειμένων των δεδομένων ανήκουν στον υπεύθυνο επεξεργασίας, από την άποψη όμως του υποκειμένου των δεδομένων και των δικαιωμάτων του, αυτή η προσέγγιση μπορεί να μην είναι η βέλτιστη καθώς το ίδιο το υποκείμενο θεωρήσει ως σημείο επαφής τα στοιχεία του προηγούμενου έργου. Κι ενώ θα ήταν λογικό να υπάρχει ένα σημείο επαφής για όλα τα ζητήματα προστασίας δεδομένων σε μια πόλη από την

[34] Πρόκειται για τα δικαιώματα ενημέρωσης, πρόσβασης, διόρθωσης, διαγραφής, περιορισμού της επεξεργασίας, φορητότητας των δεδομένων, εναντίωσης, δικαίωμα στη μη αυτοματοποιημένη λήψη αποφάσεων.

άποψη του υποκειμένου των δεδομένων, αυτό θα ερχόταν σε αντίθεση με όσα ορίζονται στον Κανονισμό.

Το πρόβλημα αυτό εντείνεται στο πλαίσιο του IoT, το οποίο αποτελεί βασικό εργαλείο για να καταστεί μια πόλη έξυπνη, καθώς η άσκηση των δικαιωμάτων των υποκειμένων φαίνεται να είναι ιδιαίτερα περίπλοκη έως και απρόσιτη. Πιο συγκεκριμένα, μέσα στο περιβάλλον IoT, τις περισσότερες φορές είναι ασαφές ποιος έχει το δικαίωμα πρόσβασης και συλλογής δεδομένων από διαφορετικές συσκευές και γενικά διεξαγωγής οποιασδήποτε μορφής επεξεργασίας [87]. Επιπλέον, είναι αντιστοίχως ασαφές για τα υποκείμενα των δεδομένων να ασκήσουν τα δικαιώματά τους, λόγω του γεγονότος της μη γνώσης του περιεχομένου των δεδομένων, του είδους της επεξεργασίας και του υπευθύνου και του εκτελούντος την επεξεργασία δεδομένων[87]. Για το λόγο αυτό, είναι πολύ σημαντικό σε ένα τόσο περίπλοκο πλαίσιο, η υποχρέωση του υπεύθυνου επεξεργασίας δεδομένων να ενημερώνει τα υποκείμενα των δεδομένων με όλα τα απαραίτητα στοιχεία που θέτει ο ΓΚΠΔ.

6.2. ΝΟΜΙΜΟΤΗΤΑ ΕΠΕΞΕΡΓΑΣΙΑΣ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΗΝ ΕΞΥΠΝΗ ΠΟΛΗ

Η νομιμότητα, η οποία στον ΓΚΠΔ αναφέρεται στο άρθρο 5 παρ. 1 είναι μια από τις θεμελιώδεις αρχές που διέπουν την επεξεργασία των προσωπικών δεδομένων, προσδιορίζεται στο άρθρο 6 του ΓΚΠΔ «Νομιμότητα της επεξεργασίας», όπου θεσπίζονται έξι νόμιμοι λόγοι [35]για την επεξεργασία δεδομένων προσωπικού

[35] Αρ. 6 ΓΚΠΔ Η επεξεργασία είναι σύννομη μόνο εάν και εφόσον ισχύει τουλάχιστον μία από τις ακόλουθες προϋποθέσεις: α) το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς, β) η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης, γ) η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας, δ) η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου, ε) η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας, στ) η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί.

χαρακτήρα (γνωστοί και ως νομικές βάσεις). Για να είναι νόμιμη η επεξεργασία μία από τις έξι νομικές βάσεις πρέπει να προσδιορίζεται και να εφαρμόζεται έγκυρα στη συγκεκριμένη πράξη επεξεργασίας. Η νομιμότητα συνδέεται επίσης στενά με τις αρχές της αντικειμενικότητας και της διαφάνειας, κάτι που αποδεικνύεται από το γεγονός ότι και οι τρεις περιλαμβάνονται μαζί στο άρθρο 5 παράγραφος 1 στοιχείο α του ΓΚΠΔ.

Προκειμένου να εξετάσουμε ποια η είναι η καταλληλότερη νομική βάση στην οποία μπορεί να στηριχθεί η επεξεργασία των προσωπικών δεδομένων στο πλαίσιο των δραστηριοτήτων μιας ΕΠ πρέπει να ληφθούν υπόψη ορισμένα χαρακτηριστικά όπως τα εξής: Με τη χρήση έξυπνων συσκευών στο πλαίσιο του IoT (κάμερες, αισθητήρες κλπ) η συλλογή των δεδομένων λαμβάνει χώρα πλέον σε μεγάλο βαθμό, τα δε έργα έξυπνων πόλεων ουσιαστικά συνδέουν τη χρήση των δημόσιων χώρων με τη συλλογή και την επεξεργασία προσωπικών πληροφοριών για τους πολίτες [88]. Η μετατροπή της παροχής των κλασικών υπηρεσιών (όπως είναι οι αστικές μετακινήσεις, η διαχείριση των απορριμμάτων μιας πόλης ή οι ασφαλέστερες συνθήκες διαβίωσης) σε ''έξυπνες'' με τη χρήση των μέσων της τεχνολογίας, δημιουργεί μια ανισορροπία μεταξύ των κατοίκων της πόλης και των αρχών αυτής ως υπευθύνων επεξεργασίας, καθώς οι κάτοικοι εξαρτώνται από τους τελευταίους για την πρόσβασης σε αυτές τις υπηρεσίες [89]. Παράλληλα, στο πλαίσιο της ΕΠ εκτός από έργα που δρομολογούνται από τους δήμους, πραγματοποιείται μια σειρά πρωτοβουλιών από τρίτους, οι οποίοι επιδιώκουν ιδιωτικούς-εμπορικούς σκοπούς και δεν έχουν κανενός είδους σχέση με τις αρχές της πόλης, και οι οποίες (πρωτοβουλίες τρίτων) πρέπει να ληφθούν υπόψη, καθώς αποτελούν μέρος ενός αυξημένου ελέγχου κάτω από τον οποίο βρίσκονται οι κάτοικοι των πόλεων στη σύγχρονη πόλη [89].

Α. ΣΥΓΚΑΤΑΘΕΣΗ

Η συγκατάθεση στον ΓΚΠΔ ορίζεται *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[36]. Ειδικότερα, ελεύθερη συγκατάθεση υπάρχει μόνο εάν το πρόσωπο στο οποίο αναφέρονται τα δεδομένα είναι σε θέση να έχει πραγματική επιλογή και δεν υπάρχει κίνδυνος εξαπάτησής, εκφοβισμού, εξαναγκασμού ή σημαντικών αρνητικών επιπτώσεων εάν δεν δώσει τη συγκατάθεσή του [90]. Περαιτέρω στην αιτιολογική σκέψη 43 του ΓΚΠΔ επισημαίνεται σαφώς ότι είναι απίθανο να μπορούν δημόσιες αρχές να βασιστούν στη συγκατάθεση για την επεξεργασία δεδομένων, καθώς, όταν ο υπεύθυνος επεξεργασίας είναι δημόσια αρχή, διαπιστώνεται συχνά σαφής ανισορροπία ισχύος στη σχέση μεταξύ υπευθύνου επεξεργασίας και υποκειμένου των δεδομένων. Είναι επίσης σαφές ότι στις περισσότερες περιπτώσεις το υποκείμενο των δεδομένων δεν έχει ρεαλιστικές εναλλακτικές δυνατότητες πέραν της αποδοχής (των όρων) της επεξεργασίας του συγκεκριμένου υπευθύνου επεξεργασίας. Τα στοιχεία αυτά αντικατοπτρίζονται και στη σχέση μεταξύ των αρχών διοίκησης μιας πόλης και του κατοίκου αυτής, καθώς η έξυπνη πόλη συνεπάγεται έναν πατερναλιστικό ρόλο για την τοπική διοίκηση να χρησιμοποιεί τα δεδομένα ως μέσο για να την υποστηρίξει στους στόχους της [91].

Ένα ακόμη στοιχείο της έννοιας της συγκατάθεσης το οποίο τίθεται σε αμφισβήτηση είναι αυτό της πλήρους επίγνωσης. Στο δημόσιο χώρο η παρουσία αισθητήρων είναι πραγματικά όχι μόνο πανταχού παρούσα αλλά και τόσο προσαρμοσμένη σε αυτό, που δύσκολα μπορούν να γίνουν αντιληπτοί από τα υποκείμενα. Δεδομένα συλλέγονται από τους πολλαπλούς αισθητήρες που είναι εγκατεστημένοι στο δρόμο, συμπεριλαμβανομένων καμερών, αισθητήρων ήχου, παρακολούθησης WiFi, οι οποίοι έχουν τη δυνατότητα να μετρούν πόσα άτομα περνούν από το δρόμο την ημέρα, πώς κινούνται, από πού προέρχονται, την προέλευση και το είδος του ήχου [92]. Το γεγονός ωστόσο ότι τα υποκείμενα τις περισσότερες φορές δεν είναι σε θέση να αντιληφθούν την ύπαρξη και λειτουργία αυτών, καθώς οι ίδιες αυτές συνδεδεμένες συσκευές προορίζονται να είναι διακριτικές και να συνδυάζονται με το περιβάλλον [318], αφαιρεί το στοιχείο της διαφάνειας που απαιτείται για να είναι η συγκατάθεση έγκυρη. Για να θεωρηθεί η συγκατάθεση εν επιγνώσει, το υποκείμενο

[36] Αρ. 4 παρ. 11 ΓΚΠΔ

των δεδομένων θα πρέπει να γνωρίζει τουλάχιστον την ταυτότητα του υπευθύνου επεξεργασίας και τους σκοπούς της επεξεργασίας για την οποία προορίζονται τα δεδομένα προσωπικού χαρακτήρα. Η συγκατάθεση δεν θα πρέπει να θεωρείται ότι δόθηκε ελεύθερα αν το υποκείμενο των δεδομένων δεν έχει αληθινή ή ελεύθερη επιλογή ή δεν είναι σε θέση να αρνηθεί ή να αποσύρει τη συγκατάθεσή του χωρίς να ζημιωθεί[37]. Αυτές οι πληροφορίες ωστόσο πρέπει να είναι άμεσα διαθέσιμες πριν από τη συλλογή των δεδομένων, και μάλλον φαίνεται εξαιρετικά δύσκολο στο αστικό περιβάλλον και στην πολυάσχολη ζωή, πως οι κάτοικοι θα μπορούσαν να ενημερώνονται με τις απαιτούμενες πληροφορίες και να παρέχουν τη συγκατάθεσή τους σύμφωνα με τις απαιτήσεις του ΓΚΠΔ. Αλλά ακόμη και να μπορούσε να υπάρξει μιας μορφής ενημέρωσης, για παράδειγμα με τη χρήση QR codes [91], το IoT όπως αναπτύσσεται μέσα στην ΕΠ συνεπάγεται ότι οποιαδήποτε συναίνεση λαμβάνεται «σχεδόν πάντα θα είναι φαινομενική ή στην καλύτερη περίπτωση χαμηλής ποιότητας όσον αφορά τη νομική απαίτηση της ΕΕ για ελεύθερα δεδομένη, συγκεκριμένη και ρητή συναίνεση [88].

Β. ΔΗΜΟΣΙΟ ΣΥΜΦΕΡΟΝ

Καθώς η νομική βάση της συγκατάθεσης φαίνεται να μην είναι ιδιαίτερα κατάλληλη σε όλες τις περιπτώσεις χρήσιμο είναι να εξετάσουμε μια άλλη νομική βάση που αναφέρεται στο άρθρο παρ. 6 στ. ε του ΓΚΠΔ και έχει ως εξής: *η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας*. Όταν η επεξεργασία είναι αναγκαία για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας, η επεξεργασία θα πρέπει να έχει βάση στο δίκαιο της Ένωσης ή κράτους μέλους. Αν και αυτή η νομική βάση αφορά κυρίως τις δημόσιες αρχές, οι ιδιωτικοί φορείς ως υπεύθυνοι επεξεργασίας θα μπορούσαν επίσης να τον εφαρμόσουν σε κατάλληλες περιστάσεις, καθώς είναι δυνατόν σε ορισμένες περιπτώσεις, δημόσιοι και ιδιωτικοί οργανισμοί να μπορούν να εφαρμόσουν από κοινού υπηρεσίες που ενδέχεται να απαιτούν επεξεργασία δεδομένων προσωπικού χαρακτήρα για λόγους δημοσίου

[37] Αιτ. σκ. 42 ΓΚΠΔ

συμφέροντος [93][38]. Αν και η διάταξη έχει ένα ιδιαίτερα ευρύ πεδίο εφαρμογής, υπάρχουν δύο περιορισμοί στην εγκυρότητά της όσον αφορά την επεξεργασία προσωπικών δεδομένων στις ΕΠ: πρώτον, η επεξεργασία πρέπει να είναι αναγκαία και δεύτερον να έχει βάση στο ενωσιακό ή εθνικό δίκαιο.

Αναφορικά με την έννοια της αναγκαιότητας, στην απόφαση Huber[39], μια απόφαση που αφορούσε τη νομική βάση του «δημόσιου καθήκοντος», η αναγκαιότητα κατανοήθηκε ως «η ανάγκη για έναν άρρηκτο δεσμό μεταξύ του σκοπού και της διαδικασίας επεξεργασίας». Υπό αυτό το πρίσμα, η αναγκαιότητα στο πλαίσιο της νομικής βάσης του «δημόσιου καθήκοντος» θα μπορούσε να είναι ιδιαίτερα εκτεταμένη, επειδή τα προσωπικά δεδομένα και οι τεχνολογίες επεξεργασίας θα μπορούσαν να χρησιμοποιηθούν ως μέσο για τη βελτιστοποίηση σχεδόν των πάντων [89]. Το κατά πόσο είναι αναγκαία η επεξεργασία προσωπικών δεδομένων προς την εκπλήρωση δημόσιου καθήκοντος, όπως ο όρος αναγκαία προσδιορίζεται και στο α. 52 του ΕΧΘΔ[40] μπορεί να κριθεί με βάση τον έλεγχο αναγκαιότητας ο οποίος λαμβάνει υπόψη του τα εξής κριτήρια, όπως αυτά έχουν διαμορφωθεί και από τον ΕΕΠΔ[41]:

-Λεπτομερής πραγματική περιγραφή του μέτρου που προβλέπει την επεξεργασία δεδομένων προσωπικού χαρακτήρα και των σκοπών του,

-Ο προσδιορισμός των θεμελιωδών δικαιωμάτων που ενδέχεται να περιοριστούν ως αποτέλεσμα του μέτρου επεξεργασίας,

---

[38] Βλ. σχετικά αιτ. σκ. 45 ΓΚΠΔ, όπου μεταξύ άλλων αναφέρεται ότι ''…. Επίσης, θα πρέπει να εναπόκειται στο ενωσιακό δίκαιο ή στο δίκαιο των κρατών μελών ο καθορισμός του κατά πόσον ο υπεύθυνος επεξεργασίας που εκπληρώνει καθήκον που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας θα πρέπει να είναι δημόσια αρχή ή άλλο φυσικό ή νομικό πρόσωπο που διέπεται από το δημόσιο δίκαιο ή, σε περίπτωση που αυτό δικαιολογείται από λόγους δημόσιου συμφέροντος, μεταξύ άλλων για λόγους υγείας, όπως η δημόσια υγεία και η κοινωνική προστασία και η διαχείριση των υπηρεσιών υγειονομικής περίθαλψης, από το ιδιωτικό δίκαιο, όπως μία επαγγελματική οργάνωση.

[39] *Huber* (CJEU, Case C-362/14; 6.10.2015)

[40] Αρ. 52 παρ. 1 ΧΘΔΕΕ ''Κάθε περιορισμός στην άσκηση των δικαιωμάτων και ελευθεριών που αναγνωρίζονται στον παρόντα Χάρτη πρέπει να προβλέπεται από το νόμο και να σέβεται το βασικό περιεχόμενο των εν λόγω δικαιωμάτων και ελευθεριών. Τηρουμένης της αρχής της αναλογικότητας, περιορισμοί επιτρέπεται να επιβάλλονται μόνον εφόσον είναι αναγκαίοι και ανταποκρίνονται πραγματικά σε στόχους γενικού ενδιαφέροντος που αναγνωρίζει η Ένωση ή στην ανάγκη προστασίας των δικαιωμάτων και ελευθεριών των τρίτων.''

[41] EDPS, 'Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit' (2017).

-Λεπτομερής εξέταση του σκοπού του μέτρου. Ως μέρος αυτού του βήματος, ο ΕΕΠΔ τονίζει την ανάγκη να επιδειχθεί ένας θεμιτός στόχος που συμβάλλει στην επίλυση ενός πραγματικού και όχι ενός υποθετικού προβλήματος, η ύπαρξη του οποίου βασίζεται σε αντικειμενικά στοιχεία,

-Η επιλογή να είναι πραγματικά αποτελεσματική και όσο το δυνατόν λιγότερο επεμβατική. Αυτά τα βήματα απαιτούν από τις ρυθμιστικές αρχές να βρουν εναλλακτικά μέτρα που είναι «πραγματικά, επαρκή και αποτελεσματικά σχετικά με το πρόβλημα που πρέπει να αντιμετωπιστεί» ώστε να επιλέξουν στη συνέχεια το λιγότερο παρεμβατικό.

Περαιτέρω, η επεξεργασία, εκτός από αναγκαία θα πρέπει να είναι και αναλογική. Σύμφωνα με πάγια νομολογία του ΔΕΕ, «η αρχή της αναλογικότητας απαιτεί οι πράξεις των θεσμικών οργάνων της ΕΕ να είναι κατάλληλες για την επίτευξη των θεμιτών στόχων που επιδιώκει η επίμαχη νομοθεσία και να μην υπερβαίνουν τα όρια του ενδεδειγμένου και αναγκαίου για την επίτευξη αυτούς τους στόχους». Ως εκ τούτου, περιορίζει τις αρχές κατά την άσκηση των εξουσιών τους απαιτώντας την επίτευξη ισορροπίας μεταξύ των μέσων που χρησιμοποιήθηκαν και του επιδιωκόμενου στόχου (ή του αποτελέσματος που επιτεύχθηκε) [94.

Περαιτέρω στο άρθρο 6 παρ. 3 του ΓΚΠΔ προβλέπεται ότι *Η βάση για την επεξεργασία που αναφέρεται στην παράγραφο 1 στοιχεία γ) και ε) ορίζεται σύμφωνα με: α) το δίκαιο της Ένωσης, ή β) το δίκαιο του κράτους μέλος στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας.* Η απαίτηση αυτή για την ύπαρξη ενός (περαιτέρω) νόμου στην περίπτωση που η βάση της επεξεργασίας δεδομένων προσωπικού χαρακτήρα είναι η ύπαρξη δημόσιου συμφέροντος θα πρέπει να διαβάζεται υπό το πρίσμα ότι υποβάλλει την επεξεργασία σε νομιμότητα και μεγαλύτερη δυνατότητα δημοκρατικής εποπτείας και διαφάνειας [91]. Η νομική αυτή βάση δεν προϋποθέτει απαραιτήτως νομοθετική πράξη εγκεκριμένη από ένα κοινοβούλιο, αλλά θα πρέπει να είναι διατυπωμένη με σαφήνεια και ακρίβεια και η εφαρμογή της να είναι προβλέψιμη για πρόσωπα που υπόκεινται σε αυτό, σύμφωνα με τη νομολογία του Δικαστηρίου της Ευρωπαϊκής Ένωσης (το Δικαστήριο) και του Ευρωπαϊκού Δικαστηρίου των Δικαιωμάτων του Ανθρώπου[42]. Η ευελιξία σχετικά με το είδος των

[42] Αιτ. σκ. 41 ΓΚΠΔ

απαιτούμενων νομικών κανόνων συνοδεύεται από μια προειδοποίηση [91]: την απαίτηση «προσβασιμότητας» που διαμορφώνεται από τη νομολογία του ΕΔΔΑ ως μέρος των θεμάτων που πρέπει να αξιολογούνται κατά την εξέταση εάν μια παρέμβαση είναι «σύμφωνη με το νόμο». Ο νόμος πρέπει να είναι επαρκώς προσβάσιμος στον πολίτη, πράγμα που σημαίνει ότι τα μέτρα που δεν δημοσιεύονται ή δεν γίνονται με άλλο τρόπο γνωστά δεν μπορούν να θεωρηθούν ως «νόμος».

Περαιτέρω, το α. 6 παρ. 3 του ΓΚΠΔ παρέχει καθοδήγηση ως προς το τι θα μπορούσαν να ρυθμίσουν οι εξωτερικές νομικές βάσεις ΕΕ/κράτους μέλους, όπου μεταξύ άλλων, αναφέρεται ότι μπορεί να περιέχουν ειδικές διατάξεις που διέπουν τη νομιμότητα της επεξεργασίας, τον περιορισμό του σκοπού, τους τύπους δεδομένων που μπορούν να υποβληθούν σε επεξεργασία, σε ποιον και για ποιον σκοπό μπορούν να αποκαλυφθούν τα δεδομένα, την περίοδο αποθήκευσης και μέτρα για τη διασφάλιση σύννομης και θεμιτής επεξεργασία. Η πρόβλεψη αυτή συνδέεται στενά με το χαρακτηριστικό της προβλεψιμότητας που πρέπει να διέπει την εκάστοτε νομική βάση. Εν προκειμένω, στην περίπτωση της επεξεργασίας προσωπικών δεδομένων προς το συμφέρον της ΕΠ, παρατηρείται ότι οι αρχές αυτής καταφεύγουν σε σύνθετες μορφές, κάποιες φορές και πολύ επεμβατικές, με μόνη νομική βάση μια διάταξη η οποία είναι απολύτως γενική στη διατύπωσή της, δεν περιορίζει επαρκώς τη διακριτική ευχέρεια των δημόσιων αρχών να επεξεργάζονται δεδομένα προσωπικού χαρακτήρα μόνο όπου είναι απαραίτητο και αναλογικό, ενώ ταυτόχρονα δεν παρέχει σαφή κατανόηση στα ενδιαφερόμενα άτομα ως προς τις επιπτώσεις που μπορεί να έχουν [K89]. Προκειμένου οι εν λόγω νομικές βάσεις να μην υπολείπονται του στοιχείου της προβλεψιμότητας, ειδικά στο περιβάλλον των ΕΠ όπου είναι εξαιρετικά επικίνδυνο να συλλέγονται πολύ περισσότερα δεδομένα από τα εντελώς απαραίτητα ή αυτά να χρησιμοποιούνται για την επεξεργασία περισσότερων σκοπών από αυτών που είχαν αρχικά συλλεχθεί και εν συνεχεία να διακυβεύονται και θεμελιώδη δικαιώματα των κατοίκων, κρίνεται σκόπιμο οι συγκεκριμένες νομικές διατάξεις να είναι υποχρεωτικό να περιλαμβάνουν τα επιπλέον στοιχεία που προβλέπονται στο α. 6 παρ. 3 του ΓΚΠΔ. Η ομάδα εργασίας του WP29 έχει πράγματι επιβεβαιώσει ότι οι εκτεταμένες παρεμβάσεις στα θεμελιώδη δικαιώματα (όπως αυτή που πιθανώς συμβαίνει στην έξυπνη πόλη, όπου η επεξεργασία είναι συχνά «υψηλού κινδύνου»), η νομική βάση θα πρέπει να είναι

αρκετά συγκεκριμένη και ακριβής, ορίζοντας το είδος της επεξεργασίας δεδομένων που μπορεί να επιτρέπεται [95].

Γ. ΕΝΝΟΜΟ ΣΥΜΦΕΡΟΝ

Μία άλλη νομική βάση στην οποία θα μπορούσε να στηριχθεί η επεξεργασία των προσωπικών δεδομένων στην ΕΠ και για την οποία δεν χρειάζεται μια περαιτέρω νομική διάταξη[43], είναι αυτή του α. 6 παρ. 1 περ. στ *σύμφωνα με την οποία η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα*. Αν και στο ανωτέρω ίδιο άρθρο διευκρινίζεται ότι *το στοιχείο στ) του πρώτου εδαφίου δεν εφαρμόζεται στην επεξεργασία που διενεργείται από δημόσιες αρχές κατά την άσκηση των καθηκόντων τους*, εντούτοις θα μπορούσε να θεωρηθεί ότι καταλείπεται ένα πεδίο εφαρμογής στις αρχές μιας πόλης, στην περίπτωση που δεν λαμβάνει χώρα άσκηση των καθηκόντων τους όπως στην περίπτωση των έργων που αναπτύχθηκαν από ερευνητικές κοινοπραξίες που περιλαμβάνουν πόλεις και άλλους φορείς, τα οποία στοχεύουν στην ανάπτυξη ή τη δοκιμή νέων τεχνολογιών. Σε ένα ερευνητικό πλαίσιο, θα μπορούσε να υποστηριχθεί ότι τα έννομα συμφέροντα θα μπορούσαν να χρησιμοποιηθούν ακόμη και για την επεξεργασία στην οποία εμπλέκονται οι τοπικές αρχές ως υπεύθυνοι επεξεργασίας ή από κοινού υπεύθυνοι επεξεργασίας, επειδή η επεξεργασία που εξυπηρετεί ερευνητικό ενδιαφέρον δεν εμπίπτει κανονικά στις δημόσιες λειτουργίες των τοπικών αρχών, όπως ορίζεται στη νομοθεσία [Κ89.] Αυτή η νομική βάση θα μπορούσε περαιτέρω να εξεταστεί και για την περίπτωση των δραστηριοτήτων εντός της ΕΠ τις οποίες διενεργούν ιδιωτικοί φορείς και όχι οι δημοτικές αρχές, όπως σε τεχνολογίες που επιτρέπουν την παρακολούθηση των κινήσεων και της συμπεριφοράς των περαστικών ή την αναγνώριση βασικών δημογραφικών χαρακτηριστικών, ακόμη και των συναισθημάτων και χρησιμοποιούνται σε δημόσιους και ημιδημόσιους χώρους για την επιδίωξη των συμφερόντων τους [89].

[43] Όπως απαιτείται στην περίπτωση του α. 6 παρ. 1 περ. ε του ΓΚΠΔ

Προκειμένου οι φορείς που επιθυμούν να προβούν σε επεξεργασία προσωπικών δεδομένων με βάση το έννομο συμφέρον θα πρέπει προηγουμένως να προβούν στην εξέταση των κατωτέρω: Αρχικά θα πρέπει ο υπεύθυνος επεξεργασίας να προσδιορίσει με ακρίβεια το έννομο συμφέρον και το σκοπό της επεξεργασίας των προσωπικών δεδομένων. Ακόμη και αν το ενδιαφέρον του υπεύθυνου επεξεργασίας για την επεξεργασία Προσωπικών Δεδομένων για συγκεκριμένο σκοπό είναι προφανές και νόμιμο, με βάση τους στόχους του υπεύθυνου επεξεργασίας, πρέπει να διατυπώνεται με σαφήνεια και να κοινοποιείται στο υποκείμενο των δεδομένων [96]. Εν συνεχεία θα πρέπει να γίνει έλεγχος αναγκαιότητας και να διαπιστωθεί ότι η επεξεργασία είναι αναπόφευκτη, αναγκαία και τίθενται με αυτή στοχευμένα και αναλογικά μέσα επεξεργασίας.

Τρίτο βήμα [96] είναι η διεξαγωγή ενός τεστ εξισορρόπησης, κατά το οποίο ο υπεύθυνος επεξεργασίας χρειάζεται να βασιστεί μόνο σε ένα γνήσιο έννομο συμφέρον , όπου τα δικαιώματα και οι ελευθερίες ενός υποκειμένου δεδομένων , του οποίου τα προσωπικά δεδομένα πρόκειται να επεξεργαστούν, δεν υπερτερούν του εννόμου συμφέροντος του υπευθύνου επεξεργασίας. Στη φάση αυτή πρέπει να ληφθούν υπόψη τα εξής:

-η φύση των εννόμων συμφερόντων, οι εύλογες προσδοκίες των υποκειμένων για επεξεργασία των δεδομένων τους, τα είδη των προσωπικών δεδομένων,

-ο αντίκτυπος της επεξεργασίας, όπως οι τυχόν θετικές ή αρνητικές επιπτώσεις στο άτομο, κατά πόσο δικαιολογείται η σοβαρότητα της επίπτωσης, η ιδιότητα του υποκειμένου των δεδομένων, η θέση του υπεύθυνου επεξεργασίας στην αγορά, το είδος της επεξεργασίας των δεδομένων, η επεξεργασία σε μεγάλη κλίμακα.

-οι διασφαλίσεις που θα μπορούσαν να τεθούν σε εφαρμογή και οι οποίες περιλαμβάνουν μια σειρά αντισταθμιστικών ελέγχων ή μέτρων για την προστασία του ατόμου ή για τη μείωση τυχόν κινδύνων ή δυνητικά αρνητικών επιπτώσεων της επεξεργασίας.

Αναφορικά με τη χρήση της νομικής βάσης για το έννομο συμφέρον αξίζει να σημειωθεί η απόφαση της ολλανδικής αρχής [97] για την καθοδήγησή αναφορικά με την παρακολούθηση Wi-Fi και Bluetooth, όπου έκρινε ότι η ικανότητα των ιδιωτικών εταιριών να βασίζονται σε έννομα συμφέροντα διαφέρει ανάλογα με το αν η παρακολούθηση πραγματοποιείται σε δημόσιο ή ημιδημόσιο χώρο. Θεωρεί ότι οι

ιδιωτικοί φορείς δεν έχουν εξουσία επί των δημόσιων χώρων, επομένως μόνο οι δημόσιες αρχές θα έχουν κανονικά το δικαίωμα να επεξεργάζονται δεδομένα προσωπικού χαρακτήρα από τέτοιους χώρους. Σε ημιδημόσιους χώρους που ανήκουν σε ιδιώτες, υπάρχει μεγαλύτερο περιθώριο να βασιστεί κανείς σε έννομα συμφέροντα, παρόλο που η αρχή εξακολουθεί να προτείνει ότι αυτό είναι δυνατό μόνο όταν ο στόχος του συστήματος παρακολούθησης δεν είναι εμπορικό αλλά στοχεύει στο να διασφαλίσει την ασφάλεια των περαστικών.

6.3. ΕΚΤΙΜΗΣΗ ΑΝΤΙΚΤΥΠΟΥ ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Με τον ΓΚΠΔ καθιερώνεται η αρχή της λογοδοσίας, σύμφωνα με την οποία ο υπεύθυνος επεξεργασίας είναι υπεύθυνος για την επεξεργασία των προσωπικών δεδομένων και πρέπει να αποδεικνύει τη συμμόρφωσή του με τις αρχές για την επεξεργασία δεδομένων προσωπικού χαρακτήρα του άρθρου 5 παράγραφος 1.2. Συνεπώς ο υπεύθυνος επεξεργασίας πρέπει να συμμορφώνεται με τις υποχρεώσεις του GDPR και αυτή η συμμόρφωση θα πρέπει επίσης να αποδεικνύεται. Για να αποδείξει υπευθυνότητα, ο υπεύθυνος επεξεργασίας πρέπει να εφαρμόσει κατάλληλα τεχνικά και οργανωτικά μέτρα[44] για την αντιμετώπιση των κινδύνων που εντοπίζονται σε μια διαδικασία αξιολόγησης κινδύνου. Υπάρχει επομένως μια στενή σχέση μεταξύ της έννοιας του κινδύνου και της έννοιας της λογοδοσίας, επειδή ο έλεγχος του κινδύνου υλοποιείται μέσω ενός νέου μοντέλου επιβεβλημένης αυτορρύθμισης [98].

Σκοπός αυτής της αρχής είναι να προστατευθούν τα φυσικά πρόσωπα από κινδύνους όχι μόνο έναντι του δικαιώματος της προστασίας της ιδιωτικής ζωής και των προσωπικών δεδομένων άλλα και έναντι άλλων θεμελιωδών δικαιωμάτων, όπως η ελευθερία του λόγου, η ελευθερία σκέψης και η απαγόρευση των διακρίσεων. Όταν οι κίνδυνοι για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων κρίνονται υψηλοί, προβλέπεται ότι πρέπει να διενεργείται εκτίμηση αντικτύπου (στην αγγλική Data Privacy Impact Assessment, εφεξής DPIA) σχετικά με την

[44] Αρ. 24 ΓΚΠΔ

προστασία των δεδομένων[45]και ενδεχομένως μια υποχρέωση για προηγούμενη διαβούλευση με την Αρχή Προστασίας Δεδομένων[46].

Καθώς νέες τεχνολογίες κάνουν την εμφάνισή τους και η επεξεργασία καθίσταται ολοένα και πιο πολύπλοκη, οι υπεύθυνοι επεξεργασίας πρέπει να αντιμετωπίζουν τους κινδύνους αυτούς εξετάζοντας τον ενδεχόμενο αντίκτυπο της σκοπούμενης επεξεργασίας προτού ξεκινήσουν την επεξεργασία. Εν προκειμένω, το Internet of Things, το οποίο αποτελεί σχεδόν το βασικότερο εργαλείο για να καταστεί μια πόλη ΄΄έξυπνη΄΄, έχει σημαντικό αντίκτυπο στην καθημερινή ζωή και το απόρρητο των ατόμων, και επομένως απαιτείται να διενεργηθεί DPIA [99]. Έτσι παρέχεται η δυνατότητα στους οργανισμούς να προσδιορίζουν, να αντιμετωπίζουν και να μετριάζουν τους κινδύνους εκ των προτέρων, περιορίζοντας σημαντικά το ενδεχόμενο αρνητικού αντικτύπου στα φυσικά πρόσωπα ως αποτέλεσμα της επεξεργασίας.

Διενεργώντας μια DPIA για την επεξεργασία προσωπικών δεδομένων στην ΕΠ παρουσιάζονται ορισμένες ειδικότερες προκλήσεις [98] οι οποίες πηγάζουν από τις ιδιαιτερότητες και την πολυπλοκότητα του περιβάλλοντος της ΕΠ και οι οποίες σχετίζονται με:

-Το πλήθος και την πολυπλοκότητα των θεμελιωδών δικαιωμάτων που διακυβεύονται στις έξυπνες πόλεις. Εκτός από το δικαίωμα προστασίας δεδομένων ενδέχεται να επηρεαστούν το δικαίωμα στην ισότητα ή το δικαίωμα στη χρηστή διοίκηση.

-Τη δυσκολία εκτίμησης των σωρευτικών επιπτώσεων που προκύπτουν από πολλαπλά έργα.

-Την έλλειψη διαφάνειας και την περιορισμένη συμμετοχή των πολιτών στην ανάπτυξη των έξυπνων πόλεων.

- Την εμπλοκή-συμμετοχή ιδιωτικών εταιρειών.

Σε μια μελέτη που πραγματοποιήθηκε για το κόστος μιας DPIA σχετικά με εφαρμογές στις ΕΠ, η οποία διενεργήθηκε στη βάση συνεντεύξεων με τους αρμόδιους για την εκτίμηση αντικτύπου σε έξυπνες πόλεις [101], ανέδειξε το στοιχείο της

[45] Αρ. 35 ΓΚΠΔ
[46]Αρ. 36 ΓΚΠΔ

πολυπλοκότητας τόσο του αστικού όσο και της παρεχόμενης ΄΄έξυπνης΄΄ υπηρεσίας. Ειδικότερα, η πολυπλοκότητα του αστικού περιβάλλοντος αποτελείται από τρία επίπεδα: i) το μέγεθος της πόλης, ii) την ποικιλομορφία των ενδιαφερομένων και iii) το σύνολο των παρεχόμενων έξυπνων υπηρεσιών σε μια συγκεκριμένη περιοχή. Αντίστοιχα, η πολυπλοκότητα της παρεχόμενης υπηρεσίας αποτελείται από πέντε επίπεδα: i) τον αριθμό διαφορετικών ροών δεδομένων, ii) τη σαφήνεια ως προς την ιδιοκτησία των δεδομένων, iii) τον αριθμό των περιπτώσεων χρήσης, iv) την παραβίαση της ιδιωτικής ζωής και v) τον έλεγχο της παρεχόμενης υπηρεσίας.

Η ολλανδική αρχή προστασίας προσωπικών δεδομένων, σε μια έκθεση που εξέδωσε τον Ιούλιο του 2021 [101] [47] σχετικά με την επεξεργασία των προσωπικών δεδομένων σε μια ΕΠ παρέθεσε ορισμένες περιπτώσεις στις οποίς η διενέργεια DPIA κρίνεται απαραίτητη:

-Σε μεγάλης κλίμακας επεξεργασία ή/και συστηματική παρακολούθηση προσωπικών δεδομένων που παράγονται από συσκευές συνδεδεμένες στο Διαδίκτυο που μπορούν να στείλουν ή να ανταλλάξουν δεδομένα μέσω Διαδικτύου ή με άλλο τρόπο (internet of things), όπως, για παράδειγμα, αισθητήρες που παρακολουθούν συστηματικά το κοινό στον δημόσιο χώρο.

---

[47] Πρόκειται για μια πολύ ενδιαφέρουσα έκθεση της Ολλανδικής Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, η οποία συνίσταται σε έρευνα που διεξήγαγε αναφορικά με το επίπεδο και τις δράσεις προστασίας προσωπικών δεδομένων και στην οποία συμμετείχαν ολλανδικές ΄΄έξυπνες πόλεις΄΄. Μεταξύ άλλων η εν λόγω αρχή κατέληξε στα εξής ενδιαφέροντα συμπεράσματα-διαπιστώσεις:

-Έλαβε ελάχιστες ή καθόλου DPIA από μικρότερους δήμους, γεγονός που εξηγείται είτε από το ότι οι συγκεκριμένοι δεν χρησιμοποιούν εφαρμογές έξυπνης πόλης ή χρησιμοποιούν μόνο εφαρμογές έξυπνων πόλεων στις οποίες δεν γίνεται επεξεργασία προσωπικών δεδομένων, είτε ότι πρόκειται για προηγούμενη επεξεργασία που είχε ήδη εφαρμοστεί πριν από το ΓΚΠΔ και που δεν άλλαξε με την έναρξη ισχύος του ΓΚΠΔ (παραδείγματα είναι οι εγγραφές πινακίδων για διάφορους σκοπούς, η παρακολούθηση με κάμερα σε δημόσιους χώρους κ.λπ.), είτε γιατί οι δήμοι αναφέρουν ότι οι κίνδυνοι των συγκεκριμένων έργων δεν χαρακτηρίζονται ως «υψηλοί» και, ως εκ τούτου, δεν απαιτείται DPIA, είτε γιατί οι εφαρμογές έξυπνων πόλεων ξεκίνησαν σε πιλοτική μορφή και δοκιμάζονται πριν την τελική κυκλοφορία τους. Ωστόσο εδώ σημειώνεται ότι τα προσωπικά δεδομένα υπόκεινται ήδη σε επεξεργασία ακόμη και σε πιλοτική φάση και ως εκ τούτου πρέπει να υπάρχει συμμόρφωση με τους κανόνες του ΓΚΠΔ, συμπεριλαμβανομένης της υποχρέωσης διεξαγωγής DPIA.

-Οι DPIA που έλαβε η αρχή αποδείχτηκαν διαφορετικού σχεδιασμού και ποιότητας μεταξύ τους, ακόμη και εντός του ίδιου δήμου. Η διαφορά στην ποιότητα ήταν εμφανής, για παράδειγμα, στην έλλειψη σαφούς ανάλυσης σχετικά με τις συνέπειες της επεξεργασίας στα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων και τις διασφαλίσεις που λαμβάνονται (ανά κίνδυνο) για τον περιορισμό των κινδύνων αυτών. Επίσης, δεν υπήρχε σε όλες τις περιπτώσεις σαφής περιγραφή της επεξεργασίας προσωπικών δεδομένων στην εφαρμογή μιας έξυπνης πόλης, αλλά γινόταν αναφορά μόνο στη λειτουργία αυτής.

-Κοινή χρήση προσωπικών δεδομένων εντός ή μέσω συνεργασιών στις οποίες δήμοι ή άλλες αρχές ανταλλάσσουν προσωπικά δεδομένα με άλλα δημόσια ή ιδιωτικά μέρη. Οι κόμβοι πληροφοριών είναι ένα παράδειγμα αυτού.
-Μεγάλης κλίμακας επεξεργασία ή/και συστηματική παρακολούθηση περιοχών προσβάσιμων από το κοινό με κάμερες, κάμερες web ή drones.
-Μεγάλης κλίμακας και/ή συστηματική χρήση ευέλικτης παρακολούθησης με κάμερα, όπως κάμερες σώματος.
-Μεγάλης κλίμακας επεξεργασία ή/και συστηματική παρακολούθηση δεδομένων τοποθεσίας από ή ανιχνεύσιμα σε φυσικά πρόσωπα. Για παράδειγμα, (σάρωση) αυτοκινήτων, τηλεφώνων ή επεξεργασία δεδομένων τοποθεσίας ταξιδιωτών στα μέσα μαζικής μεταφοράς.

Σχετικά με τη διενέργεια DPIA στο πλαίσιο των ΕΠ και λόγω της ιδιαιτερότητας αυτών θα μπορούσαν να φανούν εξαιρετικά χρήσιμες οι παρακάτω ενέργειες στις οποίες μπορούν να προβούν οι υπεύθυνοι επεξεργασίας. Η πρώτη αφορά τη δημοσίευση των εκτιμήσεων αντικτύπου, η οποία δεν αποτελεί νομική απαίτηση του ΓΚΠΔ αλλά επαφίεται στη διακριτική ευχέρεια του υπευθύνου επεξεργασίας, να τη δημοσιεύσει ολόκληρη ή μέρος αυτής. Ο σκοπός μιας τέτοιας διαδικασίας θα ήταν να βοηθήσει στην ενίσχυση της εμπιστοσύνης στις λειτουργίες επεξεργασίας του υπεύθυνου επεξεργασίας και στην ενίσχυση της λογοδοσίας και διαφάνειας, ιδιαίτερα μάλιστα στην περίπτωση όπου μια δημόσια αρχή διενεργεί ΕΑΠ [99]. Η δημοσίευση των DPIA για εφαρμογές έξυπνων πόλεων, πρέπει να επικροτείται ακριβώς επειδή οι εφαρμογές έξυπνων πόλεων χρησιμοποιούνται σε δημόσιο χώρο και πρέπει να παρέχονται περισσότερες πληροφορίες σχετικά με τα προσωπικά δεδομένα που υποβάλλονται σε επεξεργασία, την τεχνολογία που θα χρησιμοποιηθεί, τους πιθανούς κινδύνους της επεξεργασίας και τα μέτρα που λαμβάνονται για αυτό, συμβάλλοντας με αυτόν τον τρόπο στην εμπιστοσύνη για τις εφαρμογές που χρησιμοποιούνται [101]. Η πόλη του Σιάτλ για παράδειγμα διαθέτει ένα ολοκληρωμένο πρόγραμμα προστασίας απορρήτου που βασίζεται σε ένα βασικό σύνολο αρχών και πολιτικών απορρήτου και το οποίο καθορίζει με σαφήνεια τις υποχρεώσεις και τις απαιτήσεις των τμημάτων της πόλης σχετικά με το χειρισμό και τη χρήση δεδομένων, αναθέτοντας εσωτερικούς ρόλους για την υποστήριξη της

εφαρμογής τους[48]. Οι πολιτικές της πόλης επιβάλλουν τη δημοσίευση αξιολογήσεων επιπτώσεων στο απόρρητο και αναφορών σχετικά με τα προγράμματα της πόλης και τις πύλες ανοιχτών δεδομένων, καθώς και τη δημόσια δέσμευση για την εγκατάσταση τυχόν νέων τεχνολογιών επιτήρησης [102].

Η δεύτερη σύσταση προς τους υπεύθυνους επεξεργασίας και ειδικότερα στην περίπτωση που είναι αυτοί είναι οι δήμοι, είναι να ενθαρρύνουν τη συμμετοχή των πολιτών. *Στο α. 35 παρ. 9 του ΓΚΠΔ 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.* Η συμμετοχή των πολιτών ειδικά στις εφαρμογές των έξυπνων πόλεων θα πρέπει να είναι επιτακτική όταν η νομοθεσία παρέχει λιγότερο σαφές πλαίσιο σχετικά με την παραβίαση των δικαιωμάτων και ελευθεριών των υποκειμένων των δεδομένων, για παράδειγμα επειδή ο νόμος δεν καθορίζει συγκεκριμένα ποια δεδομένα μπορούν να υποβληθούν σε επεξεργασία και ποιες εγγυήσεις πρέπει να ληφθούν [K325]. Επιπλέον, η παρακολούθηση της ανθρώπινης συμπεριφοράς με τη χρήση εφαρμογών έξυπνης πόλης μπορεί, για παράδειγμα και να οδηγήσει σε ένα αρκετά άβολο αποτέλεσμα, το λεγόμενο chilling effect, με αποτέλεσμα οι άνθρωποι να συμπεριφέρονται εσκεμμένα διαφορετικά ή να μην τολμούν πλέον να χρησιμοποιήσουν το δημόσιο χώρο [325].

6.4. Η ΑΡΧΗ ΤΟΥ ΠΕΡΙΟΡΙΣΜΟΥ ΤΟΥ ΣΚΟΠΟΥ ΕΠΕΞΕΡΓΑΣΙΑΣ

Στο α. 5 παρ. 1 στ. β του ΓΚΠΔ αποτυπώνεται μία από τις πιο θεμελιώδεις αρχές της επεξεργασίας των προσωπικών δεδομένων, αυτή του περιορισμού του σκοπού, προβλέποντας ότι τα προσωπικά δεδομένα συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς. Από τη διατύπωση του εν λόγω άρθρου προκύπτει ότι το πρώτο επιμέρους στοιχείο αφορά στον καθορισμό των σκοπών της επεξεργασίας, ο οποίος πρέπει να περιγράφεται με ακρίβεια το αργότερο μέχρι τη στιγμή της συλλογής των δεδομένων, ώστε να είναι απολύτως ευδιάκριτο τι εμπίπτει

[48] https://www.seattle.gov/tech/initiatives/privacy/privacy-program

και τι όχι στο πλαίσιο της συγκεκριμένης κάθε φορά επεξεργασίας. Το δεύτερο στοιχείο προσδιορισμού του σκοπού αφορά στο κριτήριο της σαφήνειας, και εννοείται ότι ο σκοπός επεξεργασίας πρέπει να διατυπώνεται με τέτοιο τρόπο, ώστε να εξασφαλίζεται ότι όλοι οι ενδιαφερόμενοι έχουν την ίδια αντίληψη και κατανόηση ως προς την αιτία, ανεξάρτητα από οποιαδήποτε πολιτισμική ή γλωσσική ποικιλομορφία [103]. Το τρίτο χαρακτηριστικό του προσδιορισμού του σκοπού έχει να κάνει με τη νομιμότητα. Η έννοια αυτή υπερβαίνει την απαίτηση να υπάρχει νομική βάση για την επεξεργασία σύμφωνα με το άρθρο 7 της οδηγίας και επεκτείνεται επίσης σε άλλους τομείς δικαίου, χρειάζεται δε να ερμηνεύεται στο πλαίσιο της επεξεργασίας, η οποία καθορίζει τις «εύλογες προσδοκίες» του υποκειμένου των δεδομένων [103]. Με το δεύτερο επιμέρους στοιχείο καθιερώνεται η απαίτηση της συμβατότητας του νέου σε σχέση με τον σκοπό της αρχικής συλλογής. Η απαγόρευση ασυμβίβαστης χρήσης θέτει περιορισμούς στην περαιτέρω χρήση. Απαιτεί να γίνεται διάκριση μεταξύ περαιτέρω χρήσης που είναι «συμβατή» και περαιτέρω χρήσης που είναι «ασύμβατη» και επομένως απαγορεύεται [103].

Για να εξακριβωθεί αν ο σκοπός της περαιτέρω επεξεργασίας είναι συμβατός με τον σκοπό της αρχικής συλλογής των δεδομένων προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας, εφόσον πληροί όλες τις απαιτήσεις για τη νομιμότητα της αρχικής επεξεργασίας, θα πρέπει να λάβει υπόψη, μεταξύ άλλων, τα εξής κριτήρια[49]:

-τυχόν συνδέσμους μεταξύ των σκοπών αυτών και των σκοπών της επιδιωκόμενης περαιτέρω επεξεργασίας. Ο σύνδεσμος αυτός δεν πρέπει να προκύπτει μόνο από μια αυστηρή γραμματική ερμηνεία του κειμένου, καθώς στην πραγματικότητα, μπορεί στην πράξη να έχει χρησιμοποιηθεί ένα μόνο περιορισμένο, εάν υπάρχει, κείμενο, αλλά θα πρέπει να εστιάσει κανείς στην ουσία της σχέσης μεταξύ των σκοπών συλλογής και των σκοπών περαιτέρω επεξεργασίας. Αυτό μπορεί να καλύπτει καταστάσεις όπου η περαιτέρω επεξεργασία είχε ήδη υπονοηθεί περισσότερο ή λιγότερο στους αρχικούς σκοπούς ή θεωρήθηκε ως λογικό επόμενο βήμα στην επεξεργασία σύμφωνα με αυτούς τους σκοπούς, καθώς και καταστάσεις όπου υπάρχει μόνο μερική ή ακόμη και ανύπαρκτη σύνδεση με τους αρχικούς σκοπούς. Σε κάθε περίπτωση, όσο μεγαλύτερη είναι η απόσταση μεταξύ των σκοπών συλλογής

[49] Όπως αυτά αναφέρονται στην αιτ. σκ. 50 του ΓΚΠΔ.

και των σκοπών περαιτέρω επεξεργασίας, τόσο πιο μεγάλο είναι το πρόβλημα που δημιουργείται για την αξιολόγηση της συμβατότητας [103].

- το πλαίσιο στο οποίο έχουν συλλεγεί τα δεδομένα προσωπικού χαρακτήρα, ιδίως τις εύλογες προσδοκίες του υποκειμένου των δεδομένων βάσει της σχέσης του με τον υπεύθυνο επεξεργασίας ως προς την περαιτέρω χρήση τους, δηλαδή με άλλα λόγια, για ποιον σκοπό θα περίμενε ένα άτομο να χρησιμοποιηθούν τα δεδομένα του με βάση το πλαίσιο της συλλογής. Στο σημείο αυτό πρέπει να ληφθεί υπόψη η φύση της σχέσης μεταξύ του υπεύθυνου επεξεργασίας και του υποκειμένου των δεδομένων, η οποία περιλαμβάνει την έρευνα για την ισορροπία δυνάμεων μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας δεδομένων [103]. Αυτό απαιτεί όχι μόνο επανεξέταση τυχόν νομικών δηλώσεων που έγιναν, αλλά και εξέταση της συνήθους και γενικά αναμενόμενης πρακτικής στο δεδομένο πλαίσιο και στη δεδομένη (εμπορική ή άλλη) σχέση [103]. Εν προκειμένω, εύκολα μπορεί να αντιληφθεί κανείς πόσο διαφορετική μπορεί να είναι η φύση της σχέσης μεταξύ υποκειμένου δεδομένων-υπεύθυνου επεξεργασίας, όταν υπεύθυνος επεξεργασίας στη μια περίπτωση είναι μία δημόσια αρχή και στην άλλη μια ιδιωτική εταιρία. Περαιτέρω, υπάρχει μεγάλη απόσταση μεταξύ ενός σκοπού που συνδέεται με εμπορικά συμφέροντα και ενός περαιτέρω σκοπού που συνδέεται με ένα δημόσιο συμφέρον, καθώς συνήθως, η νομιμότητα της επεξεργασίας για ιδιωτικά συμφέροντα προέρχεται κυρίως από τη συγκατάθεση ή στηρίζεται στο έννομο συμφέρον που επικαλείται ο υπεύθυνος επεξεργασίας, ενώ οι νομικές βάσεις δημοσίου συμφέροντος λειτουργούν διαφορετικά, απαιτώντας περαιτέρω θεμελίωση σε νόμο που οριοθετεί αυτά τα συμφέροντα [91]. Αυτό το νομικό και πραγματικό πλαίσιο θα έκανε τις μεταφορές δεδομένων από ιδιωτικές εταιρείες σε δημόσιες αρχές που θα χρησιμοποιηθούν για σκοπούς έξυπνης πόλης απροσδόκητες. Ένα παρόμοιο επιχείρημα μπορεί να προβληθεί για κοινή χρήση και περαιτέρω χρήση μεταξύ διαφορετικών δημόσιων αρχών. Ακόμη όμως και στην περίπτωση που τόσο ο υπεύθυνος επεξεργασίας όσο και ο αποδέκτης που λαμβάνει δεδομένα από τον πρώτο, με το υποκείμενο των δεδομένων έχουν σχέση μεταξύ πολίτη και δημόσιας αρχής, δεν θα πρέπει στο υποκείμενο των δεδομένων να δημιουργούνται εύλογες προσδοκίες ότι τα δεδομένα του μπορούν να κοινοποιηθούν και να επαναχρησιμοποιηθούν, λόγω δημοσίου συμφέροντος. Το δημόσιο συμφέρον

αποτελεί από μόνο του μια αόριστη έννοια και μπορεί να αναφέρεται από την ασφάλεια έως τα οικονομικά συμφέροντα, τη δημόσια υγεία, την κοινωνική ασφάλιση, την προστασία του περιβάλλοντος. Καθώς όμως οι δημόσιες αρχές ενεργούν με βάση συγκεκριμένες αρμοδιότητες, η σχέση τους με τους πολίτες, το είδος των προσωπικών δεδομένων που αναμένεται να επεξεργαστούν και οι σκοποί για τους οποίους προβαίνουν σε αυτήν την επεξεργασία μπορεί επίσης να διαφέρουν ουσιαστικά [91].

-τη φύση των δεδομένων προσωπικού χαρακτήρα και τον αντίκτυπο της περαιτέρω επεξεργασίας στα υποκείμενα των δεδομένων. Η φύση των δεδομένων που υποβάλλονται σε επεξεργασία διαδραματίζει κρίσιμο ρόλο, συνεπώς θα ήταν ημαντικό να αξιολογηθεί εάν η περαιτέρω επεξεργασία περιλαμβάνει ευαίσθητα δεδομένα, δεδομένου ότι όσο πιο ευαίσθητες είναι οι πληροφορίες που επεξεργάζονται, τόσο στενότερο θα είναι το πεδίο για συμβατή χρήση. Κατά την αξιολόγηση του αντίκτυπου της περαιτέρω επεξεργασίας, θα πρέπει να λαμβάνονται υπόψη τόσο οι θετικές όσο και οι αρνητικές συνέπειες., οι οποίες ενδέχεται να περιλαμβάνουν πιθανές μελλοντικές αποφάσεις ή ενέργειες τρίτων μερών και καταστάσεις όπου η επεξεργασία μπορεί να οδηγήσει στον αποκλεισμό ή τη διάκριση ατόμων [103][50]. Εκτός από τα δυσμενή αποτελέσματα που μπορούν να προβλεφθούν ειδικά, πρέπει επίσης να ληφθούν υπόψη συναισθηματικές επιπτώσεις, όπως π.χ. ο εκνευρισμός, ο φόβος και η αγωνία που μπορεί να προκύψουν από το γεγονός ότι ένα υποκείμενο των δεδομένων χάσει τον έλεγχο των προσωπικών πληροφοριών ή συνειδητοποιήσει ότι έχουν παραβιαστεί [103]. Συνεπώς όσο πιο γενικές κα απρόβλεπτες είναι οι συνέπειες τόσο πιο πιθανό είναι ο σκοπός να μη θεωρείται συμβατός, και για το λόγο αυτό θα πρέπει να αναζητηθούν εναλλακτικές μέθοδοι από τον υπεύθυνο επεξεργασίας.

[50] Ο σχετικός αντίκτυπος με ευρύτερη έννοια μπορεί επίσης να περιλαμβάνει τον τρόπο με τον οποίο τα δεδομένα υποβάλλονται σε περαιτέρω επεξεργασία: όπως εάν τα δεδομένα υποβάλλονται σε επεξεργασία από διαφορετικό υπεύθυνο επεξεργασίας σε άλλο πλαίσιο με άγνωστες συνέπειες, εάν τα δεδομένα αποκαλύπτονται δημόσια ή καθίστανται με άλλο τρόπο προσβάσιμα σε μεγάλο αριθμό προσώπων, ή εάν μεγάλος όγκος δεδομένων προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία ή συνδυάζονται με άλλα δεδομένα (π.χ. στην περίπτωση κατάρτισης προφίλ, για εμπορικούς σκοπούς ή για σκοπούς επιβολής του νόμου).

- τις διασφαλίσεις που εφαρμόζει ο υπεύθυνος επεξεργασίας για τη διασφάλιση της δίκαιης επεξεργασίας και την αποτροπή τυχόν αθέμιτων επιπτώσεων στα υποκείμενα των δεδομένων. Τυχόν κατάλληλα πρόσθετα μέτρα που έχει λάβει ο υπεύθυνος επεξεργασίας θα μπορούσαν, κατ' αρχήν, να χρησιμεύσουν ως «αποζημίωση» για αλλαγή σκοπού ή για το γεγονός ότι οι σκοποί δεν είχαν καθοριστεί τόσο ξεκάθαρα στην αρχή όσο θα έπρεπε [103]. Η εφαρμογή των κατάλληλων τεχνικών και οργανωτικών μέτρων από τους υπευθύνους επεξεργασίας σε όλα τα στάδια της επεξεργασίας αποτελεί πάντα υποχρεωτική νομική απαίτηση που απορρέει από την αρχή της λογοδοσίας, την προσέγγιση βάσει κινδύνου του κανονισμού και τη διατύπωση του άρθρου 25 του ΓΚΠΔ [91]. Αυτό μπορεί να απαιτήσει τεχνικά ή/και οργανωτικά μέτρα για τη διασφάλιση του λειτουργικού διαχωρισμού (όπως μερική ή πλήρη ανωνυμοποίηση, ψευδωνυμοποίηση και συγκέντρωση δεδομένων), αλλά και πρόσθετα μέτρα που λαμβάνονται προς όφελος των υποκειμένων των δεδομένων, όπως αυξημένη διαφάνεια, και η δυνατότητα του υποκειμένου να αντιταχθεί ή να παράσχει συγκεκριμένη συγκατάθεση. Οι συμβατικοί μηχανισμοί όπως οι συμφωνίες ή τα πρωτόκολλα κοινής χρήσης δεδομένων θεωρούνται καλή πρακτική και σημαντικό εργαλείο λογοδοσίας στο πλαίσιο του περιορισμού του σκοπού, επειδή οριοθετούν το σκοπό της κοινής χρήσης δεδομένων και υποβάλουν τον υπεύθυνο επεξεργασίας που λαμβάνει τα δεδομένα σε περιορισμούς χρήσης αυτών [91].

7. ΕΦΑΡΜΟΓΕΣ BIG DATA, ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ ΚΑΙ ΑΝΟΙΧΤΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΗΝ ΕΞΥΠΝΗ ΠΟΛΗ- ΠΩΣ ΕΠΗΡΕΑΖΟΥΝ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

7.1 ΠΡΟΚΛΗΣΕΙΣ ΣΧΕΤΙΚΑ ΜΕ ΤΑ BIG DATA ΚΑΙ ΤΑ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ

Είναι σαφές ότι η εφαρμογή των μεγάλων δεδομένων, εκτός από τη χρησιμότητα στο περιβάλλον των έξυπνων πόλεων (όπως αυτή περιγράφηκε ανωτέρω στο οικείο κεφάλαιο, υπό 5.1.) έχει επιπτώσεις στο απόρρητο, την προστασία δεδομένων και τα συναφή δικαιώματα των ατόμων – δικαιώματα που θα ενισχυθούν όταν εφαρμοστεί ο Γενικός Κανονισμός για την Προστασία Δεδομένων. Υπό το πρίσμα του ΓΚΠΔ, οι οργανισμοί θα πρέπει να είναι πιο υπεύθυνοι για το τι κάνουν με τα

προσωπικά δεδομένα, όταν αυτά συνδέονται επίσης με τα μεγάλα δεδομένα και την τεχνητή νοημοσύνη.

Μία από τις προκλήσεις είναι κατά πόσο είναι εφικτή η παροχή συναίνεσης. Έχει προταθεί ότι το λεγόμενο μοντέλο «ειδοποίησης και συναίνεσης», όπου ένας οργανισμός λέει στα υποκείμενα των δεδομένων τι πρόκειται να κάνει με τα δεδομένα τους, δεν είναι πρακτικό σε ένα πλαίσιο μεγάλων δεδομένων. Η αδιαφανής φύση της ανάλυσης που χρησιμοποιεί τεχνικές τεχνητής νοημοσύνης μπορεί να δυσκολέψει την παροχή ουσιαστικής συγκατάθεσης [110]. Επιπλέον η συγκατάθεση δίνει στους ανθρώπους μόνο μια επιλογή ναι/όχι στην αρχή, γεγονός που θεωρείται ασυμβίβαστο με την ανάλυση μεγάλων δεδομένων λόγω της τάσης της να βρίσκει νέες χρήσεις για δεδομένα, καθώς και επειδή κρίνεται ανεδαφική σε περιβάλλοντα όπου δεδομένα ‘’παρατηρούνται’’ και δεν έχουν προέλθει απευθείας από το υποκείμενο των δεδομένων.

Ωστόσο, υπάρχουν νέες προσεγγίσεις για τη συναίνεση που υπερβαίνουν το απλό δυαδικό μοντέλο. Μπορεί να υπάρχει μια διαδικασία βαθμιαίας συναίνεσης, στην οποία οι άνθρωποι μπορούν να συναινέσουν ή όχι σε διαφορετικές χρήσεις των δεδομένων τους σε όλη τη σχέση τους με έναν πάροχο υπηρεσιών, αντί να έχουν μια απλή δυαδική επιλογή στην αρχή. Για παράδειγμα, στο σημείο που μια εφαρμογή θέλει να χρησιμοποιήσει δεδομένα τοποθεσίας κινητού τηλεφώνου ή να μοιραστεί δεδομένα με τρίτο μέρος, μπορεί να ζητηθεί από τον χρήστη να δώσει τη συγκατάθεσή του [110].

Ομοίως, για περιπτώσεις στις οποίες τα δεδομένα χρήστη θα χρησιμοποιηθούν για σκοπούς πέρα από αυτούς που συλλέχθηκαν αρχικά, τα υποκείμενα των δεδομένων θα πρέπει να ενημερώνονται για τις τρέχουσες διαδικασίες διατήρησης και ανάλυσης αυτών των συνόλων δεδομένων. Ωστόσο, η επεξεργασία μεγάλων δεδομένων που βασίζεται σε τεχνητή νοημοσύνη/μηχανική μάθηση οδηγεί συχνά στον επαναπροσδιορισμό των δεδομένων. Η επάρκεια των παρεχόμενων πληροφοριών και στη συνέχεια η συνειδητή επιλογή αμφισβητείται επίσης από την ικανότητα και την τάση της ανάλυσης τεχνητής νοημοσύνης να εντοπίζει νέους συσχετισμούς μεταξύ των δεδομένων και να τα (ανα)ομαδοποιεί ή να δημιουργεί νέους τύπους και κατηγορίες δεδομένων και μερικές φορές χωρίς την προνοητικότητα του υπευθύνου επεξεργασίας [113]. Στην περίπτωση αυτή μάλλον η συγκατάθεση του υποκειμένου

δεν έχει αντίκρισμα ώστε να αποτελεί νόμιμη βάση για την επεξεργασία των δεδομένων.

Μία ακόμη πρόκληση προκύπτει από την άνιση πρόσβαση στα δεδομένα και την τεχνογνωσία της επιστήμης των δεδομένων, κατάσταση που απειλεί να περιορίσει τα δικαιώματα και τις ελευθερίες σε ένα ευρύτερο κοινωνικοοικονομικό πλαίσιο. Αυτό το φαινόμενο ισχύει σε όλους τους τομείς και ισχύει εξίσου και για τα άτομα και τους οργανισμούς. Οι περιθωριοποιημένοι πολίτες και οι παραδοσιακά αποδυναμωμένες δημογραφικές ομάδες έχουν λιγότερη πρόσβαση στα δεδομένα (και τα οφέλη τους) από εκείνους που διαθέτουν καλύτερους πόρους και εκπαίδευση [114]. Κάτι παρόμοιο συμβαίνει και με εταιρείες που έχουν πρόσβαση σε απεριόριστες ποσότητες δεδομένων, έναντι μικρότερων, με αρνητικές συνέπειες για τον ανταγωνισμό και την καινοτομία. Ακόμη και στο δημόσιο τομέα και την κοινωνία των πολιτών, βλέπουμε μεγάλες αποκλίσεις στην ικανότητα των κυβερνήσεων και των μη κερδοσκοπικών ομάδων να εντοπίζουν ευκαιρίες δεδομένων και να ενεργούν με βάση αυτές για την προώθηση καλύτερης δημόσιας πολιτικής ή άλλων κοινωνικών αγαθών [114]. Ειδικότερα, η αναδυόμενη έννοια των «συνεργαζόμενων δεδομένων», στην οποία οι πληροφορίες είναι συλλογικά προσπελάσιμες και επεξεργάζονται σε όλους τους τομείς μπορεί να βοηθήσει στην κατανομή των δεδομένων και να διασφαλίσει ότι τα σωστά δεδομένα φθάνουν στα άτομα που μπορούν ωφελούνται πραγματικά από αυτό [114].

Από τις πιο σοβαρές επίσης προκλήσεις των μεγάλων δεδομένων, η οποία πλήττει την αρχή της διαφάνειας επεξεργασίας προσωπικών δεδομένων είναι η περίπτωση κατά την οποία συνάγονται νέα προσωπικά δεδομένα ή πληροφορίες που για ένα άτομο μέσω πολλαπλών σημείων δεδομένων. Οι εξελίξεις στην τεχνολογία όπως το IoT, μαζί με τις εξελίξεις στη δύναμη της ανάλυσης μεγάλων δεδομένων σημαίνει ότι το παραδοσιακό σενάριο στο οποίο οι άνθρωποι παρέχουν συνειδητά τα προσωπικά τους δεδομένα δεν είναι πλέον ο μόνος ή ο κύριος τρόπος συλλογής προσωπικών δεδομένων [110]. Σε πολλές περιπτώσεις, τα δεδομένα που χρησιμοποιούνται για τα αναλυτικά στοιχεία έχουν δημιουργηθεί αυτόματα, για παράδειγμα παρακολουθώντας τη διαδικτυακή δραστηριότητα, αντί να παρέχονται συνειδητά από άτομα [110. Οι αισθητήρες στο δρόμο ή στα καταστήματα μπορούν να καταγράψουν τη μοναδική διεύθυνση MAC των κινητών τηλεφώνων των

περαστικών. Πρόκειται για παραγόμενα δεδομένα - πληροφορίες που δεν αποκαλύπτονται ούτε ρητά ούτε σιωπηρά από τους χρήστες, αλλά προέρχονται από πολλαπλά αποκαλυπτόμενα ή παρατηρούμενα προσωπικά δεδομένα [114]. Τα ψηφιακά ''ίχνη'' που αφήνουν διάφορες δραστηριότητες παρέχουν σημαντικές πληροφορίες για την κινητικότητα των υποκειμένων των οποίων η συστηματική ανάλυση μπορεί να προσδιορίσει και να αποκαλύψουν εγγενείς πληροφορίες ή γνώσεις για μια πόλη και τους ανθρώπους της [121]. Μια εταιρεία μπορεί επίσης να συμπεράνει το φύλο, τη φυλή ή τη θρησκεία ενός χρήστη με βάση το περιεχόμενο που δημοσιεύει σε πλατφόρμες μέσων κοινωνικής δικτύωσης και εν συνεχεία να χρησιμοποιηθούν αυτές οι πληροφορίες για να εξατομικεύσουν τις προσπάθειες μάρκετινγκ προς ορισμένους χρήστες [114].

Ο στόχος των συναγόμενων προσωπικών δεδομένων, γράφει η Katarzyna Szymielewicz, η συνιδρυτής του Panoptykon Foundation, είναι να «μαντέψεις πράγματα που δεν είναι πιθανό να αποκαλύψεις πρόθυμα», όπως «τις αδυναμίες σου, το ψυχομετρικό σου προφίλ, το επίπεδο IQ, την οικογενειακή κατάσταση, τους εθισμούς και άλλα» [114]. Τα προφίλ που προκύπτουν μπορεί να είναι επεμβατικά και συχνά λανθασμένα, και συνήθως οι χρήστες δεν διαθέτουν εικόνα για το πώς δημιουργούνται και πώς να τα διορθώνουν. Η υπεύθυνη προσέγγιση θα απαιτούσε μεγαλύτερη διαφάνεια, επεξήγηση και ανθρώπινη εποπτεία σχετικά με τον τρόπο συλλογής και χρήσης τέτοιων δεδομένων.

Μία ακόμη πρόκληση που συνδέεται με τα Big Data είναι η τμηματοποίηση δεδομένων ανά δημογραφική ομάδα (π.χ. κατά φύλο ή ηλικία), μια διεργασία η οποία έχει τη δυνατότητα να προσφέρει χρήσιμες πληροφορίες, αλλά απαιτεί επίσης ιδιαίτερη προσοχή για το απόρρητο της ομάδας [114].

Η τμηματοποίηση δεδομένων ανά δημογραφικές ομάδες μπορεί να κάνει πιο συγκεκριμένες τις πληροφορίες που προέρχονται από αυτά τα δεδομένα και να οδηγήσει σε καλύτερες στοχευμένες πολιτικές και ενέργειες. Ταυτόχρονα, υπάρχει αυξανόμενη μια τέτοια ομαδοποίηση να θέσει σε κίνδυνο τα δικαιώματα μιας συγκεκριμένης ομάδας. Ένα βασικό καθήκον που αντιμετωπίζει κάθε προσπάθεια δημιουργίας ενός υπεύθυνου πλαισίου δεδομένων είναι η εξισορρόπηση των οφελών και των απειλών για το απόρρητο της ομάδας. Πρέπει να δοθεί προσοχή ώστε να αποφευχθεί το λεγόμενο «φαινόμενο μωσαϊκού. Το φαινόμενο αυτό

συμβαίνει λόγω του επαναπροσδιορισμού δεδομένων (συμπεριλαμβανομένων ανώνυμων δεδομένων) με συνδυασμό πολλαπλών συνόλων δεδομένων που περιέχουν παρόμοια ή συμπληρωματικές πληροφορίες. Το φαινόμενο μωσαϊκού μπορεί να αποτελέσει απειλή τόσο για την ατομική όσο και για την ομαδική ιδιωτικότητα [114]. Τέλος, καθώς συγκεκριμένα άτομα δεν γνωρίζουν ότι τα δεδομένα τους περιλαμβάνονται στο πλαίσιο μιας ειδικότερης, δεν μπορούν να περιορίσουν στην επεξεργασία αυτών από τους κατόχων των δεδομένων.

7.2. ΚΙΝΔΥΝΟΙ ΣΤΗΝ ΕΦΑΡΜΟΓΗ ΤΗΣ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ

Παρά τα οφέλη που μπορεί να προσφέρει η εφαρμογή της τεχνητής νοημοσύνης, μια αθέμιτη χρήση αυτής ενδέχεται να οδηγήσει σε σοβαρούς κινδύνους, ειδικά στα πρόσωπα που επηρεάζονται από αυτήν. Για το λόγο αυτό μια ομάδα εμπειρογνωμόνων υψηλού επιπέδου για την τεχνητή νοημοσύνη που συστάθηκε από την Ευρωπαϊκή Επιτροπή τον Ιούνιο του 2018, προχώρησε στην έκδοση κατευθυντήριων γραμμών, ώστε να δημιουργηθεί μια οριζόντια βάση για την επίτευξη αξιόπιστης ΤΝ. Ωστόσο, διαφορετικές καταστάσεις παρουσιάζουν διαφορετικές προκλήσεις, όπως εν προκειμένω, στο περιβάλλον της έξυπνης πόλης, όπου συναντάμε κυρίως σχέσεις επιχείρησης με καταναλωτή και δημόσιας υπηρεσίας με πολίτη.

Η τεχνητή νοημοσύνη στο πλαίσιο των Έξυπνων Πόλεων μπορεί να επεξεργάζεται προσωπικά δεδομένα (π.χ. κατά την κατανάλωση ενέργειας στο σπίτι ενός ατόμου ή την παρακολούθηση των κινήσεων και την προβολή σχετικών διαφημίσεων με βάση τη γεωγραφική τοποθεσία σε δυνητικούς καταναλωτές που μετακινούνται στο αστικό τοπίο). Μπορεί επίσης να περιλαμβάνει τη χρήση αναγνώρισης προσώπου για την παρακολούθηση ατόμων που κινούνται σε δημόσιους χώρους, τόσο για λόγους ασφαλείας όσο και για λόγους εξατομίκευσης. Όπου η τεχνητή νοημοσύνη επεξεργάζεται προσωπικά δεδομένα, υπάρχουν ορισμένες πρόσθετες προκλήσεις σχετικά με το απόρρητο και τη διακυβέρνηση των δεδομένων. Τα συστήματα ΤΝ θα πρέπει να εγγυώνται την προστασία της ιδιωτικής ζωής και των δεδομένων καθόλη τη διάρκεια του κύκλου ζωής ενός συστήματος. Αυτό περιλαμβάνει τις πληροφορίες που παρέχονται αρχικά από τον χρήστη, καθώς και τις πληροφορίες που

δημιουργούνται σχετικά με τον χρήστη κατά τη διάρκεια της αλληλεπίδρασής του με το σύστημα (π.χ. τα αποτελέσματα που παράγει το σύστημα ΤΝ για συγκεκριμένους χρήστες ή τον τρόπο με τον οποίο οι χρήστες ανταποκρίθηκαν σε συγκεκριμένες συστάσεις). Η ψηφιακή καταγραφή της ανθρώπινης συμπεριφοράς μπορεί να επιτρέψει στα συστήματα ΤΝ να συνάγουν όχι μόνο τις προτιμήσεις του ατόμου, αλλά και τον σεξουαλικό προσανατολισμό, την ηλικία, το φύλο, τις θρησκευτικές ή πολιτικές απόψεις του. Προκειμένου η διαδικασία συλλογής δεδομένων να εμπνέει εμπιστοσύνη στους χρήστες, θα πρέπει να διασφαλίζεται ότι τα δεδομένα που συλλέγονται σχετικά με αυτούς δεν θα χρησιμοποιηθούν για αθέμιτες ή παράνομες διακρίσεις απέναντί τους[117].

Οι οργανισμοί πρέπει να εξετάσουν εάν η χρήση προσωπικών δεδομένων σε εφαρμογές μεγάλων δεδομένων είναι εντός των εύλογων προσδοκιών των ανθρώπων [110]. Η πολυπλοκότητα των μεθόδων ανάλυσης μεγάλων δεδομένων, όπως της μηχανικής μάθηση μπορεί να δυσκολέψει τους οργανισμούς ως προς την εφαρμογή διαφάνειας σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα [110]. Η πλήρης ενημέρωση του υποκειμένου αποτελεί απαρέγκλιτο όρο, προκειμένου αυτό να αποκτήσει και να διατηρήσει τον έλεγχο των δεδομένων του. [118].

Επιπλέον, ενδέχεται να υπάρξουν περαιτέρω προκλήσεις σχετικά με τη δικαιοσύνη και την αξιοπιστία του αλγορίθμου. Για παράδειγμα, με τις τεχνολογίες αναγνώρισης προσώπου που χρησιμοποιούνται για την αστυνόμευση και τη δημόσια ασφάλεια, θα ελπίζαμε ότι το σύνολο δεδομένων για την εκπαίδευση της τεχνολογίας είχε ένα αρκετά ευρύ φάσμα διαφορετικών δημογραφικών στοιχείων που αντιπροσωπεύονται σε αυτό, έτσι ώστε να αναγνωρίζει σωστά άτομα διαφορετικής φυλετικής και εθνοτικής καταγωγής, αντί για μια συγκεκριμένη εθνοτική ομάδα. Οι αγοραστές αυτών των τεχνολογιών θα πρέπει να ενδιαφερθούν προηγουμένως πώς οι προγραμματιστές έλαβαν μέτρα για να διασφαλίσουν ότι η τεχνητή νοημοσύνη δεν θα δημιουργήσει και δεν ενισχύσει αθέμιτη μεροληψία στη σχεδίαση του συστήματος (για παράδειγμα, εάν ο αλγόριθμος σχεδιάστηκε με το σύνολο δεδομένων που συνήθως επεξεργαζόταν, π.χ. οι πολίτες μιας διαφορετικής πόλης και κατά πόσον υπήρχαν διαδικασίες για τον έλεγχο πιθανής μεροληψίας) [119].

Οι οργανισμοί θα πρέπει να δημιουργούν πλαίσια διακυβέρνησης, τόσο εσωτερικά όσο και εξωτερικά, ώστε να εξασφαλίζεται η λογοδοσία για τις δεοντολογικές διαστάσεις των αποφάσεων που σχετίζονται με την ανάπτυξη, την εγκατάσταση και τη χρήση της ΤΝ [115]. Κατά την ανάπτυξη, θα πρέπει να αναπτυχθούν μηχανισμοί διακυβέρνησης για να διασφαλιστεί ότι οποιαδήποτε πιθανή αδικία μπορεί να επισημανθεί από τους πολίτες, συμπεριλαμβανομένων των μεροληψιών, των διακρίσεων ή της κακής απόδοσης του συστήματος.

Μία από τις βασικές κατευθύνσεις για την ορθή εφαρμογή της ΤΝ είναι η ενημέρωση, με σαφή και ενεργό τρόπο, των ενδιαφερόμενων μερών σχετικά με τις δυνατότητες και τους περιορισμούς του συστήματος ΤΝ, ώστε να δημιουργούνται ρεαλιστικές προσδοκίες, καθώς και σχετικά με τον τρόπο με τον οποίο εφαρμόζονται οι απαιτήσεις [115]. Η ικανοποίηση των απαιτήσεων διαφάνειας είναι μια σημαντική πρόκληση στις Έξυπνες Πόλεις. Ειδικότερα, είναι απαραίτητη η αποτελεσματική επικοινωνία με τους πολίτες που κινούνται σε μια Έξυπνη Πόλη όταν αλληλεπιδρούν με συστήματα τεχνητής νοημοσύνης. Οι απαιτήσεις διαφάνειας των άρθρων 13 και 14 του ΓΚΠΔ μπορεί να είναι επαχθείς και δεν είναι απαραίτητα πρακτικές σε ένα αστικό περιβάλλον – ούτε με πολύ μεγάλες πινακίδες! Επομένως, θα ήταν σκόπιμο να αναπτυχθεί σήμανση που μπορεί να περιλαμβάνει τη χρήση κοινώς αναγνωρισμένων σημάτων και συμβόλων, μαζί με διαδραστικές πινακίδες και κωδικούς QR που μπορούν να επιτρέψουν στα άτομα να έχουν πρόσβαση σε πληρέστερες πληροφορίες (δηλαδή μια πολυεπίπεδη προσέγγιση για πληρέστερες πληροφορίες απορρήτου που είναι διαθέσιμες στο διαδίκτυο) [119].

Τα συστήματα ΤΝ θα πρέπει να στηρίζουν την ανθρώπινη αυτονομία και τη λήψη αποφάσεων, όπως προβλέπεται στην αρχή του σεβασμού της ανθρώπινης αυτονομίας. Η απαίτηση αυτή προϋποθέτει ότι τα συστήματα ΤΝ θα πρέπει και να λειτουργούν ως εργαλεία ανάπτυξης μιας δημοκρατικής, ευημερούσας και ισότιμης κοινωνίας, υποστηρίζοντας την παρέμβαση του χρήστη, αλλά και να προάγουν τα θεμελιώδη δικαιώματα, καθώς και να αφήνει περιθώριο για ανθρώπινη εποπτεία [115]. Για όσους εμπλέκονται στην προμήθεια συστημάτων τεχνητής νοημοσύνης, πρέπει να ληφθεί υπόψη το κατάλληλο επίπεδο ανθρώπινου ελέγχου για τη συγκεκριμένη υποδομή «Smart City» [119. Υπάρχουν πολλά διαφορετικά μοντέλα που θα μπορούσαν να εξεταστούν, αλλά η πρόκληση είναι ο όγκος και η ταχύτητα

των Big Data και όπου μπορεί ρεαλιστικά να εισαχθεί ουσιαστική ανθρώπινη εποπτεία. Σε κάθε περίπτωση, θα πρέπει να υπάρχει ένας μηχανισμός που θα διευκολύνει την ικανότητα ελέγχου του συστήματος.

7.3 ΑΥΤΟΜΑΤΟΠΟΙΗΜΕΝΗ ΛΗΨΗ ΑΠΟΦΑΣΕΩΝ ΚΑΙ ΚΑΤΑΡΤΙΣΗ ΠΡΟΦΙΛ

Στο α. 22 παρ. 1 του ΓΚΠΔ προβλέπεται 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*’’ και στην παρ. 3 του ίδιου άρθρου ότι ‘’…*υπεύθυνος επεξεργασίας υπεύθυνος επεξεργασίας των δεδομένων 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*’’. Το άρθρο αυτό συνδέεται στενά με τα μεγάλα δεδομένα και την εφαρμογή τεχνητής νοημοσύνης και στοχεύει στην προστασία των φυσικών προσώπων από μια τυχόν άδικη αυτοματοποιημένη απόφαση, η οποία ενδεχομένως θίξει επιπλέον διαφορετικά δικαιώματά τους, πλην του δικαιώματος προστασίας προσωπικών δεδομένων,

Ειδικότερα, σύμφωνα με την αιτ. σκ. 71 του ΓΚΠΔ, προκειμένου να διασφαλισθεί δίκαιη και διαφανής επεξεργασία σε σχέση με το υποκείμενο των δεδομένων, λαμβανομένων υπόψη των ειδικών συνθηκών και του πλαισίου εντός του οποίου πραγματοποιείται η επεξεργασία των δεδομένων προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας 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.

Ο υπεύθυνος επεξεργασίας δεδομένων οφείλει με τον κατάλληλο και εύκολα αντιληπτό τρόπο να εξηγήσει στο υποκείμενο των δεδομένων που έλαβε προκειμένου ο τελευταίος να είναι σε θέση να κατανοήσει το αποτέλεσμα και να ασκήσει τα δικαιώματά του. Αυτό το δικαίωμα στην επεξήγηση εξειδικεύει το δικαίωμα στην πληροφόρηση όπως καθορίζεται στη νομοθεσία περί προστασίας δεδομένων και ενισχύεται από τον ΓΚΠΔ. Το δικαίωμα των ατόμων να λαμβάνουν τις κατάλληλες πληροφορίες προκειμένου να μην υπόκεινται σε αποφάσεις που δεν κατανοούν και δεν έχουν κανέναν έλεγχο πηγάζει από την αρχή της (εκ των υστέρων) διαφάνειας καθώς και από την «αλγοριθμική λογοδοσία» [113].

Μία γενική διαπίστωση που συνάγεται από τα ανωτέρω είναι ότι η ανάγκη και η λήψη μέτρων για την προστασία της ιδιωτικής ζωής σε σχέση με την τεχνολογική πρόοδο δεν συμβαδίζει με την ταχύτητα της τεχνολογικής αλλαγής. Έννοιες όπως οι Έξυπνες Πόλεις και τεχνολογίες όπως το IoT, η τεχνητή νοημοσύνη και η μηχανική μάθηση εξακολουθούν να βρίσκονται στο προσκήνιο και αναμένεται να εξελιχθούν ακόμη περισσότερο καθώς η εφαρμογή τους αποκτά δημοτικότητα [120]. Ως εκ τούτου, οι προσπάθειες που στοχεύουν στη διαφύλαξη της ιδιωτικής ζωής των κατοίκων των πόλεων θα πρέπει να προβλέπουν την τεχνολογική αλλαγή και θα πρέπει να βρίσκονται στην πρώτη γραμμή των ανησυχιών για τους ψηφιακούς επιστήμονες και τους σχεδιαστές [120].

7.4.ΚΙΝΔΥΝΟΙ ΓΙΑ ΤΟ ΑΠΟΡΡΗΤΟ ΤΟ ΔΕΔΟΜΕΝΩΝ ΑΠΟ ΤΗ ΧΡΗΣΗ ΤΩΝ OPEN DATA

Όπως προέκυψε από τα ανωτέρω τα οφέλη των open data για μια ΕΠ είναι προφανή. Στα open data εκτός από μη προσωπικά δεδομένα περιλαμβάνονται επίσης προσωπικά δεδομένα τα οποία, μέσω κατάλληλων τεχνικών έχουν ανωνυμοποιηθεί. Για το λόγο αυτό πρέπει να σημειωθεί ένα βασικό μειονέκτημα, το οποίο συνίσταται στην (απίθανη?) περίπτωση κατά την οποία η δημοσίευση ενός συνόλου open data

οδηγήσει στην ταυτοποίηση των υποκειμένων των δεδομένων. Σύμφωνα με την αιτ. σκ. 26 του ΓΚΠΔ, ως ανώνυμες πληροφορίες ορίζονται εκείνες οι πληροφορίες που δεν σχετίζονται προς ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο ή σε δεδομένα προσωπικού χαρακτήρα που έχουν καταστεί ανώνυμα κατά τρόπο ώστε η ταυτότητα του υποκειμένου των δεδομένων να μην μπορεί ή να μην μπορεί πλέον να εξακριβωθεί.

Το σύνολο των ανώνυμων δεδομένων εξακολουθεί να αποτελεί προσωπικό δεδομένο για τον υπεύθυνο επεξεργασίας δεδομένων, εφόσον τα υποκείμενα μπορούν να αναγνωριστούν από τα δεδομένα σε συνδυασμό με άλλα δεδομένα που έχει στην κατοχή του ο υπεύθυνος επεξεργασίας. Δεδομένου ότι η δημοσίευση των δεδομένων σε ανοικτή μορφή είναι ένα είδος επεξεργασίας, συνεπάγεται ότι ο εκδότης των ανοιχτών δεδομένων τα επεξεργάζεται σύμφωνα με μία από τις νομικές βάσεις, που ορίζονται στο άρθρο 6 του ΓΚΠΔ [122].

Όπως αναφέρει η Ann Cavoukian σε άρθρο της [128] οι τεχνικές αποταυτοποίησης αντιμετωπίζουν γενικά τρεις κινδύνους για το απόρρητο. Πρώτον, προστατεύουν τα αρχεία ενός ατόμου ώστε να μην ταυτοποιηθεί σε ένα σύνολο δεδομένων. Δεύτερον, αποτρέπουν τη σύνδεση των εγγραφών ενός ατόμου με άλλα σύνολα δεδομένων. Εάν ένα σύνολο χαρακτηριστικών προσδιορίζει μοναδικά ένα άτομο σε ένα σύνολο δεδομένων που δεν έχει ταυτοποιηθεί και αυτά τα ίδια χαρακτηριστικά βρίσκονται σε ένα σύνολο δεδομένων που τα άτομα ταυτοποιούνται, τότε αυτό το άτομο μπορεί να επαναπροσδιοριστεί κατόπιν της σύνδεσης των δύο συνόλων δεδομένων μεταξύ τους. Τρίτον, καθιστούν δύσκολη την εξαγωγή ευαίσθητων πληροφοριών για ένα άτομο από το σύνολο δεδομένων που δεν έχει ταυτοποιηθεί. Για παράδειγμα, εάν ομάδες ατόμων προσδιορίζονται σε ένα σύνολο δεδομένων και όλα τα άτομα σε μια συγκεκριμένη ομάδα έχουν μια συγκεκριμένη ιδιότητα, τότε εάν ένα άτομο είναι γνωστό ότι ανήκει σε αυτήν την ομάδα, θα μπορούσε κανείς εύκολα να μάθει την αξία της ομαδικής ιδιοκτησίας του.

Δεν αποκλείεται ωστόσο να αντιστραφούν οι στρατηγικές ανωνυμοποίησης με το συνδυασμό συνόλου δεδομένων (μάλιστα υπάρχουν ορισμένες εταιρείες που ειδικεύονται στον επαναπροσδιορισμό δεδομένων σε σύνολα δεδομένων μεγάλων δεδομένων), εκτός εάν τα δεδομένα αποπροσδιοριστούν πλήρως [67]. Η αποταυτοποίηση απαιτεί προσεκτική αφαίρεση τόσο των άμεσων αναγνωριστικών

στοιχείων όσο και των οιονεί αναγνωριστικών (αυτών που έχουν μεγάλη συσχέτιση με μοναδικά αναγνωριστικά) [67].

Ένα ευρύτερο νομικό πρόβλημα με την ανωνυμοποίηση είναι ότι εάν το περιεχόμενο πληροφοριών των δεδομένων δεν μειωθεί κάτω από οποιοδήποτε εύλογο επίπεδο χρησιμότητας – για παράδειγμα, αντικαθιστώντας όλες τις τιμές δεδομένων με 0 – θα είναι τεχνικά δυνατός ο επαναπροσδιορισμός ατόμων από ανώνυμα δεδομένα με επαρκή βοηθητικά στοιχεία συνεπώς ο κίνδυνος ανωνυμοποίησης δεν μπορεί να μειωθεί στο μηδέν [122]. Ένα τεστ πριν από τη δημοσίευση των δεδομένων για να διαπιστωθεί εάν μπορούν να αποανωνυμοποιηθούν εύκολα είναι μια λογική ιδέα, αλλά όχι απαραίτητα και μια οικονομική επιλογή [122].

Τα παραδοσιακά πλαίσια απορρήτου και ανωνυμοποίησης επικεντρώνονται στον εντοπισμό και την αφαίρεση στοιχείων προσωπικής ταυτοποίησης. Πρόσφατη έρευνα, ωστόσο, έχει αποκαλύψει ότι αυτό το πλαίσιο είναι μη βιώσιμο και αναποτελεσματικό. Επειδή είναι πλέον διαθέσιμα τόσα πολλά δεδομένα από μια μεγάλη ποικιλία πηγών και επειδή οι βάσεις δεδομένων μπορούν να συνδυαστούν με πολύπλοκους και απρόβλεπτους τρόπους, οι πληροφορίες που μπορεί να μην θεωρούνται επαρκείς, μπορούν να οδηγήσουν στην ταυτοποίηση ενός συγκεκριμένου ατόμου και να επιτρέψουν την εξαγωγή συμπερασμάτων για αυτό το άτομο [51][K127].

Η Strava είναι μια εταιρεία με έδρα το Σαν Φρανσίσκο, η οποία παρέχει υπηρεσίες παρακολούθηση φυσικής κατάστασης βάσει τοποθεσίας για δρομείς και ποδηλάτες. Οι χρήστες μπορούν να κατεβάσουν τη δωρεάν εφαρμογή της Strava και να τη χρησιμοποιήσουν για να χαρτογραφήσουν απευθείας τις προπονήσεις τους ή να τη συνδυάσουν με μια συσκευή γυμναστικής, όπως ένα FitBit. Η ανωτέρω εταιρία δημοσίευσε στο διαδίκτυο το 2017 ένα διαδραστικό χάρτη που δημοσιεύτηκε στο Διαδίκτυο που περιείχε εξαιρετικά ευαίσθητες πληροφορίες σχετικά με τις τοποθεσίες και τις δραστηριότητες των στρατιωτών στις στρατιωτικές βάσεις των ΗΠΑ [129]. Παρά την αφαίρεση των προσωπικών πληροφοριών από τα δεδομένα από τον Strava και τη συγκέντρωση τους (στο επίπεδο του πλέγματος οδών), προσεκτικοί παρατηρητές παρατήρησαν ότι ο Χάρτης Θερμότητας περιείχε μοτίβα τοποθεσίας

51

μέσα από στρατιωτικές βάσεις των ΗΠΑ σε ζώνες ενεργών συγκρούσεων, συμπεριλαμβανομένης της Συρίας και του Αφγανιστάν. Ενώ η ύπαρξη πολλών από αυτές τις στρατιωτικές εγκαταστάσεις ήταν ήδη γνωστή, σημείωσαν ότι ο Χάρτης θερμότητας αποκάλυψε άλλους αεροδρόμους και σχήματα που μοιάζουν με βάση σε μέρη όπου ούτε οι στρατιωτικές δυνάμεις υπό την ηγεσία των ΗΠΑ ούτε η Κεντρική Υπηρεσία Πληροφοριών είναι γνωστό ότι έχουν σταθμούς προσωπικού [130].

Από τη δημοσιοποίηση των open data, τα δεδομένα τοποθεσίας μπορούν επίσης να αποκαλύψουν [131] :

-Το μοτίβο κινήσεων ενός προσώπου, από το οποίο μπορεί να προκύψουν και ευαίσθητες πληροφορίες, καθώς τα δεδομένα τοποθεσίας «δημιουργούν μια ακριβή, ολοκληρωμένη καταγραφή των δημόσιων κινήσεων ενός ατόμου που αντικατοπτρίζει έναν πλούτο λεπτομερειών σχετικά με τις οικογενειακές, πολιτικές, επαγγελματικές, θρησκευτικές και σεξουαλικές πεποιθήσεις),

-Τα μοτίβα ομαδικής κινητικότητας (στην περίπτωση του Strava, γρήγορα παρατηρήθηκε ότι στα δεδομένα μπορούσαν να εντοπιστούν διαδρομές ανεφοδιασμού και συνήθειες άσκησης στρατιωτικών και γυναικών στο εξωτερικό, γεγονότα που έχουν επιπτώσεις στην ασφάλεια) καθώς και

-Δραστηριότητες που σχετίζονται με ευαίσθητη τοποθεσία (ενώ ορισμένες τοποθεσίες, όπως κλινικές αμβλώσεων ή τζαμιά, μπορεί να είναι ευαίσθητες μόνο σε σχέση με μεμονωμένους επισκέπτες, άλλες τοποθεσίες, όπως μυστικές στρατιωτικές εγκαταστάσεις, μπορεί να είναι ‘’ευαίσθητες’’ οι ίδιες).

Από τα παραπάνω μπορεί να συνάγει κανείς ότι ακόμη και στα ανωνυμοποιημένα open data είναι δυνατόν να υπάρχει παραβίαση προσωπικών δεδομένων. Στο [126] αναφέρονται περιπτώσεις όπου η δημοσιοποίηση των open data μπορεί να οδηγήσει στην παραβίαση του δικαιώματος προστασίας προσωπικών δεδομένων: η πρώτη έχει να κάνει με την πιθανή εξαγωγή ευαίσθητων δεδομένων αναφορικά με συγκεκριμένη πληθυσμιακή ομάδα, όπως είναι για παράδειγμα οι κάτοικοι μιας περιοχής, χωρίς να υπάρξει εφαρμογή της νομοθεσίας για τα προσωπικά δεδομένα. Τα ανοιχτά δεδομένα δεν χρειάζεται να αναφέρονται σε ένα συγκεκριμένο φυσικό πρόσωπο για να προκαλέσουν αρνητικές συνέπειες, αντιθέτως μάλιστα η ανωνυμοποίηση δεν αντιμετωπίζει την πιθανότητα κακής χρήσης των δεδομένων, όπως είναι η δημιουργία ενός μοντέλου που εισάγει διακρίσεις και χρησιμοποιείται ως βάση για

αυτοματοποιημένη λήψη αποφάσεων. Η ίδια η φύση των ανοιχτών δεδομένων δε συνάδει με τις έννοιες του ελέγχου πρόσβασης και των περιορισμών χρήσης. Μάλιστα επειδή ακριβώς στον ΓΚΠΔ γίνεται λόγος για την επεξεργασία προσωπικών δεδομένων συγκεκριμένου ταυτοποιήσιμου προσώπου και αντίθετα, στο πλαίσιο των open data μπορούν να εξαχθούν δεδομένα που αφορούν ένα σύνολο δεδομένων, είναι πολύ πιθανό αυτού του είδους η επεξεργασία να μην ενεργοποιήσει απαραίτητα την εφαρμογή του, τουλάχιστον έως ότου το συμπέρασμα χρησιμοποιηθεί με σκοπό που να περιλαμβάνει το συγκεκριμένο ταυτοποιήσιμο φυσικό πρόσωπο ή έως ότου το αποτέλεσμα της επεξεργασίας δημιουργήσει κάποιου είδους συνέπειες για ένα αναγνωρίσιμο φυσικό πρόσωπο [126].

Η δεύτερη περίπτωση συνίσταται στο γεγονός ότι η κοινή χρήση και η επαναχρησιμοποίηση των open data αυξάνει τον όγκο των πληροφοριών που είναι διαθέσιμες σε κάποιον ο οποίος στοχεύει στην εκ νέου αναγνώριση ενός υποκειμένου δεδομένων από ανώνυμη εγγραφή ή στην εξαγωγή συμπερασμάτων σχετικά με ορισμένα (ευαίσθητα) χαρακτηριστικά ενός γνωστού υποκειμένου δεδομένων [126].

Περαιτέρω, παράγοντες όπως η διαδικτυακή και μη παρακολούθηση συμπεριφοράς των ατόμων, η έρευνα και η ανάπτυξη τρόπων αναγνώρισης ατόμων για μια πληθώρα σκοπών, από τη συμπεριφορική διαφήμιση έως την ασφάλεια στον κυβερνοχώρο και την επιβολή του νόμου καθώς και η παρουσία αισθητήρων από το Διαδίκτυο των Πραγμάτων στη λεγόμενη ΕΠ, συμβάλλουν στο να γίνει κάπως ασαφές το όριο μεταξύ ταυτοποίησης και ανωνυμίας [126].

Παρακάτω ακολουθούν ορισμένα παραδείγματα έξυπνων πόλεων που έχουν υιοθετήσει πολιτικές ανοιχτών δεδομένων.

Το Seattle είναι μία από τις πρωτοπόρες πόλεις που εισήγαγε μια Πολιτική Ανοικτών Δεδομένων [132] η οποία αναπτύχθηκε σε συνεργασία με διάφορους εταίρους, συμπεριλαμβανομένου του Πανεπιστημίου της Ουάσιγκτον. Αυτή η πολιτική ορίζει ότι τα κρατικά δεδομένα πρέπει να είναι «ανοιχτά κατά προτίμηση», πράγμα που σημαίνει ότι η πόλη διατηρεί το δικαίωμα να αποκρύψει δεδομένα εάν έχει τη δυνατότητα να προκαλέσει βλάβες στο απόρρητο. Σύμφωνα με την πολιτική, τα

σύνολα δεδομένων πρέπει να εξετάζονται για πιθανές βλάβες στο απόρρητο πριν από την κυκλοφορία και πρέπει να διενεργείται ετήσια αξιολόγηση κινδύνου τόσο για το Πρόγραμμα Ανοικτών Δεδομένων όσο και για την Πύλη Ανοικτών Δεδομένων.

Το Σιάτλ εξέδωσε επίσης το 2017 ένα διάταγμα που περιγράφει μια σειρά διαδικασιών που έχουν σχεδιαστεί για να αυξήσουν τη διαφάνεια σχετικά με τη χρήση τεχνολογιών επιτήρησης από την πόλη. Αυτό περιλαμβάνει τη δημιουργία απογραφής όλων των τεχνολογιών επιτήρησης και την προετοιμασία Αναφορών Επιπτώσεων Επιτήρησης για τη νέα τεχνολογία [132]. Παραδείγματα τεχνολογίας υπό εξέταση περιλαμβάνουν **Αυτοματοποιημένα Καταγραφικά πινακίδων κυκλοφορίας, τα οποία είναι προσαρτημένα σε αστυνομικά οχήματα, και Κάμερες Έκτακτης Ανάγκης.** Η προσέγγιση του Seattle δείχνει πώς μπορούν οι θεμελιώδεις ηθικές αρχές σχετικά με τη διαχείριση και τη συλλογή προσωπικών δεδομένων να μεταφραστεί σε απτές, εφαρμόσιμες πολιτικές και πρακτικές σε μια πόλη [125]. Η πρώτη ετήσια αξιολόγηση κινδύνου που διεξήχθη από το Future of Privacy Forum αναγνώρισε το Σιάτλ ως «εθνικό ηγέτη στη διαχείριση προγραμμάτων απορρήτου» και σημείωσε την πόλη με πέντε στα έξι στους τομείς «Ποιότητα Δεδομένων» και «Διαφάνεια και Δημόσια Εμπλοκή» [132].

Ωστόσο, η πόλη αναγνώρισε ότι η τυχόν δημοσιοποίηση ορισμένων δεδομένων, εάν δημοσιοποιηθούν, μπορεί να προκαλέσει βλάβες στην ιδιωτική ζωή ή να θέσει σε κίνδυνο κρίσιμες υποδομές και για το λόγο αυτό θα πρέπει να γίνεται προσεκτική αξιολόγηση των ωφελειών και τυχόν κινδύνων για το απόρρητο, πριν δημοσιευθεί ένα μεγάλο σύνολο δεδομένων. Μόλις δημοσιευθούν οι πληροφορίες δημόσια, είναι δύσκολο ή αδύνατο να ανακληθούν και ως εκ τούτου, οι κάτοχοι δεδομένων θα πρέπει [131/]:

Να χρησιμοποιούν τεχνικές, νομικές και διοικητικές διασφαλίσεις για να μειώσουν τον κίνδυνο επαναπροσδιορισμού.

Να έχουν πρόσβαση σε εμπειρογνώμονες οι οποίοι δύνανται να αξιολογήσουν τον κίνδυνο επαναπροσδιορισμού.

Να χρησιμοποιούν κατάλληλα εργαλεία για τον αποπροσδιορισμό μη δομημένων ή δυναμικών τύπων δεδομένων (π.χ. γεωγραφικά, βίντεο, ήχος, ελεύθερο κείμενο, δεδομένα αισθητήρων σε πραγματικό χρόνο).

Να θεσπίσουν πολιτικές και διαδικασίες για την αξιολόγηση του κινδύνου επαναπροσδιορισμού μεταξύ βάσεων δεδομένων.

7.5 ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΤΗ ΔΙΑΦΥΛΑΞΗ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΠΛΑΙΣΙΟ ΤΩΝ OPEN DATA

Στο [125] αναφέρονται πώς μια ΕΠ μπορεί να δημιουργήσει κανόνες για την προστασία των ατόμων από πιθανές βλάβες που προκαλούνται από ψηφιακά εργαλεία και να διασφαλίσει ότι η χρήση τεχνολογιών που βασίζονται σε δεδομένα μπορεί να ωφελήσει όλους. Αυτό θα μπορούσε να επιτευχθεί ως εξής:

-Με την κωδικοποίηση βασικών διαδικασιών για τον εντοπισμό και την εξάλειψη των κινδύνων σε ανοιχτά σύνολα δεδομένων

Τα Συμβούλια έχουν αυξημένη πρόσβαση σε δεδομένα που συλλέγονται από νέα σημεία δεδομένων σε όλη την πόλη, για οτιδήποτε, από την περιβαλλοντική ρύπανση έως την κινητικότητα. Έχει γίνει σύνηθες να δημοσιεύονται πολλές από αυτές τις πληροφορίες ως ανοιχτά δεδομένα. Όμως, καθώς η τεχνολογία γίνεται πιο εξελιγμένη και ο όγκος των προσωπικών δεδομένων που συλλέγονται σε ολόκληρη την ψηφιακή οικονομία αυξάνεται, αυξάνεται παράλληλα και η δυνατότητα επαναπροσδιορισμού ατόμων σε ένα ανοιχτό σύνολο δεδομένων. Η κωδικοποίηση βασικών διαδικασιών και απλών εργαλείων μπορεί να είναι ένας χρήσιμος τρόπος για να διασφαλιστεί ότι η βέλτιστη πρακτική είναι εύκολο να ακολουθηθεί για το προσωπικό σε διαφορετικά τμήματα.

Το Σαν Φρανσίσκο ξεκίνησε μια πλατφόρμα ανοιχτών δεδομένων που ονομάζεται DataSF το 2009, με στόχο τη χρήση δεδομένων για τη βελτίωση των υπηρεσιών της πόλης. Αναγνωρίζοντας ότι οι ισχύοντες νόμοι περί απορρήτου δεν καλύπτουν απόλυτα τον επαναπροσδιορισμό μέσω ανώνυμων δεδομένων, κυκλοφόρησε το 2016 μια εργαλειοθήκη Ανοικτών Δεδομένων, η οποία έχει σχεδιαστεί για να καθοδηγεί τους δημοτικούς υπαλλήλους σε μια διαδικασία αξιολόγησης κινδύνου πριν από τη δημοσίευση των ανοιχτών δεδομένων. Πρόκειται για ένα μοντέλο μοντέλο τεσσάρων βημάτων που βοηθά τους υπαλλήλους να εντοπίσουν ευαίσθητα σύνολα δεδομένων, να πραγματοποιήσουν αξιολογήσεις κινδύνου και να επιλέξουν

τεχνικές λύσεις προστασίας απορρήτου, προτείνοντας σε ορισμένες περιπτώσεις, να παραμείνει κλειστό ένα σύνολο δεδομένων[52].

-Με την πιλοτική χρήση τεχνικών ελαχιστοποίησης και ανωνυμοποίησης δεδομένων τελευταίας τεχνολογίας

Τα άτομα καλούνται συνεχώς να δίνουν προσωπικές πληροφορίες για τον εαυτό τους προκειμένου να χρησιμοποιούν διαδικτυακές υπηρεσίες. Για το λόγο αυτό γίνονται προσπάθειες για την ανάπτυξη και χρησιμοποίηση τεχνολογιών που συμβάλλουν στην ελαχιστοποίηση του όγκου των προσωπικών δεδομένων που πρέπει να συλλέγονται κατά την παροχή μιας υπηρεσίας σε άτομα. Όπου οι κίνδυνοι ταυτοποίησης παραμένουν υψηλοί, τα νέα τεχνικά εργαλεία μπορούν επίσης να βοηθήσουν στην ανωνυμοποίηση, παρέχοντας πρόσθετη προστασία στους πολίτες. Το χρηματοδοτούμενο από την Ευρωπαϊκή Επιτροπή έργο DECODE αναπτύσσει τεχνολογία στη Βαρκελώνη και το Άμστερνταμ η οποία επιτρέπει στο δημοτικό συμβούλιο να επαληθεύσει ορισμένες πτυχές της ταυτότητας των κατοίκων της περιοχής με ανώνυμο τρόπο. Η τεχνική που εφαρμόζεται, γνωστή ως «Attribute Based Credentials» δίνει τη δυνατότητα στους κατοίκους να επιλέξουν οι ίδιοι ποια «χαρακτηριστικά» θα αποκαλύψουν για τον εαυτό τους αντί της πλήρους ταυτότητά τους όταν αλληλεπιδρούν με τις υπηρεσίες του δήμου, π.χ.« αυτό το άτομο είναι άνω των 18 ετών» ή «αυτό το άτομο είναι κάτοικος της πόλης του Άμστερνταμ».

Εκτός βέβαια από πιο απλές διαδικασίες επαλήθευσης ταυτότητας, εξακολουθούν να υπάρχουν πολλά παραδείγματα συλλογής δεδομένων από τις κυβερνήσεις των πόλεων όπου οι κίνδυνοι ταυτοποίησης παραμένουν υψηλοί. Τα δεδομένα σχετικά με τις υπηρεσίες δημόσιων μεταφορών συχνά συλλέγονται χωρίς να το γνωρίζουν οι άνθρωποι, ωστόσο μπορούν να προσφέρουν πολύτιμα πληροφορίες σε ερευνητές και δημοτικούς υπαλλήλους που είναι επιφορτισμένοι με τη βελτίωση των υπηρεσιών της πόλης. Όπως και άλλες μορφές ανοιχτών δεδομένων, τέτοιες πληροφορίες μπορούν να θέσουν σε κίνδυνο το απόρρητο των πολιτών εάν για παράδειγμα οι διαδρομές μετακίνησης τους από-ανωνυμοποιηθούν. Πράγματι, τόσο

[52] Το San Francisco έχει καθιερώσει επίσης πολυήμερα εργαστήρια, τα Data Camps – για το προσωπικό της πόλης που έχει την ευθύνη της δημοσίευσης ανοιχτών δεδομένων προκειμένου να τους εκπαιδεύσει σχετικά με ζητήματα όπως η ποιότητα των δεδομένων, το απόρρητο δεδομένων, η ισότητα των δεδομένων και η δημόσια αποκάλυψη.

η διαθεσιμότητα όσο και η ποικιλία δεδομένων, παράλληλα με τις σύγχρονες τεχνικές μηχανικής μάθησης, καθιστούν ολοένα και πιο δυνατή την αντίστροφη μηχανική ανωνυμοποιημένων συνόλων δεδομένων.

ΕΠΙΛΟΓΟΣ

Οι έξυπνες πόλεις αποτελούν ήδη κομμάτι της σύγχρονης ζωής. Η αλματώδης αύξηση του Διαδικτύου των πραγμάτων έχει καταστήσει ένα μεγάλο μέρος των παραδοσιακών λειτουργιών του σε ψηφιοποιημένες πλέον διαδικασίες. Η αυτονόητη εξάρτηση των έξυπνων πόλεων από τις τεχνολογίες πληροφορικής και επικοινωνιών σε συνδυασμό με τους ''εγκληματίες του κυβερνοχώρου'' να επιδεικνύουν σαφή και κατανοητή προθυμία να εκμεταλλευτούν οποιαδήποτε ευπάθεια μπορούν να βρουν, πρέπει να τις αναγκάσει να παραχωρήσουν στην ασφάλεια στον κυβερνοχώρο την προτεραιότητα που της αξίζει.

Μια ολιστική προσέγγιση προκειμένου η έξυπνη πόλη να είναι ασφαλής έναντι κυβερνοεπιθέσεων περιλαμβάνει συνοπτικά τις κατωτέρω δράσεις [133]:

Οι πόλεις θα πρέπει να καθορίσουν μια λεπτομερή στρατηγική κυβερνοασφάλειας που να είναι σύμφωνη με την ευρύτερη στρατηγική τους και που μπορεί να μετριάσει τις προκλήσεις που προκύπτουν από τη συνεχή σύγκλιση, διαλειτουργικότητα και διασύνδεση συστημάτων και διαδικασιών πόλεων. Οι πόλεις θα πρέπει να εξετάσουν το ενδεχόμενο διεξαγωγής εκτενούς αξιολόγησης επιπτώσεων των δεδομένων, των συστημάτων και των περιουσιακών στοιχείων τους στον κυβερνοχώρο για τον εντοπισμό, την αξιολόγηση και τον μετριασμό των κινδύνων που σχετίζονται με τις τεχνολογικές διαδικασίες, πολιτικές και λύσεις.

Οι πόλεις πρέπει να δημιουργήσουν ένα ολοκληρωμένο μοντέλο διακυβέρνησης το οποίο θα προσδιορίζει τις ευθύνες και τους ρόλους για κάθε κρίσιμο στοιχείο στο οικοσύστημα της έξυπνης πόλης. Για να εφαρμοστεί μια προσέγγιση οικοσυστήματος για την αντιμετώπιση ζητημάτων στον κυβερνοχώρο, διάφορες οντότητες θα πρέπει να συνεργαστούν με ένα ισχυρό μοντέλο διακυβέρνησης ως θεμέλιο. Οι πολιτικές, η νομοθεσία και η τεχνολογία πρέπει να ευθυγραμμίζονται συνεχώς για να διατηρηθεί η σωστή ισορροπία προστασίας, ιδιωτικότητας, διαφάνειας και χρησιμότητας.

Οι πόλεις θα πρέπει να δημιουργήσουν στρατηγικές συνεργασίες για την ανάπτυξη των ικανοτήτων στον κυβερνοχώρο. Το χάσμα στις δεξιότητες στον κυβερνοχώρο δεν θα εξαφανιστεί σύντομα, πρέπει επομένως να είναι καινοτόμες και να δρουν προληπτικά ώστε για να καλύψουν το εν λόγω χάσμα δεξιοτήτων.

Για παράδειγμα, στην πόλη του Σικάγο στις ΗΠΑ, το έργο «Array of Things» [125] στοχεύει στη δημιουργία ενός ανοιχτού δικτύου αισθητήρων που έχει σχεδιαστεί για τη συλλογή δεδομένων σε πραγματικό χρόνο για το περιβάλλον της πόλης. Το έργο έχει μια επιτροπή εποπτείας και μια πολιτική απορρήτου, αλλά πολλές από τις προστασίες για τους πολίτες είναι ενσωματωμένες στον σχεδιασμό του ίδιου του δικτύου. Το έργο βασίζεται σε συγκεκριμένες τεχνολογικές ρυθμίσεις για την «συγκεκριμένη αποφυγή οποιασδήποτε πιθανής συλλογής δεδομένων ατόμων και η προστασία της ιδιωτικής ζωής ενσωματώνεται ήδη από το σχεδιασμό των αισθητήρων». Για παράδειγμα, οι αισθητήρες ήχου συλλέγουν μόνο δεδομένα σχετικά με τον όγκο περιβάλλοντος χωρίς εγγραφή ή μετάδοση ακατέργαστων δεδομένων μικροφώνου, ενώ οι εικόνες που επεξεργάζονται οι κάμερες θα υποστούν επεξεργασία μόνο ως αριθμητικά δεδομένα και οι εικόνες θα διαγραφούν αμέσως.

Σε συνέχεια των ανωτέρω θα πρέπει να δοθεί επιπλέον προσοχή στην προστασία των προσωπικών δεδομένων. Η αρχή Privacy by design αποτελεί θεμελιώδη αρχή του ΓΚΠΔ [53]με την οποία επιχειρείται η ελαχιστοποίηση των κινδύνων για την ασφάλεια και την προστασία των προσωπικών δεδομένων. Προκειμένου να μπορεί να αποδείξει συμμόρφωση προς τον ΓΚΠΔ, ο υπεύθυνος επεξεργασίας θα πρέπει να θεσπίζει εσωτερικές πολιτικές και να εφαρμόζει μέτρα τα οποία ανταποκρίνονται

[53] Αρ. 25 ΓΚΠΔ Λαμβάνοντας υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων από την επεξεργασία, ο υπεύθυνος επεξεργασίας εφαρμόζει αποτελεσματικά, τόσο κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας, κατάλληλα τεχνικά και οργανωτικά μέτρα, όπως η ψευδωνυμοποίηση, σχεδιασμένα για την εφαρμογή αρχών προστασίας των δεδομένων, όπως η ελαχιστοποίηση των δεδομένων, και την ενσωμάτωση των απαραίτητων εγγυήσεων στην επεξεργασία κατά τρόπο ώστε να πληρούνται οι απαιτήσεις του παρόντος κανονισμού και να προστατεύονται τα δικαιώματα των υποκειμένων των δεδομένων.

ειδικότερα στις αρχές της προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού. Κατά την ανάπτυξη, τον σχεδιασμό, την επιλογή και τη χρήση εφαρμογών, υπηρεσιών και προϊόντων που βασίζονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα ή επεξεργάζονται δεδομένα προσωπικού χαρακτήρα για την εκπλήρωση του έργου τους, οι παραγωγοί προϊόντων, υπηρεσιών και εφαρμογών θα πρέπει να ενθαρρύνονται να λαμβάνουν υπόψη τους το δικαίωμα προστασίας των δεδομένων, κατά την ανάπτυξη και τον σχεδιασμό τέτοιων προϊόντων, υπηρεσιών και εφαρμογών, ώστε, λαμβανομένων υπόψη των τελευταίων εξελίξεων, να διασφαλίζεται ότι οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία θα είναι σε θέση να εκπληρώνουν τις υποχρεώσεις τους όσον αφορά την προστασία των δεδομένων[54]. Οι αρχές της έξυπνης πόλης πρέπει να διασφαλίζουν ότι τα τρίτα μέρη με τα οποία επιλέγουν να συνεργαστούν είναι ικανά να αποδείξουν συμμόρφωση με τις απαιτήσεις του ΓΚΠΔ.

Οι πόλεις θα πρέπει να δίνουν επίσης έμφαση στη δημιουργία εργαλείων και τεχνολογιών, οι οποίες διευκολύνουν τα άτομα να έχουν τον πλήρη έλεγχο των προσωπικών τους δεδομένων, ενισχύοντας με αυτόν τον τρόπο την ανάπτυξη εμπιστοσύνης μεταξύ των διοικητικών αρχών και των πολιτών και ενθαρρύνοντας τη χρήση των εφαρμογών που προάγουν τις ψηφιοποιημένες υπηρεσίες των έξυπνων πόλεων. Ένα σύγχρονο παράδειγμα αποτελεί η εξής δράση της πόλης του Ελσίνκι [134]: Ως μέρος της δέσμευσης του Ελσίνκι να ενδυναμώσει τα άτομα βελτιώνοντας τα δικαιώματά τους στην αυτοδιάθεση όσον αφορά τα προσωπικά τους δεδομένα, η πόλη συνεργάσθηκε με τη μη κερδοσκοπική εταιρία MyData Global για τη δημιουργία προφίλ πολιτών και συστήματος διαχείρισης συναίνεσης δεδομένων. Το MyData παρέχει κατευθυντήριες αρχές ώστε οι άνθρωποι να έχουν περισσότερο έλεγχο στα ίχνη δεδομένων που αφήνουν στην καθημερινή τους ζωή. Οι άνθρωποι θα πρέπει να έχουν πρόσβαση στα δεδομένα τους, να μπορούν να τα εντοπίζουν και

[54] Αιτ. σκ. 71 ΓΚΠΔ Τέτοια μέτρα θα μπορούσαν να περιλαμβάνουν, μεταξύ άλλων, την ελαχιστοποίηση της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, την ψευδωνυμοποίηση δεδομένων προσωπικού χαρακτήρα, τη διαφάνεια όσον αφορά τις λειτουργίες και την επεξεργασία των δεδομένων προσωπικού χαρακτήρα, ώστε να μπορεί το υποκείμενο των δεδομένων να παρακολουθεί την επεξεργασία δεδομένων και να είναι σε θέση ο υπεύθυνος επεξεργασίας να δημιουργεί και να βελτιώνει τα χαρακτηριστικά ασφάλειας.

να δίνουν και να ανακαλούν τη συγκατάθεσή τους για χρήση τους από άλλους. Αυτό το μοντέλο επιτρέπει στους ανθρώπους να δίνουν τη συγκατάθεσή τους ώστε τα δεδομένα τους να χρησιμοποιηθούν για άλλο σκοπό από αυτόν για τον οποίο παρασχέθηκαν αρχικά. Για παράδειγμα, θα μπορούσαν να πάρουν δεδομένα που συλλέγονται σχετικά με τις αγοραστικές τους συνήθειες από μια κάρτα επιβράβευσης στο αγαπημένο τους παντοπωλείο και να τα χρησιμοποιήσουν σε ένα σύστημα προσωπικής οικονομικής διαχείρισης για να δουν πώς ξοδεύουν τα χρήματα σε παντοπωλεία. Εκτός από τη δυνατότητα παρακολούθησης και αλλαγής της συγκατάθεσής τους στα δεδομένα με την πάροδο του χρόνου, οι άνθρωποι μπορούν επίσης να μεταφέρουν τα δεδομένα τους από το ένα μέρος στο άλλο εάν αποφασίσουν να αλλάξουν υπηρεσίες.

Τέλος μια πόλη δεν πρέπει να χαρακτηρίζεται ΄έξυπνη΄΄ μόνο από το επίπεδο της τεχνολογίας που έχει υιοθετήσει και το εξελιγμένο επίπεδο παροχής των υπηρεσιών που προσφέρει στους κατοίκους της. ΄΄Έξυπνη΄΄ χαρακτηρίζεται επίσης η πόλη που προβλέπει να παραμείνει ΄΄βιώσιμη΄΄ μπροστά στις σημερινές προκλήσεις της έντονης αστικοποίησης. Τα κίνητρα της δεν πρέπει να είναι μόνο η αποκλειστική οικονομική εκμετάλλευση όλων των δεδομένων που παράγονται εντός της, αλλά η ανθρωποκεντρική προσέγγιση, η οποία θέτει ως στόχο την ευημερία και την εξασφάλιση όλων των θεμελιωδών δικαιωμάτων των κατοίκων της μέσα σε ένα ασφαλές αλλά και σύγχρονο περιβάλλον.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Marijn Janssen, Karin Axelsson, Olivier Glassey, Bram Klievink, Robert Krimmer, Ida Lindgren, Peter Parycek, Hans J. Scholl, Dmitrii Trutnev, Electronic Government, 16th IFIP WG 8.5 International Conference, EGOV 2017 St. Petersburg, Russia, September 4–7, 2017 Proceedings, Springer
2. Mapping Smart Cities in the EU, Directorate General for Internal policies, Policy Department, Economic and Scientific Policy, 2014, European parliament, https://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/507480/IPOLITRE_ET(2014)507480_EN.pdf
3. Sara Bannerman and Angela Orasch, Privacy and Smart Cities, January 2019, Mcmaster University, https://smartcityprivacy.ca/wp-content/uploads/2019/01/Bannerman-Orasch-Privacy-and-Smart-Cities-A-Canadian-Survey-v1-2019.pdf
4. https://www.un.org/development/desa/en/news/population/2018-revision-of-world-urbanization-prospects.html
5. Chris Conley, ACLU of Northern California, PUBLISHED BY THE ACLU OF CALIFORNIA Technology & Civil Liberties Project November 2017, MAKING SMART DECISIONS ABOUT SMART CITIES ACLUNC.ORG/SMARTCITIES/
6. https://www.eea.europa.eu/policy-documents/com-2010-2020-europe-2020
7. [1] https://cltc.berkeley.edu/2021/03/16/smart-cities/, προσπελάστηκε 10.3.2022
8. H. Samih, Smart cities and internet of things, Journal of Information Technology Case and Application Research, 2.4.2019, https://doi.org/10.1080/15228053.2019.1587572
9. Saraju P. Mohanty, Uma Choppali, and Elias Kougianos, Everything You wanted to Know about Smart Cities, July 2016, IEEE Consumer Electronics Magazine 5(3):60-70, http://dx.doi.org/10.1109/MCE.2016.2556879
10. Renata Dameri, Searching for Smart City definition: a comprehensive proposal, INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY, October, 2013, DOI: 10.24297/ijct.v11i5.1142
11. Bhagya Nathali Silvaa, Murad Khanb, Kijun Han, Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities, Sustainable Cities and Society 38 (2018) 697–713, https://doi.org/10.1016/j.scs.2018.01.053
12. https://www.thalesgroup.com/en/worldwide-digital-identity-and-security/iot/magazine/singapore-worlds-smartest-city
13. https://www.ny-engineers.com/blog/how-new-york-is-becoming-a-smart-city προσπελάστηκε 10.3.2022
14. Robert R. Harmon, Enrique G. Castro-Leon, Sandhiprakash Bhide, Smart Cities and the Internet of Things, 2015 Proceedings of PICMET '15: Management of the Technology Age, https://www.researchgate.net/figure/A-Smart-City-IoT-System_fig1_305183838
15. Patel, K. K., & Patel, S. M. (2016). Internet of things-IoT: definition, characteristics, architecture, enabling technologies, application & future challenges. Int. J. Eng. Sci. Comput. σελ. 3-4 https://ijesc.org/upload/8e9af2eca2e1119b895544fd60c3b857.Internet%20of%20Things-IOT%20Definition,%20Characteristics,%20Architecture,%20Enabling%20Technologies,%20Application%20&%20Future%20Challenges.pdf
16. https://gcn.com/data-analytics/2017/06/driving-the-future-of-smart-cities-with-iot/304281/ προσπελάστηκε 10.3.2022
17. Andrea Zanella, Nicola Bui, Angelo Castellani, Lorenzo Vangelista, Michele Zorzi, Internet of Things for Smart Cities, IEEE INTERNET OF THINGS JOURNAL, VOL. 1, NO. 1, FEBRUARY 2014, https://www.researchgate.net/publication/260540297_Internet_of_Things_for_Smart_Cities

18. H. Arasteh, V. Hosseinnezhad, V. Loia, A. Tommasetti, O. Troisi, M. Shafie-khah, P. Siano, Iot-based Smart Cities: a Survey, 978-1-5090-2320-2/16/$31.00 2016 IEEE, https://ieeexplore.ieee.org/document/7555867
19. Saber Talari, Miadreza Shafie-khah, Pierluigi Siano, Vincenzo Loia, Aurelio Tommasetti and Jo o P. S. Catal, A Review of Smart Cities Based on the Internet of Things Concept, Energies 2017, 10, 421; doi:10.3390/en10040421
20. Abbas Shah Syed, Daniel Sierra-Sosa, Anup Kumar and Adel Elmaghraby, IoT in Smart Cities: A Survey of Technologies, Practices and Challenges, Smart Cities 2021, 4, 429–475. https://doi.org/10.3390/smartcities4020024, https://www.mdpi.com/journal/smartcities
21. ENISA Threat Landscape Report 2018, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018\
22. Yasir Mehmood, Farhan Ahmad, Ibrar Yaqoob, Asma Adnane, Muhammad Imran, and Sghaier Guizani, Internet-of-Things-Based Smart Cities: Recent Advances and Challenges, https://www.telecompaper.com/news/global-iot-markettoreach-usd-17-tln-in-2020-idc--1085269, accessed, October 20, 2016, DIO:10.1109/MCOM.2017.1600514
23. https://www.bbc.com/news/technology-57012725 προσπελάστηκε 10.3.2022
24. https://hbr.org/2017/04/smart-cities-are-going-to-be-a-security-nightmare
25. [1]https://www.smartcitiesworld.net/news/news/which-smart-city-tech-poses-the-greatest-risk-for-cyber-attacks-6249, προσπελάστηκε 10.3.2022
26. Aboul Ella Hasanenien, cybersecurity and Secure Information systems, Challenges and Solutions in Smart Environments, https://doi.org/10.1007/978-3-030-16837-7
27. Hadi Habibzadeha, Brian H. Nussbaum, Fazel Anjomshoc, Burak Kantarci, Tolga Soyata, A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities, Sustainable Cities and Society 50 (2019) 101660, https://doi.org/10.1016/j.scs.2019.101660
28. Lilian Edwards, Privacy, Security and Data Protection in Smart Cities: a Critical EU Law Perspective, CREATe Working Paper Series DOI: 10.5281/zenodo.34501
29. Zaigham Mahmood, Smart Cities, Development and Governance Frameworks, https://doi.org/10.1007/978-3-319-76669-0
30. [1] https://www.dilitrust.com/en/blog/cyber-attacks-smart-cities/ προσπελάστηκε 10.3.2022
31. Chen Ma, Smart city and cyber-security; technologies used, leading challenges and future recommendations, Energy Reports 7 (2021) 7999–8012, https://doi.org/10.1016/j.egyr.2021.08.124
32. Connected Places: Cyber Security Principles, Secure design, build and managementof public realm technology, infrastructure, and data-rich environmentsfor local authorities, National Cyber Security Center, 2021, https://www.ncsc.gov.uk/collection/connected-places-security-principles
33. https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32016R0679
34. Jos L. Hern ndez-Ramos, Juan A. Martinez, Vincenzo Savarino, Marco Angelini, and Vincenzo Napolitano, Antonio F. Skarmeta, Gianmarco Baldini, Security and Privacy in Internet of Things-Enabled smart cities: Challenges and Future Direction, IEEE Computer and Reliability Societies, January/February 2021, DOI 10.1109/MSEC.2020.3012353
35. https://ec.europa.eu/justice/article-29/documentation/opinion
36. Rob Kitchin and Martin Dodge, The (In)Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention, JOURNAL OF URBAN TECHNOLOGY 2019, VOL. 26, NO. 2, 47–65, https://doi.org/10.1080/10630732.2017.1408002
37. Gang Pan, Guande Qi, Wangsheng Zhang, Shijian Li, and Zhaohui Wu, Laurence Tianruo Yang, Trace Analysis and Mining for Smart Cities: Issues, Methods, and Applications, IEEE Communications Magazine, June 2013

38. S.M. Rinaldi; J.P. Peerenboom; T.K. Kelly, Identifying, understanding, and analyzing critical infrastructureinterdependencies,https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=5488303https://doi.org/10.1109/37.969131
39. https://edition.cnn.com/2001/US/05/08/calif.power.crisis.02/
40. Dalmacio V. Posadas Jr. After the Gold Rush: The Boom of the Internet of Things, and the
41. Busts of Data-Security and Privacy, Fordham Intellectual Property, Media and Entertainment Law Journal, Volume 28 XXVIII, 2017
42. Cesar Cerrudo, An Emerging US (and World) Threat: Cities Wide Open to Cyber Attacks, 2015 https://ioactive.com/pdfs/IOActive_HackingCitiesPaper_CesarCerrudo.pdf
43. ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 8/2014 on the on Recent Developments on the Internet of Things, https://ec.europa.eu/justice/article 29/documentation/opinion-recommendation/files/2014/wp223_en.pdf
44. Talal Ashraf Butt and Muhammad Afzaal, Security and Privacy in Smart Cities: Issues and Current Solutions, Springer Nature Switzerland AG 2019, Smart Technologies and Innovation for a Sustainable Future, Advances in Science, Technology & Innovation, https://doi.org/10.1007/978-3-030-01659-3_37
45. [1] https://bigdataldn.com/intelligence/challenges-of-big-data-in-cybersecurity/ προσπελάστηκε 10.3.2022
46. https://eur-lex.europa.eu/legal-content/EI/ALL/?uri=CELEX:32019R0881
47. https://www.digital14.com/docs/default-source/reports/cyber-resilience-report.pdf προσπελάστηκε 2.4.2022
48. https://safenet.gemalto.com/iot-2018/?utm_campaign=iot&utmmedium=press-release&utm_source=-&utm_content=report-2018
49. https://www.netscout.com/sites/default/files/2021- προσπελάστηκε 2.4.2022
50. 04/ThreatReport_2H2020_FINAL_0.pdf
51. https://bits.blogs.nytimes.com/2015/06/10/traffic-hacking-caution-light-is-on
52. VIKAS HASSIJA, VINAY CHAMOLA, VIKAS SAXENA, DIVYANSH JAIN, PRANAV GOYAL, BIPLAB SIKDAR, A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures, IEEE access, VOLUME 7, 2019, Digital Object Identifier 10.1109/ACCESS.2019.2924045
53. Cyber security for Smart Cities, ENISA, December 2015, https://www.enisa.europa.eu/events/enisa-workshop-on-cyber-security-for-public-transport-in-smart-cities
54. Arne Hintz, Lina Dencik, Karin Wahl-Jorgensen, Digital Citizenship and Surveillance Society, International Journal of Communication 11(2017), 731–739, https://orca.cardiff.ac.uk/97853/8/Digital%20Citizenship%20and%20Surveillance%20Society.pdf
55. Antoni Martınez-Balleste, Pablo A. Perez-Martınez, Agusti Solanas, The Pursuit of Citizens Privacy: A Privacy-Aware Smart City is Possible, IEEE Communications Magazine, June 2013 DOI: 10.1109/MCOM.2013.6525606, http://e-madina.org/documents/Privacy/A%20Privacy-Aware%20Smart%20City%20Is%20Possible.pdf
56. https://www.theguardian.com/technology/2015/mar/11/internet-of-things-hacked-online-perils-future προσπελάστηκε 2.4.2022
57. https://www.theguardian.com/technology/2015/jul/15/internet-of-things-mass-surveillance προσπελάστηκε 2.4.2022
58. lias O. Pappas, Patrick Mikalef, Yogesh K. Dwivedi, Letizia Jaccheri, John Krogstie, Matti Mantymaki (Eds.) Digital Transformation for a Sustainable Society in the 21st Century, 18th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society, I3E 2019, Trondheim, Norway, September 18–20, 2019, Proceedings
59. K106 Λίλιαν Μήτρου, Η προστασία της Ιδιωτικότητας στην Πληροφορική και τις Επικοινωνίες Η νομική διάσταση

60. https://securitydelta.nl/innovation/living-labs/lab/3-stratumseind, προσπελάστηκε 2.4.2022
61. Galič, Maša, Surveillance and privacy in smart cities and living labs, Tilburg University, 2019, https://www.google.com/search?client=safari&rls=en&q=Gali%C4%8D%2C+Ma%C5%A1a%2C+Surveillance+and+privacy+in+smart+cities+and+living+labs%2C+Tilburg+University%2C+2019&ie=UTF-8&oe=UTF-8
62. Steven I. Friedland , Drinking from the Fire Hose: How Massive Self-Surveillance from the Internet of Things is Changing the Face of Privacy, Volume 119I ssue 3, April 2017, https://researchrepository.wvu.edu/wvlr/vol119/iss3/5
63. Friedewald, Michael; Leimbach, Timo; Wright, David; Gutwirth, Serge; De Hert, Paul; Gonzalez Fuster, Gloria; Langheinrich, Marc; Ion, Iulia, Privacy and Trust in the Ubiquitous Information Society. Analysis of the impact of convergent and pervasive ICT on privacy and data protection and needs and options for development of the legal framework, 2009, https://researchportal.vub.be/en/publications/privacy-and-trust-in-the-ubiquitous-information-society-analysis--2
64. Serge Gutwirth, Ronald Leenes, Paul de Hert, Yves Poullet, European Data Protection: Coming of Age, DOI 10.1007/978-94-007-5170-5, Springer Dordrecht Heidelberg New York London
65. https://edps.europa.eu/sites/edp/files/publication/12-06-08_smart_metering_en.pdf
66. Gemma Galdon-Clavell, (Not so) smart cities?: The drivers, impact and risks of surveillance enabled smart environments, Science and Public Policy 40 (2013) pp. 717–723, doi:10.1093/scipol/sct070
67. De Hert, Paul; Kloza, Dariusz, The challenges to privacy and data protection posed by smart grids, Europ ische Projektkultur als Beitrag zur Rationalisierung des Rechts.Tagungsband des 14. Internationalen Rechtsinformatik Symposions IRIS 2011 (pp. 191196), https://researchportal.vub.be/en/publications/the-challenges-to-privacy-and-data-protection-posed-by-smart-grid
68. Rob Kitchin, Getting smarter about smart cities: Improving data privacy and data security, January2016,https://www.researchgate.net/publication/293755608_Getting_smarter_about_smart_cities_Improving_data_privacy_and_data_security
69. Robert P. Minch, Location Privacy in the Era of the Internet of Things and Big Data Analytics, 2015 48th Hawaii International Conference on System Sciences, DOI 10Æ1109ØHICSSÆ2015Æ185, https://scholarworks.boisestate.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1050&context=itscm_facpubs
70. A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," Pervasive Comput. IEEE, vol. 2, no. 1, pp. 46–55, 2003.
71. Vincent, J. (2014) London's bins are tracking your smartphone. The Independent. 10 June 2014. www.independent.co.uk/life-style/gadgets-and-tech/news/updated-londons-bins-are-tracking-your-smartphone-8754924.html
72. Astrid Voorwinden, The privatised city: technology and public-private partnerships in the smart city, https://www.tandfonline.com/loi/rlit20, 2021, https://doi.org/10.1080/17579961.2021.1977213
73. http://www.thejakartapost.com/news/2016/01/11/jakarta-smart-city-lounge-opens-doors-public.html, προσπελάστηκε 2.4.2022
74. Smart Cities: Utopian Vision, Dystopian Reality, 2017, https://privacyinternational.org/report/638/smart-cities-utopian-vision-dystopian-reality
75. [1] https://www.law.ox.ac.uk/business-law-blog/blog/2018/04/law-and-autonomous-systems-series-cities-corporations-privatization προσπελάστηκε 5.4.2022
76. https://www.theguardian.com/sustainable-business/2016/jul/04/gurgaon-life-city-built-private-companies-india-intel-google προσπελάστηκε 2.4.2022

77. Smarter than Smart: Rio de Janeiro's Flawed Emergence as a Smart City," Christopher Gaffney and Cerianne Robertson, 29 April 2016, available at: http://www.tandfonline.com/doi/ abs/10.1080/10630732.2015.1102423?journalCode=cjut20
78. [1] https://privacyinternational.org/learn/public-private-surveillance-partnerships προσπελάστηκε 2.4.2022
79. https://privacyinternational.org/long-read/3971/one-ring-watch-them-all, προσπελάστηκε 2.4.2022
80. Wajeeha Ahmad1 and Elizabeth Dethy, Preventing Surveillance Cities: Developing a Set of Fundamental Privacy Provisions, Journal of Science Policy & Governance, JSPG., Vol. 15, Issue 1, October 2019
81. [1]https://www.imeccityofthings.be/en/blog/smart-city-meter-2019 προσπελάστηκε 2.4.2022
82. Ahmet Denker, PROTECTION OF PRIVACY AND PERSONAL DATA IN THE BIG DATA ENVIRONMENT OF SMART CITIES, The International Archives of the Photogrammetry, 2021, https://doi.org/10.5194/isprs-archives-XLVI-4-W5-2021-181-2021
83. Rob Heyman, Jonas Breuer, Athena Christofi, Mapping and modelling of the Smart Cities ecosystem and defining responsibilities for Smart Cities, SPECTRE, https://spectreproject.be/
84. [WP29, 2010].
85. Van Zeeland, Dorine Johanna; Breuer, Jonas; Christofi, Athena; Pierson, Jo, Personal data protection in smart cities: Roundtable report, 2019, Brussels
86. Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0, Adopted on 07 July 2021, EDPB
87. Draper, 2016. 'From Privacy Pragmatist to Privacy Resigned: Challenging Narratives of Rational Choice in Digital Privacy Debates', Policy & Internet, 9(2), 232-251. https://onlinelibrary.wiley.com/doi/full/10.1002/poi3.142]
88. STAVROULA RIZOU , EUGENIA ALEXANDROPOULOU-EGYPTIADOU, AND KONSTANTINOS E. PSANNIS, (Member, IEEE), GDPR Interference With Next Generation 5G and IoT Networks, Digital Object Identifier 10.1109/ACCESS.2020.3000662
89. Lilian Edwards, Privacy, Security and Data Protection in Smart Cities: a Critical EU Law Perspective CREATe Working Paper 2015/11 (December 2015)
90. **Athena Christofi, Ellen Wauters and Peggy Valcke,** Smart Cities, Data Protection and the Public Interest Conundrum: What Legal Basis for Smart City Processing?, European Journal of Law and Technology, Vol 12 No.1 (2021)
91. Γνώμη 15/2011 σχετικά με τον ορισμό της συγκατάθεσης, WP 187, 13 Ιουλίου 2011, σ. 12, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_el.pdf
92. Athena Christofi, under the supervision of Prof. Peggy Valcke, Smart cities and the data protection framework in context, D.1.2. https://www.google.com/search?client=safari&rls=en&q=91.+Athena+Christofi%2C+under+the+supervision+of+Prof.+Peggy+Valcke%2C+Smart+cities+and+the+data+protection+framework+in+context%2C+D.1.2.&ie=UTF-8&oe=UTF-8
93. Nadezhda Purtova, The law of everything. Broad concept of personal data and future of EU data protection law, LAW, INNOVATION AND TECHNOLOGY, 2018, Routledge Taylor and Francis Group, 2018, https://doi.org/10.1080/17579961.2018.1452176
94. Christopher A. Holecek, Can a City Invade Your Privacy?: Does the Rise of Smart Cities Mean the Fall of Privacy, https://www.google.com/search?client=safari&rls=en&q=93.+Christopher+A.+Holecek%2C+Can+a+City+Invade+Your+Privacy%3F%3A+Does+the+Rise+of+Smart+Cities+Mean+the+Fall+of+Privacy&ie=UTF-8&oe=UTF-8
95. EDPS, 'Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit' (2017)

96. Article 29 Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC', Adopted on 9 April 2014, WP 217, at p. 22
97. Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation, 6.4.2018, VERSION 2, Data Protection Network, https://www.google.com/search?client=safari&rls=en&q=96.+Guidance+on+the+use+of+Legitimate+Interests+under+the+EU+General+Data+Protection+Regulation%2C+6.4.2018%2C+VERSION+2%2C+Data+Protection+Network&ie=UTF-8&oe=UTF-8
98. Dutch Data Protection Authority, 'Questions about Wi-Fi and Bluetooth tracking' https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/internet-en-telecom#faq
99. Jonas Breuer, Ellen Wauters, Ine van Zeeland, Athena Christofi, Identifying GDPR enforcement problems and requirements in Smart Cities, SPECTRE, https://spectreproject.be/
100. 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, April 2017
101. Laurens Vandercruyssea,∗, Caroline Butsb, Micha l Doomsa, A typology of Smart City services: The case of Data Protection Impact Assessment Cities 104 (2020) 102731 www.elsevier.com/locate/cities
102. Smart Cities Onderzoeksrapport bescherming van persoonsgegevens in de ontwikkeling van Nederlandse Smart Cities, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/onderzoeksrapport_smart_cities_def.pdf
103. Elena Simperl, Kieron O'Hara, Analytical Report 3: Open Data and Privacy, European Data Portal, 2020, doi: 10.2830/532195
104. Opinion 03/2013 on purpose limitation**,** ARTICLE 29 DATA PROTECTION WORKING PARTY, 2013
105. Priyank Jain* , Manasi Gyanchandani and Nilay Khare, Big data privacy: a technological perspective and review, Jain et al. J Big Data (2016) 3:25DOI 10.1186/s40537-016-0059-y
106. Charith Perera, Rajiv Ranjan, Lizhe Wang, Samee U. Khan, Albert Y. Zomaya, Big Data Privacy in the Internet of Things Era
107. DIRECTORATE GENERAL FOR INTERNAL POLICIES POLICY DEPARTMENT C: CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS, CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS, Big Data and smart devices and their impact on privacy, STUDY, 2015
108. Eiman Al Nuaimi1, Hind Al Neyadi1, Nader Mohamed2* and Jameela Al-Jarood,cApplications of big data to smart cities, Al Nuaimi et al. Journal of Internet Services and Applications (2015) 6:25, DOI 10.1186/s13174-015-0041-5
109. Martin Strohbach, Holger Ziekow, Vangelis Gazis, and Navot Akiva, Towards a Big Data Analytics Framework for IoT and Smart City Applications, p.257, Springer Cham Heidelberg New York Dordrecht London,2015
110. Ibrahim Abaker Targio Hashema,∗, Victor Changb, Nor Badrul Anuara,∗,Kayode Adewolea, Ibrar Yaqooba, Abdullah Gania, Ejaz Ahmeda, Haruna Chiroma, The role of big data in smart cityIbrahim, International Journal of Information Management, http://dx.doi.org/10.1016/j.ijinfomgt.2016.05.002
111. Big data, artificial intelligence, machine learning and data protection 2017090, Version: 2.2, Information Commissioner's Office,
112. Hatem Ben Sta, Quality and the efficiency of data in ''Smart-Cities'', Future Generation Computer Systems 74 (2017) 409–416, http://dx.doi.org/10.1016/j.future.2016.12.021
113. David Kramer, Smart cities will need big data, http://dx.doi.org/10.1063/PT.3.2110

114. Prof. Dr. Lilian Mitrou, DATA PROTECTION, RTIFICIAL INTELLIGENCE AND COGNITIVE SERVICES IS THE GENERAL DATA PROTECTION REGULATION (GDPR)"ARTIFICIAL INTELLIGENCE PROOF?
115. Stefaan G. Verhulst, Reimagining data responsibility: 10 new approaches toward a culture of trust in re-using data to address critical public needs, Data & Policy (2021), 3: e doi:10.1017/dap.2021.4
116. ΛΕΥΚΗ ΒΙΒΛΟΣ Τεχνητή νοημοσύνη - Η ευρωπαϊκή προσέγγιση της αριστείας και της εμπιστοσύνης, Ευρωπαϊκή Επιτροπή, 2020
117. Artificial Intelligence in smart cities and urban mobility , How can Artificial Intelligence applications be used in urban mobility and smart cities and how can their deployment be facilitated, Ευρωπαϊκό Κοινοβούλιο, 2020
118. ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΓΡΑΜΜΕΣ ΔΕΟΝΤΟΛΟΓΙΑΣ ΓΙΑ ΑΞΙΟΠΙΣΤΗ ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ, Ομάδα εμπειρογνωμόνων υψηλού επιπέδου για την τεχνητή νοημοσύνη
119. Απόστολος Βόρρα, Λίλιαν Μήτρου, Τεχνητή νοημοσύνη και προσωπικά δεδομένα, Μια θεώρηση υπό το πρίσμα του Ευρωπαϊκού Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 2016/679, Δ.Ι.ΤΕ τ. 4/2018
120. https://www.businessgoing.digital/artificial-intelligence-in-smart-cities, προσπελάστηκε 12.5.2022
121. Zaheer Allama,*, Zaynah A. Dhunny, On big data, artificial intelligence and smart cities, Cities 89 (2019) 80–91, https://doi.org/10.1016/j.cities.2019.01.032
122. Gang Pan, Guande Qi, Wangsheng Zhang, Shijian Li, and Zhaohui Wu, Laurence Tianruo Yang, Trace Analysis and Mining for Smart Cities: Issues, Methods, and Applications, IEEE Communications Magazine • June 2013
123. Elena Simperl, Richard Gomer, Analytical Report 3: Open Data and Privacy, European Data Portal, 2020, doi: 10.2830/532195
124. [http://globalsmartcitiesalliance.org/wpcontent/uploads/2020/11/Open-Data-v1.2.pdf]
125. Deloitte, Smart Cities Big Data, January 2015, https://www2.deloitte.com/content/dam/Deloitte/fpc/Documents/services/systemes-dinformation-et-technologie/deloitte_smart-cities-big-data_en_0115.pdf
126. Theo Bass, Emma Sutherland and Tom Symons, Reclaiming the Smart City Personal data, trust and the new commons, Decode, 2018
127. Dalla Corte, Lorenzo, Safeguarding data protection in an open data world: On the idea of balancing open data and data protection in the development of the smart city environment, 2020, Tilburg University
128. Ben Green, Gabe Cunningham, Ariel Ekblaw, Paul Kominers, Andrew Linzer, Susan Crawford, OPEN DATA PRIVACY A risk-benefit, process-oriented approach to sharing and protecting municipal data, 2017, https://cyber.harvard.edu/publications/2017/02/opendataprivacyplaybook
129. Ann Cavoukian, Daniel Castro, Big Data and Innovation, Setting the Record Straight: De-identification Does Work, Information and Privacy Commissioner, Ontario, Canada, Information Technology and Innovation Foundation, 2014, www.ipc.on.ca
130. https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html, προσπελάστηκε 12.5.2022
131. https://www.nytimes.com/2018/01/29/world/middleeast/strava-heat-map.html] προσπελάστηκε 12.5.2022
132. https://fpf.org/blog/if-you-cant-take-the-heat-map-benefits-risks-of-releasing-location-datasets/ προσπελάστηκε 12.5.2022

133. City of Seattle (2016) 'Open Data Policy V1.0' [online]. Seattle: City of Seattle. Available from http://www.seattle.gov/Documents/Departments/SeattleGovPortals/CityServices/OpenDataPolicyV1.pdf,] προσπελάστηκε 12.5.2022
134. Making smart cities cybersecure, A report from the Deloiite Center for government insights, https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/Report_making_smart_cities_cyber_secure.pdf προσπελάστηκε 12.5.2022
135. DATA PEOPLE CITIES EUROCITIES CITIZEN DATA PRINCIPLES IN ACTION
136. Dr. Saraju P. Mohanty, Everything you wanted to know about smart cities, IEEE Distinguished lecture, CE Society webinar, 5.10.2017
137. Steven I. Friedland Elon University School of Law, Drinking from the Fire Hose: How Massive Self-Surveillance from the Internet of Things is Changing the Face of Privacy Volume 119Issue 3 Article 5 April 2017,https://researchrepository.wvu.edu/wvlr