ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ

ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΤΜΗΜΑ ΝΟΜΙΚΗΣ

ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

«INTERNET OF THINGS-RFID ΚΑΙ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ: ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΑΠΟΡΡΗΤΟΥ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ (IoT)»

Διπλωματική Εργασία

της

Παρασκευής Τζιούφα

Θεσσαλονίκη, Φεβρουάριος 2019

«INTERNET OF THINGS-RFID ΚΑΙ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ: ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΑΠΟΡΡΗΤΟΥ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ (IoT)»

Τζιούφα Παρασκευή

Πτυχιούχος Εφαρμοσμένης Πληροφορικής ,Πανεπιστημίου Μακεδονίας, 2016

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΟ ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής	Επιβλέπουσα Καθηγήτρια
Κωνσταντίνος Ψάννης	Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 20/02/2019

Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου	Κωνσταντίνος Ψάννης	Ευθύμιος Ταμπούρης
.....	.....	.....

Τζιούφα Παρασκευή

Περίληψη

Η παρούσα διπλωματική εργασία αποτελεί μια μελέτη του Διαδικτύου των Πραγμάτων (IoT), εστιάζοντας στους τομείς εφαρμογής του ,στις νέες ψηφιακές τεχνολογίες και ειδικότερα στα θέματα ασφαλείας και προστασίας προσωπικών δεδομένων που προκύπτουν κατά τη διάρκεια της επέκτασής του. Το Διαδίκτυο των πραγμάτων έχει αλλάξει ραγδαία την καθημερινότητα των ανθρώπων χάριν των ωφελειών που προσφέρουν οι IoT συσκευές στους διαφόρους τομείς της ζωής τους. Με τη διασύνδεση εκατομμυρίων συσκευών και αντικειμένων στο Διαδίκτυο , στέλνονται και λαμβάνονται χιλιάδες δεδομένα διευκολύνοντας έτσι την επικοινωνία μεταξύ ανθρώπων και συσκευών. Αυτό φυσικά εκτός από οφέλη κρύβει και κινδύνους καθώς η αύξηση των διασυνδεδεμένων συσκευών σε συνδυασμό με τα κενά ασφαλείας που μπορεί να υπάρχουν, δίνουν περισσότερες ευκαιρίες ώστε να πραγματοποιηθούν επιθέσεις και να διαρρεύσουν δεδομένα. Δυστυχώς σε πολλές από τις συσκευές του Διαδικτύου των Πραγμάτων δεν έχουν ληφθεί τα κατάλληλα μέτρα προστασίας ,όπως η κρυπτογράφηση, εξαιτίας της αδυναμίας τους να χρησιμοποιήσουν νέα πρωτόκολλα ασφαλείας ή εξαιτίας των ελλείψεων τους από τους κατασκευαστές τους. Παράλληλα δημιουργούνται και άλλα ζητήματα ως προς την διασφάλιση των Προσωπικών Δεδομένων. Πολλοί χρήστες δεν γνωρίζουν ότι συλλέγονται δεδομένα τους ή ακόμη δεν έχουν δώσει τη συγκατάθεσή τους για την επεξεργασία τους. Πολλά από τα δεδομένα που συλλέγουν οι αισθητήρες μπορούν να εντοπίσουν τους χρήστες και ακόμη και να καταρτίσουν ένα προφίλ για αυτούς. Αυτό συνεπάγεται τη συνεχή παραβίαση του απορρήτου, με αποτέλεσμα να χάνεται κάθε έννοια ιδιωτικότητας. Για την αντιμετώπιση όλων αυτών των κινδύνων απαραίτητη είναι η αναγκαιότητα υιοθέτησης μηχανισμών ασφαλείας. Παράλληλα η Ευρωπαϊκή Νομοθεσία έχει μεριμνήσει για την ασφαλή συλλογή και επεξεργασία προσωπικών δεδομένων στο διαδίκτυο των πραγμάτων.

Ως εκ τούτου αντικείμενο αυτής της εργασίας είναι η εισαγωγή στον κόσμο του Διαδικτύου των Πραγμάτων και σε θέματα ασφαλείας και απόρρητου που προκύπτουν ως προς την επεξεργασία προσωπικών δεδομένων. Αρχικά γίνεται μία παρουσίαση των συστημάτων και της έννοιας του Διαδικτύου των Πραγμάτων συνδέοντάς το ταυτόχρονα με τις νέες Ψηφιακές Τεχνολογίες. Εν συνεχεία γίνεται μία εκτενής περιγραφή της τεχνολογίας του IoT και των RFID συστημάτων, ενώ ακολούθως προβάλλονται οι διάφοροι κίνδυνοι που προκύπτουν στο IoT. Η επόμενη ενότητα αφορά τις τεχνικές ασφαλείας που μπορούν να εφαρμοστούν στο Διαδίκτυο των

Πραγμάτων καθώς και όλα τα απαραίτητα μέτρα για τη διασφάλιση των Προσωπικών Δεδομένων από επιθέσεις . Παράλληλα στο 7ο κεφάλαιο της εργασίας γίνεται μία συγκριτική μελέτη για τη διασφάλιση των προσωπικών δεδομένων σε τέσσερις Έξυπνες Ευρωπαϊκές πόλεις (Smart Cities). Κατόπιν, το 8ο κεφάλαιο εστιάζει στα προβλήματα προστασίας που προκύπτουν από την επεξεργασία προσωπικών δεδομένων στα συστήματα του διαδικτύου των πραγμάτων και τέλος, το τελευταίο κεφάλαιο δίνει έμφαση στη σημαντικότητα των αρχών της Ευρωπαϊκής νομοθεσίας για την προστασία των προσωπικών δεδομένων, μέσω του Γενικού Κανονισμού Προστασίας Δεδομένων 2016/679, της γνωμοδότησης 8/2014 καθώς και λοιπών Ευρωπαϊκών οδηγιών και νόμων.

Λέξεις Κλειδιά: Διαδίκτυο των Πραγμάτων (IoT), Προσωπικά Δεδομένα ,RFID ,Κίνδυνοι Ασφάλεια, Απόρρητο , Ιδιωτικότητα, IoT συσκευές ,Αισθητήρες

Abstract

This diploma thesis is a study on the Internet of Things (IoT), focusing on application uses, new digital technologies, and in particular security and privacy issues that arise during its expansion. The Internet of Things has rapidly changed people's everyday lives via the benefits of IOT devices in various aspects of life. By linking millions of devices and objects to the Internet, thousands of data are sent and received, thus facilitating communication between people and devices. This, of course, besides its benefits also hides risks, as the increase of interconnected devices, combined with the security gaps that may exist, provide more opportunities for attacks and leakage of data. Unfortunately, for many of the devices in the Internet of Things have no appropriate security measures, such as encryption, because of the devices' inability to use new security protocols, or because of their deficiencies for which their makers are responsible. At the same time other issues arise as to the security of Personal Data. Many users do not know that their data is being collected or have not given their consent to the data's processing. Many of the data collected by sensors can detect users and even create a profile for them. This entails a continuous violation of privacy, resulting its loss. To address all these risks, the need to adopt security mechanisms is essential. At the same time, European legislation has ensured the safe collection and processing of personal data on the Internet of Things.

Therefore, the subject of this thesis is the introduction to the world of the Internet of Things and the security and confidentiality issues arising in the processing of personal data. Initially, a presentation of the systems and concept of the Internet of Things is made, linking it to the new Digital Technologies simultaneously. An extensive description of the technology of the IOT and RFID systems is then made, and the various dangers that arise in the IOT are then presented. The next section is about the security techniques that can be applied to the Internet of Things and all the steps that are necessary to secure Personal Data from attacks. At the same time, in the 7th chapter of the thesis, a comparative study is being carried out to secure personal data in four European Smart Cities. The eighth chapter then focuses on the problems of protection resulting from the processing of personal data in the systems of the Internet of Things, finally the last chapter emphasizes on the importance of the principles of European legislation on the protection of personal data through the General Data Protection Regulation 2016/679, Opinion 8/2014 as well as other European opinions and laws.

Keywords: Internet of Things (IOT), Personal Data, RFID, Security, Privacy, IoT devices, Sensors

Ευχαριστίες

Θα ήθελα να ευχαριστήσω θερμά τους επιβλέποντες καθηγητές μου , κα. Ευγενία Αλεξανδροπούλου- Αιγυπτιάδου και κ. Κωνσταντίνο Ψάννη , για την αμέριστη βοήθεια τους, αλλά κυρίως για την εμπιστοσύνη και την υπομονή που μου έδειξαν κατά τη διάρκεια υλοποίησης της διπλωματικής μου εργασίας .

Ιδιαίτερες ευχαριστίες για ακόμη μια φορά στην κα. Αλεξανδροπούλου που στάθηκε σημαντικός αρωγός στην προσπάθειά μου , τόσο στο προπτυχιακό όσο και στο μεταπτυχιακό κύκλο σπουδών μου ,υποστηρίζοντας και καθοδηγώντας με σε κάθε φάση της πορείας μου.

Τέλος, θα ήθελα να ευχαριστήσω την οικογένειά μου, που με υπομονή και κουράγιο πρόσφεραν την απαραίτητη ηθική συμπαράσταση για την ολοκλήρωση της μεταπτυχιακής μου εργασίας.

Σας Ευχαριστώ πολύ

Περιεχόμενα

ΕΙΣΑΓΩΓΗ

Είναι δύσκολο να σκεφτούμε τη σημερινή κοινωνία χωρίς τη σύγχρονη τεχνολογία. Τις τελευταίες δεκαετίες η χρήση των υπολογιστών, των κινητών τηλεφώνων, του Διαδικτύου και των νέων τεχνολογιών ,αποτελούν πλέον αναπόσπαστο κομμάτι της καθημερινότητας των ανθρώπων και χρησιμοποιούνται ευρέως στην πλειοψηφία των δραστηριοτήτων τους. Οι άπειρες δυνατότητες που προσφέρουν είναι ο λόγος για τη συνεχή προσπάθεια του ανθρώπου να ανακαλύψει, να εξελίξει, και να εκμεταλλευτεί περαιτέρω δυνατότητες. Οι νέες τεχνολογίες της πληροφορικής έχουν ωφελήσει την κοινωνία και είναι υπεύθυνες για τη βελτίωση του βιοτικού επιπέδου για πολλούς πολίτες του κόσμου. Έχουν διευρυνθεί σε μεγάλο βαθμό περιλαμβάνοντας την ανάπτυξη του υλικού (hardware), τα λειτουργικά συστήματα , το λογισμικό (software), τις τεχνολογίες των δικτύων και των επικοινωνιών, τις τεχνολογίες του διαδικτύου, την ρομποτική, τη τεχνητή νοημοσύνη, το διαδίκτυο των πραγμάτων και την εικονική πραγματικότητα, συνδέοντας κυριολεκτικά την πλειοψηφία των ανθρώπινων δραστηριοτήτων σε ολόκληρο τον κόσμο και δημιουργώντας ένα νέο ψηφιακό περιβάλλον που από πολλούς θεωρείται ότι αποτελεί την 4η Βιομηχανική επανάσταση. Το διαδίκτυο των Πραγμάτων (IoT), είναι η κορύφωση της βιομηχανίας της τεχνολογίας και της μηχανικής. Η επαναστατική είσοδός του στον τεχνολογικό κόσμο, έχει δημιουργήσει μία νέα διάσταση στον τρόπο με τον οποίο διασυνδέονται και αλληλοεπιδρούν αντικείμενα χωρίς την ανθρώπινη παρέμβαση, για τη δημιουργία νέων έξυπνων υπηρεσιών και εφαρμογών. Το IoT είναι ένα δίκτυο φυσικών αντικειμένων και συσκευών, που περιέχουν ενσωματωμένα ηλεκτρονικά συστήματα, λογισμικά και αισθητήρες που επιτρέπουν να συλλέγουν και να ανταλλάσσουν δεδομένα. Ωστόσο για την εφαρμογή του, απαιτούμενη προϋπόθεση είναι η ανάπτυξη και η δικτύωση μέσω Internet, με αποτέλεσμα να εγείρονται πολλά ζητήματα όσον αφορά την ασφάλεια και την ακεραιότητα των δεδομένων που στέλνονται μέσω αυτών των δικτυακών συσκευών. Πολλοί RFID readers εμπλέκονται στην ασφάλεια των παραπάνω συστημάτων. Όπως παρατηρείται σε αρκετά πρωτόκολλα αυθεντικοποίησης RFID για IoT υπάρχουν μη ασφαλή κανάλια επικοινωνίας μεταξύ των reader και των back-end servers , με αποτέλεσμα να θεωρούνται αναξιόπιστες πολλές οντότητες RFID και να δημιουργείται η ανάγκη δημιουργίας νέων μηχανισμών ασφαλείας. Επιπλέον οι RFID tags καταγραφούν δεδομένα που μπορεί να αφορούν ακόμη και προσωπικά δεδομένα , με αποτέλεσμα να προσβάλλεται η ιδιωτικότητα και σε

συνδυασμό με τα προαναφερθέντα κενά ασφαλείας ,δεδομένα προσωπικού χαρακτήρα πολλών φυσικών προσώπων να βρίσκονται εκτεθειμένα. Το IoT έχει σταδιακά διεισδύσει σε όλες τις πτυχές τις σύγχρονης ζωής με αποτέλεσμα ο αριθμός των απειλών να αυξάνεται ραγδαία και οι επιθέσεις να αποτελούν συχνό φαινόμενο. Δημιουργείται λοιπόν το ερώτημα, αν η εφαρμογή του IoT σε μια ευρεία κλίμακα συσκευών ,εκτός από το να βελτιώσει τον τρόπο ζωής των ανθρώπων προς το καλύτερο , φτάσει στο σημείο να διαβρώσει την ιδιωτικότητα και πλέον κάθε ενέργεια μας να καταγράφεται. Τα κενά ασφαλείας που μπορεί να παρουσιάζουν τα IoT συστήματα, σε συνδυασμό με τα εργαλεία που είναι διαθέσιμα στους hackers, μπορούν να σταθούν ικανά να αποτελέσουν τεράστιες «πηγές διαρροής» προσωπικών δεδομένων, ή ακόμη και να αναπτυχθεί μία μορφή παρακολούθησης εις βάρος των χρηστών. Η ανάπτυξη του διαδικτύου των πραγμάτων δημιουργεί, νέα και σημαντικά προβλήματα για την προστασία των προσωπικών δεδομένων. Συνεπώς, για να μπορέσει το IoT να φτάσει στο μέγιστο των δυνατοτήτων του, χρειάζεται προστασία από τις απειλές και τις ευπάθειες που προκύπτουν. Παράλληλα, ακόμη και σε ασφαλή συστήματα χωρίς ευπάθειες είναι πιθανόν η επεξεργασία των Προσωπικών Δεδομένων να μην είναι σύννομη. Δηλαδή τα υποκείμενα των προσωπικών δεδομένων να μην έχουν δώσει τη ρητή συγκατάθεση τους για την επεξεργασία των δεδομένων τους . Με το Γενικό Κανονισμό Προστασίας Δεδομένων 2016/679, αλλά και με συναφείς ευρωπαϊκές οδηγίες και γνωμοδοτήσεις ,νομοθετείται η διαφύλαξη των δεδομένων στο Διαδίκτυο των Πραγμάτων.

Με βάση όλα τα παραπάνω, αδιαμφισβήτητα το όραμα του Διαδικτύου των Πραγμάτων έχει άμεση επίδραση στις σύγχρονες κοινωνίες. Η καθημερινότητα των χρηστών των IoT συσκευών έχει αλλάξει προς το καλύτερο. Ωστόσο ,όμως ζητήματα που προκύπτουν, ως προς την διαφύλαξη και την νόμιμη επεξεργασία των προσωπικών δεδομένων ,δημιουργούν νέα ερωτήματα για το αν το Διαδίκτυο των Πραγμάτων είναι η αρχή του τέλους της ιδιωτικότητας.

ΚΕΦΑΛΑΙΟ 1. Εισαγωγή στην έννοια των Συστημάτων

1.1 Η έννοια του πληροφοριακού συστήματος

Στη σημερινή εποχή της πληροφορίας και της επικοινωνίας, υπάρχει συνεχής αναφορά στα συστήματα πληροφοριών και τη διαχείριση των συστημάτων πληροφοριών. Στα δεδομένα της ψηφιακής εποχής, η αποθήκευση και η ανάκτηση γίνεται μέσω διαφόρων συστημάτων και διεπαφών. Ως εκ τούτου, ένα σύστημα πληροφοριών μπορεί να οριστεί ως σύνολο συντονισμένου δικτύου στοιχείων που δρουν μαζί για την παραγωγή, τη διανομή και επεξεργασία πληροφοριών. Ένας σημαντικός παράγοντας του συστήματος πληροφορικής βασίζεται στην ακρίβεια, η οποία μπορεί να μην ισχύει για άλλους τύπους συστημάτων. (Reynolds & Stair 2018).
Ένα πληροφοριακό σύστημα θα μπορούσε να οριστεί σαν μία σύνθετη οντότητα που περιλαμβάνει :

- Δεδομένα
- Μηχανήματα και εγκαταστάσεις
- Δίκτυα επικοινωνιών
- Λογισμικό και εφαρμογές
- Διαδικασίες
- Άνθρωποι

Στα συστήματα περιλαμβάνονται τα υπολογιστικά συστήματα, τα περιφερειακά συστήματα που συνδέονται στους υπολογιστές, οι εγκαταστάσεις των συστημάτων αυτών, και τα δίκτυα επικοινωνιών που συνδέουν τα συστήματα. Στο λογισμικό περιλαμβάνονται τα λειτουργικά συστήματα που απαιτούνται για την διεπαφή των χρηστών με τα μηχανήματα, οι εφαρμογές λογισμικού, που είναι τα προγράμματα που εκτελούν συγκεκριμένες εργασίες και τα δεδομένα, τα στοιχεία που πρέπει να εισαχθούν στα συστήματα και που με την κατάλληλη επεξεργασία θα παράγουν τις πληροφορίες. Το πληροφοριακό σύστημα ολοκληρώνεται με τους χρήστες οι οποίοι με τις κατάλληλες διαδικασίες πραγματοποιούν μια συγκεκριμένη διαδικασία. Παρόλο που σε μερικά αυτοματοποιημένα συστήματα δεν απαιτείται η παρεμβολή ανθρώπων, καθώς

έχουν προγραμματιστεί να δρούνε αυτοματοποιημένα, η επέμβαση των ανθρώπων είναι καθοριστική για την αρχική σχεδίαση και υλοποίηση των συστημάτων, ή για την επιτήρηση τους. (Μητρόπουλος & Δουληγέρης, 2015).

Ένα πληροφοριακό σύστημα δεν είναι απαραίτητα ο υπολογιστής που γνωρίζουν οι περισσότεροι άνθρωποι με την στενή έννοια του όρου, αλλά ένα σύνθετο σύστημα που περιλαμβάνει πολλές ψηφιακές συσκευές και αισθητήρες, έχοντας προγραμματιστεί να ολοκληρώνει μια συγκεκριμένη διεργασία σε καθορισμένο χρόνο ή να παράγει συγκεκριμένο αποτέλεσμα. Η βασική όμως εργασία που κάνουν όλα τα πληροφοριακά συστήματα είναι η επεξεργασία δεδομένων και η εξαγωγή πληροφοριών.

1.2 Δεδομένα και πληροφορίες

Τα δεδομένα αποτελούνται από ακατέργαστα στοιχεία, τα οποία όταν συνδυαστούν παράγουν πληροφορίες. Η μορφή των δεδομένων μπορεί να είναι διαφορετικής φύσης και εμφάνισης και ένα λογισμικό εκτός από την επεξεργασία, σχεδιάζεται στο να «ενώσει» και να παρουσιάσει με έναν κοινό τρόπο αυτές τις πληροφορίες. Οι πληροφορίες είναι μια συλλογή δεδομένων που οργανώνονται και επεξεργάζονται έτσι ώστε να έχουν πρόσθετη αξία πέρα από την αξία των μεμονωμένων γεγονότων.

Η αξία των πληροφοριών που δημιουργείται εξαρτάται από την επεξεργασία που υφίστανται τα δεδομένα. Όσο περισσότερα στοιχεία δημιουργούνται, τόσο πιο αξιόπιστες και γρήγορες γίνονται οι πληροφορίες. Η μετατροπή των δεδομένων σε πληροφορίες είναι μια διαδικασία ή μια σειρά λογικά συναφών εργασιών που εκτελούνται για να επιτευχθεί ένα καθορισμένο αποτέλεσμα. Η διαδικασία καθορισμού των σχέσεων μεταξύ των δεδομένων για τη δημιουργία χρήσιμων πληροφοριών απαιτεί γνώση και την κατανόηση ενός συνόλου πληροφοριών και τους τρόπους με τους οποίους αυτές οι πληροφορίες μπορούν να γίνουν χρήσιμες για την υποστήριξη συγκεκριμένου έργου ή την επίτευξη απόφασης. Με άλλα λόγια, οι πληροφορίες είναι ουσιαστικά δεδομένα τα οποία συνδυάζονται μέσω της εφαρμογής της γνώσης.

Ένα σύστημα πληροφοριών είναι ένα ενιαίο σύνολο υλικού, λογισμικού, βάσεων δεδομένων, δικτύων, προσώπων και διαδικασιών που έχουν ρυθμιστεί ώστε να συλλέγουν, να χειρίζονται, να αποθηκεύουν και να επεξεργάζονται δεδομένα με σκοπό να αποσπώνται πληροφορίες.

Χαρακτηριστικά Πληροφοριών	Προσδιορισμός
Προσβάσιμες	Οι πληροφορίες πρέπει να είναι εύκολα προσβάσιμες από εξουσιοδοτημένους χρήστες, ώστε να μπορούν να τις αποκτήσουν με τη σωστή μορφή και την κατάλληλη στιγμή για να καλύψουν τις ανάγκες τους.
Ακριβείς	Οι ακριβείς πληροφορίες είναι χωρίς σφάλματα. Σε ορισμένες περιπτώσεις, δημιουργούνται ανακριβείς πληροφορίες επειδή εισάγονται ανακριβή δεδομένα στη διαδικασία μετασχηματισμού.
Πλήρεις - Ολοκληρωμένες	Οι πλήρεις πληροφορίες περιέχουν όλα τα σημαντικά γεγονότα, έτσι ώστε να είναι πλήρεις.
Σχετικές - Αξιόπιστες	Οι σχετικές πληροφορίες είναι σημαντικές για τον υπεύθυνο λήψης αποφάσεων.. Σε πολλές περιπτώσεις, η αξιοπιστία των πληροφοριών εξαρτάται από την αξιοπιστία της μεθόδου συλλογής δεδομένων. Σε άλλες περιπτώσεις, η αξιοπιστία εξαρτάται από την πηγή των πληροφοριών.
Ασφαλείς	Οι πληροφορίες πρέπει να είναι ασφαλείς από την πρόσβαση από μη εξουσιοδοτημένους χρήστες.
Απλές	Οι πληροφορίες πρέπει να είναι απλές, όχι περίπλοκες. Είναι πιθανό να μην χρειάζονται εξελιγμένες και λεπτομερείς πληροφορίες. Στην πραγματικότητα, πάρα πολλές πληροφορίες μπορούν να προκαλέσουν υπερφόρτωση, όπου ο υπεύθυνος λήψης αποφάσεων έχει πάρα πολλές πληροφορίες

	και δεν είναι σε θέση να προσδιορίσει τι είναι πραγματικά σημαντικό.
Έγκαιρες	Παρέχονται έγκαιρες πληροφορίες όταν χρειάζεται.
Επιβεβαιωμένες	Οι πληροφορίες πρέπει να είναι επαληθεύσιμες. Αυτό σημαίνει ότι πρέπει να υπάρχει δυνατότητα ελέγχου από πολλές πηγές και κυρίως από αξιόπιστες πηγές.

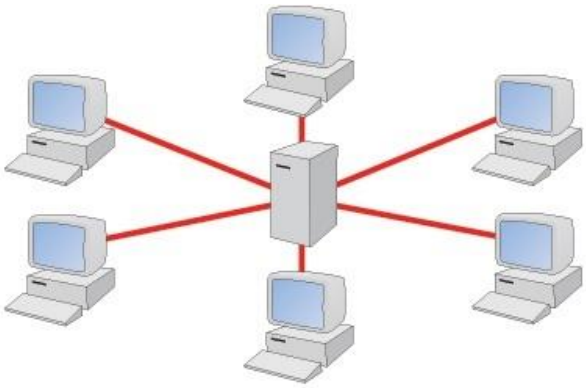
Πίνακας 1. Χαρακτηριστικά ποιότητας ενός πληροφοριακού συστήματος.

1.3 Δίκτυα και επικοινωνίες

Οι βασικές ιδέες σε όλους τους τύπους επικοινωνίας είναι ότι πρέπει να υπάρχουν τρία συστατικά για να είναι αποτελεσματική η επικοινωνία. Πρώτον, πρέπει να υπάρχουν δύο οντότητες, που ονομάζονται αποστολέας και δέκτης. Αυτές οι δύο οντότητες πρέπει να έχουν κάτι που πρέπει να μοιραστούν. Δεύτερον, πρέπει να υπάρχει ένα μέσο μετάδοσης μέσω του οποίου διοχετεύονται τα δεδομένα, και τρίτον πρέπει να υπάρχει ένα συμφωνημένο σύνολο κανόνων ή πρωτοκόλλων επικοινωνίας. Αυτά τα τρία ισχύουν για κάθε κατηγορία ή δομή του επικοινωνία. (Migga Kizza, 2017).

Δίκτυο υπολογιστών

Ένα δίκτυο υπολογιστών είναι ένα κατανεμημένο σύστημα που αποτελείται από συνδεδεμένους υπολογιστές και άλλες συσκευές. Προκειμένου αυτές οι συνδεδεμένες συσκευές να θεωρηθούν ως δίκτυο επικοινωνίας, πρέπει να υπάρχει ένα σύνολο κανόνων ή πρωτοκόλλων επικοινωνίας που πρέπει να ακολουθήσει κάθε συσκευή στο δίκτυο για να επικοινωνήσει με μια άλλη. Ο συνδυασμός που αποτελείται από υλικό και λογισμικό είναι ένα δίκτυο επικοινωνίας ηλεκτρονικών υπολογιστών ή δίκτυο υπολογιστών εν συντομία.



Σχήμα 1. Δίκτυο υπολογιστών[1]

Ένα δίκτυο υπολογιστών δεν έχει απαραίτητα συνδεμένους μόνο υπολογιστές, αλλά και άλλες ψηφιακές συσκευές ή περιφερειακά μηχανήματα (εκτυπωτές σαρωτές κ.α.) τα οποία ακολουθούν τους ίδιους κανόνες και πρωτόκολλα επικοινωνίας του δικτύου.

Το υλικό του δικτύου που αποτελείται από μια συλλογή κόμβων, περιλαμβάνει τα τελικά συστήματα, όπως κεντρικούς υπολογιστές, εκτυπωτές, ψηφιακές συσκευές, περιφερειακά μηχανήματα και ενδιάμεσα στοιχεία μεταγωγής που περιλαμβάνουν κόμβους, γέφυρες, δρομολογητές και πύλες οι οποίες, καλούνται στοιχεία δικτύου.

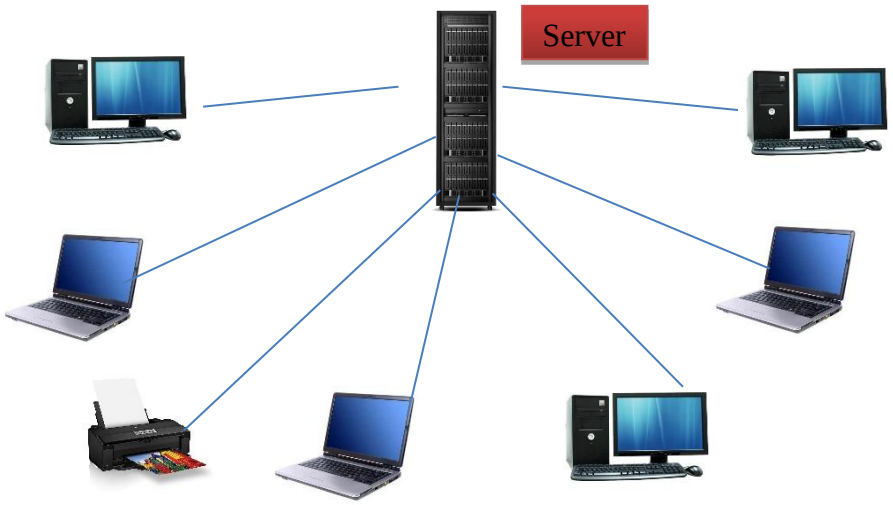
Το λογισμικό δικτύου αποτελείται από όλα τα προγράμματα εφαρμογών και τα πρωτόκολλα δικτύου που χρησιμοποιούνται για τον συγχρονισμό, τον συντονισμό και την ανταλλαγή δεδομένων μεταξύ των στοιχείων του δικτύου. Το λογισμικό δικτύου κάνει επίσης δυνατή την ανταλλαγή πόρων στο δίκτυο. Στοιχεία δικτύου, λογισμικό δικτύου, και οι χρήστες (άνθρωποι) συνεργάζονται έτσι ώστε να μπορούν να ανταλλάσσουν μηνύματα και να μοιράζονται πόρους με άλλα συστήματα που δεν είναι άμεσα διαθέσιμα σε τοπικό επίπεδο. (Migga Kizza, 2017).

Υπάρχουν πολλά μοντέλα διαμόρφωσης δικτύου υπολογιστών. Τα πιο συνηθισμένα από αυτά είναι τα κεντρικά και τα κατανεμημένα μοντέλα. **Σε ένα κεντρικό μοντέλο**, αρκετοί υπολογιστές και συσκευές είναι διασυνδεδεμένοι και μπορούν να μιλήσουν μεταξύ τους. Ωστόσο, υπάρχει μόνο ένας κεντρικός υπολογιστής, που ονομάζεται master, ή server μέσω του οποίου πρέπει να

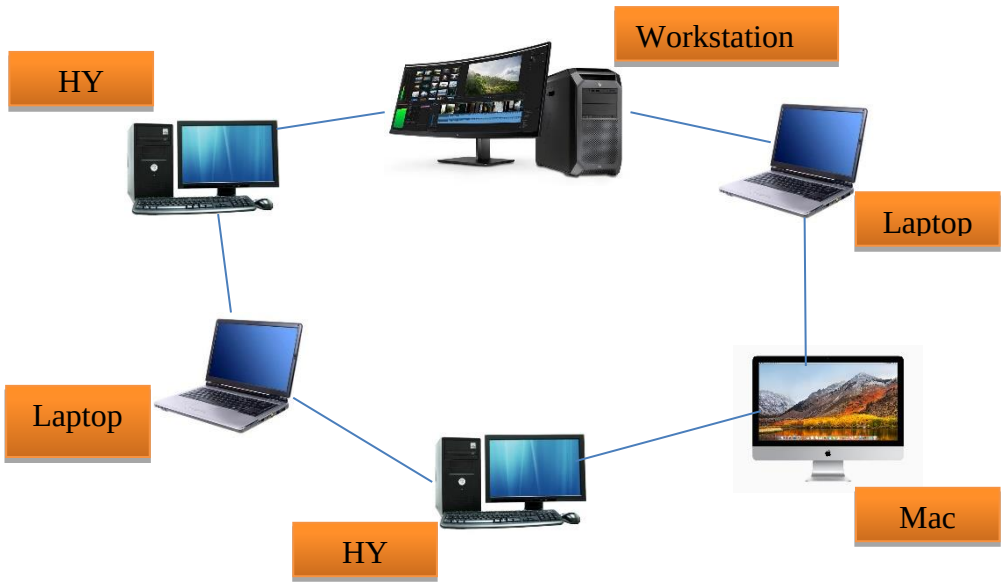
[1] https://www.quora.com/What-is-the-difference-between-network-and-Networking What is the difference between network and Networking? (Πρόσβαση 22.6.2018).

πραγματοποιηθεί όλη η επικοινωνία. Οι εξαρτημένοι υπολογιστές και οι υπόλοιπες συσκευές, μπορεί να έχουν μειωμένους τοπικούς πόρους, όπως η μνήμη, και οι συνολικοί πόροι που διαχειρίζονται να ελέγχονται από τον κεντρικό υπολογιστή.

Σε αντίθεση με το κεντρικό μοντέλο, **το κατανεμημένο δίκτυο** αποτελείται από συνδεδεμένους υπολογιστές με ένα δίκτυο επικοινωνίας που αποτελείται από στοιχεία σύνδεσης και κανάλια επικοινωνίας. Οι υπολογιστές αυτοί και οι συσκευές είναι ανεξάρτητες και αυτόνομες οντότητες που χρησιμοποιούν το δίκτυο για ανταλλαγή δεδομένων και μπορούν να λειτουργήσου ανεξάρτητα και αυτόνομα από τον κεντρικό υπολογιστή. Στην πράξη τις περισσότερες φορές λειτουργούν σύνθετα συστήματα και δίκτυα που περιλαμβάνουν τόσο κεντρικές μονάδες όσο και αυτόνομους υπολογιστές λειτουργώντας ανάλογα με το είδος του έργου που έχουν να επιτελέσουν. (Migga Kizza, 2017).Τα Σχήματα 2 και 3 δείχνουν ένα μοντέλο κεντρικού δικτύου και ένα μοντέλο κατανεμημένου δικτύου, αντίστοιχα.



Σχήμα 2. Κεντρικό δίκτυο υπολογιστών – συσκευών



Σχήμα 3. Κατανεμημένο δίκτυο υπολογιστών – συσκευών

Ανάλογα με την χρησιμότητα υπάρχουν πολλά διαφορετικά δίκτυα και τρόποι ταξινομήσεως. Συνήθως ταξινομούνται ανάλογα με το μέγεθός τους ή για την ακρίβεια με το μέγεθος της γεωγραφικής περιοχής που καλύπτουν) σε τρεις βασικές κατηγορίες:

- LAN – Local Area Network (Δίκτυο Τοπικής Περιοχής).
- MAN – Metropolitan Area Network (Δίκτυο Μητροπολιτικής Περιοχής).
- WAN – Wide Area Network (Δίκτυο Ευρείας Περιοχής). (Φουληράς, 2015).

Η Δικτύωση είναι πολύπλοκο πρόβλημα καθώς υπάρχουν πάρα πολλά επί μέρους ζητήματα που πρέπει να επιλυθούν: Το υλικό που πρόκειται να χρησιμοποιηθεί (π.χ., καλώδια, πρίζες, κάρτες δικτύου), η κωδικοποίηση των μεταδιδόμενων πληροφοριών στην κατάλληλη μορφή των σημάτων που χρησιμοποιούνται, τα πρωτόκολλα, τα πρότυπα υπηρεσιών, ο τρόπος προγραμματισμού κατάλληλων εφαρμογών, κλπ.

Εάν είχε δημιουργηθεί ένα πρότυπο που να μπορούσε να επιλύει όλα τα ζητήματα θα είχε ως αποτέλεσμα ένα τεράστιο και πολύπλοκο δίκτυο, το οποίο θα ήταν πολύ δύσκολο να υλοποιηθεί, αλλά και να τροποποιηθεί όταν θα υπήρχε ανάγκη. Με την πρόοδο της τεχνολογίας, τα πρότυπα επικοινωνίας αλλάζουν διαρκώς. Η έλευση και η καθολική επικράτηση του διαδικτύου

δημιούργησε νέες ανάγκες με τον τεράστιο όγκο δεδομένων που πρέπει να μεταδοθεί (**big data**) ενώ το διαδίκτυο των πραγμάτων (**Internet Of Things**) έχει φτάσει σε οριακό σημείο τα δίκτυα και την συνεργασία μεταξύ τους. Νέες τεχνολογίες εφαρμόζονται προκειμένου να αντιμετωπιστεί η τεράστια αυτή συγκέντρωση δεδομένων και πληροφοριών αλλά και να εξασφαλιστεί η ασφάλεια όλου αυτού του νέου ψηφιακού περιβάλλοντος. (Φουληράς, 2015).

ΚΕΦΑΛΑΙΟ 2. Το Διαδίκτυο των Πραγμάτων

2.1 Η ανάπτυξη του Διαδικτύου (Internet)

Ο ψηφιακός κόσμος, υπήρχε εδώ και πολλά χρόνια, και συγκεκριμένα από την δεκαετία του ’50, όταν άρχισαν να παίρνουν υπόσταση και να γίνονται διαθέσιμοι οι πρώτοι υπολογιστές. Μηχανήματα, λογισμικό, επικοινωνίες, δίκτυα, υπήρχαν από την εποχή εκείνη, αλλά αφορούσαν ένα περιορισμένο κοινό, ενώ τα επόμενα χρόνια με την έλευση των προσωπικών υπολογιστών, η πλειοψηφία των λειτουργιών τους αφορούσε συγκεκριμένες εφαρμογές και συγκεκριμένες πληροφορίες. Αυτό που έκανε την μεγάλη διαφορά, αυτό που βοήθησε στην εξάπλωση των πληροφοριών είναι το διαδίκτυο.

Το Διαδίκτυο είναι η μεγαλύτερη τεχνολογική επανάσταση που είδε η ανθρωπότητα. Η καθολική επικράτηση του διαδικτύου (Internet), δεν ήταν εύκολη ούτε άμεση. Για να επιτευχθεί η σημερινή ταχύτητα και η ευκολία σύνδεσης στο διαδίκτυο, χρειάστηκε έρευνα, νέες εφευρέσεις, βελτίωση των υπαρχόντων τεχνολογιών και η διορατικότητα πολλών ανθρώπων και επιστημόνων από πολλούς τομείς έτσι ώστε το σημερινό αποτέλεσμα να γίνει εφικτό. Το διαδίκτυο με μια απλή περιγραφή, είναι μια παγκόσμια σύνδεση υπολογιστών και δικτύων υπολογιστών, η οποία επιτρέπει την ανταλλαγή και μετάδοση ενός γιγάντιου όγκου δεδομένων και πληροφοριών. (Ryan, 2010).
Το 1969 γεννιέται το δίκτυο **ARPANET** με πόρους της υπηρεσίας έρευνας υψηλής τεχνολογίας ARPA (**Advanced Research Project Agency)** (*σήμερα ονομάζεται DARPA*). Στην αρχική του μορφή, το πρόγραμμα απέβλεπε στον πειραματισμό με την **μεταγωγή πακέτων** (packet switching), σύμφωνα με την οποία τα προς μετάδοση δεδομένα κόβονται σε πακέτα και πολλοί χρήστες μπορούν να μοιραστούν την ίδια επικοινωνιακή γραμμή.[2]

Με αυτό τον τρόπο και γι’ αυτό τον λόγο δημιουργήθηκε το διαδίκτυο (internet). Δεν είχε ακόμη την δομή και την λειτουργικότητα που έχει σήμερα, ούτε υπήρχε πρόσβαση από τους απλούς

[2] http://www.computerhistory.org/timeline/computers/#169ebbe2ad45559efbc6eb35720b5528 Ιστορία των Υπολογιστών. (Πρόσβαση, 24.6.2018).

ανθρώπους, αλλά η φιλοσοφία του ήταν ή ίδια και φυσικά δεν υπήρχε μεγάλη δυνατότητα μετάδοσης γραφικών και βίντεο. Μόνο όταν επιτεύχθηκε η δημιουργία του Παγκόσμιου Ιστού (**World Wide Web**) το διαδίκτυο πήρε τη μορφή καταναλωτικού προϊόντος και χρησιμοποιείται σε αυτή την μορφή που ξέρουμε και σήμερα. Το επόμενο βήμα ήταν η ανάπτυξη του πρωτοκόλλου ελέγχου μετάδοσης, το **TCP / IP**, ένα μοντέλο επικοινωνίας που καθόριζε πρότυπα για τον τρόπο μετάδοσης δεδομένων μεταξύ πολλών δικτύων. Το 1985, το National Science Foundation (NSF) δημιουργεί ένα δικό του γρήγορο δίκτυο, το **NSFNET** χρησιμοποιώντας και αυτό το πρωτόκολλο TCP/IP, προκειμένου να συνδέσει πέντε κέντρα με υπέρ-υπολογιστές μεταξύ τους και με την υπόλοιπη επιστημονική κοινότητα. Στα τέλη της δεκαετίας του ‘80, όλο και περισσότερες χώρες συνδέονται στο NSFNET. Χιλιάδες πανεπιστήμια και οργανισμοί δημιουργούν τα δικά τους ανεξάρτητα δίκτυα και τα συνδέουν πάνω στο νέο αυτό παγκόσμιο δίκτυο το οποίο παίρνει την ονομασία INTERNET και εξαπλώνεται με ιλιγγιώδεις ρυθμούς σε ολόκληρο τον κόσμο. Το 1990, το ARPANET καταργείται. (Ryan, 2010), ενώ το 1993, το εργαστήριο CERN στην Ελβετία παρουσιάζει το **World Wide Web (WWW)** (Παγκόσμιο Ιστό).

2.2 Εισαγωγή στο διαδίκτυο των πραγμάτων (Internet of things)

Από την στιγμή που η σύνδεση του διαδικτύου, έγινε γρήγορη και άμεσα προσπελάσιμη στους περισσότερους ανθρώπους, ήταν φυσικό επακόλουθο να συνδεθούν όλο και περισσότερες ψηφιακές συσκευές. Μέχρι και πριν 10 χρόνια η σύνδεση συσκευών στο διαδίκτυο, εκτός των υπολογιστών ήταν σχετικά περιορισμένη. Σήμερα όμως υπάρχουν πανίσχυρες υπολογιστικές συσκευές που με την βοήθεια του κατάλληλου λογισμικού, εκτελούν εργασίες που μόλις πριν 10 χρόνια φάνταζαν σαν επιστημονική φαντασία. Η φιλοσοφία της απομακρυσμένης σύνδεσης και του ελέγχου άλλων συσκευών δεν είναι νέα, αλλά ήταν πολύ εξειδικευμένη, καθώς απαιτούνταν ειδικός εξοπλισμός, και ασύρματες συνδέσεις περιορισμένης εμβέλειας. Η δυνατότητα μιας συσκευής να επικοινωνεί με άλλες συσκευές έδωσε το έναυσμα για την διασύνδεση όλο και περισσοτέρων συσκευών μέσω διαδικτύου. Αν για παράδειγμα, με ένα κινητό τηλέφωνο μπορεί ένας χρήστης να κατευθύνει ένα ιπτάμενο drone, να ελέγχει κάμερες ασφαλείας από χιλιάδες χιλιόμετρα μακριά, να εκτελεί τραπεζικές συναλλαγές σε οποιοδήποτε μέρος και αν βρίσκεται,

τότε μπορεί να συνδέεται με κάθε συσκευή που θα μπορεί να συνδεθεί στο διαδίκτυο. (Anuradha & Tripathy, 2018).

Αυτή είναι και η βασική ιδέα του Διαδικτύου των πραγμάτων , η σύνδεση δηλαδή οποιασδήποτε συσκευής με το Internet και η ικανότητα ελέγχου αυτής της συσκευής απομακρυσμένα. Αυτό περιλαμβάνει έξυπνες συσκευές, από κινητά τηλέφωνα, ακουστικά, λάμπες, φορητές συσκευές, μέχρι εξειδικευμένα ιατρικά μηχανήματα διατήρησης ζωής και σχεδόν οτιδήποτε άλλο μπορεί να σκεφτεί ένας χρήστης. Η εταιρεία αναλυτών Gartner αναφέρει ότι μέχρι το 2020 θα υπάρχουν πάνω από 26 δισεκατομμύρια συνδεδεμένες συσκευές, με αποτέλεσμα να θεωρούμε το IoT είναι ένα γιγαντιαίο δίκτυο συνδεδεμένων «πραγμάτων».

Η έννοια του IoT εκτός από συσκευές που είναι συνδεμένες στο Διαδίκτυο ,συνδέεται και με συσκευές που επικοινωνούν με μεγάλα κεντρικά μηχανήματα, τα οποία συχνά παίρνουν αποφάσεις και αναλαμβάνουν δράση χωρίς την ανθρώπινη παρέμβαση. Δισεκατομμύρια συσκευές επικοινωνούν μεταξύ τους και συνδέονται αυτοματοποιημένα για την εκτέλεση εργασιών, είτε γιατί παρουσιάζουν μεγαλύτερη αποτελεσματικότητα ,είτε γιατί το αποτέλεσμα ή η υπηρεσία που παρέχεται έχει μεγαλύτερη προστιθέμενη αξία. Το IoT παρουσιάζει επιχειρηματικές ευκαιρίες σε όλους σχεδόν τους βιομηχανικούς τομείς και θεωρείται πλέον αναπόσπαστο στοιχείο για το μέλλον των αγαθών και των υπηρεσιών. (Macaulay, 2017).

2.3 Ορισμός του Διαδικτύου των Πραγμάτων

Το Internet of Things είναι μια έννοια που αφορά τα αντικείμενα της καθημερινότητάς μας – από βιομηχανικές μηχανές μέχρι wearable συσκευές που χρησιμοποιούν ενσωματωμένους αισθητήρες για τη συλλογή δεδομένων και την ανάληψη κάποιας δράσης σε αυτά μέσα σε ένα δίκτυο. Κάπως έτσι λειτουργεί ένα κτίριο που χρησιμοποιεί αισθητήρες (sensors) για την αυτόματη ρύθμιση της θέρμανσης ή του φωτισμού. Άλλο παράδειγμα είναι ο ένας εξοπλισμός παραγωγής που προειδοποιεί το προσωπικό συντήρησης για μια επικείμενη βλάβη.

Ο όρος Internet of Things (ή αλλιώς Διαδίκτυο των Πραγμάτων) επινοήθηκε στα τέλη της δεκαετίας του 1990 από τον επιχειρηματία Kevin Ashton. Ο Ashton, ήταν μέρος μιας ομάδας που ανακάλυψε τον τρόπο να συνδέσει τα αντικείμενα με το διαδίκτυο μέσω μιας ετικέτας RFID. Για πρώτη φορά χρησιμοποίησε τον όρο Internet of Things ,με αποτέλεσμα να καθιερωθεί από τότε. [3]

Παρόλο που υπάρχει και λειτουργεί εδώ και πολλά χρόνια, για τους περισσότερους ανθρώπους η έννοια του IoT, φαντάζει ως κάποια φυσική εξέλιξη του διαδικτύου ή ακόμη το ταυτίζουν με το ίδιο το διαδίκτυο, Το μέγεθος του, οι δυνατότητες που προσφέρει , οι νέες προοπτικές που τείνουν να αλλάξουν οικονομικές και κοινωνικές δομές, δεν έχουν γίνει ακόμη ευρέως κατανοητές, όπως και τα προβλήματα ή οι κίνδυνοι που πιθανολογούνται. Πολλοί επίσης μπερδεύουν και συγκρίνουν την τεχνολογία του αυτοματισμού που λειτουργεί στην βιομηχανία εδώ και πολλές δεκαετίες με το διαδίκτυο των πραγμάτων, αλλά σίγουρα είναι κάτι πιο μεγαλύτερο, καινοτόμο και ίσως επικίνδυνο, αν δεν εξεταστούν αναλυτικά όλες οι παράμετροι ασφαλείας και της προστασίας των προσωπικών δεδομένων.

Το διαδίκτυο των πραγμάτων είναι ένα σύστημα αλληλένδετων υπολογιστικών συσκευών, μηχανικών και ψηφιακών μηχανών, αντικειμένων ή προσώπων που διαθέτουν μοναδικά αναγνωριστικά στοιχεία και τη δυνατότητα μεταφοράς δεδομένων μέσω δικτύου, αλληλοεπιδρώντας μεταξύ ανθρώπων και μηχανών ή αντικειμένων ή αντικειμένων και αντικειμένων. (Soro, Brereton & Roe, 2018).

2.4 Η Ανατομία του Διαδικτύου των Πραγμάτων

Οι περισσότερες καινοτόμες τεχνολογίες που εξελίχθηκαν και εξελίσσονται σήμερα, επικεντρώνονται γύρω από την βιομηχανική παραγωγή, ή σε μια πιο γενικευμένη έννοια στην παραγωγή αγαθών και υπηρεσιών και στον τελικό χρήση, τον άνθρωπο. Το διαδίκτυο των πραγμάτων λειτούργησε αρχικά στην βιομηχανική παραγωγή και στο έλεγχο των διαφόρων

[3] http://www.rfidjournal.com/articles/view?4986 That 'Internet of Things', (πρόσβαση 28.6.2018).

συσκευών, χρησιμοποιώντας ψηφιακές συσκευές ελέγχου και πρωτόκολλα επικοινωνίας. Στην βιομηχανία, η έννοια των διασυνδεμένων συσκευών – μηχανών, κάτω από το ευρύ πεδίο του αυτοματισμού, δημιουργήθηκε από την δεκαετία του ’50 και θεωρείται κεντρική συνιστώσα της 3^{η} βιομηχανικής επανάστασης, μαζί με την ανάπτυξη των υπολογιστών και του λογισμικού. Οι διαδικασίες όμως αυτές ήταν κλειστές και εξειδικευμένες διαδικασίες, που ελέγχονταν από υπολογιστές και ρομποτικές συσκευές κάτω από την επίβλεψη του ανθρώπινου παράγοντα και φυσικά δεν υπήρχε εξωτερική πρόσβαση.

Η μεγάλη αλλαγή σε αυτή την διαδικασία, δημιουργήθηκε από την μετατροπή πολλών συσκευών σε ψηφιακές, αλλά κυρίως η δυνατότητα που απέκτησαν να επικοινωνούν μέσω εσωτερικών δικτύων αρχικά και κατόπιν μέσω διαδικτύου με υπολογιστές ή άλλες συσκευές.

Κατ’ επέκταση στο καθαρά βιομηχανικό μέρος, οι περισσότερες μηχανές λειτουργούν αναλογικά (ακόμη και αν ελέγχονται ψηφιακά). Στην περίπτωση των αναλογικών μηχανημάτων έχουμε την μηχανική λειτουργία. Για παράδειγμα στα παλιά αεροπλάνα το πάτημα ενός πεταλιού του αεροσκάφους από ένα πιλότο, ενεργοποιούσε έναν συρματόσχοινο που άλλαζε θέση στις επιφάνειας ελέγχου και άλλαζε η άνοδος ή η κάθοδος ή η πορεία του αεροπλάνου. Σήμερα η εντολή αυτή (η μηχανική) τείνει να αντικατασταθεί από ψηφιακή εντολή. Σε ένα σύγχρονο αεροπλάνο οι κινήσεις του πιλότου, ενεργοποιούν ψηφιακές συσκευές, οι οποίες στέλνουν ένα ψηφιακό σήμα στο αντίστοιχο τμήμα του αεροσκάφους και εκτελείται η λειτουργία. Το πλεονέκτημα σε αυτή την περίπτωση είναι ότι δεν απαιτείται η ανθρώπινη δύναμη, η εντολή μεταδίδεται άμεσα και ταχύτατα και υπάρχει η δυνατότητα ψηφιακή ένδειξης σε μια οθόνη της ολοκλήρωσης της διαδικασίας.

Η ψηφιακή τεχνολογία επικράτησε σε πολλές συσκευές, αν και αυτή που εισήγαγε την έννοια του ψηφιακού ελέγχου από απόσταση, για τους περισσότερους ανθρώπους, ήταν το έξυπνο κινητό τηλέφωνο (smart –phone) όπου μετατράπηκε σε ένα μικρό πανίσχυρο υπολογιστή, ο οποίος μπορεί να ελέγχει κάμερες ασφαλείας, να ενεργοποιεί μια απομακρυσμένη συσκευή (ένα φούρνο, το αυτοκίνητο, ένα υπολογιστή, μια μηχανή) επικοινωνώντας με ειδικό λογισμικό. Η διασύνδεση όλων αυτών των συσκευών μέσω του διαδικτύου δημιούργησε το διαδίκτυο των πραγμάτων τα οποία πλέον επικοινωνούν ή αλληλοεπιδρούν μεταξύ τους ή με τους ανθρώπους.

Σήμερα, το 2018 υπολογίζεται ότι υπάρχουν παγκοσμίως, περίπου 18 δισεκατομμύρια συσκευές που «συνδέονται» στο διαδίκτυο και αναθεωρείται η πρόβλεψη των 28 δισεκατομμυρίων προς τα πάνω, στα 50 δισεκατομμύρια μέχρι το 2020. Το μεγαλύτερο μέρος αυτών των συσκευών δεν είναι υπολογιστές με παραδοσιακή μορφή (smartphone/laptop/tablet), αλλά είναι «πράγματα» (things).

Αναμένεται ότι το IoT θα βελτιώσει την ενεργειακή απόδοση, την απομακρυσμένη παρακολούθηση και τον έλεγχο των φυσικών περιουσιακών στοιχείων, της παραγωγικότητας μέσω εφαρμογών τόσο διαφορετικών που θα ανατρέψουν, αν δεν το έχουν κάνει ήδη, τις παραδοσιακές μεθόδους παραγωγής, την ασφάλεια στο σπίτι, την παρακολούθηση και ενημέρωση συσκευών. Μέχρι στιγμής το IoT έχει χρησιμοποιηθεί, στον τομέα της υγειονομικής περίθαλψης, των οικιακών συσκευών και των κτιρίων, των λιανικών αγορών, των επιχειρήσεων παραγωγής ενέργειας και μεταποίησης, της κινητικότητας και των μεταφορών, των εταιρειών logistics και των μέσων ενημέρωσης. (Anuradha & Tripathy, 2018).

Οι αισθητήρες συμβάλλουν στην αναγνώριση της κατάστασης των πραγμάτων, με την οποία αποκτούν το πλεονέκτημα της πρόβλεψης των ανθρώπινων αναγκών με βάση τις πληροφορίες που συλλέγονται ανά αντικείμενο. Οι διασυνδεμένες συσκευές ,όχι μόνο συγκεντρώνουν πληροφορίες από το περιβάλλον τους αλλά είναι επίσης σε θέση να λαμβάνουν αποφάσεις χωρίς την ανθρώπινη παρέμβαση, με βάση βέβαια κάποιο ενσωματωμένο λογισμικό. Η τεχνολογία IoT χρησιμοποιείται στην καθημερινή ζωή ,για το ξεκλείδωμα της πόρτας χωρίς κλειδί, στους αναγνώστες καρτών, στις αυτόματες κλειδαριές, στα συστήματα ανίχνευσης οχημάτων, στα σύστημα πληρωμής διοδίων, καθώς χρησιμοποιείται ακόμη και για την παρακολούθηση ζώων, τον έλεγχο πρόσβασης, τα συστήματα πληρωμών, τις ασύρματες έξυπνες κάρτες, τις αντικλεπτικές συσκευές, κλπ. (Anuradha & Tripathy, 2018).

Το Διαδίκτυο των πραγμάτων, ή αλλιώς το «IoT», δεν είναι μια συγκεκριμένη συσκευή (υπολογιστής) ή μια τεχνολογία. Είναι ένα ευρύ πεδίο, με καινοτόμες και διαφορετικές τεχνολογίες -πολλές φορές τελείως διαφορετικές μεταξύ τους- που προσπαθεί να υλοποιήσει την ενσωμάτωση ,τη συνδεσιμότητα και την ευφυΐα σε ένα ευρύ φάσμα συσκευών και λειτουργιών.

Η δυνατότητα συλλογής τεράστιων ποσοτήτων δεδομένων σε σχεδόν πραγματικό χρόνο από ένα ευρύ φάσμα έξυπνων συνδεδεμένων συσκευών, αποτελεί τη βάση του IoT. Αυτά τα δεδομένα μπορούν στη συνέχεια να αποκτηθούν απευθείας μέσω διαδικτύου ή μέσω του cloud και να επεξεργασθούν και να .Με αυτό τον τρόπο, το IoT μπορεί και θα χρησιμοποιηθεί για τη δημιουργία σύνθετων πληροφοριακών συστημάτων που είναι μεγαλύτερα από το άθροισμα των μεμονωμένων στοιχείων. (Greengard, 2015).

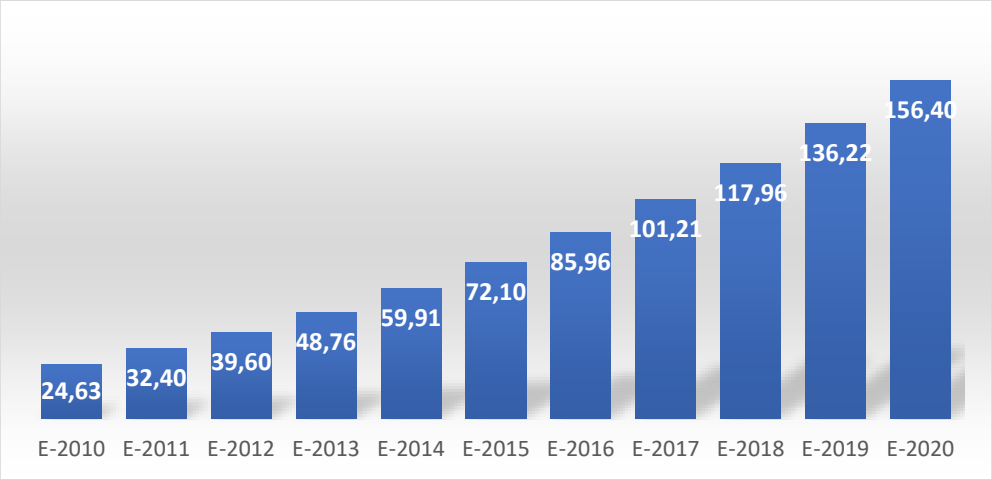
ΚΕΦΑΛΑΙΟ 3. Οι Νέες Ψηφιακές Τεχνολογίες και η σύνδεσή τους με το IoT.

Με την εξάπλωση του διαδικτύου , όλο και περισσότεροι άνθρωποι συνδέονται στο διαδίκτυο ενώ ταυτόχρονα διαχειρίζονται όλο και μεγαλύτερο όγκο δεδομένων. Η ανάγκη διαχείρισης αυτών των τεράστιων ποσοτήτων δεδομένων αλλά και η δυνατότητα άμεσης πρόσβασης , αποστολής και λήψης αυτών έχει δημιουργήσει νέες ψηφιακές τεχνολογίες για την αναμετάδοση τους.

3.1 Τεχνολογία νέφους (Cloud Computing)

Το Cloud Computing είναι ένα δικτυακό μοντέλο αποθήκευσης δεδομένων, όπου τα δεδομένα αποθηκεύονται σε απομακρυσμένες δικτυακές τοποθεσίες. Τα δεδομένα αποθηκεύονται σε μεγάλα κέντρα αποθήκευσης δεδομένων (data centers) τα οποία μπορεί να βρίσκονται διασκορπισμένα σε περισσότερους από έναν εξυπηρετητές (servers), ενώ ο χρήστης μπορεί να έχει πρόσβαση σε αυτά μέσω κάποιας δικτυακής διεπαφής (web interface). (Barrie Sosinsky, 2011)

Ο όρος cloud computing αναφέρεται σε εφαρμογές και υπηρεσίες οι οποίες τρέχουν σε κατανεμημένο δίκτυο με πρόσβαση μέσω κοινών πρωτοκόλλων του διαδικτύου και προτύπων δικτύωσης. Για τις υπηρεσίες αυτές υπάρχουν εταιρείες που διαθέτουν αποθηκευτικούς χώρους όπου μπορεί ένας χρήστης να ανεβάσει τα αρχεία του και να έχει πρόσβαση σε άλλα αρχεία μέσω μιας σύνδεσης. Με την δημιουργία του παγκόσμιου δικτύου (Internet) ο κάθε χρήστης μπορεί να συνδεθεί σε οποιαδήποτε μέρος του κόσμου και σε οποιαδήποτε υπηρεσία που προσφέρει online προγράμματα ή χώρους αποθήκευσης. (Mavromoustakis, Mastorakis & Dobre, 2017).



Διάγραμμα 1. Μέγεθος του cloud computing και φιλοξενία αγοράς στην παγκόσμια αγορά από το 2010 έως το 2020 (σε δισεκατομμύρια δολάρια ΗΠΑ)[4]

Πλεονεκτήματα του cloud computing

Το Cloud computing επέφερε τεράστιες αλλαγές από τον παραδοσιακό τρόπο συλλογής και αποθήκευσης δεδομένων. Σήμερα όλο και περισσότερες επιχειρήσεις και οργανισμοί στρέφονται στις υπηρεσίες cloud computing για διάφορους λόγους όπως:

Κόστος : Το Cloud computing εξαλείφει το κόστος κεφαλαίου για την αγορά υλικού και λογισμικού και τη δημιουργία και λειτουργία κέντρων δεδομένων, που σε μερικές από αυτές αποτελεί σημαντική επένδυση.

Ταχύτητα: Οι περισσότερες υπηρεσίες cloud computing παρέχονται με αυτοεξυπηρέτηση και κατ' απαίτηση, οπότε ακόμη και μεγάλοι υπολογιστικοί πόροι μπορούν να διατεθούν μέσα σε λίγα λεπτά.

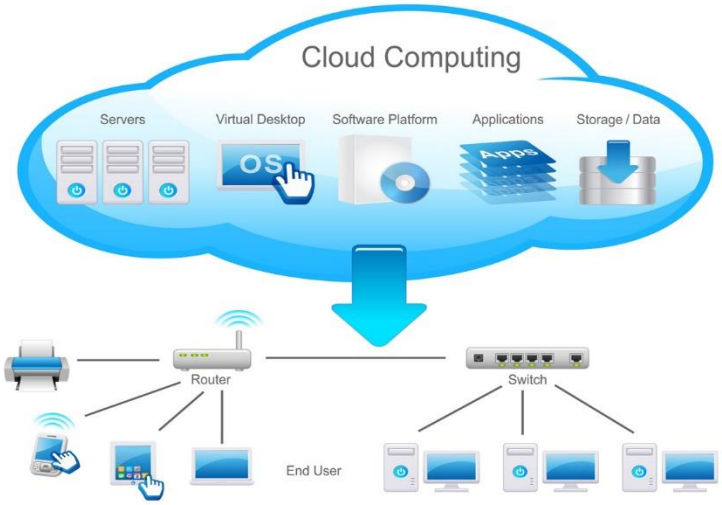
Παραγωγικότητα: Τα παραδοσιακά data centers (κέντρα μηχανογράφησης και ελέγχου δεδομένων) απαιτούν συνήθως πολλές ρυθμίσεις, συντήρηση, εγκατάσταση λογισμικού, επιδιόρθωση λογισμικού και άλλες χρονοβόρες εργασίες διαχείρισης της πληροφορικής με μεγάλο κόστος. Το Cloud computing εξαλείφει την ανάγκη για πολλά από αυτά τα καθήκοντα.

[4] (πηγή:https://www.statista.com/statistics/500541/worldwide-hosting-and-cloud-computing-market/)

Αξιοπιστία: Το Cloud computing καθιστά ευκολότερη και λιγότερο δαπανηρή την δημιουργία αντιγράφων ασφαλείας των δεδομένων, την αποκατάσταση καταστροφών και την ομαλότερη λειτουργία ενός οργανισμού. (Fox & Hao, 2018).

Μειονεκτήματα του cloud computing

Ασφάλεια δεδομένων. Ορισμένα δεδομένα, είτε εταιρειών, είτε χρηστών όπως είναι φυσικό είναι απόρρητα, οπότε υπάρχει ο κίνδυνος να κλαπούν. Αν και οι εταιρείες, πάροχοι προσφέρουν εγγύηση για την ασφάλεια των δεδομένων από επιθέσεις χάκερ έχοντας κορυφαία συστήματα προστασίας όσοι χρήστες έχουν ευαίσθητα δεδομένα είναι επιφυλακτικοί. (Fox & Hao, 2018). Παράλληλα η χρήση των υπηρεσιών cloud computing προκάλεσε την προσοχή των hackers για εκμετάλλευση και προκλήσεις που δημιουργούν προβλήματα στις υπηρεσίες επιβολής του νόμου. Για παράδειγμα, γίνεται όλο και πιο εύκολο για τους hackers να αποθηκεύουν ενοχοποιητικά αρχεία στο cloud computing περιβάλλον, ενώ είναι εξαιρετικά δύσκολο για τις υπηρεσίες ελέγχου και επιβολής του νόμου να αποκτήσουν πρόσβαση σε αυτά τα αρχεία, καθώς μπορεί να έχουν αποθηκευτεί σε οποιαδήποτε χώρα που φιλοξενεί τους κεντρικούς υπολογιστές των εταιρειών **Cloud Computing**. (Mavromoustakis, Mastorakis & Dobre, 2017).

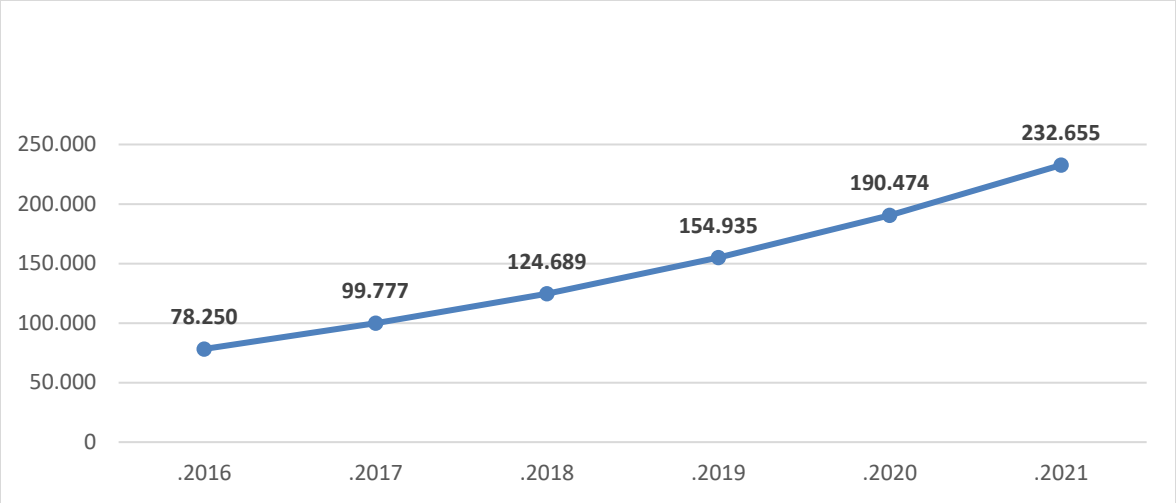


Σχήμα 4. Cloud Computing

3.2 Μεγάλα δεδομένα (Big Data)

Ο όρος Big Data χρησιμοποιείται για να περιγράψει τις τεράστιες (petabytes ή μεγαλύτερες) και σύνθετες (από δεδομένα αισθητήρων έως δεδομένα των κοινωνικών μέσων) συλλογές δεδομένων όπου τα παραδοσιακά μέσα διαχείρισης λογισμικού, υλικού και ανάλυσης δεδομένων δεν είναι σε θέση να αντιμετωπίσουν.[5] Η χρήση του διαδικτύου και των κοινωνικών μέσων, έχει αυξήσει δραματικά την διακίνηση δεδομένων και πληροφοριών, με αποτέλεσμα να δημιουργούνται τεράστιοι όγκοι δεδομένων οι οποίοι δεν είναι διαχειρίσιμοι από τις κλασσικές σχεσιακές βάσεις δεδομένων .Αντίστοιχα οι συσκευές IoT συλλέγουν και επεξεργάζονται χιλιάδες δεδομένα .Το Διαδίκτυο των πραγμάτων (IoT) και τα μεγάλα δεδομένα (Big Data) είναι δύο όψεις του ίδιου νομίσματος. Η εξέλιξη της Πληροφορικής αυξήθηκε οδηγώντας στη σύνδεση των φυσικών αντικειμένων / συσκευών στο Internet με τη δυνατότητα να ταυτιστούν με άλλες συσκευές. Αυτό αναφέρεται στο **Διαδίκτυο των πραγμάτων (IoT),** το οποίο μπορεί επίσης να περιλαμβάνει άλλες ασύρματες τεχνολογίες, τεχνολογίες αισθητήρων ή κώδικες που οδηγούν σε μαζικά σύνολα δεδομένων. Η διαχείριση σε αυτά τα μεγάλα δεδομένα απαιτεί την τεχνολογία της τεχνητής νοημοσύνη (Artificial intelligence AI) για την ανάλυση δεδομένων και για τη διατήρηση, την ανάκτηση, την αποθήκευση και την αποστολή πληροφοριών, χρησιμοποιώντας ένα συγκεκριμένο είδος τεχνολογίας, όπως υπολογιστές, κινητά τηλέφωνα, δίκτυα υπολογιστών και πολλά άλλα. Συνεπώς, τα big data περιέχουν τεράστιες πληροφορίες που παράγονται από την τεχνολογία IoT, η οποία εξυπηρετεί ένα ευρύ φάσμα εφαρμογών σε διάφορους τομείς. (Nilanjan, et all, 2018).

[5] https://www.researchgate.net/publication/322291489_Performance_Evaluation_of_Routing_Protocols_for_BIG_Data_application

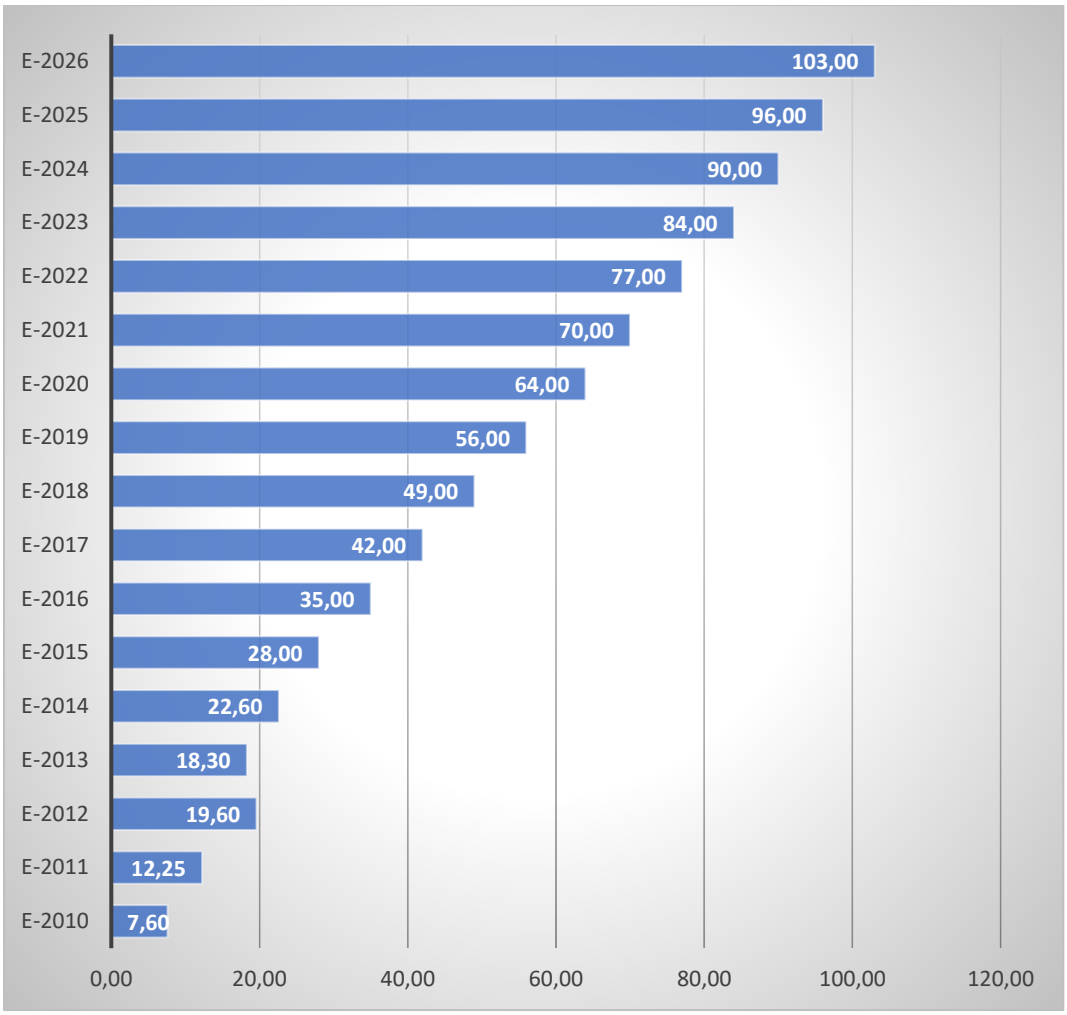


(πηγή: https://www.statista.com/statistics/267202/global-data-volume-of-consumer-ip-traffic/).

Διάγραμμα 2. Όγκος δεδομένων της παγκόσμιας κίνησης IP των καταναλωτών από το 2015 έως το 2021 (σε petabytes[6] ανά μήνα)

[6] Ένα petabyte (PB) είναι 10^{15} bytes δεδομένων, που ισούται με 1.000 terabytes (TB) ή 1.000.000 gigabytes (GB) στο δυαδικό σύστημα.

https://www.webopedia.com/TERM/P/petabyte.html petabyte, (πρόσβαση 5.8.2018).



(πηγή: https://www.statista.com/statistics/254266/global-big-data-market-forecast/)

Διάγραμμα 3. Έσοδα, από το 2011 έως το 2027 της αγοράς για τα Big Data (σε δισεκατομμύρια δολάρια ΗΠΑ)

Τα στοιχεία για τα έτη μετά το 2018 αποτελούν προβλέψεις οι οποίες αναθεωρούνται προς τα πάνω, καθώς οι εξελίξεις, οι απαιτήσεις αλλά και η παραγωγή όλο και περισσοτέρων δεδομένων καθώς και η αξιοποίηση τους, αποτελούν τον στόχο της βιομηχανίας πληροφορικής.

Τα μεγάλα δεδομένα περιλαμβάνουν επίσης δεδομένα σε διάφορες μορφές όπως κείμενο, ήχο, βίντεο, εικόνα εκτός από τα αριθμητικά δεδομένα. Αυτά τα αδόμητα δεδομένα αυξάνονται ταχύτερα από ό, τι δομημένα και έχουν συγκεντρώσει το 90% όλων των δεδομένων. (Skourletopoulos, et al. 2018).

3.2.1 Η σχέση του Internet of Things με τα big data

Στην περίπτωση του Internet of Things (Διαδίκτυο των Πραγμάτων), πολλά στοιχεία που συγκεντρώνονται προέρχονται από δεδομένα του πραγματικού κόσμου από κατάλληλες συσκευές και αισθητήρες που τα καταγράφουν. Οι αισθητήρες ενσωματώνονται σε διάφορες συσκευές και μηχανήματα στον πραγματικό κόσμο συλλέγοντας διάφορα είδη δεδομένων, όπως περιβαλλοντικά στοιχεία, γεωγραφικά δεδομένα, αστρονομικά δεδομένα, διοικητικά στοιχεία κλπ. Τα Big Data που παράγονται από IoT έχουν διαφορετικά χαρακτηριστικά σε σύγκριση με τα γενικά Big Data λόγω του διαφορετικού τύπου των δεδομένων που συλλέγονται με χαρακτηριστικά στοιχεία την ετερογένεια, την ποικιλία και τον αδόμητο χαρακτήρα.[7] Παρά το γεγονός ότι τα τρέχοντα δεδομένα από το IoT δεν αποτελούν το κυρίαρχο μέρος των Big Data, από το 2030 όπου ο αριθμός των αισθητήρων θα φτάσει το 1 τρισ. τα δεδομένα του IoT θα αποτελούν το βασικότερο τμήμα των Big Data.

Μια έκθεση από την Intel επισήμανε ότι τα δεδομένα στο IoT έχουν τρία χαρακτηριστικά που συμμορφώνονται με το πρότυπο των Big Data:

α) μεγάλος αριθμός τερματικών που δημιουργούν πληθώρα δεδομένων,

β) τα δεδομένα που προέρχονται από το IoT είναι συνήθως ημιδομημένα ή αδόμητα και

γ) τα δεδομένα του IoT είναι χρήσιμα μόνο όταν αναλύονται (Chen , 2014 :177).

Προς το παρόν, η ικανότητα επεξεργασίας δεδομένων του IoT βρίσκεται ακόμα σε χαμηλότερα επίπεδα έναντι των Big Data καθιστώντας αναγκαία την εισαγωγή των νέων τεχνολογιών δεδομένων για την προώθηση της ανάπτυξης του IoT. Πολλοί φορείς εκμετάλλευσης του IoT έχουν κατανοήσει τη σημασία των Big Data για την τελική του επιτυχία μέσω αποτελεσματικής ενσωμάτωσής τους και αξιοποίησης του Cloud. Υπάρχει επιτακτική ανάγκη να υιοθετηθούν νέες τεχνολογίες για το IoT ενώ και η ανάπτυξη των Big Data μέσω IoT βρίσκεται σε πρώιμο στάδιο. Έχει αναγνωριστεί ότι οι δύο τεχνολογίες είναι αλληλένδετες και θα πρέπει να αναπτυχθούν από κοινού: από τη μία πλευρά, η ευρεία διάδοση του IoT οδηγεί σε υψηλή αύξηση των Big Data, τόσο σε ποσότητα και σε είδη παρέχοντας έτσι νέες ευκαιρίες στην εφαρμογή και ανάπτυξή τους ενώ από την άλλη πλευρά η απαίτηση νέων δεδομένων στο IoT επιταχύνει την έρευνα και την πρόοδο στα επιχειρηματικά μοντέλα (Zaslavsky et all, 2012 :4-5).

[7] https://www.researchgate.net/publication/325767407_Security_Privacy_Efficiency_of_Sustainable_Cloud_Computing_for_Big_Data_IoT

3.3 Εξόρυξη Δεδομένων (Data Mining)

Ο όρος Εξόρυξη Δεδομένων (**Data Mining**) αναφέρεται στην διαδικασία της ανάλυσης μεγάλων βάσεων δεδομένων για εύρεση χρήσιμων μοτίβων. Υπάρχει μια ποικιλία πιθανών τύπων μοτίβων που χρησιμοποιούνται για την εξόρυξη δεδομένων. Στον επιχειρηματικό κόσμο η εξόρυξη δεδομένων είναι μια διαδικασία που χρησιμοποιούν οι εταιρείες για να μετατρέψουν τα ακατέργαστα δεδομένα σε χρήσιμες πληροφορίες. Με τη χρήση λογισμικού για αναζήτηση μοτίβων σε μεγάλες ομάδες δεδομένων, οι επιχειρήσεις για παράδειγμα μπορούν να μάθουν περισσότερα για τους πελάτες τους και να αναπτύξουν πιο αποτελεσματικές στρατηγικές μάρκετινγκ, καθώς και να αυξήσουν τις πωλήσεις και να μειώσουν το κόστος. Η εξόρυξη δεδομένων εξαρτάται από την αποτελεσματική συλλογή δεδομένων και την αποθήκευση καθώς και την επεξεργασία τους. (Boo, et all, 2017).

Το Data Mining, επίσης αναφέρεται και σαν ανακάλυψη γνώσεων σε βάσεις δεδομένων, στην επιστήμη των υπολογιστών, στη διαδικασία ανεύρεσης ενδιαφέρουσας και χρήσιμης μορφής και σχέσεων σε μεγάλους όγκους δεδομένων. Το πεδίο συνδυάζει εργαλεία από τις στατιστικές και την τεχνητή νοημοσύνη (όπως τα νευρωνικά δίκτυα και τη μηχανική μάθηση) με τη διαχείριση βάσεων δεδομένων για την ανάλυση μεγάλων ψηφιακών συλλογών, γνωστά ως σύνολα δεδομένων. Η εξόρυξη δεδομένων χρησιμοποιείται ευρέως στις επιχειρήσεις (ασφάλειες, τραπεζικά, λιανική), στην επιστήμη (αστρονομία, ιατρική) στην ασφάλεια της κυβέρνησης (εντοπισμός εγκληματιών και τρομοκρατών). Τα τελευταία χρόνια η εφαρμογή της επεκτείνεται σε όλες τις ανθρώπινες δραστηριότητες με όλο και πιο αναλυτικά και πολύπλοκα εργαλεία κατηγοριοποίησης για την εξόρυξη δεδομένων.[8]

Το διαδίκτυο των πραγμάτων (IoT) γίνεται η επόμενη βιομηχανική επανάσταση. Το IoT θα δημιουργήσει ένα τεράστιο όγκο δεδομένων και το αποτέλεσμά του θα γίνει αισθητό σε ολόκληρο τον κόσμο μεγάλων δεδομένων, αναγκάζοντας τις επιχειρήσεις να ενημερώσουν τις τρέχουσες διαδικασίες και τα εργαλεία, την κατάλληλη τεχνολογία για να αναπτυχθεί για να φιλοξενήσει αυτόν τον επιπλέον όγκο δεδομένων και να πάρει το πλεονέκτημα των στοιχείων

[8] https://www.britannica.com/technology/data-mining Data mining, (πρόσβαση 25.6.2018).

από τα πρόσφατα δεδομένα. Το τεράστιο ποσό των δεδομένων που δημιουργεί το IoT θα ήταν άχρηστο χωρίς την **αναλυτική ισχύ των μεγάλων δεδομένων.** Η εκθετική αύξηση των δεδομένων που δημιουργήθηκε από το IoT καθιστά σημαντικά τα μεγάλα δεδομένα. Χωρίς την καλύτερη συλλογή δεδομένων, δεν είναι δυνατό οι επιχειρήσεις και οι οργανισμοί να αναλύσουν τα δεδομένα που παράγονται. Τα δεδομένα αυτά που παράγονται από μηχανές και συσκευές είναι συχνά σε απλή μορφή και προκειμένου να καταστούν χρήσιμα για αναλυτικές αποφάσεις, τα δεδομένα πρέπει να οργανωθούν, να μετατραπούν και να εμπλουτιστούν.

Η ανάλυση μεγάλων δεδομένων (**big data analytics**) απεικονίζονται από τρία βασικά χαρακτηριστικά: τον **όγκο**, την **ταχύτητα** και την **ποικιλία**. Αναμφίβολα τα δεδομένα θα συνεχίσουν να παράγονται και να συλλέγονται, οδηγώντας σε έναν απίστευτο όγκο. Δεύτερον, τα δεδομένα αυτά συλλέγονται σε πραγματικό χρόνο με γρήγορη ταχύτητα. Τρίτον, οι διαφορετικοί τύποι δεδομένων συλλέγονται σε τυπική μορφή και αποθηκεύονται σε υπολογιστικά φύλλα ή σε σχεσιακές βάσεις δεδομένων. Λαμβάνοντας υπόψη τον : (όγκος ταχύτητα, ποικιλία), οι αναλυτικές τεχνικές έχουν επίσης αναπτυχθεί ώστε να ταιριάζουν σε αυτά τα χαρακτηριστικά για να κλιμακωθούν μέχρι τα περίπλοκα και εκλεπτυσμένα αναλυτικά λογισμικά που χρειάζονται. Ορισμένοι οι ερευνητές και επαγγελματίες έχουν θεωρήσει ένα τέταρτο χαρακτηριστικό: Την **διασφάλιση δεδομένων**. Έτσι, τα δεδομένα που συλλέγονται και τα αναλυτικά στοιχεία που παράγονται πρέπει να είναι εξαιρετικά αξιόπιστα και χωρίς σφάλματα. (Nilanjan, et al 2018).

3.4 Διασυνδεδεμένα Δεδομένα (Linked Data)

Προκειμένου να γίνου κατανοητά τα Διασυνδεδεμένα Δεδομένα (Linked Data), είναι σημαντικό να παρουσιαστεί η έννοια του Σημασιολογικού Ιστού και η έννοια των Συνδεδεμένων Δεδομένων. Η βασική ιδέα του «Σημασιολογικού Ιστού» (Semantic Web) είναι ότι το περιεχόμενο του Διαδικτύου, προκειμένου να είναι κατανοητό τόσο από τον άνθρωπο όσο και από το λογισμικό, πρέπει να ενσωματώνει το νόημά του, τη σημασιολογία του. (Konstantinou, & Spanos, 2015).

Ο **Σημασιολογικός Ιστός** [9] είναι μια επέκταση του σημερινού Ιστού, όπου στοχεύει στη μετατροπή του υπάρχοντος διαδικτύου μη δομημένων εγγράφων σε έναν ιστό πληροφοριών / δεδομένων. Ο βασικός στόχος του Σημασιολογικού Ιστού είναι να ενεργοποιήσει την εξέλιξη του υπάρχοντος ιστού, ώστε να επιτρέπει στους χρήστες να αναζητούν, να ανακαλύπτουν, να μοιράζονται και να ενώνουν πληροφορίες με λιγότερες προσπάθειες.

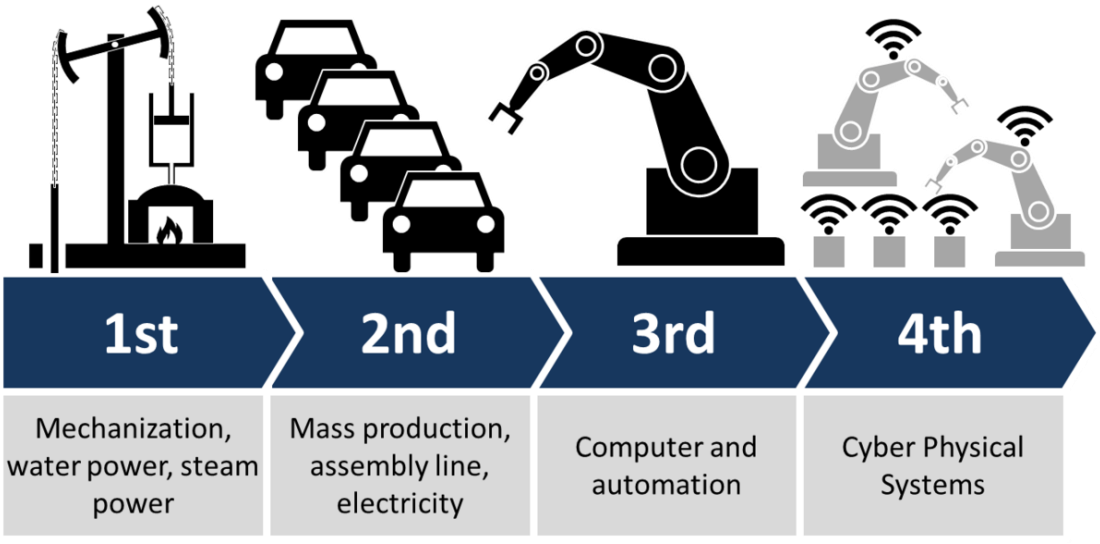
Τα **συνδεδεμένα δεδομένα** αποτελούν ένα παράδειγμα για τη δημοσίευση δεδομένων στον Ιστό και τη συνεργασία με χρήστες και μηχανές. Προωθεί αυτά τα δεδομένα να είναι απλά και δομημένα. Προωθεί μια προσέγγιση από τη βάση προς την κορυφή για τη δημοσίευση δεδομένων και βοηθά τα δεδομένα να είναι διασυνδεδεμένα και πλούσια σε περιβάλλον, με αποτέλεσμα τα δεδομένα να είναι ένα πιο αξιόλογο περιουσιακό στοιχείο. (Sakr, at el, 2018).

Η φύση του World Wide Web εξελίχθηκε από έναν ιστό συνδεδεμένων εγγράφων σε έναν ιστό, συμπεριλαμβανομένων των Συνδεδεμένων Δεδομένων. Παραδοσιακά, δημοσιευόταν έγγραφα στον ιστό και δημιουργούνταν δεσμοί μεταξύ τους. Ωστόσο, οι σύνδεσμοι αυτοί επέτρεψαν τη διασταύρωση των εγγράφων χωρίς να κατανοούν τις σχέσεις μεταξύ των εγγράφων και χωρίς να συνδέονται με συγκεκριμένες πληροφορίες. Τα **Συνδεδεμένα Δεδομένα** επιτρέπουν τη δημιουργία **σημαντικών συνδέσμων** μεταξύ τμημάτων δεδομένων στον Ιστό. Η υιοθέτηση των τεχνολογιών **Linked Data** έχει μετατοπίσει τον ιστό από ένα χώρο σύνδεσης εγγράφων σε ένα παγκόσμιο χώρο όπου τμήματα δεδομένων από διαφορετικούς τομείς συνδέονται σημασιολογικά και ενσωματώνονται για να δημιουργήσουν ένα Global Web δεδομένων. Τα Linked Data δίνουν τη δυνατότητα στις λειτουργίες να παράγουν ολοκληρωμένα αποτελέσματα καθώς προστίθενται νέα δεδομένα στον παγκόσμιο χώρο. Αυτό ανοίγει νέες ευκαιρίες για εφαρμογές όπως μηχανές αναζήτησης, προγράμματα περιήγησης δεδομένων και διάφορες εφαρμογές συγκεκριμένου τομέα. (Sakr, et al, 2018).

[9] https://www.techopedia.com/definition/27961/semantic-web Semantic Web, (πρόσβαση 25.8.2018).

3.5 Βιομηχανία 4.0 (Industry 4)

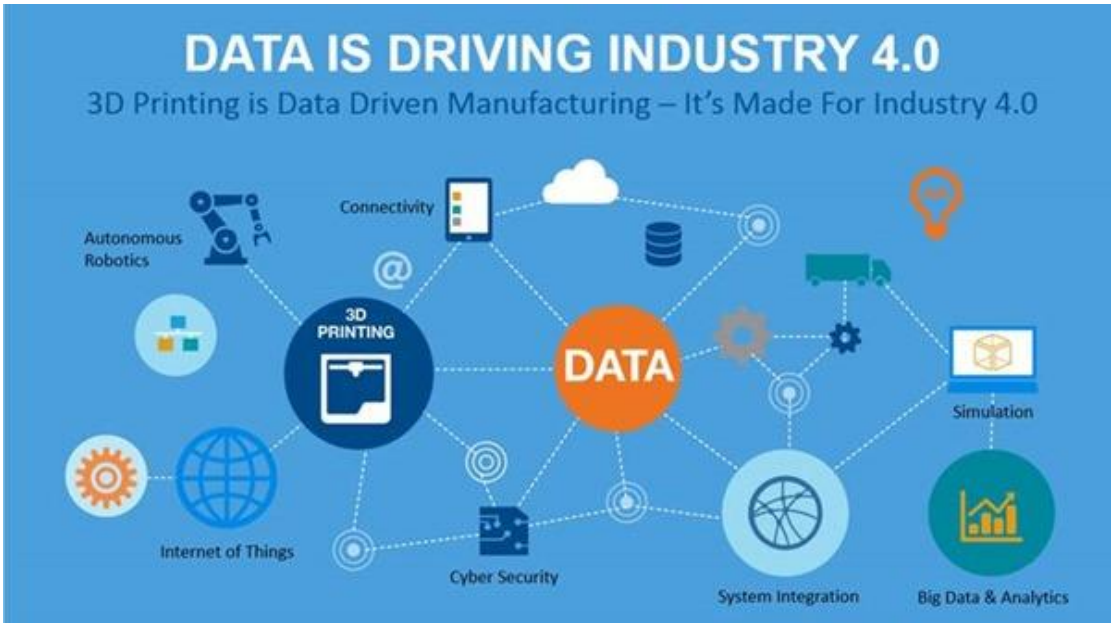
Σύμφωνα με τον ΟΗΕ, η ανθρωπότητα βρίσκεται στην αιχμή της Τέταρτης Βιομηχανικής Επανάστασης. Καθώς τα ευφυή συστήματα ενσωματώνονται σε κάθε πτυχή της ζωής των ανθρώπων, αυτή η επανάσταση θα προκαλέσει πολιτισμική και κοινωνική αλλαγή μεγέθους που μέχρι τώρα έχει απρόβλεπτες συνέπειες. Αυτές οι τεχνολογίες προκαλούν τις αξίες των πολιτών, τα προσωπικά δεδομένα, τις κοινωνικές σχέσεις, την ασφάλεια, την εμπειρία και την συμμετοχή των καταναλωτών, τις επιχειρηματικές προτάσεις που αποτέλεσαν το στυλοβάτη σχεδόν όλων των υφιστάμενων επιχειρήσεων και οργανισμών, τις νέες εργασιακές σχέσεις. Με τον επαναπροσδιορισμό και την ενσωμάτωση νέων δομών αξίας με αναδυόμενες ευφυείς τεχνολογίες, δημιουργούνται νέα καινοτόμα μοντέλα και κυκλοφορούν στην αγορά. Η κατανόηση των δυνατοτήτων και των επιπτώσεων αυτών των αλλαγών θα αποτελέσει θεμελιώδη απαίτηση όλου κοινωνικού συνόλου και των ηγεσιών κατά τα προσεχή χρόνια. (Skilton & Hovsepian, 2018). Η ρομποτική, η τεχνητή νοημοσύνη, το Διαδίκτυο των πραγμάτων, τα κυβερνό-φυσικά συστήματα και το blockchain είναι μόνο παραδείγματα νέων τεχνολογιών που θα επιφέρουν αλλαγές στην ζωή των ανθρώπων. Στην πραγματικότητα, η αποκαλούμενη 4η Βιομηχανική Επανάσταση θα συνεχίσει την πρόοδο των άλλων τριών επαναστάσεων . (Skilton & Hovsepian, 2018).



Σχήμα 5. Οι βιομηχανικές επαναστάσεις

Οι ψηφιακές τεχνολογίες που έχουν πυρήνα υπολογιστικού υλικού, λογισμικού και δικτύων δεν είναι καινούργιες, αλλά σε μια διακοπή με την τρίτη βιομηχανική επανάσταση, γίνονται όλο και πιο εξελιγμένες και ολοκληρωμένες και ως εκ τούτου μετασχηματίζουν τις κοινωνίες και την παγκόσμια οικονομία. Η νέα τεχνολογία και η ψηφιοποίηση όλων των συσκευών μέσω του Internet of Things θα φέρουν ρηξικέλευθες αλλαγές . Με απλά λόγια, οι μεγάλες τεχνολογικές καινοτομίες βρίσκονται πίσω από την έναρξη σημαντικών αλλαγών σε όλο τον κόσμο αναπόφευκτα. Η κλίμακα και η εμβέλεια της αλλαγής εξηγούν γιατί οι διαταραχές και η καινοτομία είναι τόσο έντονες σήμερα. Η ταχύτητα της καινοτομίας όσον αφορά την ανάπτυξη και τη διάδοσή της είναι ταχύτερη από ποτέ. Οι σημερινοί γίγαντες του διαδικτύου και της ηλεκτρονικής αγοράς Airbnb, Uber, Alibaba και άλλα παρόμοια τώρα γνωστά ονόματα, ήταν σχετικά άγνωστα μόλις πριν από λίγα χρόνια. Το iPhone κυκλοφόρησε για πρώτη φορά το 2007. Ωστόσο, στο τέλος του 2015 υπήρχαν μέχρι και 2 δισεκατομμύρια έξυπνα τηλέφωνα και στο τέλος του 2017 εκτιμάται ότι έχουν ξεπεράσει τα 5 δισεκατομμύρια. Το 2010 η Google ανακοίνωσε το πρώτο πλήρως αυτόνομο αυτοκίνητο. Τέτοια οχήματα θα μπορούσαν σύντομα να γίνουν μια διαδεδομένη πραγματικότητα στο δρόμο.[10] (Skilton & Hovsepian, 2018).

[10] https://en.oxforddictionaries.com/definition/technology Definition of technology in English, (πρόσβαση 26.8.2018).



Σχήμα 6. Η βιομηχανία 4.0 που αποτελεί μέρος της 4ης Βιομηχανικής επανάστασης με τους αντίστοιχους ψηφιακούς τομείς.

Η **Industrie 4.0** - Βιομηχανία 4.0 και το **Industrie Internet of Things** - Βιομηχανικό Διαδίκτυο των πραγμάτων (**IIoT**) αναπτύχθηκε το 2010 από τη γερμανική κυβέρνηση.[11] Το 2006, στο Αμερικανικό Εθνικό Ίδρυμα Επιστημών (NSF) εφαρμόστηκε ο όρος **Cyber-Physical Systems (CPS),** ο οποίος γεννήθηκε στον τομέα της αυτοματοποίησης μηχανής που οδηγεί στο Smart Factory. Αυτό θεωρείται τώρα ως μέρος της 4ης Βιομηχανικής Επανάστασης και αποτελεί μέρος μιας ευρύτερης αναδιάρθρωσης όλων των βιομηχανιών και ενός νέου είδους οικονομικής και κοινωνικής αλλαγής. Η **βιομηχανία 4.0** αναφέρεται στη σύγκλιση του **Διαδίκτυο των πραγμάτων (IoT),** του **Ίντερνετ των ανθρώπων (IoP)** και του **Internet of Everything (IoE)**. (Skilton & Hovsepian, 2018).

[11] https://www.computer-automation.de/steuerungsebene/steuern-regeln/artikel/93559/0/ Industrie 4.0, (πρόσβαση 26.8.2018).

Η βιομηχανία 4.0 βασίζεται σε έξι αρχές σχεδιασμού. Αυτές οι αρχές υποστηρίζουν τις εταιρείες στον προσδιορισμό και την εφαρμογή των σεναρίων του Industry 4.0.[12]

- **Δια-λειτουργικότητα**: η ικανότητα των κυβερνό-φυσικών συστημάτων (π.χ. φορέων εργασίας, σταθμών συναρμολόγησης και προϊόντων), των ανθρώπων και των Smart Factories να συνδέονται και να επικοινωνούν μεταξύ τους μέσω του Διαδικτύου των πραγμάτων και του Διαδικτύου των Υπηρεσιών
- **Virtualization:** ένα εικονικό αντίγραφο του έξυπνου εργοστασίου το οποίο δημιουργείται συνδέοντας δεδομένα αισθητήρων (από την παρακολούθηση φυσικών διεργασιών) με μοντέλα εικονικών εγκαταστάσεων και μοντέλα προσομοίωσης
- **Αποκέντρωση**: η ικανότητα των κυβερνό-φυσικών συστημάτων εντός των Smart Factories να λαμβάνουν αποφάσεις από μόνοι τους
- **Δυνατότητα πραγματικού χρόνου**: η δυνατότητα συλλογής και ανάλυσης δεδομένων και η παροχή των πληροφοριών αμέσως
- **Προσανατολισμός υπηρεσιών**: προσφορά υπηρεσιών (των κυβερνό-φυσικών συστημάτων , των ανθρώπων και των Smart Factories) μέσω του Διαδικτύου των Υπηρεσιών
- **Modularity:** ευέλικτη προσαρμογή των Smart Factories για την αλλαγή των απαιτήσεων των επιμέρους ενοτήτων.

[12] https://blogs.sap.com/2015/06/30/industry-40-fourth-industrial-revolution/ Βιομηχανία 4.0 - τέταρτη βιομηχανική επανάσταση, (πρόσβαση 29.8.2018).

ΚΕΦΑΛΑΙΟ 4: Η Τεχνολογία του Internet of Things

4.1 Ροές δεδομένων (Data Streams) στο IoT

Το Διαδίκτυο των πραγμάτων (IoT) παράγει, αποθηκεύει και κατευθύνει δεδομένα συνεχώς. Βασική σχεδίαση στα συστήματα αυτά είναι η διαχείριση της ροής δεδομένων. Η ροή δεδομένων είναι ένας από τους βασικούς καθοριστικούς παράγοντες στον τρόπο με τον οποίο αναπτύσσονται οι αρχιτεκτονικές πληροφοριών και οι εφαρμογές λογισμικού. Μεγάλο μέρος της προσοχής της περιλαμβάνει την αυτοματοποίηση των υποδομών.

Ο αυξανόμενος όγκος, η ποικιλία, η ταχύτητα και η ακρίβεια ειλικρίνεια των δεδομένων που παράγονται από το διαδίκτυο θα συνεχίσουν να δημιουργούν μια έκρηξη δεδομένων για το προβλεπόμενο μέλλον. Με εκτιμήσεις που κυμαίνονται από 16 έως 50 δισεκατομμύρια συσκευές συνδεδεμένες στο Διαδίκτυο μέχρι το 2020, η πιο δύσκολη πρόκληση για τις ευρείας κλίμακας εφαρμογές και τα έξυπνα περιβάλλοντα είναι η αξιοποίηση διαφόρων και συνεχώς αυξανόμενων ροών δεδομένων που προέρχονται από καθημερινές συσκευές και η εξαγωγή ουσιαστικών πληροφοριών και ο εντοπισμός προτύπων συμπεριφοράς. Για να αποκομίσουν τα πλήρη οφέλη, οποιαδήποτε επιτυχημένη λύση για την ανάπτυξη εφαρμογών και υπηρεσιών με γνώμονα το περιβάλλον και τα δεδομένα, πρέπει να είναι σε θέση (η εφαρμογή) να καταστήσει αυτές τις πολύτιμες ή σημαντικές πληροφορίες διαφανείς και διαθέσιμες με πολύ μεγαλύτερη συχνότητα, ώστε να βελτιώσουν σημαντικά τις δυνατότητες λήψης αποφάσεων και πρόβλεψης. (Kale, 2018).

Ροή δεδομένων σε πραγματικό χρόνο.

Όταν υπάρχουν δυνατότητες συνεχούς ροής στις υποδομές δεδομένων, δημιουργείται η ικανότητα αυτόματης ροής δεδομένων σε πραγματικό χρόνο. Προστίθεται δηλαδή η ευελιξία της επεξεργασίας και της αυξημένης διαθεσιμότητας δεδομένων του IoT, (για παράδειγμα των κοινωνικών μέσων ενημέρωσης και άλλων πηγών δεδομένων συνεχούς ροής) με την παράλληλη διαχείριση δεδομένων βάσει μεταφοράς πακέτων.

Σε αντίθεση με τις παραδοσιακές ροές που βασίζονται σε πακέτα μεταγωγών, όπου τα δεδομένα φορτώνονται σε σύνολα σε προγραμματισμένη βάση (π.χ. ωριαία, ημερήσια ή μηνιαία), οι ροές δεδομένων σε πραγματικό χρόνο διαφέρουν με τους ακόλουθους τρόπους:

- Είναι συχνά πιο ευαίσθητες στο χρόνο.
- Είναι συνήθως μεγαλύτερες σε όγκο.
- Μπορούν ή όχι να έχουν μακροπρόθεσμη αξία μετά την επεξεργασία.

Οι ροές δεδομένων σε πραγματικό χρόνο ή οι πηγές δεδομένων συνεχούς ροής μπορούν να προέρχονται από πολλές περιοχές δεδομένων μιας επιχείρησης, συμπεριλαμβανομένων μονάδων εντός της επιχείρησης, που μοιράζονται δεδομένα βασισμένα σε αισθητήρες, συστήματα υπολογιστών, βάσεις δεδομένων η και περιοχές όπως τροφοδοσία δεδομένων από το διαδίκτυο, τα κοινωνικά μέσα, ερευνητικά προγράμματα ικανοποίησης πελατών (για ανάλυση και επεξεργασία). (Kale, 2018).

4.2 Μοντέλα Διασύνδεσης Συσκευών

Από αρχιτεκτονικής πλευράς αντιλαμβανόμαστε, ότι οι συσκευές που συνδέονται στο πλαίσιο του Internet of Things συνδέονται και επικοινωνούν κάνοντας χρήση προκαθορισμένων πρωτοκόλλων επικοινωνίας. Το 2015 το συμβούλιο αρχιτεκτονικής του Διαδικτύου «Internet Architecture Board» (IAB) εξέδωσε ένα κατευθυντήριο οδηγό για την διασύνδεση των έξυπνων συσκευών , το οποίο περιλαμβάνει το γενικό πλαίσιο αρχιτεκτονικής μοντέλων επικοινωνίας που χρησιμοποιείται από IoT συσκευές. Παρακάτω παρατίθενται τα βασικά χαρακτηριστικά του κάθε μοντέλου:

4.2.1 Μοντέλο Device-to-Device

Το Device-to-Device Communication μοντέλο αναπαριστά την άμεση σύνδεση και επικοινωνία μεταξύ δύο συσκευών, χωρίς την χρήση κάποιου διακομιστή ενδιάμεσου server εφαρμογών, και χρησιμοποιούν πρωτόκολλα όπως το Bluetooth, το Z-Wave και το ZigBee. Αυτές οι συσκευές επικοινωνούν μέσω πολλών τύπων δικτύων IP ή το Internet. Τα δίκτυα

επικοινωνίας Device-to-Device ακολουθούν συγκεκριμένα πρωτόκολλα και ανταλλάσσουν μηνύματα για να επιτύχουν την λειτουργία τους. Αυτό το μοντέλο επικοινωνίας χρησιμοποιείτε κατά κύριο λόγο σε εφαρμογές οικιακού αυτοματισμού όπου τα πακέτα που ανταλλάσσονται σε χαμηλό ρυθμό μετάδοσης δεδομένων. Τέτοιες συσκευές είναι λαμπτήρες, θερμοστάτες ,διακόπτες ενεργοποίησης ή απενεργοποίησης ηλεκτρικών συσκευών .Η άμεση αυτή σχέση επικοινωνίας τους επιτρέπει να έχουν ενσωματωμένους μηχανισμούς ασφάλειας και πιστοποίησης στοιχείων και επίσης τους επιτρέπει να χρησιμοποιούν μοντέλα δεδομένων άρρηκτα συνδεδεμένα με την οικογένεια συσκευών που την χρησιμοποιεί. Οι συσκευές που χρησιμοποιούν ένα συγκεκριμένο πρωτόκολλο τείνουν να επικοινωνούν καλύτερα μεταξύ τους. Αυτό έχει ως αποτέλεσμα συσκευές που χρησιμοποιούν το πρωτόκολλο ZigBee να μην είναι συμβατές με αυτές που επικοινωνούν με το Bluetooth.[13] Υπάρχουν πολλά πρότυπα, που αναπτύσσονται γύρω από αυτό το μοντέλο όπως το Bluetooth Low Energy, που είναι δημοφιλές για φορητές συσκευές εξαιτίας των χαμηλών του απαιτήσεων σε ενέργεια που μπορούν να δώσουν αυτονομία μηνών ή και ενός χρόνου στις συσκευές. Η χαμηλή του πολυπλοκότητα μπορεί, επίσης, να ελαττώσει το μέγεθος και το κόστος του.[14]

Σχήμα 7.Μοντέλο επικοινωνίας Device-to-Device

[13] [RFC 7452] Tschofenig, H., et. al., (2015) “Architectural Considerations in Smart Object Networking. Tech”., Internet Architecture Board

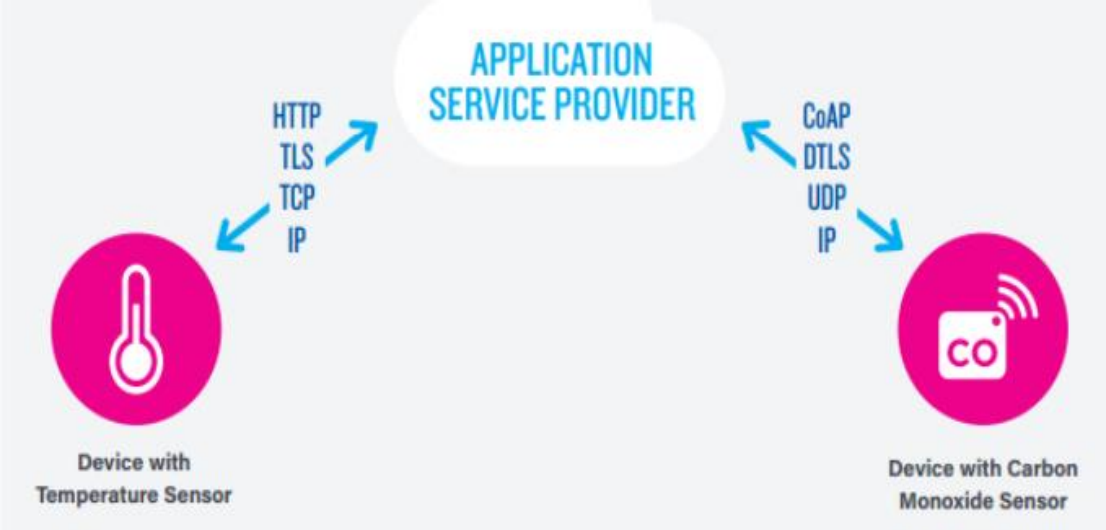
[14] http://www.rfc-editor.org/rfc/rfc7452.txt

4.2.2 Μοντέλο Device-to-Cloud

Το μοντέλο Device-to-Cloud επιτρέπει την σύνδεση IoT συσκευών μέσα από μια διαδικτυακή υπηρεσία Cloud η οποία επιβλέπει την ανταλλαγή δεδομένων και ελέγχει την ροή των μηνυμάτων. Η συγκεκριμένη προσέγγιση εκμεταλλεύεται υπάρχοντα πρωτόκολλα επικοινωνίας, όπως το Ethernet ή το Wi-fi, για να εγκαταστήσει μία σύνδεση μεταξύ της συσκευής και του δικτύου IP, το οποίο συνδέεται τελικά με την υπηρεσία Cloud. Το μοντέλο αυτό επικοινωνίας χρησιμοποιείται από αρκετές IoT εφαρμογών με γνωστότερη αυτών τον "έξυπνο" θερμοστάτη από την Nest Labs και η Smart TV της Samsung. Η συσκευή αυτή, πέρα από τον παραδοσιακό τρόπο χρήσης της, στηρίζεται στην επικοινωνίας της με μια βάση δεδομένων σε Cloud πλατφόρμα όπου αποθηκεύονται οι πληροφορίες που συλλέγει η συσκευή με βάση τις ώρες χρήσης της, την θερμοκρασία δωματίου, την θερμοκρασία που ορίστηκε από τον χρήστη καθώς και την θερμοκρασία περιβάλλοντος ώστε να γίνει ανάλυση των δεδομένων κατανάλωσης ενέργειας μια οικίας. Η Cloud αυτή σύνδεση επιτρέπει στον χρήστη να αποκτήσει απομακρυσμένη πρόσβαση στην διαχείριση του. [15]Αντίστοιχα η Smart TV της Samsung χρησιμοποιεί μα διαδικτυακή σύνδεση για να μεταδίδει πληροφορίες ,να ενεργοποιεί διαδραστικές λειτουργίες όπως η αναγνώριση ομιλίας.[16] Η Cloud συνδεσιμότητα επιτρέπει στον χρήστη (και την εφαρμογή) να αποκτήσει απομακρυσμένο έλεγχο σε μια συσκευή. Επίσης , ενδεχομένως να υποστηρίζει ενημερώσεις λογισμικού για τις συσκευές.

[15] "Meet the Nest Thermostat | Nest." (2015) Nest Labs https://nest.com/thermostats/nest-learning-thermostat/overview/ (πρόσβαση 15.9.2018).

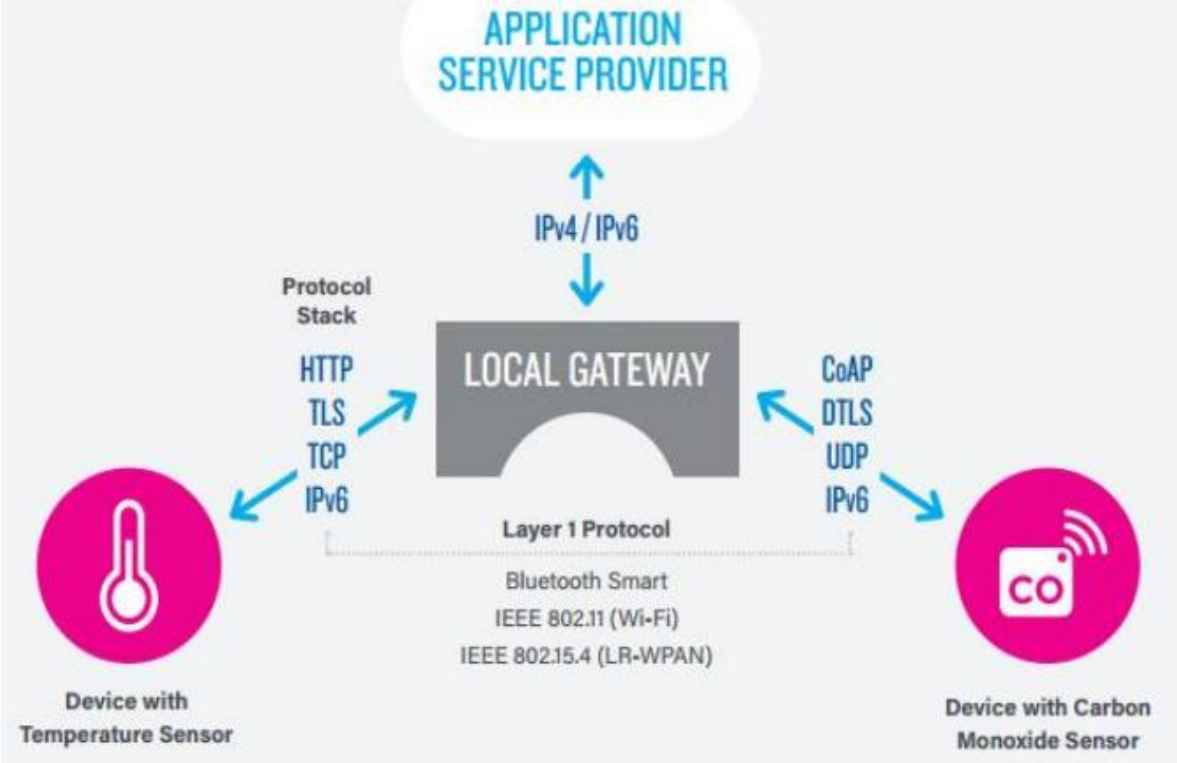
[16] Samsung Privacy Policy--SmartTV Supplement https://www.samsung.com/sg/info/privacy/smarttv/



Σχήμα 8.Μοντέλο επικοινωνίας Device-to-Cloud

4.2.3 Μοντέλο Device-to-Gateway

Στο μοντέλο επικοινωνίας Device-to-Gateway, οι IoT συσκευές, συνδέονται σε μια ενδιάμεση συσκευή προκειμένου να αποκτήσουν πρόσβαση σε μια Cloud υπηρεσία Αυτό το μοντέλο συχνά περιλαμβάνει το λογισμικό της εφαρμογής που τρέχει σε μια τοπική πύλη-συσκευή (π.χ. ένα smartphone), που ενεργεί σαν ένας μεσάζων μεταξύ της IoT συσκευής και της Cloud υπηρεσίας. Αυτή η πύλη-συσκευή θα μπορούσε να παρέχει ασφάλεια και άλλες λειτουργίες όπως μετάφραση δεδομένων και πρωτοκόλλων. Αν η πύλη συσκευή του επιπέδου εφαρμογής είναι ένα smartphone, το λειτουργικό της εφαρμογής μπορεί να έχει την μορφή ενός app, που πραγματοποιεί σύζευξη με την IoT συσκευή και επικοινωνεί με την Cloud υπηρεσία. (Duffy Marsan C.,2015). Αυτή μπορεί να είναι μια συσκευή όπως ένα «έξυπνο ρολόι (smart watches), παλμογράφος και συσκευές καταγραφής σωματικής δραστηριότητας (activity trackers) διότι δεν υποστηρίζουν την άμεση επικοινωνία με Cloud υπηρεσίες εξαιτίας των περιορισμένων δυνατοτήτων συνδεσιμότητας τους, που συνδέεται με την Cloud υπηρεσία μέσω μιας smartphone εφαρμογής, ή εφαρμογές αυτοματοποίησης εργασιών κατοικίας. Επιπλέον η χρήση αυτού του μοντέλου επιτρέπει την εισαγωγή νέων έξυπνων συσκευών σε μία ήδη υπάρχουσα τοπική πύλη δικτύου κάτι που επιτρέπει την επεκτασιμότητα των IoT εφαρμογών, κανόνας που αποτελεί σημαντικό παράγοντα εξέλιξης στην ανάπτυξη και εδραίωση του IoT.

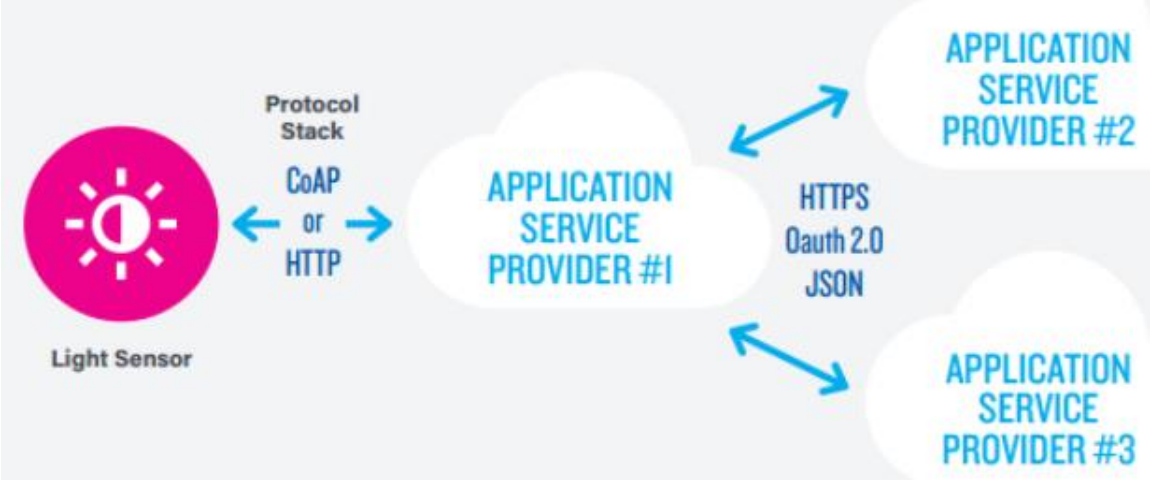


Σχήμα 9.Μοντέλο επικοινωνίας Device-to-Gateway

4.2.4 Μοντέλο Back-End Data Sharing

Το μοντέλο επικοινωνίας Back-End Data Sharing ουσιαστικά επεκτείνει την Device-to Cloud επικοινωνία έτσι ώστε οι IoT συσκευές να μπορούν να ανεβάζουν τα δεδομένα μόνο για ένα πάροχο υπηρεσιών εφαρμογής. Σύμφωνα με αυτό το μοντέλο, οι χρήστες μπορούν να εξάγουν και να αναλύσουν δεδομένα έξυπνων αντικειμένων από μια Cloud υπηρεσία σε συνδυασμό με δεδομένα από άλλες πηγές. Το μοντέλο επικοινωνίας Back-End Data Sharing επιτρέπει τα δεδομένα που συλλέγονται από μια IoT συσκευή να συγκεντρώνονται και να αναλύονται.[17]

[17] Communication Models in Internet of Things: A Survey
http://www.ijste.org/articles/IJSTEV3I11049.pdf



Σχήμα 10.Μοντέλο επικοινωνίας Back-End Data Sharing

4.3 Η Αρχιτεκτονική του IoT

Μέχρι στιγμής, οι IoT εφαρμογές βασίζονται σε αποσπασματικές εφαρμογές λογισμικού για συγκεκριμένα συστήματα και περιπτώσεις χρήσης. Η μεγάλη ανάγκη για αρχιτεκτονικές αναφοράς στην βιομηχανία έχει γίνει απτή με τον ταχέως αυξανόμενο αριθμό των πρωτοβουλιών που εργάζονται προς την υλοποίηση ολοκληρωμένων αρχιτεκτονικών. Αυτές οι πρωτοβουλίες αποσκοπούν στην διευκόλυνση της διαλειτουργικότητας, την απλοποίηση της ανάπτυξης και ευκολία εφαρμογής. Ακολούθως αναφέρονται πέντε τέτοιες πρωτοβουλίες:

1. Reference Architecture Model Industry 4.0 (RAMI 4.0): Μια αρχιτεκτονική αναφοράς για έξυπνα εργοστάσια αφοσιωμένα σε IoT πρότυπα.

2. Industrial Internet Reference Architecture (IIRA): Το IIRA είναι ένα αρχιτεκτονικό πρότυπο και μεθοδολογία που σχεδιάστηκε από ένα ευρύ των μελών του Industrial Internet Consortium (IIC), συμπεριλαμβανομένων των αρχιτεκτόνων του συστήματος και του λογισμικού, ειδικούς των επιχειρήσεων και ειδικούς ασφαλείας.

3. Internet of Things-Architecture (IoT-A): Το IoT-A παρέδωσε μια λεπτομερή αρχιτεκτονική και ένα μοντέλο από λειτουργική και πληροφοριακή άποψη. Επίσης, εκτέλεσε μια λεπτομερή ανάλυση των απαιτήσεων του συστήματος.

4. Standard for an Architectural Framework for the Internet of Things (IoT): Έχει δημιουργηθεί μία ομάδα εργασίας σχετικά με ένα IoT αρχιτεκτονικό πλαίσιο που δίνει έμφαση στην προστασία, την ασφάλεια, την ιδιωτικότητα και γενικά ζητήματα ασφαλείας.

5. Arrowhead Framework: Η πρωτοβουλία αυτή δίνει την δυνατότητα συνεργατικού αυτοματισμού με ανοιχτού δικτύου ενσωματωμένες συσκευές. Είναι ένα σημαντικό project της Ευρωπαϊκής Ένωσης για την παροχή βέλτιστων πρακτικών σχετικά με τον συνεργατικό αυτοματισμό.[18]

4.4 Το λειτουργικό σύστημα του IoT (RIoT)

Το διαδίκτυο των πραγμάτων (IoT) χαρακτηρίζεται από ετερογενείς συσκευές. Το εύρος των συσκευών που χρησιμοποιούνται ή που αναμένεται να χρησιμοποιηθούν στο μέλλον, αποτελούνται από μικρούς και πολύ ελαφρούς αισθητήρες που τροφοδοτούνται από μικρό-ελεγκτές 8 bit (**MCUs - multipoint control unit**) μέχρι συσκευές εξοπλισμένες με πιο ισχυρούς, αλλά αποδοτικούς επεξεργαστές 32/64 bit. Ούτε τα παραδοσιακά λειτουργικά συστήματα (OS) που λειτουργούν επί του παρόντος στο Διαδίκτυο, ούτε ένα τυπικό λειτουργικό σύστημα για δίκτυα αισθητήρων είναι ικανά να ικανοποιήσουν τις ποικίλες απαιτήσεις ενός τόσο ευρέος φάσματος συσκευών. Το RIOT OS, είναι ένα λειτουργικό σύστημα που εξετάζει ρητά συσκευές με ελάχιστους πόρους, αλλά διευκολύνει την ανάπτυξη σε ένα ευρύ φάσμα συσκευών. Το RIOT OS επιτρέπει τον τυπικό προγραμματισμό C και C ++, παρέχει δυνατότητες πολλαπλών αντιγράφων καθώς και πραγματικού χρόνου και απαιτεί μόνο ελάχιστη μνήμη RAM 1,5 kB. [19]

Το RIOT είναι για το Διαδίκτυο των Πράξεων, ότι είναι το Linux, για το Διαδίκτυο. Είναι το κύριο λειτουργικό που υπερισχύει και είναι ένα ελεύθερο λειτουργικό σύστημα ανοιχτού κώδικα που αναπτύχθηκε από συλλογικές κοινότητες, ακαδημαϊκούς και ανθρώπους που το χρησιμοποιούσαν σαν χόμπι, και διανέμεται σε όλο τον κόσμο. Στοχεύει στην εφαρμογή όλων

[18] https://www.computer.org/csdl/mags/so/2016/01/mso2016010112.pdf

[19] https://hal.inria.fr/file/index/docid/945122/filename/2013-riot_os.pdf RIOT OS: Towards an OS for the Internet of Things, (πρόσβαση 3.10.2018).

των σχετικών ανοιχτών προτύπων που υποστηρίζουν ένα Διαδίκτυο των Πραγμάτων που είναι συνδεδεμένο, ασφαλές, ανθεκτικό και φιλικό προς την ιδιωτικότητα.

Το λειτουργικό σύστημα θα πρέπει να είναι διαθέσιμο σε όλες τις συσκευές IoT. Οι απαιτήσεις αυτές επικεντρώνονται στα χαρακτηριστικά του Linux, αφού αποτελεί καλό παράδειγμα για ένα λειτουργικό σύστημα ανοιχτού κώδικα μεταξύ των μεγάλων λειτουργικών συστημάτων. Σε σύγκριση με ένα τυπικό ελαφρύ λειτουργικό σύστημα που στοχεύει στα ασύρματα δίκτυα αισθητήρων (**WSNs - Wireless sensor network**), το Linux είναι πιο φιλικό προς τους προγραμματιστές με πολλές διαθέσιμες βιβλιοθήκες συστημάτων, πρωτόκολλα δικτύου και αλγόριθμους, με την έννοια ότι οι προγραμματιστές μπορούν να κωδικοποιήσουν το πρότυπο σε γλώσσα C ή C ++. Ωστόσο, οι ελάχιστες απαιτήσεις του Linux όσον αφορά την CPU και τη μνήμη δεν ταιριάζουν με των περιορισμένων δυνατοτήτων συσκευές του IoT που τροφοδοτούνται από μικρές μονάδες MCU. Ενώ γίνονται προσπάθειες για την εξάλειψη αυτών των απαιτήσεων, το Linux δεν έχει σχεδιαστεί για το IoT και δεν μπορεί να εκπληρώσει με αποτελεσματικότητα αυτές τις ιδιομορφίες του IoT.

Το Linux δεν μπορεί να γίνει το μόνο λειτουργικό σύστημα που θα τους χρησιμοποιείται στο IoT για τους παραπάνω λόγους. Από την άλλη μεριά, οι ένα ελαφρύ λειτουργικό σύστημα που στοχεύει στα ασύρματα δίκτυα αισθητήρων (WSNs) για να τρέχει στων περιορισμένων δυνατοτήτων συσκευές του IoT καθιστούν σημαντικά λιγότερο φιλική για τους προγραμματιστές τη χρήση του, ενώ δεν μπορεί να χρησιμοποιηθεί σε πιο ισχυρές συσκευές IoT και θα οδηγήσει σε λιγότερο αποδοτική υλοποίηση, μην μπορώντας να αξιοποιήσει τις πλήρεις δυνατότητες των συσκευών. Το κυρίαρχο λειτουργικό σύστημα των ασύρματων αισθητήρων WSN, και το TinyOS, ακολουθούν έναν σχεδιασμό που βασίζεται σε συμβάντα, ο οποίος είναι χρήσιμος για τυπικά σενάρια WSN, αλλά παρουσιάζει μειονεκτήματα για αποδοτική και λειτουργική υλοποιήσεις δικτύων.

Ένα λειτουργικό σύστημα χαρακτηρίζεται από τις ακόλουθες βασικές πτυχές σχεδιασμού: τη δομή του πυρήνα, τον προγραμματιστή και το μοντέλο προγραμματισμού.

Ο πυρήνας μπορεί επίσης

1. Να είναι χτισμένο μονολιθικά,
2. Να ακολουθεί μια πολύ-επίπεδη προσέγγιση, ή
3. Να υλοποιεί την αρχιτεκτονική microkernel.

Η επιλογή της στρατηγικής προγραμματισμού συνδέεται στενά με την υποστήριξη σε πραγματικό χρόνο (ή την έλλειψή της), την υποστήριξη για διαφορετικές προτεραιότητες εργασιών ή τον υποστηριζόμενο βαθμό αλληλεπίδρασης των χρηστών. Τέλος, το μοντέλο προγραμματισμού καθορίζει εάν:

- όλες οι εργασίες εκτελούνται μέσα στο ίδιο πλαίσιο και δεν έχουν κατακερματισμό του χώρου διεύθυνσης μνήμης, ή
- κάθε διαδικασία μπορεί να τρέξει στο νήμα της και έχει τη δική της στοίβα μνήμης.

Το μοντέλο προγραμματισμού συνδέεται επίσης με τις διαθέσιμες γλώσσες προγραμματισμού για προγραμματιστές εφαρμογών.

Το λειτουργικό σύστημα RIOT στοχεύει στη γεφύρωση του χάσματος που υπάρχει μεταξύ του λειτουργικού συστήματος για τα ασύρματα δίκτυα αισθητήρων (WSN) και του παραδοσιακού λειτουργικού συστήματος που τρέχει σε κεντρικούς υπολογιστές του Διαδικτύου. Το RIOT λειτουργεί σε διάφορες πλατφόρμες, συμπεριλαμβανομένων των ενσωματωμένων συσκευών καθώς και των κοινών υπολογιστών. Ο εξαρτώμενος από το υλικό κώδικας μειώνεται στο ελάχιστο και απορροφάται από τον ίδιο τον πυρήνα.[20]

[20] https://riot-os.org/#features RIOT: The friendly Operating System for the Internet of Things, (πρόσβαση 3.10.2018).

ΚΕΦΑΛΑΙΟ 5: RFID Systems

Η αναγνώριση ραδιοσυχνοτήτων (RFID- Radio-frequency identification) είναι μια τεχνολογία που έχει εξελιχθεί την τελευταία δεκαετία. Τα σαφή πλεονεκτήματα αυτής της τεχνολογίας οδήγησαν σε μεγάλο αριθμό προσπαθειών έρευνας στις αρχές της δεκαετίας του 2000. Ωστόσο, η ευρεία και καθολική υιοθέτηση της RFID δεν έχει ακόμη πλήρως υλοποιηθεί. Αυτό οφείλεται σε ένα συνδυασμό πολλών τεχνικών και εμπορικών παραγόντων.

Κάθε φυσικό αντικείμενο (things – πράγμα-αντικείμενο) στο Διαδίκτυο πρέπει να ενσωματώνει τεχνολογίες αυτόματης αναγνώρισης ταυτότητας, ώστε το αντικείμενο να μπορεί να αναγνωριστεί με μοναδικό τρόπο. Η αναγνώριση ραδιοσυχνοτήτων (RFID) είναι μία από τις πιο ευρέως χρησιμοποιούμενες τεχνολογίες αυτόματης αναγνώρισης ταυτότητας. Οι τεχνολογίες RFID ενσωματώνουν απλές συνιστώσες επικοινωνίας, αποθήκευσης και υπολογισμών σε προσαρτημένες ετικέτες που μπορούν να επικοινωνούν με τους αναγνώστες ασύρματα σε απόσταση. Επομένως, οι τεχνολογίες RFID παρέχουν έναν απλό και φθηνό τρόπο σύνδεσης φυσικών αντικειμένων με το IoT - όσο ένα αντικείμενο φέρει μια ετικέτα, όπου μπορεί να ταυτοποιηθεί και να εντοπιστεί από τους αναγνώστες. Οι τεχνολογίες RFID χρησιμοποιούνται ευρέως σε πολυάριθμες εφαρμογές, όπως η διαχείριση αποθεμάτων, η αλυσίδα εφοδιασμού, η παρακολούθηση προϊόντων, η μεταφορά, η εφοδιαστική και η είσπραξη διοδίων κ.α. (Chen & Chen, 2016).

5.1 Συστατικά ενός συστήματος RFID

Ένα σύστημα RFID αποτελείται από ένα μεγάλο αριθμό ετικετών RFID, έναν ή περισσότερους αναγνώστες RFID και ένα διακομιστή back end. Οι σημερινές εμπορικές ετικέτες μπορούν να ταξινομηθούν σε τρεις κατηγορίες:

1. Παθητικές ετικέτες, οι οποίες τροφοδοτούνται από το ραδιοκύμα από τον αναγνώστη RFID και επικοινωνούν με τον αναγνώστη μέσω της ανάστροφης κατανομής,
2. Ενεργές ετικέτες, οι οποίες τροφοδοτούνται από τις δικές τους πηγές ενέργειας και

3. Ημι-ενεργές ετικέτες, οι οποίες χρησιμοποιούν εσωτερικές πηγές ενέργειας για να τροφοδοτούν τα κυκλώματά τους ενώ επικοινωνούν με τον αναγνώστη μέσω οπίσθιας σάρωσης.

Όπως καθορίζεται στο πρωτόκολλο EPC Class-1 Gen-2[21](C1G2), κάθε ετικέτα έχει ένα μοναδικό αναγνωριστικό που αναγνωρίζει το αντικείμενο στο οποίο είναι συνδεδεμένο. Το αντικείμενο μπορεί να είναι ένα όχημα, ένα προϊόν σε μια αποθήκη, ένα ηλεκτρονικό διαβατήριο που μεταφέρει προσωπικές πληροφορίες, μια ιατρική συσκευή που καταγράφει τα δεδομένα υγείας ενός ασθενούς ή οποιοδήποτε άλλο φυσικό αντικείμενο στο Διαδίκτυο. Ο ενσωματωμένος πομποδέκτης κάθε ετικέτας του επιτρέπει να μεταδίδει και να λαμβάνει ραδιοσήματα. Ως εκ τούτου, ένας αναγνώστης μπορεί να επικοινωνήσει με μια ετικέτα σε μια απόσταση όσο η ετικέτα βρίσκεται στην περιοχή εμβέλειας της. Ωστόσο, οι επικοινωνίες μεταξύ των ετικετών RFID γενικά δεν είναι εφικτές λόγω της χαμηλής ισχύος μετάδοσης τους. Οι αναδυόμενες ετικέτες δικτύου φέρνουν μια θεμελιώδη ενίσχυση στις ετικέτες RFID επιτρέποντας στις ετικέτες να επικοινωνούν μεταξύ τους. Οι δικτυωμένες ετικέτες ενσωματώνονται με συστατικά συγκομιδής ενέργειας που μπορούν να συγκεντρώσουν ενέργεια από το περιβάλλον. (Chen & Chen, 2016).

Η ευρεία χρήση των ετικετών RFID στο διαδίκτυο συνεπάγεται νέα ζητήματα σχετικά με την αποτελεσματικότητα, την ασφάλεια και την ιδιωτικότητα, τα οποία είναι αρκετά διαφορετικά από αυτά των παραδοσιακών συστημάτων δικτύωσης.

Εκτός από αυτά τα ιδανικά χαρακτηριστικά, υπάρχουν και πολλά άλλα επιθυμητά χαρακτηριστικά που οι ερευνητές προσπαθούν να φέρουν σε πρακτικά συστήματα UHF RFID. Ορισμένα από αυτά περιλαμβάνουν: (Bolic, Simplot-Ryl & Stojmenovic, 2010).

- Υψηλό επίπεδο ασφάλειας ενός συστήματος RFID.
- Εντοπισμός κάθε ετικέτας μέσα στη ζώνη ανάγνωσης με υψηλό επίπεδο ακρίβειας.
- Χαμηλό κόστος των στοιχείων RFID και υψηλή απόδοση της επένδυσης.

[21] http://www.rfidjournal.com/articles/view?2481 Gen 2 EPC Protocol Approved as ISO 18000-6C, (πρόσβαση 10.10.2018).

- Εύκολη ενσωμάτωση του λογισμικού RFID σε υπάρχον λογισμικό εφαρμογών.
- Απλή ανάπτυξη και δικτύωση πολλαπλών αναγνωστών.
- Απλός συγχρονισμός πολλαπλών αναγνωστών.

5.2 Θεμελιώδεις αρχές λειτουργίας

Η τεχνολογία RFID ή η αναγνώριση ραδιοσυχνοτήτων είναι μια τεχνολογία όπου οι πληροφορίες που αποθηκεύονται σε ένα ολοκληρωμένο κύκλωμα ή τσιπ μπορούν να διαβαστούν εξ αποστάσεως χωρίς φυσική επαφή χρησιμοποιώντας το φάσμα ραδιοσυχνοτήτων. Ένα σύστημα RFID αποτελείται από έναν πομποδέκτη (Transponders) ή RFID ετικέτες (RFID tags) και από τον αναγνώστη (Reader). Μια ετικέτα RFID είναι ένα μικρό ολοκληρωμένο κύκλωμα, που περιλαμβάνει μνήμη, για να αποθηκεύει δεδομένα, και κεραία, για να επικοινωνεί με τον αναγνώστη. ο οποίος εκπέμπει σήμα RF μέσω κεραίας. Η μνήμη της ετικέτας τροφοδοτείται ηλεκτρικά από τον αναγνώστη, αλλά υπάρχουν και ετικέτες RFID που μπορούν να αντλούν ενέργεια από κάποια πηγή, όπως μια μπαταρία. (Παρασκευάς, Ασημακόπουλος & Τριανταφύλλου, 2015).

Ο αναγνώστης RFID έχει ενσωματωμένες μια κεραία και μια μονάδα ελέγχου. Όταν μια ετικέτα RFID βρεθεί στην εμβέλεια ενός αναγνώστη, τότε η μονάδα ελέγχου του τελευταίου επικοινωνεί ασύρματα με την ετικέτα. Αυτή ενεργοποιείται και επιστρέφει στον αναγνώστη τα δεδομένα που περιέχει. Τα δεδομένα που βρίσκονται αποθηκευμένα σε μια ετικέτα αποτελούνται από ένα μοναδικό αναγνωριστικό και μια περιγραφή για το αντικείμενο το οποίο αφορά η ετικέτα.

Η ετικέτα μπορεί να περιλαμβάνει ένα λειτουργικό σύστημα και έναν ηλεκτρονικό κώδικα προϊόντων (Electronic Product Code / EPC). Το μέγεθος των δεδομένων δεν υπερβαίνει τα 2 KB, είναι όμως αρκετό για να αποθηκευτούν τα απαραίτητα δεδομένα κάθε αντικειμένου. Ο αναγνώστης προωθεί τα δεδομένα που λαμβάνει σε κάποιο ειδικό ενδιάμεσο λογισμικό, το οποίο τα επεξεργάζεται και λαμβάνει τις κατάλληλες αποφάσεις, στο πλαίσιο του ευρύτερου

πληροφοριακού συστήματος. Σε πολλές περιπτώσεις ο αναγνώστης έχει και δυνατότητα εγγραφής, δηλαδή μπορεί να τροποποιεί τα δεδομένα της ετικέτας. (Chen & Chen, 2016).

Η μνήμη σε μια ετικέτα RFID μπορεί να είναι:

- **Μνήμη μόνο για ανάγνωση (Read Only Memory - ROM).**[22] Είναι η μνήμη που υπάρχει σε όλους τους υπολογιστές (στο BIOS του κάθε υπολογιστή από τον κατασκευαστή). Με τον ίδιο τρόπο τα δεδομένα και στην ετικέτα εγγράφονται από τον κατασκευαστή κατά την διάρκεια της παραγωγής της ετικέτας και δεν έχουν την δυνατότητα επανεγγραφής. Τα δεδομένα που είναι αποθηκευμένα σε αυτά τα τσιπ δεν χάνονται όταν αφαιρείται η ισχύς (η πηγή της ενέργειας).

- **Επανεγγράψιμη μνήμη (Read-Write).** Στην περίπτωση αυτή, τα δεδομένα της ετικέτας μπορούν όχι μόνο να διαβάζονται από τον αναγνώστη, αλλά και να εγγράφονται, δηλαδή να τροποποιούνται.

- **Μνήμη μιας εγγραφής και πολλών αναγνώσεων (Write Once and Read Many Memory WORM**). Στην περίπτωση αυτή, η ετικέτα προγραμματίζεται από τον χρήστη αλλά χωρίς να υπάρχει δυνατότητα επανεγγραφής της για δεύτερη φορά.

Η ετικέτα RFID μπορεί να έχει εμβέλεια λίγων εκατοστών έως και 100 μέτρων, ακόμα και χωρίς να υπάρχει άμεση οπτική επαφή με τον αναγνώστη. Αυτό γίνεται ανάλογα με τη συχνότητα επικοινωνίας που χρησιμοποιεί το κάθε σύστημα RFID Το μεγάλο εύρος τιμών της απόστασης αναγνώρισης είναι ένα σημαντικό χαρακτηριστικό των συστημάτων RFID. Η απόσταση αναγνώρισης που θα επιλεγεί εξαρτάται από την εφαρμογή η οποία θα χρησιμοποιηθεί στο σύστημα. Υπάρχουν διαφορετικά εύρη συχνοτήτων που χρησιμοποιούνται στην RFID, όπως χαμηλής συχνότητας (LF, 125 kHz), υψηλής συχνότητας (HF, 13.56 MHz), υπερύψηλης

[22] https://computer.howstuffworks.com/rom.htm How ROM Works, (πρόσβαση 10.10.2018).

συχνότητας (UHF, 433 MHz, 860-960 MHz) και μικροκυμάτων (2.45 GHz, 5.8 GHz). Αυτές οι ζώνες, γενικά, δεν απαιτούν άδεια αν η μεταδιδόμενη ισχύς είναι περιορισμένη. Ορισμένες ζώνες μπορούν να χρησιμοποιηθούν σε παγκόσμιο επίπεδο (HF), ενώ άλλες είναι συγκεκριμένες σε ορισμένες περιοχές (UHF στις ΗΠΑ, στην ΕΕ και στην Ιαπωνία). (Παρασκευάς, Ασημακόπουλος & Τριανταφύλλου, 2015).

Ζώνη συχνοτήτων RFID	**Απόσταση αναγνώρισης**
120-150 KHz (χαμηλές συχνότητες / LF)	Μέχρι 10 εκατοστά
13.56 MHz (υψηλές συχνότητες / HF)	Μέχρι 1 μέτρο
433 MHz (πολύ υψηλές συχνότητες / UHF)	Από 1-100 μέτρα
865-868 MHz και 902-928 MHz (UHF)	Από 1-2 μέτρα
2450-5800 MHz (μικροκύματα)	Από 1-2 μέτρα
3.1-10 GHz (μικροκύματα)	Μέχρι 200 μέτρα

Πίνακας 2. Συχνότητες λειτουργίας και εμβέλεια συστημάτων RFID

Ένα σύστημα RFID έχει πολλά πλεονεκτήματα όπως:

- Αναγνώριση ενός αντικειμένου, από απόσταση, με μεγάλη ταχύτητα, χωρίς λάθη
- Δυνατότητα αποθήκευσης δεδομένων,
- Οι ετικέτες RFID μπορούν να αναγνωριστούν χωρίς να υπάρχει οπτική επαφή,
- Ο προγραμματισμός των ετικετών μπορεί να πραγματοποιηθεί από απόσταση,
- Μπορούν να υποστηρίζονται και επιπρόσθετες λειτουργίες, όπως η παρακολούθηση και η καταγραφή της θερμοκρασίας, ή μετρήσεις κ.λπ.

Τα πλεονεκτήματα της τεχνολογίας RFID χρησιμοποιούνται σε εμπορικές εφαρμογές από επιχειρήσεις ειδικά στον έλεγχο των αποθηκών και των πωλήσεων όπως:

- Από την εφοδιαστική αλυσίδα μιας επιχείρησης με την αναγνώριση και καταγραφή των αντικειμένων που φέρουν ετικέτα RFID, αυτόματα, από απόσταση, με σωστό τρόπο όπως προϊόντα, συσκευασίες ή παλέτες προϊόντων. Η ιχνηλασιμότητα αυτή των προϊόντων εξυπηρετεί την γρήγορη αποθήκευση, ανεύρεση, ενδό-διακίνηση μετακίνηση, εξαγωγή, φόρτωση, αποστολή, εκφόρτωση τους, όπως και των μεταφορικών μέσων που χρησιμοποιούνται για τη διαδικασία, έχοντας την δυνατότητα υπολογισμού και του όγκου για παράδειγμα που μπορούν να φορτωθούν. (Παρασκευάς, Ασημακόπουλος & Τριανταφύλλου, 2015).

- Ταυτόχρονα με την οργάνωση της εφοδιαστικής αλυσίδας μιας επιχείρησης, εξυπηρετείται και ο έλεγχος της αποθήκης, με συχνές, γρήγορες και ακριβείς απογραφές, τη μείωση του αριθμού των αποθεμάτων, των απωλειών και των ελλείψεων, τον άμεσο έλεγχο και την ορθή εκτέλεση παραγγελιών και παραλαβών, τη δυνατότητα ασφαλούς και γρήγορης ανάκλησης ελαττωματικών παρτίδων, (διαδικασία μεγάλης σπουδαιότητας για ορισμένους κλάδους όπως οι φαρμακευτικές εταιρείες).

- Στις πωλήσεις, από τον εύκολο εντοπισμό προϊόντων, την ακριβή διαθεσιμότητα, την άμεση έκδοση παραστατικών, την καλύτερη εξυπηρέτηση πελατών, την αύξηση των πωλήσεων.

- Με την και αυτόματη ενημέρωση σε πραγματικό χρόνο των κεντρικών πληροφοριακών συστημάτων διαχείρισης της επιχείρησης (π.χ. ERP, CRM κτλ.) και την πλήρη ενημέρωση όλων των τμημάτων για την πορεία και διαθεσιμότητα των προϊόντων.

Οι βασικές λειτουργικές παράμετροι είναι η απόσταση λειτουργίας, η απόδοση του συστήματος και η ακρίβεια εντοπισμού. Τα συστήματα RFID καθορίζονται από το κόστος, το μέγεθος και την απόδοσή τους, όπου η απόδοση καθορίζεται από το εύρος ανάγνωσης, την ταχύτητα, την

ακεραιότητα της επικοινωνίας και τη συμβατότητα μεταξύ των συστημάτων από διαφορετικούς προμηθευτές. (Bolic, Simplot-Ryl & Stojmenovic, 2010).

5.3 Χαρακτηριστικά διαφοροποίησης των συστημάτων RFID

Τα συστήματα RFID υπάρχουν σε αμέτρητες παραλλαγές, που παράγονται από σχεδόν εξίσου μεγάλο αριθμό κατασκευαστών. Τα σημαντικότερα κριτήρια διαφοροποίησης για συστήματα RFID είναι η συχνότητα λειτουργίας του αναγνώστη, η μέθοδος φυσικής σύζευξης και το εύρος του συστήματος. Ένα άλλο σημαντικό κριτήριο διάκρισης των διαφόρων συστημάτων RFID είναι ο τρόπος με τον οποίο λειτουργεί η παροχή ενέργειας του αναμεταδότη. Η ταξινόμηση των συστημάτων RFID σύμφωνα με το φάσμα των λειτουργιών πληροφόρησης και επεξεργασίας δεδομένων που προσφέρει ο πομποδέκτης και το μέγεθος της μνήμης δεδομένων του, αποκτά ένα ευρύ φάσμα παραλλαγών.

Οι ετικέτες RFID χωρίζονται σε ενεργές ή παθητικές βάσει του τρόπου με τον οποίο τροφοδοτούνται. Οι ενεργές ετικέτες τροφοδοτούνται με μπαταρία και στην πραγματικότητα μεταδίδουν ενεργά ένα σήμα. Οι ενεργές ετικέτες έχουν το μεγαλύτερο εύρος ανάγνωσης (~ 100 μέτρα) και είναι οι πιο ακριβές λόγω του κόστους της μπαταρίας και του πομπού. Οι παθητικές ετικέτες δεν έχουν τροφοδοσία ετικετών. Η ενέργεια για την ενεργοποίηση του τσιπ προέρχεται αποκλειστικά από το εισερχόμενο κύμα από τον αναγνώστη RFID. Το εύρος ανάγνωσης περιορίζεται από τη μεταφερόμενη πυκνότητα ισχύος που απαιτείται για να επιτευχθεί επαρκής τάση για την ενεργοποίηση του τσιπ. Οι παθητικές ετικέτες είναι σημαντικά λιγότερο δαπανηρές από τις ενεργές ετικέτες και γενικά, έχουν σημαντικά μικρότερη εμβέλεια. Μια τρίτη κατηγορία ετικετών είναι η ημι-ενεργή ή ετικέτες με παθητική υποβοήθηση μπαταρίας (BAP). Αυτές οι ετικέτες περιλαμβάνουν μια μπαταρία έτσι ώστε το τσιπ θα έχει πάντοτε αρκετή ενέργεια για να ενεργοποιηθεί αλλά δεν έχει ενεργό πομπό.

5.4 Η χρήση των RFID systems

Η χρήση των RFID έδωσε νέες δυνατότητες σε διάφορες μορφές οικονομικών δραστηριοτήτων και υπηρεσιών, συνδέοντας όχι μόνο αντικείμενα, αλλά δημιουργώντας την βάση των στοιχείων που επιτρέπει σε επιχειρήσεις και οργανισμούς να έχουν άμεση πληροφόρηση από τις λειτουργικές διαδικασίες τους, δίνοντας τους την δυνατότητα να βελτιώσουν, να παρακολουθήσουν και να εξυπηρετήσουν σε ελάχιστο χρόνο τους πελάτες τους.

Η βιομηχανία έχοντας την εμπειρία από τις προηγούμενες διαδικασίες αυτοματοποίησης, εκμεταλλεύτηκε πρώτη την δυνατότητα διασύνδεσης των «αντικειμένων» με το διαδίκτυο μέσω RFID, αποκτώντας σε πραγματικό χρόνο στοιχεία για την καλύτερη οργάνωση της παραγωγής, την παραγγελία των α’ υλών των βοηθητικών υλικών και των υλικών συσκευασίας, την σωστή χρονική στιγμή, μειώνοντας το κόστος διατήρησης μεγάλων αποθεμάτων υλικών, ή αντίστοιχα αποφεύγοντας την έλλειψη κρίσιμων υλικών στην διάρκεια της παραγωγής. Στις κατασκευές και σε άλλες συναφείς βιομηχανίες, τα υλικά αποτελούν συχνά τις μεγαλύτερες δαπάνες για έργα. Σε μεγάλους χώρους εργασίας, η απλή εύρεση ενός υλικού μπορεί να είναι προβληματική και χρονοβόρα. Λόγω της αλυσίδας παραγωγής, η έλλειψη ενός μόνο υλικού ή εργαλείου, μπορεί να καθυστερήσει ολόκληρη την γραμμή παραγωγής και αυτό μπορεί να αποβεί καταστροφικό για μια βιομηχανική μονάδα.

Ο έλεγχος και η συντήρηση των μηχανημάτων, είναι ένας άλλος τομέας που βοήθησε σε μεγάλο βαθμό η χρήση αυτής της τεχνολογίας, με την πρόσθετη δυνατότητα αποστολής δεδομένων από τα RFID σε ειδικά λογισμικά απεικόνισης και της ταυτόχρονης αποστολής τους μέσω διαδικτύου σε οποιαδήποτε μέρος του κόσμου. Με αυτόν τον τρόπο μια εταιρεία, μπορεί να παρακολουθεί από οποιαδήποτε απόσταση μέσω εξελιγμένων οθονών υψηλής ανάλυσης την κατάσταση μηχανημάτων και εργαλείων, ελέγχοντας διάφορες παραμέτρους καλής λειτουργίας και επεμβαίνοντας σε ορισμένες περιπτώσεις αν χρειάζεται στο ίδιο το μηχάνημα. Η χρήση αυτής της λειτουργίας των RFID και της διασύνδεσης στο διαδίκτυο, επεκτείνεται σε ολόκληρη την βιομηχανία, ενώ εκεί στηρίχθηκε και η νέα καινοτόμος τεχνολογία **Industrie 4.0** - Βιομηχανία 4.0 και το **Industrie Internet of Things** - Βιομηχανικό Διαδίκτυο των πραγμάτων (**I.I.o.T.**).

Τα RFID εξυπηρετούν όλο και περισσότερους τομείς και η χρησιμοποίηση τους επεκτείνεται σε κάθε δραστηριότητα του ανθρώπου από την γεωργία, την ιατρική, τον αθλητισμό, μέχρι την στρατιωτική τεχνολογία και τα δορυφορικά συστήματα. Η χρησιμοποίηση των ετικετών RFID έχει βρει πεδίο στα πιο απίθανα συστήματα, τα οποία για μερικές επιχειρήσεις έχουν μειώσει δραματικά τα κόστη ορισμένων λειτουργιών ή τους επέτρεψαν να βελτιώσουν τις υπηρεσίες τους.

ΚΕΦΑΛΑΙΟ 6: Ασφάλεια στο IoT και RFID

Ένα από τα μεγαλύτερα θέματα που έχουν προκύψει από την καθολική χρήση του διαδικτύου, την αυξανόμενη εισαγωγή συσκευών στο διαδίκτυο των πραγμάτων και την χρήση του cloud , είναι η ασφάλεια όλου αυτού του ψηφιακού παγκόσμιου περιβάλλοντος. Για παράδειγμα η αυτοματοποίηση των εργοστασίων, η χρήση δικτύων υπολογιστών για την έρευνα και τεχνολογία, ήταν εξίσου σημαντική και τα προηγούμενα χρόνια, αλλά ουσιαστικά ήταν περιορισμένη σε ένα εξειδικευμένο κύκλο επιστημόνων, τεχνικών και υπαλλήλων, με κλειστά ασφαλή κυκλώματα. Ακόμη και οι επιθέσεις σε συστήματα υπολογιστών, είχαν συγκεκριμένη μορφή, συγκεκριμένες τακτικές και αντιμετωπιζόταν με συγκεκριμένους τρόπους. Δίκτυα ανταλλαγής δεδομένων και πληροφοριών υπήρχαν εδώ και 50 χρόνια, αλλά ήταν απροσπέλαστα στην πλειοψηφία του κοινού, με ειδικά πρωτόκολλά ασφαλείας κα ειδικές συσκευές πρόσβασης.

Η δημιουργία του διαδικτύου, η εξάπλωση του σε ολόκληρο τον κόσμο, η όλο και πιο ευρεία χρησιμοποίηση του ακόμη και σε κρίσιμες εργασίες, απετέλεσε την αφορμή για την ραγδαία αύξηση των κρουσμάτων ασφαλείας. Η δυνατότητα της ασύρματης επικοινωνίας και η εξάπλωση της κινητής τηλεφωνίας, ήταν τα εργαλεία της μετατροπής της ανθρωπότητας σε μια παγκόσμια ψηφιακή κοινότητα, χωρίς σύνορα, με πολύ μεγάλες δυνατότητες αλλά ταυτόχρονα και πολύ μεγάλους κινδύνους. Η δημιουργία, ή για πολλούς η μετεξέλιξη το διαδικτύου στο διαδίκτυο των πραγμάτων και η χρήση δισεκατομμυρίων και πιθανώς σε λίγο διάστημα εκατοντάδων δισεκατομμυρίων συσκευών, από τις πιο απλές συσκευές για παράδειγμα καταγραφής της θερμοκρασίας, μέχρι σε εξειδικευμένες συσκευές ελέγχου σημαντικών βιομηχανικών μονάδων, κρίσιμων ιατρικών μηχανημάτων, στρατιωτικών όπλων και κυρίως συσκευών καταγραφής και ελέγχουν των ανθρώπων, τα οποία επικοινωνούν ασύρματα και αλληλοεπιδρούν μέσω του διαδικτύου, έχει εγείρει και τον σοβαρότερο προβληματισμό ασφαλείας και προστασίας της ανθρώπινης ύπαρξης όσο ποτέ άλλοτε στην ιστορία της ανθρωπότητας.

Ένα ασύρματο δίκτυο αισθητήρων (ΑΔΑ / Wireless Sensor Network - WSN) αποτελείται από διασκορπισμένους αυτόνομους αισθητήρες για την παρακολούθηση φυσικών ή περιβαλλοντολογικών συνθηκών, όπως η θερμοκρασία, ο ήχος, η ατμοσφαιρική πίεση κτλ. και

μέσω συνεργασίας να μεταφέρει τα δεδομένα μέσω του δικτύου σε μια συγκεκριμένη τοποθεσία. Τα πιο μοντέρνα δίκτυα ικανά και να δίνουν αλλά και να δέχονται πληροφορίες πράγμα που τους επιτρέπει να ελέγχουν την δραστηριότητα των αισθητήρων. Σήμερα τέτοια δίκτυα χρησιμοποιούνται σε πολλές καταναλωτικές και βιομηχανικές εφαρμογές, η παρακολούθηση και ο έλεγχος της βιομηχανικής παραγωγής, την παρακολούθηση των μηχανημάτων υγείας και πολλά άλλα. Το ασύρματο δίκτυο αισθητήρων (WSN) είναι ένας τομέας μεγάλης σημασίας τόσο για την βιομηχανία, τις υπόλοιπες οικονομικές δραστηριότητες, αλλά και τους απλούς πολίτες. Ανοίγει την πόρτα σε μεγάλο αριθμό στρατιωτικών, βιομηχανικών, επιστημονικών, πολιτικών και εμπορικών εφαρμογών. Επιτρέπουν την οικονομικά αποδοτική ανίχνευση, ειδικά σε εφαρμογές όπου η ανθρώπινη παρατήρηση ή οι παραδοσιακοί αισθητήρες θα ήταν ανεπιθύμητοι, αναποτελεσματικοί, δαπανηροί ή επικίνδυνοι. Οι ασύρματες αισθητήρες έχουν περιορισμένες δυνατότητες ενέργειας και υπολογιστικής, καθιστώντας πολλές παραδοσιακές μεθοδολογίες ασφαλείας δύσκολες ή αδύνατο να χρησιμοποιηθούν. (Oreku & Pazynyuk, 2016). Επίσης, αναπτύσσονται συχνά σε ανοιχτές περιοχές, επιτρέποντας φυσικές επιθέσεις όπως μπλοκάρισμα κόμβου και παραβίαση. Οι απειλές που παρουσιάζονται σε ένα WSN και η οργάνωση του WSN ως απάντηση σε αυτές τις απειλές επηρεάζονται άμεσα από την εφαρμογή WSN. Ως αποτέλεσμα, ο σχεδιασμός και η ανάλυση της ασφάλειας του WSN πρέπει να είναι ευαίσθητοι σε αυτό το πλαίσιο.

Το πλαίσιο ασφάλειας των ασύρματων επικοινωνιών των αισθητήρων και του διαδικτύου, δεν είναι μια ακριβής τεχνική προδιαγραφή. Αντίθετα, πρόκειται για ένα σύνολο παραγόντων που σχετίζονται με την ασφάλεια, τις δυνατότητες και τον χώρο σχεδιασμού του ασύρματου δικτύου αισθητήρων. Καθώς το WSN συνεχίζει να αναπτύσσεται, το ίδιο ισχύει και για την ανάγκη αποτελεσματικών μηχανισμών ασφαλείας. Επειδή τα δίκτυα αισθητήρων μπορούν να αλληλοεπιδρούν με ευαίσθητα δεδομένα ή και να λειτουργούν σε εχθρικά περιβάλλοντα χωρίς παρακολούθηση, είναι επιτακτική ανάγκη να αντιμετωπίζονται αυτές οι ανησυχίες ασφάλειας από την αρχή του σχεδιασμού του συστήματος. Ωστόσο, λόγω εγγενών περιορισμών πόρων και υπολογισμών, η ασφάλεια στα δίκτυα αισθητήρων δημιουργεί διαφορετικές προκλήσεις από την παραδοσιακή ασφάλεια δικτύου - υπολογιστή. Εκτίθενται σε μια μεγαλύτερη ποικιλία επιθέσεων από άλλα δίκτυα. Η ποιότητα και η πολυπλοκότητα αυτών των επιθέσεων αυξάνονται

καθημερινά. [23] Οι πληροφορίες που μεταφέρονται μέσω του WSN πρέπει να προστατεύονται από κακή χρήση.

Οι σύγχρονες μέθοδοι ασφαλείας πρέπει να εγγυώνται την ασφάλεια της μετάδοσης δεδομένων σε σχέση με τις ανάγκες ασφαλείας, δηλαδή την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα. (Oreku & Pazynyuk, 2016).

6.1 Κίνδυνοι στο Διαδίκτυο των Πραγμάτων

Το σημαντικότερο πρόβλημα ασφαλείας στο διαδίκτυο των πραγμάτων, είναι ότι παρέχει το κατάλληλο έδαφος για πολλές κακόβουλες επιθέσεις. Αυτό οφείλεται αρχικά στο γεγονός ότι το διαδίκτυο των πραγμάτων, είναι ένα οικοσύστημα που αποτελείται χιλιάδες διασυνδεδεμένες συσκευές, οι οποίες δεν μπορούν στην πλειονότητα τους να ελέγχονται. Έτσι δημιουργούνται κενά ασφαλείας στο σύστημα , με αποτέλεσμα οι κίνδυνοι διαρροής ή απώλειας δεδομένων να είναι πολλοί.

Χαρακτηριστικά θα μπορούσαμε να αναφέρουμε ότι οι κίνδυνοι ασφαλείας στο IoT είναι οι εξής:

- Απώλεια κρυπτογράφησης στη μεταφορά δεδομένων

Οι περισσότερες συσκευές που χρησιμοποιούνται στο διαδίκτυο των πραγμάτων, δεν διαθέτουν την απαραίτητη επεξεργαστική ισχύ ώστε να πραγματοποιήσουν πολύπλοκους υπολογισμούς όπως για είναι παράδειγμα η εφαρμογή ισχυρών αλγόριθμων για ασφαλή επικοινωνία ή η κρυπτογράφηση δεδομένων. Έτσι τα δεδομένα που συλλέγονται μεταδίδονται χωρίς κρυπτογράφηση με αποτέλεσμα να είναι εύκολα παραβιάσιμα.

- Μη ασφαλής διαδικτυακή επαφή

Τα διαπιστευτήρια που χρησιμοποιούνται είναι αδύναμα.

- Ελλιπής πιστοποίηση και εξουσιοδότηση

Η έλλειψη χρήσης κωδικών ή και χρήση μη ισχυρών κωδικών πρόσβασης μπορούν να θέσουν σε κίνδυνο ολόκληρο το σύστημα IoT.

[23] https://www.iec.ch/whitepaper/pdf/iecWP-internetofthings-LR-en.pdf

- Μη ασφαλή λογισμικά

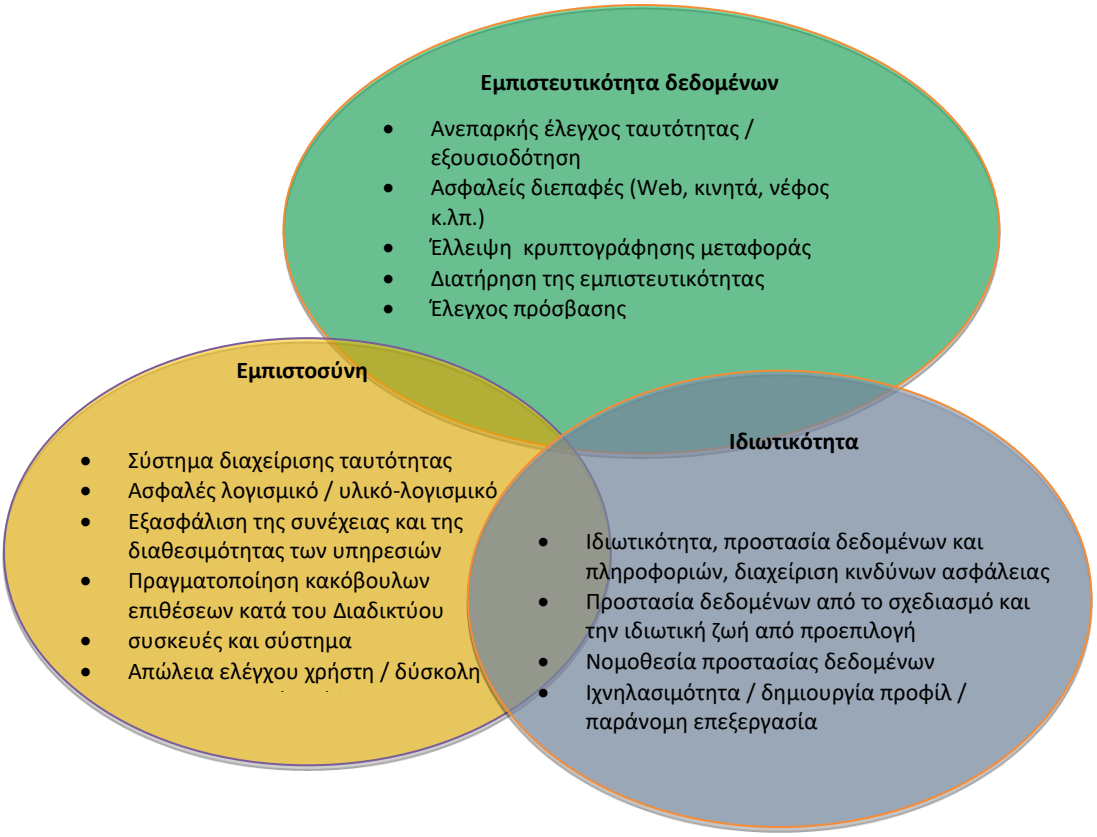
Πολλές IoT συσκευές δεν μπορούν να δεχτούν αναβαθμίσεις και ενημερώσεις λογισμικού. Αυτό έχει ως συνέπεια να είναι εξαιρετικά δύσκολη η εξάλειψη μιας ευπάθειας εφόσον δεν γίνονται ενημερώσεις. (Weber, R. H., & Studer, E.)

6.2 Τεχνικές Ασφάλειας στο IoT

Στο διαδίκτυο των πραγμάτων (IoT), κάθε συνδεδεμένη συσκευή θα μπορούσε να αποτελέσει πιθανή πόρτα για την υποδομή IoT ή τα προσωπικά δεδομένα. Οι ανησυχίες σχετικά με την ασφάλεια των δεδομένων και την προστασία της ιδιωτικής ζωής είναι πολύ σημαντικές, αλλά οι δυνητικοί κίνδυνοι που συνδέονται με το Διαδίκτυο θα φθάσουν σε νέα επίπεδα, καθώς η δια-λειτουργικότητα και η αυτόνομη λήψη αποφάσεων αρχίζουν να ενσωματώνουν την πολυπλοκότητα, τα κενά ασφαλείας και την πιθανή ευπάθεια των συστημάτων. Οι κίνδυνοι ιδιωτικού απορρήτου θα προκύψουν στο Διαδίκτυο, καθώς η πολυπλοκότητα μπορεί να δημιουργήσει περισσότερη ευπάθεια που σχετίζεται με την προσφορά υπηρεσιών

Σε πολλούς πολίτες, πολλές πληροφορίες σχετίζονται με τα προσωπικά τους στοιχεία, όπως η ημερομηνία γέννησης, στοιχεία ταυτότητας, η τοποθεσία κατοικίας, οικονομικά στοιχεία, οικογενειακά δεδομένα κλπ. Αυτή είναι μια πτυχή των μεγάλων δεδομένων που προκαλεί προβλήματα και τα επαγγέλματα ασφάλειας θα πρέπει να διασφαλίσουν ότι σκέφτονται μέσω των δυνητικών κινδύνων προστασίας της ιδιωτικής ζωής με ολόκληρο το σύνολο δεδομένων. Το IoT θα πρέπει να εφαρμόζεται με νόμιμο, δεοντολογικό, κοινωνικό και πολιτικά αποδεκτό τρόπο, όπου πρέπει να λαμβάνονται υπόψη οι νομικές προκλήσεις, οι τεχνικές προκλήσεις και οι επιχειρηματικές προκλήσεις. (Li & Xu, 2017).

Η ασφάλεια πρέπει να εξασφαλίζεται καθ’ όλη τη διάρκεια του κύκλου ζωής του έργου στο διαδίκτυο των πραγμάτων από τον αρχικό σχεδιασμό για τις υπηρεσίες που εκτελούνται. Οι κύριες ερευνητικές προκλήσεις στο IoT περιλαμβάνουν, το απόρρητο των δεδομένων, την ιδιωτικότητα και την εμπιστοσύνη, όπως φαίνεται στο παρακάτω διάγραμμα.



Διάγραμμα 4. Η αντιμετώπιση των κυρίων προκλήσεων στο IoT.

Στο IoT, υπάρχουν 4 επίπεδα ελέγχου ασφαλείας:

- Επίπεδο ανίχνευσης,
- Επίπεδο δικτύου,
- Επίπεδο υπηρεσιών και
- Επίπεδο διεπαφής εφαρμογής.

Κάθε επίπεδο είναι σε θέση να παρέχει αντίστοιχα στοιχεία ασφαλείας, όπως έλεγχος πρόσβασης, έλεγχος ταυτότητας συσκευών, ακεραιότητα δεδομένων και εμπιστευτικότητα στη μετάδοση, διαθεσιμότητα και ικανότητα αντιμετώπισης κακόβουλου λογισμικού ή επιθέσεων.

6.2.1 Ασφάλεια στο επίπεδο ανίχνευσης

Αυτό το επίπεδο χαρακτηρίζεται ως τομή των ανθρώπων, των τόπων και των πραγμάτων. Αυτά τα πράγματα μπορούν να είναι απλές συσκευές όπως τα συνδεδεμένα θερμόμετρα και οι λαμπτήρες, ή σύνθετες συσκευές όπως τα ιατρικά εργαλεία και ο εξοπλισμός παραγωγής. Προκειμένου να διασφαλιστεί η πλήρης αξιοποίηση της ασφάλειας στο διαδίκτυο, πρέπει να σχεδιαστεί και να ενσωματωθεί στις ίδιες τις συσκευές. Αυτό σημαίνει ότι οι συσκευές IoT πρέπει να είναι σε θέση να αποδείξουν την ταυτότητά τους για να διατηρήσουν την αυθεντικότητα, να υπογράψουν και να κρυπτογραφήσουν τα δεδομένα τους για να διατηρήσουν την ακεραιότητά τους και να περιορίσουν τα τοπικά αποθηκευμένα δεδομένα για την προστασία της ιδιωτικής ζωής. Το μοντέλο ασφαλείας για συσκευές πρέπει να είναι αρκετά αυστηρό για να αποτρέπεται η μη εξουσιοδοτημένη χρήση, αλλά αρκετά ευέλικτο για να υποστηρίζει ασφαλείς αλληλεπιδράσεις με ανθρώπους και άλλες συσκευές σε προσωρινή βάση.
Επειδή οι συσκευές IoT τελικά θα υπάρχουν παντού στο περιβάλλον, η φυσική ασφάλεια είναι επίσης σημαντική. Αυτό δημιουργεί την ανάγκη σχεδιασμού ανθεκτικότητας σε παραβιάσεις σε συσκευές, ώστε να είναι δύσκολο να εξαχθούν ευαίσθητα στοιχεία όπως προσωπικά δεδομένα, κρυπτογραφικά κλειδιά ή διαπιστευτήρια. Τέλος, αναμένεται ότι οι συσκευές IoT θα έχουν μεγάλη διάρκεια ζωής, οπότε είναι σημαντικό να είναι ενεργοποιημένες ενημερώσεις λογισμικού για την αντιμετώπιση των αναπόφευκτων δυσλειτουργιών που ανακαλύπτονται μετά την εγκατάσταση τους. (Li & Xu, 2017).

6.2.2 Ασφάλεια στο επίπεδο δικτύου

Αυτό το επίπεδο του πλαισίου IoT αντιπροσωπεύει τη συνδεσιμότητα και την ανταλλαγή μηνυμάτων μεταξύ των πραγμάτων και των υπηρεσιών cloud. Οι επικοινωνίες στο Διαδίκτυο είναι συνήθως συνδυασμός ιδιωτικών και δημόσιων δικτύων, οπότε η διασφάλιση της κυκλοφορίας είναι προφανώς σημαντική. Αυτό είναι ίσως ο πιο κατανοητός τομέας της ασφάλειας του IoT, με τεχνολογία όπως η κρυπτογράφηση TLS / SSL ιδανική για την επίλυση του προβλήματος. Η κύρια δυσκολία προκύπτει όταν απαιτούνται διαδικασίες κρυπτογράφησης σε συσκευές με περιορισμένους πόρους, δηλαδή μικρό-ελεγκτές 8 bit με περιορισμένη μνήμη

RAM. Ένα άλλο θέμα ασφάλειας για το επίπεδο δικτύου είναι ότι πολλές συσκευές IoT επικοινωνούν μέσω πρωτοκόλλων διαφορετικών από WiFi. [24]Αυτό σημαίνει ότι η πύλη IoT είναι υπεύθυνη για τη διατήρηση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας κατά τη μετάφραση μεταξύ διαφορετικών ασύρματων πρωτοκόλλων, από το Z-Wave ή το ZigBee στο WiFi για παράδειγμα.

6.2.3 Ασφάλεια στο επίπεδο υπηρεσιών

Αυτό το επίπεδο του πλαισίου αντιπροσωπεύει το σύστημα διαχείρισης του Διαδικτύου και είναι υπεύθυνο για την διαχείριση συσκευών και χρηστών, την εφαρμογή πολιτικών και κανόνων και συντονισμό της αυτοματοποίησης σε όλες τις συσκευές. Ο έλεγχος πρόσβασης βάσει ρόλων για τη διαχείριση της ταυτότητας των χρηστών και των συσκευών και οι ενέργειες στις οποίες έχουν εξουσιοδοτηθεί να λαμβάνουν είναι κρίσιμες σε αυτό το επίπεδο. Για να επιτευχθεί η μη αναδημοσίευση, είναι επίσης σημαντικό να διατηρηθεί ένα ίχνος ελέγχου των αλλαγών που γίνονται από κάθε χρήστη και συσκευή, έτσι ώστε να είναι αδύνατο να αντικρούονται οι ενέργειες που λαμβάνονται στο σύστημα. Αυτά τα δεδομένα παρακολούθησης θα μπορούσαν επίσης να χρησιμοποιηθούν για τον εντοπισμό πιθανώς συμβιβαζόμενων συσκευών όταν ανιχνεύεται μη φυσιολογική συμπεριφορά. (Li & Xu, 2017).

6.2.4 Ασφάλεια στο επίπεδο διεπαφής

Υπάρχουν πολλές προκλήσεις για την εξασφάλιση του IoT, πολλές από τις οποίες είναι μοναδικές σε κάθε επίπεδο του πλαισίου IoT. Η ισχυρή ασφάλεια αρχίζει με την ενσωμάτωσή της στις ίδιες τις συσκευές. Ακόμη και οι μικρές, περιορισμένες από τους πόρους συσκευές που είναι κοινές στο IoT πρέπει να εφαρμόσουν κρυπτογραφία για να διατηρήσουν την εμπιστευτικότητα, την ακεραιότητα και την αυθεντικότητα κατά την επικοινωνία μέσω του

[24]https://www.researchgate.net/publication/317841088_Transferring_Wireless_High_Update_Rate_Supermedia_Streams_Over_IoT

δικτύου. Τέλος, πρέπει να βρεθεί μια ισορροπία μεταξύ της ιδιωτικής ζωής των καταναλωτών και των επιχειρήσεων και της διορατικότητας και της αξίας που προέρχεται από τα βουνά των δεδομένων που παράγονται από το Διαδίκτυο.

Μεγάλη ανάλυση δεδομένων των συγκεντρωτικών δεδομένων που παράγονται από το IoT περιγράφεται συχνά ως η πιο πολύτιμη πτυχή του IoT για παρόχους συσκευών και παρόμοιων υπηρεσιών. Αντίστροφα, η διατήρηση της προστασίας της ιδιωτικής ζωής των καταναλωτών αποτελεί επίσης κορυφαία προτεραιότητα για τις κρατικές υπηρεσίες με την Ομοσπονδιακή Επιτροπή Εμπορίου (FTC) και τον Οργανισμό για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) της Ευρωπαϊκής Ένωσης, που απελευθερώνουν τις αντίστοιχες κατευθυντήριες γραμμές για την εξασφάλιση του IoT.

Αυτό δημιουργεί ένα σύνολο απαιτήσεων ασφάλειας που σχετίζονται με την προστασία της ιδιωτικής ζωής, όπως γνωστοποίηση σαφούς χρήσης δεδομένων, ώστε οι πελάτες να έχουν ορατότητα και λεπτομερή έλεγχο των δεδομένων που αποστέλλονται στην υπηρεσία σύννεφο, διατηρώντας δεδομένα πελατών αποθηκευμένα στην υπηρεσία cloud διαχωρισμένα ή και κρυπτογραφημένα με τα κλειδιά που παρέχονται από τον πελάτη και κατά την ανάλυση των δεδομένων συνολικά μεταξύ των πελατών, τα δεδομένα θα πρέπει να είναι ανώνυμα.

Μια κρίσιμη απαίτηση του IoT είναι ότι οι συσκευές πρέπει να αλληλοσυνδεθούν, πράγμα που καθιστά την διαδικασία, ικανή να εκτελεί συγκεκριμένα καθήκοντα, όπως η επικοινωνία, η επεξεργασία πληροφοριών κλπ. Το IoT είναι σε θέση να λάβει αποκτήσει, να μεταδώσει και να επεξεργαστεί τις πληροφορίες από κόμβους (όπως συσκευές RFID, αισθητήρες, πύλες, έξυπνες συσκευές κ.λπ.) μέσω δικτύου για την εκτέλεση πολύπλοκων εργασιών. Το IoT θα πρέπει να είναι σε θέση να παρέχει εφαρμογές με ισχυρή προστασία ασφαλείας (π.χ. για αιτήσεις ηλεκτρονικής πληρωμής, το IoT πρέπει να μπορεί να προστατεύει την ακεραιότητα των πληροφοριών πληρωμής). (Li & Xu, 2017).

Η αρχιτεκτονική του συστήματος πρέπει να παρέχει λειτουργικές εγγυήσεις για το IoT, το οποίο γεφυρώνει το χάσμα μεταξύ των φυσικών συσκευών και των εικονικών κόσμων. Κατά τον

σχεδιασμό του πλαισίου της διασύνδεσης, πρέπει να λαμβάνονται υπόψη οι ακόλουθοι παράγοντες:

1. τεχνικοί παράγοντες, όπως τεχνικές ανίχνευσης, μέθοδοι επικοινωνίας, τεχνολογίες δικτύου κλπ.
2. προστασία της ασφάλειας, όπως εμπιστευτικότητα πληροφοριών, ασφάλεια μετάδοσης, προστασία της ιδιωτικής ζωής κ.λπ.
3. επιχειρησιακά ζητήματα, όπως επιχειρηματικά μοντέλα, επιχειρηματικές διαδικασίες κ.λπ.

6.3 Εμπιστευτικότητα και ακεραιότητα προσωπικών δεδομένων

Η προστασία των προσωπικών δεδομένων αποτελεί θεμελιώδη προϋπόθεση κατά την έναρξη οποιασδήποτε διαδικασίας σχεδιασμού υπηρεσίας IoT. Ο τελικός καταναλωτής συνήθως ανησυχεί προσωπικά, για διαρροές δεδομένων (εμπιστευτικότητα) που συνήθως αναφέρεται επίσης ως «Προστασία προσωπικών δεδομένων» στην κοινότητα ασφάλειας των πληροφοριών. Ο συνεχόμενος πολλαπλασιασμός του IoT θα επιτρέψει την πρόσβαση σε πληροφορίες για οποιοδήποτε περιβάλλον και για την κατάσταση, οποιουδήποτε αντικειμένου, οποτεδήποτε και οπουδήποτε. Όπως είναι φυσικό ο κίνδυνος της διάθεσης-όχι μόνο προσωπικών δεδομένων-, αλλά και δεδομένων που μπορούν να σχηματίσουν διάφορα προφίλ των καταναλωτών, (όπως ποιες τροφές προτιμά, ή πιο είδος μουσικής ακούει, ποιες είναι οι προτιμήσεις του στα ταξίδια, μπορεί να φαντάζουν σχετικά αθώες, αλλά ακόμη και οι επιστήμονες της πληροφορικής, οι οργανώσεις προστασίας δεδομένων και οι ίδιοι οι καταναλωτές ανησυχούν, καθώς ο συνδυασμός των διαφόρων δεδομένων και η επεξεργασία τους, μπορεί να αποδώσει πληροφορίες που οι περισσότεροι άνθρωποι δεν θα ήθελαν να γνωστοποιηθούν.

Το απόρρητο δεν είναι εγγενές στο IoT, δηλαδή όπου βρίσκεται ένα σύστημα ή μια υπηρεσία IoT, δεν είναι απαραίτητο ότι υπάρχει πιθανή παραβίαση της ιδιωτικής ζωής. Το απόρρητο, όπως και κάθε άλλη πιθανή απαίτηση ή ευπάθεια σε ένα δεδομένο σύστημα ή υπηρεσία IoT, είναι κάτι που πρέπει να εκτιμηθεί και όχι να υποτεθεί. Η τεράστια ποσότητα δεδομένων που υπάρχει στο

σύνολο του διαδικτύου των πραγμάτων, σε όλα τα στοιχεία και τις υπηρεσίες του, ανεξάρτητα από τη διαφορά ιδιοκτησίας και διαχείρισης του, τη φυσική και λογική αποθήκευση, σημαίνει ότι δεν υπάρχει αμφιβολία ότι το IOT, είναι δυνητικά μια τεράστια και μαζική πηγή δεδομένων, πολλές φορές και προσωπικών δεδομένων. (Macaulay, 2017).

Ενώ υπάρχει μεγάλος κίνδυνος που συνδέεται με την ιδιωτική ζωή στο Διαδίκτυο, ο κίνδυνος αυτός πρέπει να γίνει κατανοητός στο πλαίσιο των απαιτήσεων που απορρέουν τόσο από τη ρύθμιση του νόμου όσο και από τις απαιτήσεις του IoT.

6.4 Διαθεσιμότητα και Αξιοπιστία IoT

Ένα από τα σημαντικότερα θέματα είναι η διαφορετικότητα των κινδύνων του IoT με το συμβατικό περιβάλλον των επιχειρήσεων, και το διαδίκτυο όπως ήταν μέχρι πρόσφατα. Για τη χρήση του IoT, για εφαρμογές, συστήματα και υπηρεσίες κρίσιμης σημασίας, τα εξαρτήματα (πράγματα) που πρέπει να πληρούν τις απαιτήσεις για αξιοπιστία και διαθεσιμότητα, είναι πολύ περισσότερα, μερικές φορές «ξεφεύγουν» από τα όρια της πληροφορικής και πρέπει να μπορούν να καθοριστούν με τους όρους ανθεκτικότητας και διαθεσιμότητας που χρησιμοποιούν οι μηχανικοί των βιομηχανικών συστημάτων και οι μηχανικοί και διαχειριστές συστημάτων πληροφορικής.

Τα κύρια σημεία που πρέπει να πληρούν τα πράγματα (thinks) του IoT είναι:

Ευστάθεια: ένα σύστημα IoT πρέπει να παρέχει τη δυνατότητα μιας υπηρεσίας, αλλά ταυτόχρονα να αντιστέκεται στην αλλαγή λόγω εξωτερικών διαταραχών ή επιθέσεων χωρίς να τροποποιεί τη διαμόρφωση της υπηρεσίας. Πρέπει δηλαδή να είναι σε θέση να ολοκληρώσει την υπηρεσία που έχει σχεδιαστεί να πραγματοποιεί.

Ανθεκτικότητα: ένα σύστημα IoT πρέπει να παρέχει τη δυνατότητα μιας υπηρεσίας να ανταποκρίνεται στις αλλαγές λόγω εξωτερικών διαταραχών και να επιστρέφει την υπηρεσία στην επιθυμητή διαμόρφωσή της. (Macaulay, 2017).

Η απαίτηση αξιοπιστίας και διαθεσιμότητας έχει επιπτώσεις στους ακόλουθους τομείς εφαρμογής του IoT:

Η απλότητα είναι μία από τις σημαντικές λειτουργικές απαιτήσεις αντιστάθμισης που σχετίζονται με τη διαθεσιμότητα και την αξιοπιστία στο IoT. Το διαδίκτυο των πραγμάτων είναι ήδη πολύ περίπλοκη τεχνολογία. Η πολυπλοκότητα που εισάγεται από τη διαχείριση ασφάλειας και κινδύνων είναι πολύ σοβαρή, πράγμα που επηρεάζει το μοντέλο διαθεσιμότητας και αξιοπιστίας.

Οι επιχειρησιακοί έλεγχοι των διαφόρων μορφών επιχειρηματικών και οργανωτικών απαιτήσεων θα επεκταθούν σε τουλάχιστον τρεις διαφορετικές διαστάσεις της τεκμηρίωσης σχεδιασμού που θα απαιτηθούν για την αποτελεσματική διαχείριση του κινδύνου στο Διαδίκτυο:

- Εφαρμογή και σχεδιασμός συστήματος
- Σχέδιο διεπαφής χρήστη
- Τεκμηρίωση και αναφορά

Ένα σημαντικό στοιχείο αξιοπιστίας και διαθεσιμότητας είναι η μικρότερη δυνατή συντήρηση κατά την λειτουργία. Οι συσκευές IoT και οι πύλες θα πρέπει να λειτουργούν για μεγαλύτερες περιόδους χωρίς φυσική συντήρηση ή τεχνική υποστήριξη για την επίλυση προβλημάτων. (Liu et al, 2017).

6.5 Απειλές και επιπτώσεις από το IoT

Το διαδίκτυο των πραγμάτων εισήγαγε νέες καινοτόμες τεχνολογίες και διαδικασίες σε πολλές μορφές της ανθρώπινης δραστηριότητας, ενώ αναμένεται να κυριαρχήσει στο μέλλον πάνω στην νέα παγκόσμια ψηφιακή κοινότητα.

Η διασύνδεση τόσων αντικειμένων (συσκευών, αισθητήρων, υπολογιστών, υπηρεσιών) όπου μερικά από αυτά πραγματοποιούν κρίσιμες λειτουργίες που άπτονται της ασφάλειας της φυσικής

υπόστασης των ανθρώπων, αλλά και της ιδιωτικότητα των προσωπικών τους στοιχείων, αποτελεί ήδη το επόμενο μεγάλο στοίχημα που έχει να αντιμετωπίσει το ανθρώπινο γένος. Οι τεχνολογίες που παρουσιάζονται με καταιγιστικούς ρυθμούς ειδικά στην ρομποτική και την αυτόνομη λειτουργία πολλών δραστηριοτήτων, έχει ανησυχήσει την επιστημονική κοινότητα.

Το Διαδίκτυο των πραγμάτων (IoT) αλλάζει ταχύτατα τον τρόπο με τον οποίο οι καταναλωτές και οι κατασκευαστές αλληλοεπιδρούν με τον κόσμο. Όμως, παρά τα οφέλη που επιτρέπουν αυτές οι συσκευές, φέρνουν επίσης μαζί τους κρίσιμες ευπάθειες ασφαλείας που θέτουν τους πελάτες και τις επιχειρήσεις σε κίνδυνο.
Όμως, καθώς η βιομηχανία επεκτείνεται, έτσι και οι ευκαιρίες για τους χάκερ και τους κυβερνό-τρομοκράτες να διεισδύσουν σε αυτές τις συσκευές και να καταχραστούν τα δεδομένα αυξάνεται. Ως εκ τούτου, οι επιχειρήσεις πρέπει να αρχίσουν να επενδύουν τους πόρους τους στην ασφάλεια, ή να αντιμετωπίσουν τις καταστροφικές συνέπειες.[25]

Η εταιρεία Netflix και πλήθος άλλων υπηρεσιών δέχθηκαν επίθεση από το botnet Mirai, μια επίθεση **Distributed Denial of Service (DDoS)[26],**η οποία διεξήχθη από έναν τεράστιο αριθμό διαγραμμένων συσκευών IoT.
Αυτό το συγκεκριμένο botnet μολύνει πολυάριθμες συσκευές IoT (κυρίως παλιότερους δρομολογητές και κάμερες IP), και στη συνέχεια τους χρησιμοποίησε για να πλημμυρίσει τον παροχέα DNS Dyn με μια επίθεση DDoS. Αυτό το κομμάτι κακόβουλου κώδικα εκμεταλλεύτηκε τις συσκευές που χρησιμοποιούν παλιότερες εκδόσεις του πυρήνα του Linux και βασίστηκε στο γεγονός ότι οι περισσότεροι χρήστες δεν αλλάζουν τα προεπιλεγμένα ονόματα χρήστη και τους κωδικούς πρόσβασης στις συσκευές τους. Εάν οι συσκευές IoT χρησιμοποιούνται ως μέρος ενός μεγαλύτερου στρατού **botnet** ή είναι μόνιμα καταχρηστικές από κακόβουλο λογισμικό κακόβουλης λειτουργίας, όλες αυτές οι επιθέσεις καταδεικνύουν την επικίνδυνη έλλειψη ασφάλειας στον κόσμο του Διαδικτύου των πραγμάτων (IoT).

[25] https://www.zdnet.com/article/5-nightmarish-attacks-that-show-the-risks-of-iot-security
[26] Μία επίθεση διανεμημένης άρνησης παροχής υπηρεσίας (DDoS) είναι μια προσπάθεια να μην είναι διαθέσιμη μια διαδικτυακή υπηρεσία, χάρη στην κυκλοφορία από πολλαπλές πηγές. Στοχεύουν σε μια μεγάλη ποικιλία σημαντικών πόρων, από τις τράπεζες έως τις ιστοσελίδες ειδήσεων, και αποτελούν μια μεγάλη πρόκληση για να διασφαλιστεί ότι οι άνθρωποι μπορούν να δημοσιεύουν και να έχουν πρόσβαση σε σημαντικές πληροφορίες.

Botnet: Οι επιτιθέμενοι χτίζουν δίκτυα μολυσμένων υπολογιστών, γνωστούς ως «**botnets**», διαδίδοντας κακόβουλο λογισμικό μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου, ιστότοπων και κοινωνικών μέσων. Μόλις μολυνθούν, αυτά τα μηχανήματα μπορούν να ελεγχθούν εξ αποστάσεως χωρίς τη γνώση των ιδιοκτητών τους και να χρησιμοποιηθούν σαν στρατός για να ξεκινήσουν μια επίθεση εναντίον οποιουδήποτε στόχου. Ορισμένα botnets είναι τόσο ισχυρά όσο εκατομμύρια υπολογιστές μαζί. Τα botnets μπορούν να δημιουργήσουν τεράστιες υπερχειλίσεις της κυκλοφορίας για να συντρίψουν έναν στόχο. Αυτές οι υπερχειλίσεις μπορούν να δημιουργηθούν με πολλούς τρόπους, όπως η αποστολή περισσότερων αιτημάτων σύνδεσης από ό, τι μπορεί να χειριστεί κάποιος διακομιστής ή η αποστολή ηλεκτρονικών υπολογιστών στο θύμα – στόχο, τεράστιων ποσοτήτων τυχαίων δεδομένων για τη χρήση του εύρους ζώνης του στόχου. Ορισμένες επιθέσεις είναι τόσο μεγάλες που μπορούν να εξαντλήσουν τη διεθνή χωρητικότητα καλωδίων μιας χώρας. Ειδικές online αγορές υπάρχουν για να αγοράζουν και να πωλούν botnets ή μεμονωμένες επιθέσεις DDoS. Χρησιμοποιώντας αυτές τις υπόγειες αγορές, ο καθένας μπορεί να πληρώσει μια ονομαστική αμοιβή για να σιωπήσει ιστοσελίδες με τις οποίες διαφωνεί ή να διακόψει τις online λειτουργίες μιας επιχείρησης ή ενός οργανισμού.

Οι επιθέσεις στον κυβερνοχώρο στις συσκευές IoT είναι αναπόφευκτες και η ανθεκτικότητα των συσκευών και των δικτύων πρέπει να εξεταστεί προσεκτικά. Ένας διαχωρισμός των πολύτιμων στοιχείων του δικτύου μπορεί να είναι ο καλύτερος τρόπος για την προστασία από τις επιθέσεις.[27]

- Η ανθεκτικότητα των συσκευών είναι σημαντική όταν τοποθετούνται σε περιβάλλοντα για μεγάλες χρονικές περιόδους. Πρέπει να είναι ανθεκτικά όσον αφορά την ασφάλεια, την τροφοδοσία με ενέργεια, το λογισμικό (ενημέρωση) και το υλικό, αλλά και να παραμένουν δια-λειτουργικά με τις συσκευές IoT του μέλλοντος. Οι συσκευές πρέπει να είναι «ασφαλείς από προεπιλογή».
- Η κοινωνία πρέπει να επανεξετάσει τη νομοθεσία και τις κανονιστικές ρυθμίσεις σε μια δικτυωμένη κοινωνία για να λάβει υπόψη τα δεδομένα που παράγονται από συσκευές IoT

[27] https://royalsociety.org/~/media/events/2017/10/tof-iot/iot-conference%20report-final.pdf The Internet of Things: opportunities and threats, (πρόσβαση 15.10.2018).

και τη δύναμη που δίνει σε όσους την κατέχουν. Περισσότερη διαφάνεια για το ποιος συλλέγει τα δεδομένα και για το τι χρησιμοποιείται για αυτούς πρέπει να παρέχεται στους χρήστες συσκευών.

- Οι ιδιοκτήτες συσκευών IoT, τα δίκτυα στα οποία φιλοξενούνται και τα δεδομένα που παράγουν πρέπει να λογοδοτούν όταν προκύψουν προβλήματα.
- Οι χρήστες συσκευών πρέπει να κατανοούν την επιλογή που κάνουν όταν συναινούν στην παροχή των δεδομένων τους στους παρόχους υπηρεσιών. Η συναίνεση στο πλαίσιο αυτό θα πρέπει να επανεξεταστεί, και την ευαισθητοποίηση σχετικά με τα θέματα κλειδιών που προωθούνται.
- Η βιομηχανία είναι πιθανό να οδηγήσει τα πρότυπα στο Διαδίκτυο πιο γρήγορα από ότι μπορεί να νομοθετεί η κυβέρνηση. Ο δημόσιος τομέας μπορεί να οδηγήσει τη δημιουργία και την υιοθέτηση προτύπων μέσω πολιτικών.

Η κύρια απειλή από την χρήση και εξάπλωση του διαδικτύου των πραγμάτων θα την δεχθεί ο άνθρωπος, σύμφωνα με πολλούς ερευνητές. Εκτός από την προστασία των προσωπικών δεδομένων και την φυσική ασφάλεια της ανθρωπότητας από τις συσκευές, ο κίνδυνος για τους εργαζόμενους είναι ακόμη μεγαλύτερος. Πολλά εργοστάσια έχουν αντικαταστήσει τους εργαζόμενους, με ρομποτικές μηχανές, κάτι που δεν έγινε βέβαια το τελευταίο διάστημα, αλλά όλες αυτές οι μηχανές διασυνδέονται ταυτόχρονα στο διαδίκτυο και θα αρχίσουν να λειτουργούν πλήρως αυτόνομα, από το να παραγγέλνουν τα υλικά που χρειάζονται, μέχρι και να αυτό-επισκευάζονται, χρησιμοποιώντας τις βιβλιοθήκες δεδομένων και πληροφοριών που θα είναι διαθέσιμες. Η σύνδεση επίσης όλων των καινοτόμων τεχνολογιών και ειδικά της τεχνητής νοημοσύνης με το διαδίκτυο των πραγμάτων, ήδη δίνει εκπληκτικά, αλλά και ταυτόχρονα τρομακτικά αποτελέσματα.

6.6 Απαιτήσεις ασφάλειας και διαχείριση κινδύνων των RFID

Η τεχνολογία RFID έχει αποδειχθεί αξιόπιστη και παρουσιάζει τεράστια οφέλη. Ωστόσο, καθίσταται αναγκαία η προστασία της ιδιωτικής ζωής, της ταυτότητας και της μη διάχυσης των δεδομένων και οι επιχειρήσεις και οι οργανισμοί που την χρησιμοποιούν πρέπει να διασφαλίζουν ότι η τεχνολογία RFID που υιοθετούν υποστηρίζει τις απαιτήσεις ασφαλείας τους. Οι εταιρείες

πρέπει να έχουν επίγνωση των κινδύνων ασφαλείας, όπως η δημιουργία προφίλ, η παρακολούθηση, οι επιθέσεις άρνησης εξυπηρέτησης και η διακοπή λειτουργίας.

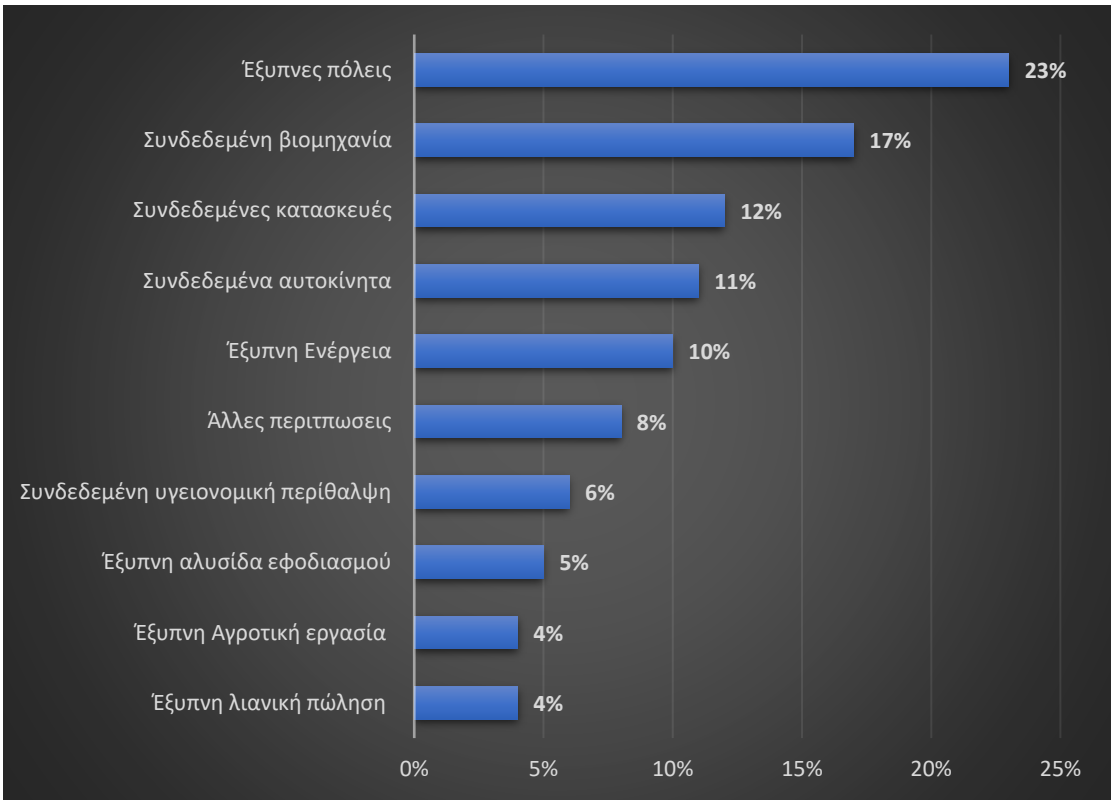
Η πιθανότητα μια επιχείρηση να χάσει τον έλεγχο της ιδιωτικότητας των πληροφοριών της είναι ένας από τους μεγαλύτερους κινδύνους που συνδέονται με την RFID. Για παράδειγμα, υπάρχει το δυναμικό για την ετικέτα μιας τρέχουσας γραμμής παραγωγής από το χώρο στάθμευσης. Όπως τα δίκτυα Ethernet, οι επικοινωνίες ασύρματων ετικετών υπόκεινται σε καταγραφή και ανάλυση. Παρόλο ότι η χρησιμοποίηση ολοένα και ισχυρότερων αλγορίθμων ασφάλειας δεδομένων, τα περιστατικά επιτυχών επιθέσεων χρησιμοποιώντας φορητούς ή δικτυωμένους υπολογιστικούς πόρους είναι ορατοί. Οι κρυπτογραφικές δυνατότητες των ετικετών καθίστανται το πιο σημαντικό στοιχείο στην επιλογή τους. (Finkenzeller & Müller, 2010).

Οι πληροφορίες μέσα στην RFID είναι ευάλωτες σε αλλοίωση, διαφθορά και διαγραφή. Το πρώτο ερώτημα που πρέπει να απαντηθεί είναι το πόσο ευάλωτα είναι τα δεδομένα των ετικετών. Η ασφάλεια της ετικέτας μπορεί να εκφραστεί με βάση την ισχύ της κρυπτογραφίας που χρησιμοποιείται, την ταχύτητα επεξεργασίας της ετικέτας και το χρονικό διάστημα που χρειάζεται για να δημιουργηθεί ένας ασφαλής δίαυλος επικοινωνίας με αυτήν την ετικέτα . Υποβαθμίζοντας πολλές φορές τις τεχνικές ασφαλείας που χρησιμοποιούνται σε μια προσπάθεια να μειωθεί η πολυπλοκότητα της ετικέτας και το κόστος των ετικετών, ο μέσος χρόνος για να «σπάσει» η ασφάλεια μετριέται σε λίγα λεπτά. (Liu et al, 2017).

Ισχυρές κρυπτογραφικές τεχνικές χρησιμοποιούνται συνήθως για να διασφαλιστεί η ιδιωτικότητα των δεδομένων, η απόδειξη της πρωτοτυπίας και η μη αντανακλαστικότητα των πληροφοριών που μεταφέρονται. Εκτός από το υπολογιστικό φορτίο, δεν είναι πιο δύσκολο να εντοπιστούν οι κρυπτογραφημένες πληροφορίες και να αποκτηθεί κάποιος βαθμός ασφαλείας μέσα στα όρια ενός εργοστασίου ή περιβάλλοντος αποθήκης. Αλλά αυτό το σενάριο γίνεται πιο περίπλοκο όταν το στοιχείο που έχει επισημανθεί πρέπει να μεταφερθεί από το ένα μέρος στο άλλο. Στην περίπτωση αυτή, κάθε συμβαλλόμενο μέρος πρέπει να συμφωνήσει σχετικά με τη μορφή των πληροφοριών και τις τεχνικές κρυπτογράφησης που χρησιμοποιούνται. Στην ισορροπία μεταξύ ασφάλειας, δια-λειτουργικότητας, την ευκολία και το κόστος, η ασφάλεια συχνά διακυβεύεται για περιορισμό του κόστους.

ΚΕΦΑΛΑΙΟ 7: Εφαρμογές του IoT στις ανθρώπινες δραστηριότητες

Το IoT χρησιμοποιείται πλέον όλο και περισσότερο προκειμένου να δώσει λύσεις σε διάφορους τομείς της καθημερινότητας. Σύμφωνα με στατιστικά στοιχεία τα πρωτεία στην χρήση του IoT έχουν οι έξυπνες πόλεις, οι λύσεις δηλαδή που εφαρμόστηκαν σε πολλές πόλεις του κόσμου, προκειμένου να επιλύσουν μεγάλα προβλήματα της καθημερινής διαβίωσης των ανθρώπων.[28]

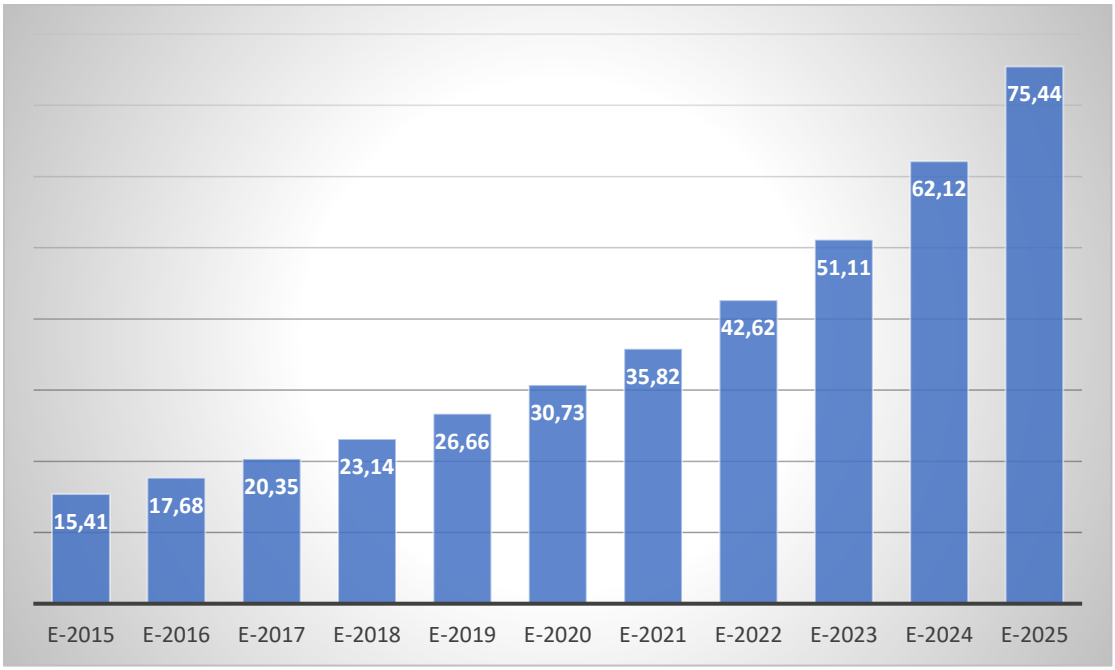


Διάγραμμα 5. Κατανομή των έργων του διαδικτύου των πραγμάτων (IoT) σε όλο τον κόσμο από τον Ιανουάριο του 2018, κατά τομέα

Το 23% των παγκόσμιων έργων IoT συνδέονται με τις έξυπνες πόλεις. Αυτά τα στατιστικά στοιχεία είναι ενδεικτικά, καθώς οι περισσότεροι τομείς που φαίνονται στο παραπάνω διάγραμμα είναι αλληλένδετοι. Για παράδειγμα τα έργα IoT για την ενέργεια εξυπηρετούν και τις έξυπνες πόλεις και την βιομηχανία, ή οι κατασκευές εξυπηρετούν και τις έξυπνες πόλεις αλλά και τον

[28] https://www.statista.com/statistics/869335/world-internet-of-things-projects-by-segment-enterprise/

τομέα της ενέργειας, όπου με την χρήση έξυπνων λύσεων στην κατασκευή των κτιρίων και ειδικά στον τομέα της ενέργειας, μειώνουν την ποσότητα ενέργειας που χρειάζονται τα κτίρια, (θέρμανση – ψύξη) συμμετέχοντας με αυτό τον τρόπο και στην προστασία του περιβάλλοντος, αλλά και στην εξοικονόμηση δημόσιων πόρων για την παραγωγή ενέργειας. [29]



Διάγραμμα 6. Οι συνδεδεμένες συσκευές Διαδικτύου των πραγμάτων (IoT) που εγκαθίστανται σε παγκόσμιο επίπεδο από το 2015 έως το 2025 (σε δισεκατομμύρια)
(2018 – 2025 – εκτίμηση)

Αυτά τα στατιστικά στοιχεία δείχνουν τον αριθμό των συνδεδεμένων συσκευών (Internet of Things, IoT) παγκοσμίως από το 2015 έως το 2025. Για το 2020, η εγκατεστημένη βάση των συσκευών Internet of Things προβλέπεται να αυξηθεί σε σχεδόν 31 δισεκατομμύρια σε όλο τον κόσμο, εκτίμηση που συνεχώς όμως αναθεωρείται.[30]

7.1 Έξυπνες πόλεις και διαδίκτυο των πραγμάτων

Μια «Έξυπνη Πόλη» είναι μια αστική περιοχή η οποία είναι ιδιαίτερα προηγμένη από άποψης της υποδομής, των επικοινωνιών, της βιωσιμότητας των κατοίκων της αλλά και της βιωσιμότητας της αγοράς. Η τεχνολογία πληροφοριών και επικοινωνιών είναι η κύρια υποδομή και επίσης η βάση για την παροχή βασικών υπηρεσιών ως προς τους κατοίκους της. Σε μία

[29] https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide
[30] https://eu-smartcities.eu/

έξυπνη πόλη χρησιμοποιούνται διαφορετικοί τύποι ηλεκτρονικών αισθητήρων συλλογής δεδομένων για την παροχή πληροφοριών .Υπάρχουν πολλές τεχνολογικές πλατφόρμες όπου εμπλέκονται και οι οποίες δεν περιορίζονται μόνο σε αυτοματοποιημένα δίκτυα αισθητήρων και κέντρα δεδομένων. Η έννοια της έξυπνης πόλης ενσωματώνει την τεχνολογία πληροφοριών και επικοινωνιών (ΤΠΕ) και τις διάφορες συσκευές που συνδέονται στο Διαδίκτυο των πραγμάτων για τη βελτιστοποίηση της αποτελεσματικότητας των λειτουργιών και των υπηρεσιών της πόλης .

7.2 Χαρακτηριστικά Έξυπνων Πόλεων

Μερικά παραδείγματα εφαρμογών για έξυπνες πόλεις είναι το έξυπνο Parking, η πολεοδομική «υγεία», χάρτες αστικού θορύβου, ανίχνευση μέσω smartphones, κυκλοφοριακή αποσυμφόρηση, έξυπνος φωτισμός, έξυπνοι δρόμοι και σύστημα διαχείρισης αποβλήτων.

Έξυπνα Κτίρια (Smart Building):

Υπάρχουν αλγόριθμοι οι οποίοι δίνουν στους διαχειριστές μία πιο ολοκληρωμένη εικόνα για τα Έξυπνα Κτίρια, αλλά και για τον έλεγχο των κτιρίων . Για να γίνει αυτό θα πρέπει οι διαχειριστές ενός τέτοιου κτιρίου – συστήματος να συλλέξουν προηγμένα δεδομένα που σχετίζονται με την ενέργεια, την ασφάλεια, την χωρητικότητα, το νερό και την θερμοκρασία του κτιρίου – συστήματος. Συνεπώς οι αλγόριθμοι αυτοί, επιτρέπουν στους διαχειριστές να μειώσουν το κόστος και ταυτόχρονα να βελτιστοποιήσουν το σύστημα.

Έξυπνη Μεταφορά (Smart Transportation):

Βάση των δεδομένων που συλλέγει ένα Έξυπνο Σύστημα Μεταφοράς (παραδείγματος χάριν λεωφορείο), σε σχέση με την κυκλοφοριακή συμφόρηση και του οδικού δικτύου σε πραγματικό χρόνο, έχουν σαν αποτέλεσμα την μείωση των εκπομπών του άνθρακα (CO_2) μέσω της καλύτερης διαχείρισης της κυκλοφορίας, τον εντοπισμό για διαθέσιμο χώρο στάθμευσης και επιπλέον την φόρτιση ηλεκτρικών οχημάτων.

Έξυπνες Υποδομές (Smart Infrastructure):

Μέσα από τις Έξυπνες Υποδομές, υπάρχει μείωση των κινδύνων, και μείωση του κόστους το οποίο έχει άμεση σχέση με το νερό και τον φωτισμό μιας Έξυπνης Πόλης. Οι Έξυπνες Πόλεις

“φροντίζουν” για την καλύτερη συντήρηση, την διαχείριση και την αποτελεσματικότητα της Έξυπνης Υποδομής της πόλης.

Έξυπνη Ενέργεια (Smart Energy):

Οι οικονομικά αποδοτικές λύσεις για εφαρμογές Έξυπνων Ενεργειακών, καθιστούν ευκολότερη την παρακολούθηση και την διαχείριση ενέργειας σε πραγματικό χρόνο, με ευφυείς μετρητές για το έξυπνο δίκτυο μιας πόλης, βοηθώντας τις έτσι στην μείωση των εκπομπών, και στην εξοικονόμηση χρημάτων.

7.3 Παραδείγματα Έξυπνων Πόλεων στην Ευρώπη

Σύμφωνα με τις σύγχρονες προσεγγίσεις μια έξυπνη πόλη, δε στηρίζεται μόνο από την ανάπτυξη Τ.Π.Ε αλλά σε περισσότερα στοιχεία, όπως τη δυνατότητα για συμμετοχή και πρόσβαση σ’ ένα ευρύτερο πλαίσιο κοινωνικής οικονομικής και πολιτιστικής ανάπτυξης.

Κατά την εξέταση των στοιχείων των έξυπνων πόλεων σε όλο τον κόσμο, χωρίστηκαν σε τρεις κατηγορίες:

1. Πρωτοπόρες έξυπνες πόλεις ,δηλαδή πόλεις που βρίσκονται στην αιχμή της ανάπτυξης της ιδέας ‘Smart City’ και παρουσιάζουν όλη την απαραίτητη υποδομή.

2. Αναδυόμενες έξυπνες πόλεις, δηλαδή πόλεις που είναι στα πρόθυρα της αληθινής καινοτομίας και έχουν τις προδιαγραφές εκείνες που βοηθούν στην υιοθέτηση έξυπνων λύσεων)

3. Έξυπνες πόλεις της επόμενης φάσης , δηλαδή πόλεις που με αρκετή προσπάθεια θα μπορέσουν σύντομα να είναι στην αιχμή της καινοτομίας.

Χαρακτηριστικά 4 έξυπνες πόλεις παρουσιάζονται κάτωθι:

Βαρκελώνη

Η Βαρκελώνη, θεωρείται μία από τις πλέον πρωτοπόρες πόλεις στον κόσμο όσον αφορά την υιοθέτηση έξυπνων τεχνολογιών και του Internet of Things. Η Ευρωπαϊκή Ένωση ανέφερε τη Βαρκελώνη ως την πιο καινοτόμο πόλη της Ευρώπης για το 2018.[31]

Data available to citizens on demand (Δεδομένα διαθέσιμα στους πολίτες κατόπιν αιτήματος)

[31] https://ec.europa.eu/info/news/smart-city-matchmaking-barcelona-2018-nov-12_en

Η προσέγγιση για την έξυπνη πόλη της Βαρκελώνης ήταν η ιδέα ότι η πόλη θα λειτουργεί ως ένα δίκτυο δικτύων. Με αυτόν τον τρόπο, θα μπορούν να συνδεθούν διαφορετικά μεμονωμένα δίκτυα στην πόλη. Αυτό οδήγησε τη Βαρκελώνη σε δύο κατευθύνσεις. Η πρώτη απαιτούσε την ανάπτυξη μιας νέας υποδομής δεδομένων που αποτελείται από τρία στοιχεία: Την Sentilo, μια πλατφόρμα συλλογής ανοιχτού κώδικα και αισθητήρων, το CityOS, μια άλλη πλατφόρμα ανοιχτού κώδικα που αναλύει δεδομένα καθώς και ένα επίπεδο διεπαφής χρήστη των εφαρμογών υπηρεσίας για την ευκολότερη πρόσβαση στα δεδομένα.

Η δεύτερη κατεύθυνση ήταν το πώς θα χρησιμοποιηθεί αυτός ο ολοκληρωμένος έλεγχος . Για παράδειγμα η νέα πλατφόρμα και όλα τα δεδομένα για αυτήν θα ανήκουν στην πόλη, για παράδειγμα. Θα είναι στη διάθεση των πολιτών, των ιδιωτικών εταιρειών και άλλων ενδιαφερομένων, αλλά η πόλη και οι πολίτες της θα διατηρήσουν την απόλυτη ιδιοκτησία τους και θα αποφασίσουν ποια θα ήταν η κατάλληλη πρόσβαση, διασφαλίζοντας την προστασία της ιδιωτικής τους ζωής κλπ.[32]

Οι αισθητήρες που υπάρχουν στην Βαρκελώνη μετρούν:

- Ηλεκτρισμό
- Καιρό
- Εξωτερικές συνθήκες περιβάλλοντος
- Θέσεις στάθμευσης
- Συλλογή απορριμμάτων
- Ποιότητα αέρα
- Θόρυβο
- Ροή ανθρώπων
- Κίνηση στους Δρόμους

Smart Parking

Η Βαρκελώνη έχει εφαρμόσει ένα σύστημα αισθητήρων για τους οδηγούς που τους καθοδηγούν σε ελεύθερα σημεία στάθμευσης. Ενσωματωμένα κάτω από την άσφαλτο, οι αισθητήρες μπορούν να εντοπίσουν τους διαθέσιμους χώρους στάθμευσης και να ειδοποιήσουν τους οδηγούς. Το πρόγραμμα έχει μειώσει τις εκπομπές ρύπων και την κυκλοφοριακή συμφόρηση

[32] http://www.urban-hub.com/cities/smart-city-3-0-ask-barcelona-about-the-next-generation-of-smart-cities/

κατευθύνοντας τους οδηγούς σε κενές θέσεις στάθμευσης. Μέσα σε ένα έτος εφαρμογής, η πόλη χορήγησε 4.000 άδειες για στάθμευση ανά ημέρα.

Smart Lighting

Το σύστημα φωτισμού που βασίζεται σε LED μαζί με ένα δίκτυο αισθητήρων, έχουν αντικαταστήσει τα φώτα του δρόμου σε όλη τη Βαρκελώνη. Αυτό το σύστημα φωτισμού είναι πιο αποδοτικό ενεργειακά και μειώνει τη θερμότητα που παράγεται από τους παλαιούς λαμπτήρες, οδηγώντας έτσι σε εξοικονόμηση του κόστους για την πόλη. Το σύστημα φωτισμού λαμβάνει πληροφορίες σχετικά με το περιβάλλον (ρύπανση, υγρασία, θερμοκρασία, παρουσία ανθρώπων και θόρυβος) με τη βοήθεια αισθητήρων. Μια κεντρική μονάδα στο δρόμο επιτρέπει την επικοινωνία με τα φώτα και η μονάδα διαχειρίζεται επίσης διάφορες άλλες υπηρεσίες, όπως ηλεκτρικούς σταθμούς φόρτισης, Wi-Fi και καλωδιώσεις οπτικών ινών. Οι αισθητήρες μπορούν να προσαρμόσουν το φωτισμό με βάση την παρουσία ανθρώπων και τον χρόνο καθυστέρησης. [33]

Smart Bus Stops

Οθόνες αφής που τροφοδοτούνται με ηλιακή ενέργεια δείχνουν τους χρόνους άφιξης και τις διαθέσιμες θέσεις του επόμενου λεωφορείου. Επιπλέον προσφέρουν τουριστικές πληροφορίες και δωρεάν Wi-Fi. Τα λεωφορεία διαθέτουν GPS, αισθητήρες θέσεων, και στέλνουν πληροφορίες στη στάση του λεωφορείου.[34]

Άμστερνταμ

Στο Άμστερνταμ εφαρμόζονται διάφορες καινοτόμες τεχνολογίες όπως το Smart mobility ,ενώ παράλληλα χρησιμοποιούνται αισθητήρες οι οποίοι καταγράφουν τα ποσοστά διοξειδίου του άνθρακα στην ατμόσφαιρα και τα ποσοστά κατανάλωσης ενέργειας τόσο στους δρόμους όσο και στα καταστήματα και εστιατόρια. Παράλληλα έχουν τοποθετηθεί ‘έξυπνοι’ μετρητές που χαμηλώνουν ή σβήνουν τα φώτα όταν αυτά δεν χρησιμοποιούνται όπως και μετρητές που μετρούν την κατανάλωση ενέργειας σε συσκευές οι οποίες αν χρειαστεί θα αντικαθίστανται με συσκευές χαμηλής κατανάλωσης. Όσον αφορά το θέμα της μόλυνσης του αέρα, οι αρχές της πόλης αποφάσισαν να εγκαταστήσουν αρχικά, μερικά ‘TreeWiFi’ τα οποία θα λειτουργούν σαν

[33] http://www.barcinno.com/barcelona-smart-city-technologies/
[34] https://www.hackerearth.com/blog/internet-of-things/barcelona-smart-city/

αισθητήρες και θα είναι τοποθετημένα σε δέντρα. Όταν η ποιότητα του αέρα βελτιώνεται, οι περαστικοί θα έχουν δωρεάν σύνδεση στο διαδίκτυο. Για να γίνει όμως αυτό, απαιτείται και η συμβολή των πολιτών οι οποίοι συστήνεται να αποφεύγουν όσο γίνεται την χρήση αυτοκινήτων και να μετακινούνται με ποδήλατα ή δημόσια μέσα συγκοινωνίας.

Smart mobility

Έξυπνη διαχείριση της κυκλοφορίας προτείνοντας εναλλακτικά δρομολόγια στους πολίτες, καθώς και παρακολούθηση αυτών σε πραγματικό χρόνο ώστε να μειώνεται η κυκλοφοριακή συμφόρηση και να διευκολύνεται η κίνηση των πολιτών, μειώνοντας έτσι την αστική ρύπανση. Παράλληλα ,μέσω της πλατφόρμας Mobypark, σε συνεργασία με το Amsterdam Smart City, παρέχονται θέσεις στάθμευσης, οι οποίες μπορούν να ενοικιαστούν είτε βραχυπρόθεσμα ή μακροπρόθεσμα μετά από κράτηση (Parking in Amsterdam - Mobypark, 2016). Οι διαθέσιμες επιλογές της πλατφόρμας είναι ενημερωμένες με ιδιωτικούς χώρους στάθμευσης, δημόσιους χώρους, ξενοδοχεία, νοσοκομεία κλπ. .[35]Ενώ με το Digital Road Authority, οι κάτοικοι λαμβάνουν συμβουλές μέσω μιας εφαρμογής στο κινητό τους, τον προορισμό τους και την τρέχουσα κατάσταση στους φωτεινούς σηματοδότες. Έτσι, ανάλογα με τη προσέλευση των πολιτών και την πυκνότητα στα φανάρια, η Digital Road Authority μπορεί να ρυθμίσει κάθε φορά τον χρόνο διέλευσης των οχημάτων με τους αντίστοιχους σηματοδότες.

Smart Lighting

Το Άμστερνταμ χρησιμοποιεί για τον έλεγχο του δημόσιου φωτισμού το «Flexible Street Lighting». Μέσω της συγκεκριμένης πλατφόρμας οι δήμοι και οι επαρχίες μπορούν να ελέγχουν τους διακόπτες και τις συσκευές ρύθμισης έντασης φωτισμού (dimming) για τον φωτισμό των δημόσιων χώρων. Μέσω των «έξυπνων φώτων» και του απομακρυσμένου χειρισμού ή αισθητήρων, ο φωτισμός μπορεί να ρυθμιστεί ή να προσαρμοστεί ανάλογα με τις καιρικές συνθήκες, συμβάλλοντας με αυτό τον τρόπο στη βελτίωση της ασφάλειας και την εξοικονόμηση ενέργειας. Η ενέργεια που εξοικονομείται μπορεί να χρησιμοποιηθεί για άλλες λειτουργίες, όπως την τροφοδοσία του δικτύου Wi-Fi ή τη μέτρηση της ποιότητας του αέρα.[36]

[35] https://www.mobypark.com/en/parking-amsterdam
[36] https://amsterdamsmartcity.com/projects/flexible-street-lighting

IoT Living Lab

Το iBeacon Living Lab, είναι μία πρωτοβουλία μέσω της οποίας τα αντικείμενα αποκτούν προσωπικότητα . Η εγκατάσταση beacons, επιτρέπει την σύνδεση ενός smartphone με μία άλλη συσκευή χωρίς σύνδεση στο διαδίκτυο. Μέσω των beacons που χρησιμοποιούνται οι χρήστες ενημερώνονται, για παράδειγμα, αν βρίσκονται κοντά σε ένα προϊόν που τους αρέσει, αν περνούν μπροστά από ένα εστιατόριο, ένα μουσείο, δίνοντας σημαντικές πληροφορίες για το εκάστοτε μέρος. Επίσης, δίνουν τη δυνατότητα στις τουριστικές πινακίδες να μεταφράζονται στην εκάστοτε γλώσσα των τουριστών.[37]

Urban data and data platforms

Αστικές πλατφόρμες δεδομένων, δίνοντας τη δυνατότητα στους πολίτες έναν έλεγχο των υπηρεσιών της πόλης , με την ενσωμάτωση πολλών συστημάτων.

Κοπεγχάγη

Το 2017 η πρωτεύουσα της Δανίας ψηφίστηκε ως η πιο έξυπνη πόλη του κόσμου, αναφερομένη πάντα στην ψηφιακή εξέλιξη και στην παροχή έξυπνων λύσεων για τους πολίτες της. Και αυτό γιατί οι πολίτες είχαν την καλύτερη διαθεσιμότητα σε 4G, hotspot Wi-Fi, αισθητήρες κυκλοφορίας και σε διασυνδεδεμένες ψηφιακές πλατφόρμες. Η Κοπεγχάγη χαρακτηρίστηκε η πλέον «smart city», ιδίως λόγω του Smart Parking, του Smart Building , των ισχυρών επιχειρηματικών οικοσυστημάτων και της διείσδυσης των smartphones. Οι IoT εφαρμογές που χρησιμοποιούνται στην Κοπεγχάγη και την χαρακτηρίζουν Έξυπνη πόλη είναι οι παρακάτω:

- Smart City infrastructure
- Smart Environment
- Smart Mobility
- Smart waste
- Plant sensing
- City WiFi-Tracking

Smart Environment

Μέσω του συστήματος Smart Water Defense αξιοποιούνται γίνεται ενημέρωση των πολιτών , σε όλη την πόλη έτσι ώστε να αποφεύγονται κίνδυνοι αποκλεισμών όταν θα υπάρχουν πλημμύρες

[37] http://iotlivinglab.com/

ενώ μέσω του συστήματος Smart Waste αποστέλλονται ειδοποιήσεις προς τα φορτηγά της καθαριότητας ώστε να βελτιστοποιούν τις διαδρομές τους και να μην χάνουν πολύτιμο χρόνο, καύσιμα και ενέργεια για τους κενούς κάδους .

Smart Mobility

Τα έξυπνα συστήματα Smart Traffic Systems αντλούν πληροφορίες σε πραγματικό χρόνο και ρυθμίζουν την κυκλοφορία, τη σηματοδότηση και τη σήμανση ανάλογα με τις τρέχουσες ανάγκες της κυκλοφορίας. Επιπρόσθετα με το σύστημα Smart Parking δύναται η δυνατότητα κράτησης μιας θέσης στάθμευσης. Ενώ με την ανοικτή πύλης δεδομένων (Open Data) είναι διαθέσιμα πάνω από 100 βάσεις δεδομένων, όπως χάρτες, θέσεις στάθμευσης, και προσομοιώσεις της ροής κυκλοφορίας. Επίσης, ένα μεγάλο ποσό των μελλοντικών δεδομένων είναι η έκδοση αποτελεσμάτων από τις στατιστικές ενέργειας της πόλης καθώς και δημογραφικά δεδομένα .Άλλη μια δυναμική καινοτομία, είναι η πλατφόρμα Copenhagen Connecting με κοινή χρήση ιδιωτικών και δημόσιων δεδομένων (City Data Exchange) , με σκοπό τη χρήση των δεδομένων για την επίλυση προβλημάτων και τη διαμόρφωση νέων τρόπων συμμετοχής των πολιτών προτείνοντας ιδέες και λύσεις, ώστε να καλυφθούν οι ανάγκες τους. Ωστόσο ένα πιθανά αρνητικό στοιχείο της συγκεκριμένης πλατφόρμας αφορά τους κινδύνους παραβίασης της ιδιωτικής ζωής, καθώς προσωπικά δεδομένα θα βρίσκονται διαθέσιμα σε ιδιωτικές επιχειρήσεις που έχουν εταιρική σχέση με το Copenhagen Connecting.[38]

City WiFi-Tracking

Για την σύνδεση των πολιτών στο internet , η Κοπεγχάγη διαθέτει σχεδόν σε ολόκληρη την πόλη free WiFi, ενώ οι περισσότεροι χρησιμοποιούν το ελεύθερο δίκτυο για εφαρμογές GPS .

[38] http://www.copcap.com/newslist/2014/copenhagen-is-the-worlds-smartest-city

			TRANSPORT AND MOBILITY				SUSTAINABILITY				GOVERNANCE				INNOVATION ECONOMY	DIGITALIZATION				LIVING STANDARD	EXPERT PERCEPTION	
#	CITY	COUNTRY																				RANK/ SCORE
1	Copenhagen	Denmark	9.81	8.62	8.18	6.82	7.92	9.83	8.24	6.11	9.38	8.53	7.09	5.85	9.13	8.63	7.66	4.12	9.74	8.70	9.12	8.24
2	Singapore	Singapore	7.30	6.63	4.20	10.00	2.26	8.44	7.62	7.15	10.00	5.47	7.82	5.12	8.62	8.71	7.75	6.63	7.55	8.18	9.30	7.83
3	Stockholm	Sweden	7.49	5.93	6.71	6.54	8.44	6.88	8.94	8.79	9.29	10.00	7.62	7.66	9.57	8.37	9.22	6.28	8.69	7.32	8.20	7.82
4	Zurich	Switzerland	7.80	7.75	4.98	9.83	8.62	10.00	10.00	8.70	2.07	8.10	9.03	9.02	9.74	4.69	4.38	5.59	7.55	10.00	9.00	7.75
5	Boston	United States	8.01	8.70	7.71	7.21	3.60	5.15	4.26	6.56	5.30	6.97	5.12	10.00	10.00	6.06	9.39	6.80	9.17	8.22	9.30	7.70
6	Tokyo	Japan	9.57	7.13	7.66	8.79	3.86	8.36	8.24	4.25	6.60	6.28	3.59	7.71	7.19	6.37	6.50	9.57	8.61	7.21	8.60	7.59
7	San Francisco	United States	9.05	9.05	5.08	3.43	3.60	5.15	4.26	6.38	6.23	6.59	5.44	5.67	9.91	7.91	10.00	9.05	9.17	9.01	9.10	7.55
8	Amsterdam	Netherlands	7.95	7.06	8.36	7.06	2.47	7.32	7.79	3.86	9.02	9.83	5.94	7.84	8.82	8.40	6.63	5.33	6.85	9.01	8.20	7.54
9	Geneva	Switzerland	8.06	4.98	6.11	6.97	8.62	10.00	10.00	9.13	1.80	8.36	8.59	9.14	8.96	8.11	8.79	3.94	7.55	9.80	8.10	7.53
10	Melbourne	Australia	7.97	7.14	4.55	8.72	2.90	6.29	5.15	2.90	9.82	5.38	9.24	9.31	6.02	10.00	7.84	6.72	9.30	8.01	7.30	7.51

Διάγραμμα 7. Οι 10 κορυφαίες έξυπνες πόλεις στον κόσμο για το 2017[39]

Τρίκαλα

Χαρακτηριστικό παράδειγμα έξυπνης πόλης στην Ελλάδα ,είναι η πόλη των Τρικάλων . Τα Τρίκαλα είναι η πρώτη ελληνική πόλη που εφαρμόζει επιτυχημένα την τεχνολογία IoT. Συγκεκριμένα χρησιμοποιούνται εφαρμογές όπως:

Σύστημα Έξυπνης Διαχείρισης Στάθμευσης

Με το Σύστημα Έξυπνης Διαχείρισης Στάθμευσης ,επιτυγχάνεται η εύρεση, η απεικόνιση και ο έλεγχος οριοθετημένων θέσεων στάθμευσης στο κέντρο της πόλης. Έχει γίνει εγκατάσταση δικτύου εξειδικευμένων αισθητήρων στο οδόστρωμα συγκεκριμένων οδών της πόλης, έτσι ώστε να αντιστοιχεί ένας αισθητήρας για κάθε διακριτή, διαγραμμισμένη θέση στάθμευσης. Ο αισθητήρας τροφοδοτεί τα σημεία ελέγχου του δικτύου (controllers) στέλνοντας τα ανάλογα σήματα, όταν η θέση είναι ή δεν είναι κατειλημμένη. Επιπλέον οι πολίτες ενημερώνονται σε πραγματικό χρόνο για τη διαθεσιμότητα θέσεων στην επιλεγμένη περιοχή, τόσο μέσω της εφαρμογής στάθμευσης (mobile app) για κινητά τηλέφωνα, όσο και από πινακίδες που μπορούν

[39] https://scandasia.com/copenhagen-ranked-the-smartest-city-in-the-world-singapore-is-second/

να εγκατασταθούν σε κομβικά σημεία της πόλης. Επίσης παρέχεται και στα όργανα ελέγχου της στάθμευσης, ενημέρωση σε πραγματικό χρόνο για περιπτώσεις παράνομου παρκαρίσματος. Μέσω της εφαρμογής παρέχεται και δυνατότητα αυτόματης πληρωμής του τιμήματος στάθμευσης.

Σύστημα παρακολούθησης περιβαλλοντικών συνθηκών

Με τη χρήση ειδικών συσκευών περιβαλλοντικών μετρήσεων (όπως για συγκέντρωση αέριων ρύπων, αιωρούμενων σωματιδίων και θορύβου), μπορεί να εκτιμηθεί η ποιότητα της ατμόσφαιρας και να αξιολογηθεί πιθανός αντίκτυπος στη δημόσια υγεία. Επίσης, απεικονίζονται σε πραγματικό χρόνο τυποποιημένοι δείκτες ποιότητας του περιβάλλοντος που επιτρέπουν συγκριτική αξιολόγηση (benchmarking), επισημάνσεις (alerts) και την αναγνώριση τάσεων που θα μπορούσαν να οδηγήσουν στη λήψη μέτρων.

Έξυπνη και Διασυνδεδεμένη Ψηφιακή Πλατφόρμα

Έχει εγκατασταθεί η πλατφόρμα έξυπνης πόλης Cisco Smart+Connected Digital Platform – CDP. Πρόκειται για ένα ολοκληρωμένο πληροφοριακό σύστημα που αξιοποιεί τα πλεονεκτήματα του Internet of Things (IoT) και διαχειρίζεται τις επιμέρους εφαρμογές εποπτείας και ενημέρωσης, τροφοδοτώντας ταυτόχρονα τρίτα συστήματα, μέσα από ανοιχτά πρωτόκολλα διασύνδεσης (APIs). Η πλατφόρμα συγκεντρώνει, αποθηκεύει, κανονικοποιεί και οπτικοποιεί τα δεδομένα που παράγονται από τις παραπάνω υποδομές και εφαρμογές και τα διαθέτει προς ανάλυση σε όποιους ενδιαφέρονται να τα αξιοποιήσουν προς όφελος των πολιτών και των επιχειρήσεων της πόλης.

Σύστημα Έξυπνου Φωτισμού

Έχει υλοποιηθεί Σύστημα Έξυπνου Φωτισμού, μέσω του οποίου γίνεται διαχείριση του δημοτικού ηλεκτροφωτισμού και επιτυγχάνεται εξοικονόμηση ενέργειας μεγαλύτερη από 60% έναντι των συμβατικών φωτιστικών συστημάτων. Πιο συγκεκριμένα, αντικαταστάθηκαν τα υφιστάμενα φωτιστικά συστήματα συμβατικής τεχνολογίας, από νέα φωτιστικά συστήματα τεχνολογίας LED, σε αντιπροσωπευτικό δρόμο του ενδοαστικού οδικού δικτύου. Επίσης, εγκαταστάθηκε σύστημα ασύρματης διαχείρισης, που παρέχει τη δυνατότητα έγκαιρου εντοπισμού δυσλειτουργιών, «έξυπνου» προγραμματισμού επεμβάσεων, δυναμικής προσαρμογής του φωτισμού όπου, όσο και όταν χρειάζεται, για τη μέγιστη δυνατή ενεργειακή εξοικονόμηση και τη βελτίωση ορατότητας για οδηγούς, ποδηλάτες, πεζούς.

Κέντρο διαχείρισης της «έξυπνης πόλης»

Υλοποιήθηκε ένα κέντρο ελέγχου όλων των υπηρεσιών. Συγκεκριμένα εγκαταστάθηκαν οθόνες παρακολούθησης των παρακάτω συστημάτων:

- GIS, προβάλει τα χωρικά – χωροταξικά δεδομένα και σημεία ενδιαφέροντος του Δήμου
- Σύστημα παρακολούθησης λειτουργίας φωτεινών σηματοδοτών. Προσφέρεται online παρακολούθηση βλαβών και καμένων λαμπτήρων στους κυκλοφοριακούς κόμβους της πόλης που ελέγχονται από φανάρια.
- Σύστημα αποτύπωσης κίνησης των δημοτικών οχημάτων.
- Οθόνη παρακολούθησης λειτουργίας κόμβων ασυρμάτου δικτύου παροχής δωρεάν internet.
- Σύστημα παρακολούθησης και ρύθμισης ηλεκτροβανών δικτύου ύδρευσης
- Καταγραφή και παρακολούθηση πορείας επίλυσης αιτημάτων πολιτών.[40]

7.4 Τα προσωπικά δεδομένα διαφυλάσσονται σε μία έξυπνη πόλη;

Οι αισθητήρες των smart cities συλλέγουν δεδομένα ,ακόμη και προσωπικά , για παραχθούν πληροφορίες. Το ζήτημα λοιπόν που τίθεται είναι το κατά πόσο θίγεται η ιδιωτικότητα και τα δεδομένα που συλλέγονται διατηρούνται ασφαλή;

Σύμφωνα με τον Masa Galic , ερευνητής για την Προστασία της Ιδιωτικής Ζωής στον Δημόσιο Χώρο του Ινστιτούτου Τεχνολογίας και Κοινωνίας του Tilburg, «οι πολίτες και οι επισκέπτες μιας έξυπνης πόλης δεν συνειδητοποιούν ότι εισέρχονται σε ένα ζωντανό εργαστήριο» και αυτό γιατί μια έξυπνη πόλη συλλέγει δεδομένα συνεχώς προς επεξεργασία.[41]

Σε πολλές πόλεις δεδομένα που συλλέγονται από τους αισθητήρες χρησιμοποιούνται για τη δημιουργία προφίλ και τη στόχευση πολιτών, με αποτέλεσμα το εν λόγω «πείραμα έξυπνης πόλης» υπόκειται στη νομοθεσία περί ιδιωτικότητας. Σύμφωνα με τον Κανονισμό ΕΚ 2016/679 [42]περί προστασίας προσωπικών δεδομένων, οι πολίτες της ΕΕ πρέπει να ενημερώνονται εκ των προτέρων για τη συλλογή δεδομένων και να διευκρινίζεται ο σκοπός για τον οποίον συμβαίνει

[40] https://trikalacity.gr/smart-trikala/

[41] https://tvxs.gr/news/eyropi-eop/ollandikes-poleis-sygkentronoyn-dedomena-anypopsiaston-politon

[42] https://www.researchgate.net/publication/325347942_Will_the_GDPR_slow_down_development_of_Smart_Cities

αυτό. Δυστυχώς όμως σε πολλές άλλες «έξυπνες πόλεις» δεν γίνεται κάτι τέτοιο. Και όχι δεν ενημερώνονται ,αλλά δεν γνωρίζουν ούτε ποιος συλλέγει τα δεδομένα τους, πώς επεξεργάζονται και πώς χρησιμοποιούνται .

Ειδικότερα στις έξυπνες πόλεις συλλέγονται προσωπικά δεδομένα που χρησιμοποιούνται για στατιστικούς λόγους (δημογραφικά δεδομένα όπως γεννήσεις ,θάνατοι ,γάμοι, δεδομένα δημοσκοπήσεων , εργασιακά δεδομένα), διαφημιστικούς λόγους ,παρακολούθηση των προτιμήσεων των πολιτών, για λόγους επιτήρησης (δεδομένα καμερών CCTV) κτλ.[43]

Στις πόλεις που έγινε αναφορά οι αρχές χρησιμοποιούν την «έξυπνη τεχνολογία» από τη ρύθμιση της κυκλοφορίας μέχρι την εγκληματικότητα. Πώς προστατεύονται λοιπόν η ιδιωτικότητα των πολιτών των έξυπνων πόλεων και πώς οι ίδιοι δίνουν την συγκατάθεση τους για συλλογή και επεξεργασία των δεδομένων τους;

Συγκεκριμένα στη Βαρκελώνη διατίθεται μια νέα ατζέντα ψηφιακού μετασχηματισμού, η οποία λαμβάνει τα δεδομένα ως «κοινά» μαζί με οδηγίες που επιβάλλουν την σωστή και νόμιμη χρήση των δεδομένων. Η πόλη ξεκίνησε μια νέα διαδικασία προμηθειών που αποσκοπούσε στην παροχή κινήτρων για υπεύθυνη καινοτομία και σεβασμό της ιδιωτικής ζωής και επί του παρόντος υπόκειται σε πλήρη εσωτερική αντικατάσταση της χρήσης λογισμικού ανοιχτού κώδικα μέχρι την άνοιξη του 2019. Επιπλέον για πρώτη φορά εντός του η κυβέρνηση θα δοκιμάσει σε πιλοτικό στάδιο νέα online εργαλεία που επιτρέπουν στους ανθρώπους να αποκαλύπτουν επιλεκτικά τις πληροφορίες που θα ήθελαν να μοιραστούν όταν χρησιμοποιούν την επίσημη ψηφιακή πλατφόρμα του δήμου «Decidim», διατηρώντας παράλληλα την ανωνυμία των πολιτών.[44] Αυτό θα επιτυγχάνεται με την κρυπτογράφηση των δεδομένων και την ελαχιστοποίηση συλλογής ευαίσθητων δεδομένων. Τέλος θα ζητείται πρώτα η συγκατάθεση του χρήστη για οποιαδήποτε συλλογή ή επεξεργασία δεδομένων.

Παράλληλα στο Άμστερνταμ οι IoT εφαρμογές προωθούν την υπεύθυνη χρήση δεδομένων σε ολόκληρη την πόλη. Το TADA manifesto, το οποίο αναπτύχθηκε από το ανεξάρτητο Οικονομικό Συμβούλιο του Άμστερνταμ και εγκρίθηκε από την κυβέρνηση της πόλης, περιγράφει ένα σύνολο έξι αρχών που αποσκοπούν να βοηθήσουν τους οργανισμούς να χρησιμοποιούν

[43] https://www.researchgate.net/publication/261636975_A_Framework_for_Privacy_Protection_and_Usage_Control_of_Personal_Data_in_a_Smart_City_Scenario

[44] https://www.decidim.barcelona/

προσωπικά δεδομένα με πιο υπεύθυνο τρόπο. Η Ομάδα Καινοτομίας του Άμστερνταμ καταρτίζει επίσης ένα μητρώο όλων των εγκατεστημένων σε όλη την Κοινότητα αισθητήρων σε όλη την πόλη καθώς και πιλότους που θα επιτρέψουν στους χρήστες να έχουν πρόσβαση σε τοπικές υπηρεσίες ηλεκτρονικής διακυβέρνησης με ανώνυμο τρόπο, ελαχιστοποιώντας ταυτόχρονα την άσκοπη συλλογή προσωπικών δεδομένων.

Συγκριτικά, η Κοπεγχάγη ,είναι η πλέον «οικολογική έξυπνη πόλη» της Ευρώπης καθώς οι περισσότερες εφαρμογές IoT αφορούν το Περιβάλλον. Επίσης θα μπορούσε να χαρακτηριστεί και ως η πιο «πληροφορούμενη» καθώς οι πολίτες μέσω της ανοικτής πύλης δεδομένων ,έχουν διάχυτη πρόσβαση σε πληροφορίες. Η Κοπεγχάγη έχει δώσει ιδιαίτερη σημασία στις βάσεις δεδομένων και είναι ίσως η πιο χαρακτηριστική πόλη σε αυτή την κατηγορία. Ωστόσο , γίνεται συλλογή μεγάλου όγκου προσωπικών δεδομένων μέσω του Copenhagen Connecting, με αποτέλεσμα πολλά προσωπικά δεδομένα να βρίσκονται διαθέσιμα σε ιδιωτικές επιχειρήσεις .Οι επιχειρήσεις αυτές συλλέγουν τα δεδομένα χωρίς τη συγκατάθεση των χρηστών , ενώ ταυτόχρονα παραμένει άγνωστος ο τρόπος επεξεργασίας τους και ο χρόνος διατήρησης τους.

Αναφορικά με τα «Smart »Τρίκαλα ,η πλέον τεχνολογικά πρωτοπόρα πόλη της Ελλάδος , λαμβάνει και διαχειρίζεται χιλιάδες δεδομένα προσωπικού χαρακτήρα. Οι πολίτες έχουν την δυνατότητα πρόσβασης σε υπηρεσίες και εφαρμογές ,στις οποίες όμως ζητούνται δεδομένα τους για την παροχή της πληροφορίας. Ιδιαίτερα στη διασυνδεδεμένη ψηφιακή πλατφόρμα τα δεδομένα τροφοδοτούν και τρίτα συστήματα ,τα οποία δεν γνωρίζουμε αν κρυπτογραφούνται και έχουν παρθεί μέτρα διαφύλαξης των προσωπικών δεδομένων.

7.5 Συμπεράσματα

Συνοψίζοντας , οι έξυπνες πόλεις και οι IoT εφαρμογές που χρησιμοποιούν έχουν αλλάξει τον τρόπο ζωής των κατοίκων τους. Οι εφαρμογές που χρησιμοποιούνται ,εξυπηρετούν τους πολίτες προσφέροντας τους λύσεις σε καθημερινά τους προβλήματα , όπως για παράδειγμα η εύρεση θέσης στάθμευσης (Smart Parking). Ταυτόχρονα όμως, η συλλογή δεδομένων από τους αισθητήρες των πόλεων για την λειτουργία αυτών των εφαρμογών , μπορεί να κρύβει και κάποιους κινδύνους. Η λήψη και η επεξεργασία δεδομένων ,οδηγεί σε πληροφορίες οι οποίες να θέτουν σε κίνδυνο την ιδιωτικότητα των πολιτών. Πολλά από τα δεδομένα που συλλέγονται μπορούν σε συνδυασμό να καταρτίσουν ακόμη και το προφίλ κάθε πολίτη . Επιπλέον δεν γνωρίζουμε αν εξασφαλίζεται η ακεραιότητα των δεδομένων και η ασφάλεια τους. Χαρακτηριστικό παράδειγμα είναι οι ανοιχτές πλατφόρμες στις οποίες έχουν επενδύσει οι έξυπνες πόλεις. Η κακή διαχείριση αυτών και η έλλειψη μέτρων προστασίας δεδομένων θα μπορούσε να μετατρέψει τις ίδιες τις πόλεις σε περιβάλλοντα στα οποία οι πολίτες συνεχώς παρακολουθούνται και εξετάζονται. Επιπλέον όσον αφορά τα προσωπικά δεδομένα που συλλέγονται ,σε πολλές έξυπνες πόλεις όπως στην Κοπεγχάγη ,η παρακολούθηση και η συλλογή κάποιων δεδομένων γίνεται χωρίς την άμεση και ρητή συγκατάθεση των πολιτών, με αποτέλεσμα οι πολίτες να αγνοούν για τον αν τα δεδομένα τους τίθενται και σε περαιτέρω επεξεργασία πέρα από την προβλεπόμενη . Παρόλα αυτά ,πόλεις όπως η Βαρκελώνη και το Άμστερνταμ, έχουν λάβει περισσότερα μέτρα προώθησης της υπεύθυνης χρήσης των δεδομένων. Ιδιαίτερα μετά τις 25 Μαΐου του 2018 όπου ο Γενικός Κανονισμός Προστασίας Δεδομένων εφαρμόζεται στην Ευρώπη , η ανάγκη διαφύλαξης των δεδομένων και κυρίως των προσωπικών είναι στις άμεσες ανάγκες των Ψηφιακών πόλεων. Η ύπαρξη αρχών, που θα διασφαλίζουν την ομαλή και ασφαλή αλληλεπίδραση των προσφερόμενων υπηρεσιών και των χρηστών είναι απαραίτητη . Η διαφύλαξη της ιδιωτικότητας και της ασφάλειας είναι ένα μείζων θέμα για τις έξυπνες πόλεις , αν σκεφτεί κανείς ότι ακόμα και δεδομένα GPS και IPs μπορούν να ταυτοποιήσουν ένα πρόσωπο και να θεωρούνται προσωπικά δεδομένα.

ΚΕΦΑΛΑΙΟ 8 :Προσωπικά Δεδομένα στο Διαδίκτυο των Πραγμάτων

8.1 Εισαγωγή στα Προσωπικά Δεδομένα

Η μεγαλύτερη πρόκληση που έχει δημιουργηθεί στην νέα ψηφιακή εποχή, ή την 4η Βιομηχανική επανάσταση ή την διασυνδεδεμένη ανθρωπότητα ή όπως αλλιώς ονομάζεται η σημερινή τεχνολογική εποχή, είναι η ασφάλεια των ανθρώπων και των προσωπικών δεδομένων. Στον κόσμο της πληροφορικής και των υπολογιστών, από τα πρώτα χρόνια, είχε γίνει κατανοητό ότι δεν υπάρχει ασφαλής κατάσταση για οποιαδήποτε σύστημα.

Οι εξελιγμένες μέθοδοι ασφάλειας και κρυπτογράφησης (σε επίπεδο υλικού και λογισμικού) μπορούν να προστατέψουν τα κρίσιμα συστήματα όταν δέχονται επιθέσεις, αλλά πολλές φορές το μέγεθος, το κόστος, η απαίτηση προσωπικού και το κόστος, είναι τεράστια και όπως είναι φυσικό είναι ταυτόχρονα και αδύνατη η χρησιμοποίηση τους σε μικρές πλακέτες και ασύρματους αισθητήρες, οι οποίοι αποτελούν την πλειοψηφία του IoT.

Καθώς το αντικείμενο ασφάλειας σε επίπεδο υλικού, αποτελεί ένα τομέα εργασίας του εξειδικευμένου προσωπικού, οι ανησυχίες των περισσότερων ανθρώπων επικεντρώνονται στην προστασία της φυσικής τους υπόστασης και την ασφάλεια των προσωπικών δεδομένων, τα οποία μπορεί να διατεθούν ελεύθερα στην δημοσιότητα είτε εσκεμμένα είτε από λάθος.

Ως **Προσωπικά Δεδομένα** ή «δεδομένα προσωπικού χαρακτήρα»: κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική,

ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου. [45]

Τα προσωπικά δεδομένα διακρίνονται σε απλά και ευαίσθητα. Απλά δεδομένα είναι το όνομα, το επώνυμο ,η κατοικία, η περιουσιακή κατάσταση, η IP [46]διεύθυνση, γεωχωρικά δεδομένα (GPS) ,στοιχεία δηλαδή που δεν σχετίζονται με τον πυρήνα της ιδιωτικής ζωής ενός ατόμου.[47] Αντίθετα τα ευαίσθητα αφορούν τον σκληρό πυρήνα της προσωπικής ζωής ενός ατόμου. Ο νομοθέτης παρέχει στα ευαίσθητα προσωπικά δεδομένα διευρυμένη προστασία, ορίζοντας αυστηρότερες προϋποθέσεις για την πρόσβαση σε αυτά και την επεξεργασία αρχείων που τα εμπεριέχουν. Η βασική διαφορά μεταξύ των απλών προσωπικών δεδομένων και ευαίσθητων είναι, ότι για τα ευαίσθητα το επίπεδο προστασίας είναι υψηλότερο συγκριτικά με τα απλά δεδομένα.[48]

Προσωπικά δεδομένα μπορεί να είναι οι πληροφορίες που να επεξεργάζεται το IoT για το σύνολο των συνδεδεμένων συσκευών. Ορισμένες από τις πληροφορίες αυτές μπορεί να είναι αυστηρά προσωπικές (συστήματα παρακολούθησης, πληροφορίες υγείας) άλλες λιγότερο (έξυπνοι λαμπτήρες). Στο πλαίσιο του IoT, η δυνατότητα αναγνώρισης ενός ατόμου με βάση δεδομένα που προκύπτουν από «πράγματα» αποτελεί συχνό φαινόμενο. Μάλιστα, με βάση τα συγκεκριμένα δεδομένα είναι δυνατό να προσδιοριστεί ο τρόπος ζωής ενός συγκεκριμένου ατόμου ή μιας οικογένειας – π.χ. δεδομένα που παράγονται από τον κεντρικό χειρισμό συστημάτων φωτισμού, θέρμανσης, αερισμού και κλιματισμού.

Επιπλέον, ως δεδομένα προσωπικού χαρακτήρα μπορούν να χαρακτηρίζονται ακόμα και εκείνα τα δεδομένα ατόμων που προορίζονται για επεξεργασία μόνο μετά τη χρησιμοποίηση ψευδωνύμων ή ακόμη και την εφαρμογή τεχνικών ανωνυμοποίησης. Για την ακρίβεια, ο μεγάλος

[45] Άρθρο 4 παρ.1 του Κανονισμού (ΕΕ) 2016/679, Ορισμοί https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679&from=EL

[46] Τα φυσικά πρόσωπα μπορεί να συνδέονται με επιγραμμικά αναγνωριστικά στοιχεία ταυτότητας, τα οποία παρέχονται από τις συσκευές, τις εφαρμογές, τα εργαλεία και τα πρωτόκολλά τους, όπως διευθύνσεις διαδικτυακού πρωτοκόλλου, αναγνωριστικά cookies ή άλλα αναγνωριστικά στοιχεία όπως ετικέτες αναγνώρισης μέσω ραδιοσυχνοτήτων. Αυτά μπορεί να αφήνουν ίχνη τα οποία, ιδίως όταν συνδυαστούν με μοναδικά αναγνωριστικά στοιχεία ταυτότητας και άλλες πληροφορίες που λαμβάνουν οι εξυπηρετητές, μπορούν να χρησιμοποιηθούν για να δημιουργηθεί το προφίλ των φυσικών προσώπων και να αναγνωριστεί η ταυτότητά τους. Παράγραφος 30 του Κανονισμού (ΕΕ) 2016/679

[47] Σύμφωνα με τη γνώμη 2/2002 της Ομάδας του άρθρου 29 η IP διεύθυνση είναι προσωπικό δεδομένο

[48] Τζώρτη Βιργινία (2018), Προστασία Δεδομένων Προσωπικού Χαρακτήρα στον Χώρο Ελευθερίας, Ασφαλείας & Δικαιοσύνης, Νομική Βιβλιοθήκη

όγκος δεδομένων που υποβάλλονται σε αυτόματη επεξεργασία στο πλαίσιο του IoT εγκυμονεί κινδύνους για την εκ νέου ταυτοποίηση των δεδομένων. [49]
Το βέβαιο είναι πως ο χρήστης θα πρέπει να νιώθει ασφάλεια για κάθε πληροφορία που μοιράζεται με την νέα αυτή τεχνολογία.

8.2 Επεξεργασία Προσωπικών Δεδομένων στο IoT

Επεξεργασία προσωπικών δεδομένων σύμφωνα με το άρθρο 4, παρ2 του Κανονισμού 2016/679, είναι *«κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή»*[50].Στο άρθρο 6 παρ. 1 του Κανονισμού (ΕΕ) 2016/679 ορίζεται η νομιμότητα της επεξεργασίας.

Οι εφαρμογές του IoT είναι πιθανό να επεξεργάζονται δεδομένα προσωπικού χαρακτήρα , με αποτέλεσμα οι υπεύθυνοι της επεξεργασίας οφείλουν να λαμβάνουν τη ρητή συγκατάθεση του χρήστη, για να επεξεργαστούν τα δεδομένα. Η συγκατάθεση (άρθρο 7 του Κανονισμού 2016/679,) αποτελεί την πρώτη νομική βάση που πρέπει κατά κύριο λόγο να χρησιμοποιείται στο πλαίσιο του IoT και αφορά κατασκευαστές συσκευών, πλατφόρμες κοινωνικής δικτύωσης ή πλατφόρμες δεδομένων, φορείς που διαθέτουν συσκευές προς δανεισμό και σχεδιαστές εφαρμογών τρίτων. Η συγκατάθεση πρέπει να είναι κάθε ελεύθερη, ρητή και να εκφράζεται με τρόπο σαφή, και εν πλήρη επίγνωση, και με την οποία, το υποκείμενο των δεδομένων, αφού προηγουμένως ενημερωθεί, δέχεται να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν. Υπάρχουν όμως και περιπτώσεις, που κατ' εξαίρεση, η επεξεργασία των δεδομένων γίνεται και χωρίς τη συγκατάθεση του υποκειμένου. Σύμφωνα με το άρθρο 6 Κανονισμού επιτρέπεται η επεξεργασία απλών δεδομένων χωρίς συγκατάθεση όταν :

[49] Γνώμη 8/2014 σχετικά με τις πρόσφατες εξελίξεις στο διαδίκτυο των πραγμάτων
[50] Άρθρο 4 του Κανονισμού (ΕΕ) 2016/679, Ορισμοί

α) Η επεξεργασία είναι αναγκαία για την εκτέλεση σύμβασης, στην οποία συμβαλλόμενο μέρος είναι υποκείμενο δεδομένων ή για τη λήψη μέτρων κατόπιν αιτήσεως του υποκειμένου κατά το προσυμβατικό στάδιο.

β) Η επεξεργασία είναι αναγκαία για την εκπλήρωση υποχρεώσεως του υπεύθυνου επεξεργασίας, η οποία επιβάλλεται από το νόμο.

γ) Η επεξεργασία είναι αναγκαία για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου, εάν αυτό τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του.

δ) Η επεξεργασία είναι αναγκαία για την εκτέλεση έργου δημόσιου συμφέροντος ή έργου που εμπίπτει στην άσκηση δημόσιας εξουσίας και εκτελείται από δημόσια αρχή ή έχει ανατεθεί από αυτή είτε στον υπεύθυνο επεξεργασίας είτε σε τρίτο, στον οποίο γνωστοποιούνται τα δεδομένα.

ε) Η επεξεργασία είναι απολύτως αναγκαία για την ικανοποίηση του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας ή ο τρίτος ή οι τρίτοι στους οποίους ανακοινώνονται τα δεδομένα και υπό τον όρο ότι τούτο υπερέχει προφανώς των δικαιωμάτων και συμφερόντων των προσώπων στα οποία αναφέρονται τα δεδομένα και δεν θίγονται οι θεμελιώδεις ελευθερίες αυτών.[51]

Ενώ κατ' εξαίρεση, σύμφωνα με το άρθρο 9 Κανονισμού ,επιτρέπεται η επεξεργασία ευαίσθητων δεδομένων και χωρίς τη συγκατάθεση, όταν:

α) Η επεξεργασία είναι απαραίτητη για την εκτέλεση των υποχρεώσεων και την άσκηση συγκεκριμένων δικαιωμάτων του υπευθύνου επεξεργασίας ή του υποκειμένου των δεδομένων.

β) Η επεξεργασία είναι απαραίτητη για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου, εάν το υποκείμενο των δεδομένων είναι σωματικά ή νομικά ανίκανο να συγκατατεθεί.

γ) Η επεξεργασία διενεργείται, με κατάλληλες εγγυήσεις, στο πλαίσιο των νόμιμων δραστηριοτήτων ιδρύματος, οργάνωσης ή άλλου μη κερδοσκοπικού φορέα με πολιτικό, φιλοσοφικό, θρησκευτικό ή συνδικαλιστικό στόχο και υπό την προϋπόθεση ότι η επεξεργασία

[51] Άρθρο 6 του Κανονισμού (ΕΕ) 2016/679, Νομιμότητα της Επεξεργασίας.

αφορά αποκλειστικά τα μέλη ή τα πρώην μέλη του φορέα ή πρόσωπα τα οποία έχουν τακτική επικοινωνία μαζί του σε σχέση με τους σκοπούς του και ότι τα δεδομένα προσωπικού χαρακτήρα δεν κοινοποιούνται εκτός του συγκεκριμένου φορέα χωρίς τη συγκατάθεση των υποκειμένων των δεδομένων.

δ) Η επεξεργασία αφορά δεδομένα προσωπικού χαρακτήρα τα οποία έχουν προδήλως δημοσιοποιηθεί από το υποκείμενο των δεδομένων.

ε) η επεξεργασία είναι απαραίτητη για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας, όπως η προστασία έναντι σοβαρών διασυνοριακών απειλών κατά της υγείας ή η διασφάλιση υψηλών προτύπων ποιότητας .

στ) η επεξεργασία είναι απαραίτητη για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς.[52]

Άρα, ο χρήστης εφαρμογών IoT δεν μπορεί να θεωρείται ότι συγκατατίθεται σε επεξεργασία δεδομένων του, όταν έχει άγνοια ή μη επαρκή ενημέρωση για την επεξεργασία αυτή. Σε κάθε περίπτωση πρέπει να εκτιμάται από τις εκάστοτε ισχύουσες συνθήκες κατά πόσο η συγκατάθεση δόθηκε ελεύθερα. Η συγκατάθεση θεωρείται ότι δε δόθηκε ελεύθερα εάν υπήρχε ανισότητα μεταξύ του χρήστη και του υπεύθυνου επεξεργασίας , εάν δεν υπάρχει αληθινή επιλογή, ή ο χρήστης δεν είναι σε θέση να αρνηθεί ή να αποσύρει τη συγκατάθεση του χωρίς ζημία. Οι υπεύθυνοι επεξεργασίας πρέπει να δίνουν τη δυνατότητα στο υποκείμενο της επεξεργασίας να ανακαλέσει την συγκατάθεση του οποτεδήποτε. Πιο συγκεκριμένα, ο υπεύθυνος επεξεργασίας στο περιβάλλον του IoT ταυτίζεται σε πολλές περιπτώσεις με τον χρήστη των υπηρεσιών του IoT ο οποίος καθορίζει τους στόχους και τον τρόπο επεξεργασίας των προσωπικών δεδομένων από τη στιγμή που αποφασίζει να μεταφέρει τα δεδομένα και τις εφαρμογές του από τους παραδοσιακούς, φυσικούς φορείς σε ένα εικονικό ψηφιακό περιβάλλον.[53]

[52] Άρθρο 9 του Κανονισμού (ΕΕ) 2016/679, Επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα.
[53] Ομάδα εργασίας του άρθρου 29, Γνώμη 1/2010 σχετικά με τις έννοιες του «υπευθύνου της επεξεργασίας» και του« εκτελούντος την επεξεργασία»

8.3 Αρχές Επεξεργασίας Προσωπικών Δεδομένων στο IoT

Η επεξεργασία των προσωπικών δεδομένων για να είναι νόμιμη πρέπει να τηρεί κάποιους κανόνες που προβλέπονται από τον νόμο και ανάγονται σε αρχές επεξεργασίας. Πρόκειται για τις αρχές του σκοπού, της αναλογικότητας, της ακρίβειας και της καθορισμένης χρονικής διάρκειας τήρησης των δεδομένων.

Στον νέο κανονισμό 2016/679(άρθρο 5),προστέθηκαν και άλλες αρχές επεξεργασίας, όπως της διαφάνειας, της ακεραιότητας και εμπιστευτικότητας και της λογοδοσίας.

Σύμφωνα με την αρχή νομιμότητας του σκοπού και του τρόπου επεξεργασίας η επεξεργασία δεδομένων πρέπει να εξυπηρετεί έναν συγκεκριμένο νόμιμο σκοπό. Η απαίτηση αυτή αποκτά ακόμα μεγαλύτερη σημασία σε σχέση με το IoT, καθώς οι αισθητήρες είναι ουσιαστικά σχεδιασμένοι με τέτοιο τρόπο ώστε να μην γίνονται αντιληπτοί, δηλαδή να είναι κατά το δυνατόν αόρατοι. Ωστόσο, οι υπεύθυνοι της επεξεργασίας δεδομένων οι οποίοι δραστηριοποιούνται στο IoT (κατά πρώτο και κύριο λόγο οι κατασκευαστές συσκευών) οφείλουν να ενημερώνουν όλα τα άτομα που βρίσκονται κοντά σε συνδεδεμένες συσκευές – είτε γεωγραφικά είτε ψηφιακά – όταν συλλέγονται δεδομένα που αφορούν τα άτομα αυτά ή το περιβάλλον τους. Η συμμόρφωση με αυτή τη διάταξη υπερβαίνει τα όρια μιας αυστηρής νομικής απαίτησης: η σύννομη συλλογή αποτελεί μία από τις σημαντικότερες προσδοκίες του χρήστη σε σχέση με το IoT, όσον αφορά κυρίως τις φορετές υπολογιστικές συσκευές.

Παράλληλα σύμφωνα με την αρχή της αναλογικότητας, τα προς επεξεργασία δεδομένα πρέπει να είναι συναφή, πρόσφορα και όχι περισσότερα από όσα κάθε φορά απαιτείται ενόψει των σκοπών της επεξεργασίας. Η επεξεργασία των δεδομένων θα πρέπει να μην είναι μεγαλύτερη από όσο ορίζει ο αρχικός σκοπός της, δηλαδή κατά την επεξεργασία των δεδομένων θα πρέπει αυτά να σχετίζονται άμεσα με τον σκοπό της επεξεργασίας και να μην είναι ανεξάρτητα ή περισσότερα από όσα απαιτούνται (αρχή της αναλογικότητας). Ωστόσο η αρχή της ελαχιστοποίησης των δεδομένων μπορεί να περιορίσει τις δυνητικές ευκαιρίες που προσφέρει το IoT και, ως εκ τούτου, να αποτελέσει εμπόδιο για την καινοτομία, με βάση το σκεπτικό ότι τα δυνητικά οφέλη που προσφέρει η επεξεργασία των δεδομένων προκύπτουν από την προπαρασκευαστική ανάλυση των δεδομένων η οποία αποσκοπεί στην εξεύρεση μη προφανών συσχετίσεων και τάσεων.

Αναλυτικά παρουσιάζονται παρακάτω οι Αρχές Επεξεργασίας Προσωπικών Δεδομένων στο IoT :

- Η αρχή της Νομιμότητας, Αντικειμενικότητας και Διαφάνειας. (Διαφάνεια όρων)
- Η αρχή του Περιορισμού του Σκοπού. (Τα δεδομένα πρέπει να συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και να μην υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο με τους σκοπούς αυτούς.)
- Η αρχή της Αναλογικότητας, (Τα δεδομένα πρέπει να είναι τα ελάχιστα).
- Αρχή της Ακρίβειας (Πλήρης ενημέρωση τρόπου συλλογής δεδομένων, ορθότητα των δεδομένων , χρήση συστημάτων ανίχνευσης/ πρόσληψης εισβολών (IPS/IDS)
- Αρχή της καθορισμένης χρονικής διάρκειας τήρησης των δεδομένων(Διαγραφή των δεδομένων μετά το πέρας του χρόνου- ρητή συμβατική ρύθμιση)
- Η αρχή της Ακεραιότητας και Εμπιστευτικότητας, (τα δεδομένα πρέπει να υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ασφάλεια ,πχ. διαθεσιμότητα σε περίπτωση DoS και προστασία τους από παράνομη επεξεργασία, απώλεια, καταστροφή ή φθορά τους π.χ. χρήση κρυπτογραφίας .
- Η αρχή της λογοδοσίας του υπευθύνου επεξεργασίας, (ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και θα πρέπει να είναι σε θέση να αποδείξει τη συμμόρφωσή με τον Κανονισμό ενώπιον των εποπτικών αρχών και των δικαστηρίων.)[54]

8.4 Προβλήματα που προκύπτουν από την επεξεργασία Προσωπικών Δεδομένων

Όπως είναι φυσικό η συλλογή και η επεξεργασία δεδομένων ,επιφέρει πληροφορίες . Έτσι και στο Διαδίκτυο των Πραγμάτων τα δεδομένα που επεξεργάζονται είναι δυνατόν να ταυτοποιήσουν ένα φυσικό πρόσωπο .Το γεγονός αυτό δημιουργεί τεράστια προβλήματα ως προς τη διαφύλαξη της ιδιωτικότητας .

Ταυτοποίηση των χρηστών

Η απειλή της ταυτοποίησης, υποδηλώνει τη συσχέτιση κάποιου αναγνωριστικού χαρακτηριστικού με ένα συγκεκριμένο άτομο ή με δεδομένα που σχετίζονται με αυτό το άτομο, προσδίδοντάς του έτσι ταυτότητα. Η απειλή της αναγνώρισης της ταυτότητας των ατόμων στο

[54] http://www.dpa.gr/portal/page?_pageid=33,211315&_dad=portal&_schema=PORTAL

διαδίκτυο των πραγμάτων (IoT) κυριαρχεί ιδιαίτερα στο στάδιο που γίνεται η επεξεργασία των πληροφοριών από τα συστήματα υποστήριξης του δικτύου, όπου και συγκεντρώνονται τεράστιες ποσότητες δεδομένων που βρίσκονται εκτός του ελέγχου του υποκειμένου το οποίο και αφορούν**.** Χαρακτηριστικό παράδειγμα αποτελούν τα κυκλώματα cctv , τα οποία καταγράφουν φυσικά πρόσωπα .

Παρακολούθηση χρηστών- Εντοπισμός θέσης

Ο εντοπισμός και η παρακολούθηση είναι η απειλή που αναφέρεται στον καθορισμό και την αποθήκευση της τοποθεσίας ενός ατόμου ανεξαρτήτως χρονικής περιόδου ή χώρου. Η διαδικασία της παρακολούθησης είναι ένα είδος ταυτοποίησης ενός ατόμου. Δεδομένα GPS ή και IP θεωρούνται προσωπικά δεδομένα καθώς μπορεί να γίνει άμεσος εντοπισμός ενός χρήστη. Μια υπηρεσία εντοπισμού θέσης χρησιμοποιεί τη γεωγραφική θέση του κινητού τηλεφώνου του χρήστη και άλλων κινητών συσκευών εξοπλισμένων με τη δυνατότητα εντοπισμού θέσης για να παρέχει διάφορες υπηρεσίες όπως διαφήμισης και ενημερώσεις για την κίνηση και τον καιρό κ.τ.λ.

Κατάρτιση Προφίλ

Η διαμόρφωση προφίλ ενός χρήστη, είναι η διαδικασία που αφορά την συλλογή πληροφοριών για άτομα με σκοπό την εξαγωγή συμπερασμάτων για τα ενδιαφέροντά τους, σε συσχέτιση με άλλα δεδομένα. Συγκεκριμένα σύμφωνα με το Άρθρο 4 παρ. 4 του Κανονισμού (ΕΕ) 2016/679, η «κατάρτιση προφίλ» αναφέρεται ως *«οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που συνίσταται στη χρήση δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση ορισμένων προσωπικών πτυχών ενός φυσικού προσώπου, ιδίως για την ανάλυση ή την πρόβλεψη πτυχών που αφορούν την απόδοση στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις, τα ενδιαφέροντα, την αξιοπιστία, τη συμπεριφορά, τη θέση ή τις μετακινήσεις του εν λόγω φυσικού προσώπου»* .Επιπρόσθετα σύμφωνα με το άρθρο 22 παρ.1 , που αναφέρεται στην Αυτοματοποιημένη ατομική λήψη αποφάσεων, περιλαμβανομένης της κατάρτισης προφίλ , *«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.»*

Διαρροή πληροφοριών μέσω διασύνδεσης συστημάτων

Η διασύνδεση διαφορετικών συστημάτων που προηγουμένως λειτουργούσαν ξεχωριστά, με το συνδυασμό των πηγών δεδομένων τους μπορούν να δημιουργήσουν πληροφορίες τις οποίες ο χρήστης δεν αποκάλυψε ή δεν ήθελε να αποκαλύψει με τη χρήση των προηγουμένως μεμονωμένων συστημάτων. Η διασύνδεση αρχείων αποτελεί κατά τον Ν. 2472/97 ειδική μορφή επεξεργασίας δεδομένων (βλ. άρθρο. 8), και υποβάλλεται σε ρύθμιση ανάλογη με τη γενικότερη ρύθμιση της επεξεργασίας[55]. Στον Κανονισμό (ΕΕ) 2016/679, δεν υπάρχει ακριβής ορισμός της διασύνδεσης αρχείων. Ωστόσο σύμφωνα με το άρθρο 4 του Κανονισμού ορίζεται πως επεξεργασία είναι κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως διάδοση , η συσχέτιση και ο συνδυασμός. Αυτές οι τρεις έννοιες καλύπτουν σχετικά και την έννοια της διασύνδεσης αρχείων.[56]

Έλλειψη συγκατάθεσης της χρήσης δεδομένων

Η έλλειψη συγκατάθεσης συλλογής και επεξεργασίας δεδομένων είναι από τα συνηθέστερα προβλήματα στο IoT. Οι περισσότερες συσκευές IoT είναι σχεδιασμένες με τρόπο τέτοιο όπου ο χρήστης δεν μπορεί να δίνει τη συγκατάθεση του για την επεξεργασία των δεδομένων του. Προϋπόθεση για έγκυρη συγκατάθεση αποτελεί η προηγούμενη πλήρης ενημέρωση του υποκειμένου για την επεξεργασία των δεδομένων του (informed consent) , έτσι ώστε η συγκατάθεση να δίδεται «εν πλήρη επιγνώσει». (Ε.Αλεξανδροπούλου-Αιγυπτιαδου).[57]Πρέπει πάντως να τονισθεί ,ότι σε μία συσκευή IoT που μπορεί να έχει ζητηθεί η συγκατάθεσή του υποκειμένου , δεν σημαίνει αυτόματα ότι η συγκατάθεση είναι γενική ,δηλαδή ότι αναφέρεται για κάθε μελλοντική επεξεργασία προσωπικών δεδομένων του υποκειμένου. Αντίθετα η συγκατάθεση πρέπει να είναι ειδική ,να αφορά δηλαδή τη συγκεκριμένη επεξεργασία έτσι ώστε να μπορεί να λειτουργήσει ως παράγοντας νομιμότητας της τελευταίας .

---

[55] Νόμος 2472/1997 προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα με ενσωματωμένες τις τροποποιήσεις, άρθρο 8.
http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/PROSOPIKA%20DEDOMENA/FILES/2472_97_JUNE2013.PDF

[56] Άρθρο 4 παρ.1 του Κανονισμού (ΕΕ) 2016/679, Ορισμοί https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679&from=EL

[57] Ε. Αλεξανδροπούλου-Αιγυπτιαδου, Προσωπικά Δεδομένα , σελ.93-94

8.5 Απόρρητο και Ασφάλεια στο IoT

Η επεξεργασία των προσωπικών δεδομένων είναι απόρρητη και πρέπει να θωρακίζεται με αυστηρούς μηχανισμούς ασφαλείας. Σύμφωνα με το άρθρο 25 του ΓΚΠΔ 679/2016 *,«ο υπεύθυνος επεξεργασίας πρέπει να εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλίζει ότι, εξ ορισμού, υφίστανται επεξεργασία μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για τον εκάστοτε σκοπό της επεξεργασίας.»*[58] Επιπρόσθετα σύμφωνα με το άρθρο 32 του ΓΚΠΔ 679/2016 όπου περιγράφεται η ασφάλεια της επεξεργασίας *«ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων, περιλαμβανομένων, μεταξύ άλλων, κατά περίπτωση: α) της ψευδωνυμοποίησης και της κρυπτογράφησης δεδομένων προσωπικού χαρακτήρα, β) της δυνατότητας διασφάλισης του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση, γ) της δυνατότητας αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο σε περίπτωση φυσικού ή τεχνικού συμβάντος, δ) διαδικασίας για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας.»*[59]

Κατά συνέπεια, ο υπεύθυνος της επεξεργασίας έχει και την ευθύνη για την ασφάλεια της επεξεργασίας των δεδομένων και τυχών σφάλματα, ή επιθέσεις οφείλονται στον ανεπαρκή σχεδιασμό ή στην ανεπαρκή συντήρηση των χρησιμοποιούμενων συσκευών. Στο ίδιο πλαίσιο, καθίσταται απαραίτητη η εφαρμογή μηχανισμών πιστοποίησης για τις συσκευές, καθώς επίσης και η εναρμόνισή τους με διεθνώς αναγνωρισμένα πρότυπα ασφάλειας, προκειμένου να βελτιωθεί η συνολική ασφάλεια του οικοσυστήματος του IoT. Τα απαραίτητα μέτρα ασφάλειας πρέπει να εφαρμόζονται έχοντας λάβει υπόψη τους λειτουργικούς περιορισμούς των συσκευών του IoT.

Οι περισσότεροι αισθητήρες που χρησιμοποιούνται στις IoT συσκευές δεν μπορούν να δημιουργήσουν κρυπτογραφημένη σύνδεση εξαιτίας της προτεραιότητας που δίνεται στη φυσική αυτονομία της συσκευής ή στον έλεγχο του κόστους. Επίσης, οι συσκευές που λειτουργούν στο IoT είναι δύσκολο να θεωρούνται ασφαλείς τόσο για τεχνικούς όσο και για εμπορικούς λόγους.

[58] Άρθρο 25 του Κανονισμού (ΕΕ) 2016/679 Προστασία των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού
[59] Άρθρο 32 του Κανονισμού (ΕΕ) 2016/679 Ασφάλεια επεξεργασίας

Επειδή τα εξαρτήματά τους χρησιμοποιούν συνήθως υποδομές ασύρματης επικοινωνίας και χαρακτηρίζονται από περιορισμένους πόρους όσον αφορά την ενέργεια και την υπολογιστή τους ισχύ, οι συσκευές είναι ευάλωτες σε φυσικές επιθέσεις, σε υποκλοπές ή επιθέσεις εναντίον διακομιστών. Ως εκ τούτου, πρέπει να εξεταστεί η ανάγκη χρήσης ασφαλών και ελαφριών πρωτοκόλλων που θα μπορούν να χρησιμοποιούνται σε περιβάλλοντα περιορισμένων πόρων. [60] Επιπλέον, οι παράμετροι των συσκευών που είναι ειδικά σχεδιασμένες για να είναι προσπελάσιμες απευθείας από το διαδίκτυο δεν ρυθμίζονται πάντα από τον χρήστη. Οι συσκευές αυτές επομένως ενδέχεται να αποτελούν μια εύκολη πύλη εισόδου για τους εισβολείς εφόσον συνεχίσουν να λειτουργούν με τις προεπιλεγμένες ρυθμίσεις. Επιπρόσθετα ορισμένα από τα συστήματα αυτοπαρακολούθησης (π.χ. βηματόμετρα, συσκευές παρακολούθησης ύπνου) που κυκλοφορούν στην αγορά επίσης είναι ευάλωτα σε πιθανά σφάλματα ασφάλειας, επιτρέποντας σε εισβολείς να παραποιούν τις παρατηρούμενες τιμές που παρέχονται στις εφαρμογές και στους κατασκευαστές συσκευών. Οι συσκευές αυτές πρέπει οπωσδήποτε να προσφέρουν επαρκείς μηχανισμούς προστασίας από την παραποίηση δεδομένων, ιδίως μάλιστα αν οι τιμές που παρέχονται από αυτούς τους αισθητήρες επηρεάζουν έμμεσα τις αποφάσεις των χρηστών σχετικά με την υγεία τους. Συνεπώς αποτελεί υποχρέωση του υπεύθυνου επεξεργασίας η τήρηση ικανοποιητικού επιπέδου ασφαλείας, κάνοντας χρήση τεχνολογιών που συμβάλλουν στην διασφάλιση της ιδιωτικότητας ,που θα αποτρέπει κάθε αθέμιτη ενέργεια που μπορεί να διαπραχθεί, με απώτερο σκοπό την παραβίαση του απορρήτου των προσωπικών δεδομένων ,αποκλείοντας έτσι την αθέμιτη καταστροφή, απώλεια ,ή αλλοίωση των δεδομένων.

[60] Γνώμη 8/2014 σχετικά με τις πρόσφατες εξελίξεις στο διαδίκτυο των πραγμάτων https://www.dataprotection.ro/servlet/ViewDocument?id=1088

ΚΕΦΑΛΑΙΟ 9: Νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων στο IoT και σε RFID τεχνολογίες

Ο κόσμος του διαδικτύου των πραγμάτων (IoT) είναι άρρηκτα συνδεδεμένος με τα προσωπικά δεδομένα. Καθημερινά εκατομμύρια διασυνδεδεμένες συσκευές συλλέγουν , λαμβάνουν , επεξεργάζονται και μεταδίδουν δεδομένα και πληροφορίες, όπου πολλά από αυτά είναι και προσωπικά δεδομένα. Όπως έγινε κατανοητό από το προηγούμενο κεφάλαιο η προστασία των προσωπικών δεδομένων είναι ένα ιδιαίτερο ζήτημα για το Διαδίκτυο των Πραγμάτων . Το απόρρητο , η ασφάλεια επεξεργασίας δεδομένων , η ασφάλεια διαβίβασης δεδομένων κ.π.λ, αποτελούν σοβαρά θέματα ως προς την υπόσταση του Διαδικτύου των Πραγμάτων και στην ανάπτυξη του. Είναι αναγκαίο να θεσμοθετηθούν δικλείδες ασφαλείας που προστατεύουν τα υποκείμενα και τα δεδομένα τους από αυθαίρετη χρήση. Οι χρήστης έξυπνων συσκευών που λαμβάνουν και αποστέλλουν δεδομένα πρέπει να προστατεύεται νομικά , έτσι ώστε να αισθάνονται ότι η ασφάλεια των δεδομένων τους είναι εγγυημένη. Η ανάπτυξη ενός νομικού πλαισίου που θα προάγει μια εποικοδομητική εξάπλωση του Διαδικτύου των Πραγμάτων είναι αναγκαία. Λόγω του γεγονότος ότι το IoT εμφανίστηκε τα τελευταία χρόνια στην ζωή μας δεν είχε οριστεί ένα σαφές νομικό πλαίσιο που να το διέπει, ωστόσο ως προς την κατεύθυνση της προστασίας προσωπικών δεδομένων τα τελευταία χρόνια έχουν γίνει σημαντικά βήματα καταγραφής ενός νομικού πλαισίου , με αποκορύφωμα τον Γενικό Κανονισμό Προστασίας Δεδομένων (General Data Protection Regulation 2016/679) . Επιπλέον η ΕΕ έχει εκδώσει οδηγίες και σχετικές γνωμοδοτήσεις αναφορικά με την προστασία των δεδομένων σε εφαρμογές RFID και σε συσκευές IoT. Συγκεκριμένα η ομάδα εργασίας του άρθρου 29 της οδηγίας 95/46/ΕΚ προτείνει χρήσιμες σχετικές γνώμες που αφορούν το IoT ,όπως την Γνώμη 8/2014 σχετικά με τις πρόσφατες εξελίξεις στο διαδίκτυο των πραγμάτων. Παρακάτω γίνεται μία λεπτομερής αναφορά του νομοθετικού πλαισίου για την προστασία των προσωπικών δεδομένων στο IoT και σε RFID τεχνολογίες. Στο παρόν κεφάλαιο θα εξετασθεί το νομικό πλαίσιο , τόσο σε ευρωπαϊκό ,όσο και σε εθνικό επίπεδο.

9.1 Εφαρμογή του δικαίου της ΕΕ στην επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο του IoT

Το IoT έχει εισχωρήσει στις ζωές μας. Καθημερινά γίνεται χρήση χιλιάδων έξυπνων συσκευών που λαμβάνουν και επεξεργάζονται δεδομένα. Είναι επιτακτική η ανάγκη επιβολής ενός κατάλληλου νομοθετικού πλαισίου που θα είναι σε θέση να διασφαλίσει ότι οι υπηρεσίες του Διαδικτύου των Πραγμάτων θα διαθέτουν ρυθμίσεις που θα εξασφαλίζουν την ιδιωτικότητα και θα ενισχύουν την ασφάλεια των προσωπικών δεδομένων που θα επεξεργάζονται .

Το συναφές νομικό πλαίσιο για την αξιολόγηση των ζητημάτων που τίθενται από το IoT στην ΕΕ σε σχέση με την προστασία της ιδιωτικής ζωής και των δεδομένων αποτελείται από τις γνωμοδοτήσεις της ομάδας του άρθρου 29 καθώς συστάσεις που προτείνονται , με κυριότερη γνωμοδότηση την 8/2014 σχετικά με τις πρόσφατες εξελίξεις στο Διαδίκτυο των Πραγμάτων ,λόγω του εξειδικευμένου περιεχομένου της .Η γνώμη 8/2014, ερμηνεύει την οδηγία 95/46/ΕΚ, η οποία παρά την κατάργηση και αντικατάστασή της από τον Γενικό Κανονισμό Προστασίας Δεδομένων (General Data Protection Regulation 2016/679), περιέχει διατάξεις που αφορούν το IoT , όπως και ο Κανονισμός. Τέλος αναλύονται επιμέρους διατάξεις της οδηγίας 2002/58/ΕΚ ,όπως τροποποιήθηκε από την οδηγία 2009/136/ΕΚ.

9.1.1 Γνώμη 8/2014 σχετικά με τις πρόσφατες εξελίξεις στο Διαδίκτυο των Πραγμάτων

Το διαδίκτυο των πραγμάτων τείνει να ενσωματωθεί στις ζωές των ευρωπαίων πολιτών. Ήδη σήμερα, χιλιάδες συνδεδεμένες συσκευές καλύπτουν με επιτυχία τις ανάγκες πολλών ανθρώπων. Ωστόσο όμως η χρήση αυτών εμπεριέχει και πολλούς κινδύνους για την ασφάλεια των προσωπικών τους δεδομένων. Για να μπορέσει να υπάρξει εφησύχαση των ευρωπαίων πολιτών γύρω από την χρήση των εφαρμογών του IoT η ομάδα εργασίας του άρθρου 29 εξέδωσε τον Σεπτέμβριο του 2014 την σχετική γνώμη 8/2014 σχετικά με τις πρόσφατες εξελίξεις στο Διαδίκτυο των Πραγμάτων. Το κλειδί για να πετύχει η καινοτόμος ιδέα του IoT και να κερδίσει την εμπιστοσύνη των καταναλωτών, έγκειται στη σαφή και πλήρη ενημέρωσή τους γύρω από όλους τους πιθανούς κινδύνους. Έτσι, στην παρούσα γνώμη προσδιορίζονται οι κυριότεροι κίνδυνοι που απειλούν την προστασία των δεδομένων στο εσωτερικό του οικοσυστήματος του IoT . Ακόμα και αν δεν καλύπτονται όλες οι πτυχές του, η σχετική γνώμη περιλαμβάνει εκτενείς

αναφορές στο διαδίκτυο των πραγμάτων, ενώ εστιάζει σε τρείς τομείς οι οποίοι είναι πιο κοντά στην καθημερινότητα του μέσου καταναλωτή .
Συγκεκριμένα σε :

Φορετές υπολογιστικές συσκευές (wearable devices)

Ως «φορετές υπολογιστικές συσκευές» αναφέρονται καθημερινά αντικείμενα και είδη ρουχισμού, όπως ρολόγια χειρός και γυαλιά, τα οποία διαθέτουν αισθητήρες για να επεκτείνουν τις δυνατότητές τους . Οι φορετές υπολογιστικές συσκευές έχουν τη δυνατότητα να ενσωματώνουν κάμερες, μικρόφωνα και αισθητήρες, που καταγράφουν και μεταφέρουν δεδομένα σε απομακρυσμένα τερματικά. Επιπλέον, η ύπαρξη διαθέσιμων διεπαφών προγραμματισμού εφαρμογών για φορετές υπολογιστικές συσκευές υποστηρίζει και τη δημιουργία εφαρμογών από τρίτους, οι οποίοι μπορούν με τον τρόπο αυτό να αποκτούν πρόσβαση στα δεδομένα που συλλέγονται και να εκμαιεύουν πληροφορίες από τα εν λόγω αντικείμενα.

Ποσοτικοποιημένος εαυτός (quantified self)

Οι συσκευές αυτές είναι σχεδιασμένες να καταγράφουν τις κινήσεις και δραστηριότητες των ανθρώπων και μετέπειτα εξάγουν πληροφορίες. Τέτοιες συσκευές καταγράφουν τη διανυθείσα απόσταση ,τη θερμιδική κατανάλωση, τις ώρες ύπνου των χρηστών , με αποτέλεσμα να γίνεται μια συνεχή παρακολούθηση αυτών και να υπάρχει ο κίνδυνος γνωστοποίησης των παραπάνω δεδομένων. Πιο συγκεκριμένα, εκτός από το τελικό συμπέρασμα που παρέχεται στο χρήστη θα μπορούσε οποιαδήποτε ιδιωτική εταιρεία να αξιοποιήσει την πληθώρα δεδομένων, που συλλέγονται από τις εν λόγω συσκευές, χωρίς φυσικά ο χρήστης να έχει να έχει δώσει τη συγκατάθεση του.

Οικιακούς αυτοματισμούς «δομοτική» (domotics)

Μέσω των συσκευών IoT ,πλέον είναι δυνατόν , να ελέγχονται απομακρυσμένα σχεδόν όλες οι λειτουργίες μια έξυπνης κατοικίας . Ανιχνευτές κίνησης είναι σε θέση να αντιλαμβάνονται την ύπαρξη ατόμων στο σπίτι και ανάλογα με τις προτιμήσεις του να προσαρμόζουν συνθήκες όπως ο φωτισμός ή η θερμοκρασία. Είναι φανερό ότι η οικιακή αυτοματοποίηση αναδύει ζητήματα

ιδιωτικότητας, καθώς πολλές καθημερινές συνήθειες και ο οικιακός τρόπος ζωής κατοίκων τέτοιων σπιτιών, καταχωρούνται σε βάσεις δεδομένων ιδιωτικών εταιρειών. [61]

9.1.1.1 Προκλήσεις που προκύπτουν από το διαδίκτυο των πραγμάτων σε σχέση με την προστασία της ιδιωτικής ζωής και των δεδομένων.

Το Διαδίκτυο των Πραγμάτων θέτει πολλές σημαντικές προκλήσεις σε σχέση με την προστασία της ιδιωτικής ζωής και των δεδομένων. Ιδιαίτερα με την όλο και αυξανόμενη εξέλιξη του, οι προκλήσεις αυτές , μεγεθύνονται ακόμα περισσότερο με αποτέλεσμα να γεννάται η ανάγκη θέσπισης και εφαρμογής ενός νομικού πλαισίου για την προστασία των δεδομένων προσωπικού χαρακτήρα στο Διαδίκτυο των Πραγμάτων. Στην γνωμοδότηση 8/2014 εξάγονται κάποια χρήσιμα συμπεράσματα και γίνονται συστάσεις προς τα ενδιαφερόμενα μέρη (κατασκευαστές, σχεδιαστές, πλατφόρμες, οργανισμούς τυποποίησης, κλπ.).

Ορισμένα από τα σημεία στα οποία επικεντρώνεται η εν λόγω Γνωμοδότηση είναι:

1. **Η έλλειψη ελέγχου των χρηστών ως προς την επεξεργασία των δεδομένων τους λόγω της αυτοματοποιημένης ροής πληροφοριών:**

   Η επικοινωνία και η αλληλεπίδραση μεταξύ αντικειμένων και συσκευών, αλλά και η διάδραση μεταξύ των χρηστών και των συσκευών IoT ,έχει οδηγήσει στη δημιουργία μιας ροής δεδομένων η οποία δεν είναι δυνατό να ελεγχθεί επαρκώς, με αποτέλεσμα ο τελικός χρήστης να μην διασφαλίζει την προστασία των προσωπικών του δεδομένων . Το Διαδίκτυο των πραγμάτων εγείρει ανησυχίες σχετικά με το ποιος μπορεί να συλλέγει και να επεξεργάζεται τα δεδομένα ,ποιος έχει το δικαίωμα να προβεί σε μια τέτοια ενέργεια ,εάν διατηρούνται ανώνυμα ,δημοσιοποιούνται ή μεταβιβάζονται σε τρίτους. Αποτελεί τον μεγαλύτερο κίνδυνο καθώς το άτομο υποβάλλεται σε συνεχόμενη, μη ελεγχόμενη παρακολούθηση με αδιαφανή τρόπο.

2. **Ζητήματα συγκατάθεσης των χρηστών (ως προς το σκοπό επεξεργασίας, ως προς την προγενέστερη ενημέρωση κ.οκ.)**

[61] Γνώμη 8/2014 σχετικά με τις πρόσφατες εξελίξεις στο διαδίκτυο των πραγμάτων

Οι περισσότερες IoT συσκευές δε διαθέτουν κατάλληλους μηχανισμούς, όπου ο τελικός χρήστης να μπορεί να δίνει τη συγκατάθεση του, για τα δεδομένα που επεξεργάζονται, αποθηκεύονται και διαμοιράζονται. Σε πολλές περιπτώσεις ο χρήστης ενδέχεται να μην είναι ενήμερος για την επεξεργασία των δεδομένων του από τις συσκευές του IoT, αυτή η έλλειψη ενημέρωσης οδηγεί στην παραχώρηση "χαμηλής ποιότητας" συγκατάθεσης στο χρήστη και είναι αδύνατο να παραχωρηθεί αποτελεσματική συγκατάθεση σύμφωνα με τις προτιμήσεις των χρηστών. Έτσι δεν διασφαλίζεται η συναίνεση για την επεξεργασία των προσωπικών του δεδομένων. Σε αυτή την περίπτωση, πρέπει να δημιουργηθούν νέοι μέθοδοι απόκτησης της έγκυρης συναίνεσης από τον τελικό χρήστη , όπως «privacy proxies». Ως εκ τούτου μπορεί να επιτρέψει τη χρήση των δεδομένων για δευτερεύοντες σκοπούς, άσχετους με τον αρχικό σκοπό επεξεργασίας

3. **Η δυνατότητα λεπτομερούς profiling των χρηστών (κατάρτιση προφίλ) και των συμπεριφορών τους**

   Η κατοχή ακόμη και μεμονωμένων πληροφοριών από ενδιάμεσους και μη σχετικούς φορείς (third parties), πολλές φορές οδηγεί στην εκ νέου παραγωγή δεδομένων για σκοπούς διαφορετικούς από την αρχική πρόβλεψη. Αυτό οφείλεται στην πλήρη ανάπτυξη των ικανοτήτων του IoT όπου το άτομο ελέγχεται, επιτηρείται συνέχεια, καθώς δεν υπάρχει επαρκής ενημέρωση για συλλογή και καταγραφή των δεδομένων του. Πιο συγκεκριμένα, μπορούν να εξαχθούν πληροφορίες με τις οποίες να δημιουργείται ένα «προφίλ» των χρηστών. Κάτι τέτοιο θα συνιστούσε πολύ έντονη επέμβαση στην ιδιωτική και προσωπική ζωή .

4. **Ζητήματα ασφάλειας**

   Οι περισσότερες IoT συσκευές δεν πληρούν το κατάλληλο επίπεδο ασφαλείας με αποτέλεσμα πολλά δεδομένα να είναι ευάλωτα από επιθέσεις , μεταξύ άλλων στο επίπεδο επικοινωνίας και της αποθήκευσης. Συγκεκριμένα, δεν είναι ακόμα σαφές με ποιον τρόπο οι κατασκευαστές των συσκευών θα εξισορροπήσουν την εφαρμογή μέτρων εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας σε όλα τα επίπεδα της επεξεργασίας. Όταν οι κατασκευαστές καλούνται να επιλέξουν ανάμεσα στην αποδοτικότητα και την ασφάλεια,

πάντα επιλέγουν την αποδοτικότητα θυσιάζοντας την ασφάλεια του συστήματος. Με αυτή την επιλογή ,εύλογα οδηγούμαστε στην ύπαρξη κινδύνων καθώς υπάρχουν ευπάθειες. Κίνδυνοι όπως η μη εξουσιοδοτημένη πρόσβαση, η παραβίαση τοπικών δικτύων με σκοπό την υποκλοπή ευαίσθητων πληροφοριών, η αποστολή ιών, μπορούν να προκαλέσουν ανεπανόρθωτες βλάβες σε συστήματα.

9.1.1.2 Συστάσεις χρήσης εφαρμογών IoT.

Η ομάδα εργασίας του άρθρου 29 με την γνωμοδότηση 8/2014 εξέδωσε κάποιες συστάσεις , που αφορούν των σύνολο των εφαρμογών γύρω από το IoT . Για την ακρίβεια στην εν λόγω γνωμοδότηση δίνονται κατευθυντήριες γραμμές ως προς τη χρήση των εφαρμογών του Διαδικτύου των Πραγμάτων από τους χρήστες και τους κατασκευαστές αυτών ,έτσι ώστε η επεξεργασία των προσωπικών δεδομένων στις συσκευές IoT να γίνεται με ασφαλή τρόπο.

Συγκεκριμένα:

<u>Συστάσεις που αφορούν όλα τα ενδιαφερόμενα μέλη:</u>

- Τα ενδιαφερόμενα μέρη πρέπει να διαγράφουν τα μη επεξεργασμένα δεδομένα, μετά την εξαγωγή των δεδομένων που είναι απαραίτητα για την επεξεργασία δεδομένων που εκτελούν.[62]
- Τα ενδιαφερόμενα μέρη οφείλουν να σχεδιάζουν συσκευές IoT με συγκεκριμένα πρότυπα ιδιωτικότητας (Privacy by Design) .Αλλά ακόμη και από την αναγγελία δημιουργίας νέων συσκευών IoT η ιδιωτικότητα να είναι εξ 'ορισμού δεδομένη. (Privacy by Default). [63]
- Εφαρμογή Αρχών Προστασίας ιδιωτικής ζωής. Οφείλουν να σέβονται το ιδιωτικό απόρρητο του χρήστη και να τον γνωστοποιούν για τις πληροφορίες που διακινούνται, με σαφήνεια.[64]

[62] Άρθρο 2 του Κανονισμού (ΕΕ) 2016/679 Εκτελών την επεξεργασία
[63] Άρθρο 25 του Κανονισμού (ΕΕ) 2016/679 Προστασία των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού
[64] Άρθρο 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες (οδηγία 2002/58/Ε.Κ, όπως τροποποιήθηκε από την οδηγία 2009/136/ΕΚ)

- Οι μέθοδοι της παροχής πληροφοριών, της παροχής του δικαιώματος άρνησης ή αίτησης συγκατάθεσης θα πρέπει να είναι όσο το δυνατόν πιο προσιτές για τον χρήστη.[65]

Κατασκευαστές λειτουργικών συστημάτων & συσκευών:

- Να ενημερώνουν τους χρήστες για όλες τις λεπτομέρειες της επεξεργασίας των δεδομένων τους.[66]
- Τα δεδομένα να είναι σε μορφή τέτοια που να επιτρέπει τους χρήστες να ασκήσουν το δικαίωμα της πρόσβασης[67] και της φορητότητας των δεδομένων τους. [68]
- Οφείλουν να προστατεύουν τα δεδομένα των υποκειμένων ,λαμβάνοντας τα κατάλληλα μετρά ,όπως την ανανέωση των υπηρεσιών τους σύμφωνα με τα εκάστοτε πρότυπα αντιμετώπισης ηλεκτρονικών επιθέσεων.
- Οι κατασκευαστές συσκευών πρέπει να ακολουθούν διαδικασία ασφάλειας ήδη από το στάδιο του σχεδιασμού και να διαθέτουν ορισμένα εξαρτήματα για τα προκαταρκτικά συστήματα κρυπτογράφησης κλειδιού.

Πλατφόρμες κοινωνικής δικτύωσης:

- Με βάση τις προεπιλεγμένες ρυθμίσεις, οι πληροφορίες που δημοσιεύονται από συσκευές του IoT σε πλατφόρμες κοινωνικής δικτύωσης δεν πρέπει να δημοσιοποιούνται ούτε να καταχωρίζονται σε ευρετήρια μηχανών αναζήτησης.
- Να δίνεται η δυνατότητα στους χρήστες , να διαμορφώνουν οι ίδιοι τις προκαθορισμένες ρυθμίσεις , που αφορούν την κοινοποίηση των δεδομένων τους από τις συσκευές IoT.

Σχεδιαστές εφαρμογών :

- Να αναπτύσσουν προγράμματα, που να ενημερώνουν τους χρήστες IoT συσκευών σχετικά με τη συλλογή προσωπικών ή μη δεδομένων.

[65] Άρθρο 7 του Κανονισμού (ΕΕ) 2016/679 Προϋποθέσεις για συγκατάθεση
[66] Άρθρο 12 του Κανονισμού (ΕΕ) 2016/679, Δικαίωμα Ενημέρωσης
[67] Άρθρο 15 του Κανονισμού (ΕΕ) 2016/679, Δικαίωμα πρόσβασης του υποκειμένου των δεδομένων.
[68] Άρθρο 20 του Κανονισμού (ΕΕ) 2016/679, Δικαίωμα στη φορητότητα των δεδομένων

- Να παρέχουν στο χρήστη τη δυνατότητα επεξεργασίας και το δικαίωμα διαγραφής των δεδομένων του που συλλέγονται και τον αφορούν.
- Οι σχεδιαστές εφαρμογών πρέπει να δίνουν ιδιαίτερη προσοχή στα είδη των δεδομένων που υποβάλλονται σε επεξεργασία και στην πιθανότητα εξαγωγής ευαίσθητων δεδομένων προσωπικού χαρακτήρα με βάση αυτά τα δεδομένα.
- Εφαρμογή της Αρχής της Ελαχιστοποίησης των Δεδομένων.

Κάτοχοι συσκευών IoT και πρόσθετοι αποδέκτες:

- Δεν θα πρέπει να έχουν κάποιου είδους ποινή ή μειωμένες δυνατότητες στις IoT εφαρμογές, σε περίπτωση που δεν δώσουν τη συγκατάθεσή τους για την επεξεργασία των δεδομένων τους.
- Οφείλουν να ενημερώνουν τους μη-χρήστες συσκευών IoT, ότι δεδομένα που σχετίζονται με την παρουσία τους είναι πιθανό να συλλέγονται.

Οργανισμοί τυποποίησης και πλατφόρμες δεδομένων:

- Οφείλουν να προωθούν φορητές και διαλειτουργικές μορφές δεδομένων, που θα επιτρέπουν την ομαλή μεταφορά τους.
- Να προωθούν την ανωνυμία στο Διαδίκτυο και να μεριμνούν ώστε στις πλατφόρμες που συλλέγονται οι πληροφορίες, να υφίστανται όσο το δυνατόν λιγότερα πιστοποιητικά ταυτοποίησης των χρηστών.
- Οι οργανισμοί τυποποίησης θα πρέπει να αναπτύξουν ελαφριά πρωτόκολλα κρυπτογράφησης και επικοινωνίας που θα είναι ειδικά προσαρμοσμένα στις ιδιαιτερότητες του IoT, διασφαλίζοντας την εμπιστευτικότητα, την ακεραιότητα, τον έλεγχο ταυτότητας και τον έλεγχο πρόσβασης

9.1.2 Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR)

Στην Ευρωπαϊκή Ένωση έχουν εκδοθεί μία σειρά από κοινοτικές οδηγίες και αποφάσεις που πλαισιώνουν νομικά τα προσωπικά δεδομένα. Όπως έγινε παραπάνω αναφορά η **Οδηγία 95/46/ΕΚ για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών,**

αποτέλεσε σταθμό για την προστασία των Προσωπικών Δεδομένων. Η Οδηγία εκδόθηκε με σκοπό την πλήρη εναρμόνιση της εθνικής νομοθεσίας των κρατών μελών για την προστασία των προσωπικών δεδομένων, θέτοντας τις νόμιμες προϋποθέσεις για τη θεμιτή επεξεργασία των προσωπικών δεδομένων, με την ίδρυση υποχρεώσεων και την αναγνώριση δικαιωμάτων, τα οποία εξοπλίζονται με ένδικα μέσα και επιβολή κυρώσεων.

Ωστόσο με το νέο Κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και την ελεύθερη κυκλοφορία των δεδομένων αυτών ,γίνεται κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων).

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων εγκρίθηκε και υιοθετήθηκε από την Ευρωπαϊκή Ένωση τον Απρίλιο του 2016. Ο Κανονισμός αποτελεί μια ισχυρότερη και εκσυγχρονισμένη εκδοχή της Οδηγίας του 1995 (Data Protection Directive 95/46/EC), με τη διαφορά ότι τώρα ο Κανονισμός έχει καθολική ισχύ στα κράτη μέλη, ορίζει αυστηρότερες απαιτήσεις και προβλέπει υψηλά πρόστιμα για τους παραβάτες.

Ο Κανονισμός στηρίζεται στο οικοδόμημα της Οδηγίας, αλλά εισάγει νέες καινοτομίες και δικαιώματα όπως το δικαίωμα στη λήθη και στη φορητότητα δεδομένων. Επιπλέον γίνεται προσθήκη νέων αρχών επεξεργασίας όπως της διαφάνειας, της λογοδοσίας, της ακεραιότητας και εμπιστευτικότητας.(Μήτρου ,2017)

Παράλληλα ενισχύονται οι υποχρεώσεις του υπευθύνου επεξεργασίας -λογοδοσία, γνωστοποίηση παραβιάσεων προσωπικών δεδομένων στην Εποπτική Αρχή- και στο υποκείμενο, η προστασία των δεδομένων γίνεται ήδη από το σχεδιασμό της επεξεργασίας και εξ'ορισμού: privacy by design/privacy by default, ενώ είναι υποχρεωτική η εκτίμηση αντικτύπου όταν η επεξεργασία ενέχει σοβαρούς κινδύνους για τα προσωπικά δεδομένα) . Με όλα τα παραπάνω ενισχύεται η νομική θέση των πολιτών ενώ με τη θέσπιση νέων δικαιωμάτων δίνεται η δυνατότητα ανάκλησης της συγκατάθεσης του υποκειμένου ενώ ταυτόχρονα επιβάλλονται νέες υποχρεώσεις στους υπεύθυνους επεξεργασίας και αυξάνονται οι υποχρεώσεις των εκτελούντων την επεξεργασία. (Κοτσαλής ,Μενουδάκος, 2018)

Επιπρόσθετα θεσπίζεται ο ρόλος του υπευθύνου προστασίας δεδομένων και πλέον είναι εφικτή η γνωστοποίηση παραβιάσεων δεδομένων. Ο νέος κανονισμός εξουσιοδοτεί τις εκάστοτε Αρχές Προστασίας Προσωπικών Δεδομένων στην Ευρώπη, να επιβάλουν για σοβαρές παραβάσεις πρόστιμα σε ύψος έως και 4% του ετήσιου παγκόσμιου κύκλου εργασιών του προηγούμενου οικονομικού έτους μιας επιχείρησης.(Παναγοπούλου,2017)

9.1.2.1 Εφαρμογή του Κανονισμού (ΕΕ) 2016/679 στο πλαίσιο του Διαδικτύου των Πραγμάτων

Ο Γενικός Κανονισμός Προστασίας Δεδομένων έχει δημιουργήσει μία καινούργια σελίδα στη διαχείριση και στην προστασία των προσωπικών δεδομένων. Η σημερινή δυνατότητα της άμεσης και καθολικής πληροφόρησης έρχεται σε σύγκρουση με το Κανονισμό που διαφυλάττει την ιδιωτικότητα και προστατεύει τα προσωπικά δεδομένα. Η εφαρμογή του Γενικού Κανονισμού Προστασίας δεδομένων προσφέρει πλούσια νομική βάση για τα ζητήματα που προκύπτουν από τις εφαρμογές του Διαδικτύου των Πραγμάτων. Αυτό που δεν είναι σαφές είναι ο τρόπος με τον οποίο οι οργανισμοί θα είναι σε θέση να επιτύχουν συμμόρφωση του IoT με το ΓΚΠΔ. Παρόλο που οι συμβουλές που προσφέρονται στις επιχειρήσεις σχετικά με τη γενικότερη συμμόρφωση με το Κανονισμό ισχύουν, η εφαρμογή τους σε ένα περιβάλλον IoT μπορεί να είναι μια πραγματική πρόκληση, εξαιτίας της ίδιας της φύσης των συσκευών IoT και της επεξεργασίας που καθιστά τα επιχειρηματικά μοντέλα IoT βιώσιμα.

Όπως έγινε αναφορά και στο προηγούμενο κεφάλαιο το άρθρο 5 του Κανονισμού αναφέρεται στις *«Αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα».* Μια αρχή που ισχύει είναι ότι τα δεδομένα συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς. Επιπρόσθετα ένα σημαντικό ζήτημα στο IoT είναι αυτό της συγκατάθεσης. Ο ΓΚΠΔ απαιτεί την συγκατάθεση των υποκειμένων για την επεξεργασία των δεδομένων τους , ωστόσο πολλές συσκευές IoT συνεπάγεται από το σχεδιασμό τους , απουσία της τυπικής διεπαφής του χρήστη με την οθόνη. Το γεγονός αυτό έρχεται σε σύγκρουση με το κανονισμό ο οποίος ορίζει στο άρθρο 6 ότι η επεξεργασία είναι σύννομη μόνο εάν και εφόσον το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς. Για παράδειγμα η περίπτωση ενός έξυπνου κουδουνιού πόρτας. Καθώς οι επισκέπτες ενός σπιτιού θα χτυπήσουν την κουδούνι, το τηλέφωνο

του ιδιοκτήτη του σπιτιού ειδοποιείται ώστε να μπορεί να ελέγξει ποιος βρίσκεται στην πόρτα μέσω video link .Ο κατασκευαστής των θυροτηλεφώνων με βίντεο μπορεί εύκολα να πάρει τη συγκατάθεση του ιδιοκτήτη του σπιτιού χρησιμοποιώντας την επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου (ή παρόμοια), αλλά δεν μπορεί να έχει την συγκατάθεση όλων των επισκεπτών των οποίων η εικόνα, δηλαδή τα δεδομένα, θα συλλεχθούν και θα υποβληθούν σε επεξεργασία - πιθανότατα μέσω cloud - και ίσως αποθηκευτούν εκεί. Ομοίως, σύμφωνα με το ΓΚΠΔ, η συγκατάθεση που απαιτείται δεν μπορεί να εφαρμοστεί σε πολλές περιπτώσεις IoT, λόγω της αφαίρεσης του δικαιώματος συγκατάθεσης.

Στο άρθρο 7 του Κανονισμού αναφορικά με τις προϋποθέσεις συγκατάθεσης ορίζει μεταξύ άλλων, ότι ο υπεύθυνος επεξεργασίας των προσωπικών δεδομένων φέρει το βάρος της αποδείξεως όσον αφορά την παροχή της συγκατάθεσης του προσώπου, του οποίου τα δεδομένα προσωπικού χαρακτήρα αποτελούν το αντικείμενο της προστασίας. Η δήλωση συγκατάθεσης του χρήστη για την επεξεργασία των προσωπικών του δεδομένων πρέπει να ναι διατυπωμένη εκ των προτέρων από τον υπεύθυνο επεξεργασίας σε απλή και κατανοητή γλώσσα, χωρίς καταχρηστικές ρήτρες. Ως εκ τούτου η συγκατάθεση του χρήστη θεωρείται πολύ σημαντική και δηλώνει ότι είναι επαρκώς ενημερωμένος σχετικά με την επεξεργασία των δεδομένων του.

Χαρακτηριστικά θα μπορούσαμε να αναφέρουμε μια εταιρεία ενοικίασης αυτοκινήτων εγκαθιστά μια έξυπνη συσκευή παρακολούθησης οχήματος στα ενοικιαζόμενα αυτοκίνητά της. Μολονότι η εταιρεία ενοικίασης αυτοκινήτων πρέπει να θεωρείται ο κάτοχος της συσκευής παρακολούθησης, το άτομο που ενοικιάζει το αυτοκίνητο χαρακτηρίζεται ο χρήστης της συσκευής. Σύμφωνα με το άρθρο 7 του Κανονισμού 679/2016, ο κατασκευαστής της συσκευής οφείλει να λάβει τη συγκατάθεση του χρήστη της συσκευής, εν προκειμένω του ατόμου που ενοικιάζει το αυτοκίνητο.

Ο χρήστης των συσκευών αυτών με βάση το νέο Κανονισμό έχει δικαιώματα προστασίας των προσωπικών του δεδομένων. Μεταξύ αυτών είναι το δικαίωμα να λαμβάνει ενημέρωση από τον υπεύθυνο επεξεργασίας σχετικά με την συλλογή και την επεξεργασία των προσωπικών του δεδομένων κατά τρόπο σαφή και ακριβή. Παράλληλα ο Κανονισμός προβλέπει διαδικασίες και μηχανισμούς για την άσκηση των δικαιωμάτων του προσώπου, στο οποίο αναφέρονται τα δεδομένα. Μεταξύ άλλων, προβλέπεται ότι εάν τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία με αυτοματοποιημένα μέσα, ο υπεύθυνος επεξεργασίας προβλέπει

μέσα για την υποβολή των αιτημάτων με ηλεκτρονικό τρόπο. Αυτό ακούγεται λογικό όσον αφορά την προστασία της ιδιωτικής ζωής των ατόμων, αλλά όταν πρόκειται για εφαρμογές IoT οποιασδήποτε κλίμακας, προκύπτουν προκλήσεις.

Το ζήτημα περί του δικαιώματος πρόσβασης του υποκειμένου στα δεδομένα του αναλύεται στο άρθρο 15,σύμφωνα με το οποίο *«το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει από τον υπεύθυνο επεξεργασίας επιβεβαίωση για το κατά πόσον ή όχι τα δεδομένα προσωπικού χαρακτήρα που το αφορούν υφίστανται επεξεργασία» και, εάν συμβαίνει τούτο έχει το δικαίωμα πρόσβασης σε πληροφορίες όπως α) τους σκοπούς της επεξεργασίας ,β) τις σχετικές κατηγορίες δεδομένων προσωπικού χαρακτήρα, γ)τους αποδέκτες ή τις κατηγορίες αποδεκτών στους οποίους κοινολογήθηκαν ή πρόκειται να κοινολογηθούν τα δεδομένα προσωπικού χαρακτήρα, δ)το χρονικό διάστημα για το οποίο θα αποθηκευτούν τα δεδομένα προσωπικού χαρακτήρα ή, όταν αυτό είναι αδύνατο, τα κριτήρια που καθορίζουν το εν λόγω διάστημα.»*

Σήμερα, οι τελικοί χρήστες σπάνια έχουν τη δυνατότητα πρόσβασης στα ακατέργαστα δεδομένα που καταχωρίζονται από συσκευές του IoT. Σαφώς, οι τελικοί χρήστες ενδιαφέρονται περισσότερο άμεσα για τα επεξεργασμένα δεδομένα παρά για τα ακατέργαστα δεδομένα τα οποία μπορεί και να μην είναι κατανοητά γι' αυτούς. Ωστόσο, η πρόσβαση σε τέτοιου είδους δεδομένα μπορεί να βοηθήσει τους τελικούς χρήστες να κατανοήσουν τα συμπεράσματα που μπορούν να συναγάγουν για τους ίδιους οι κατασκευαστές συσκευών με βάση τα δεδομένα αυτά.

Ένα πολύ σημαντικό άρθρο που παίζει καθοριστικό ρόλο είναι το άρθρο 17 που αναφέρεται στο δικαίωμα στη λήθη, στο δικαίωμα διαγραφής. Οποιοσδήποτε οργανισμός επεξεργάζεται προσωπικές πληροφορίες φυσικών προσώπων, πρέπει να μπορεί να διαθέσει αυτά τα δεδομένα στο αντίστοιχο υποκείμενο των δεδομένων εάν αυτά ζητηθούν από το ίδιο το υποκείμενο. Παράλληλα ο οργανισμός ή η εταιρεία που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα οφείλει να διαγράψει τα δεδομένα ενός υποκείμενου που αιτηθεί το «δικαίωμα της λήθης». Σύμφωνα με την παράγραφο 1 του άρθρου 17 *«το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή δεδομένων προσωπικού χαρακτήρα που το αφορούν χωρίς αδικαιολόγητη καθυστέρηση και ο υπεύθυνος επεξεργασίας υποχρεούται να διαγράψει δεδομένα προσωπικού χαρακτήρα χωρίς αδικαιολόγητη καθυστέρηση. Αποφεύγοντας την δημιουργία προφίλ του υποκειμένου τω δεδομένων.»* Είναι γεγονός ότι η συλλογή και επεξεργασία δεδομένων δύναται να συνθέσει ένα προφίλ του υποκειμένου των δεδομένων και,

ως εκ τούτου, το υποκείμενο των δεδομένων δέον είναι να έχει το δικαίωμα διαγραφής των στοιχείων του, καθώς αυτά δεν θα μπορούσε να θεωρηθεί ότι συντρέχουν στη διατήρηση της ιστορικής μνήμης ή την ελευθερία της πληροφορήσεως. Σε μία IoT συσκευή η οποία παραδείγματος χάριν γίνεται καταγραφή των χιλιομέτρων που περπάτησε ένας χρήστης ημερησίως , θα πρέπει να ορίζεται πως είναι δυνατή η διαγραφή αυτών των δεδομένων και από τη συσκευή και από τον πάροχο του cloud που επεξεργάζεται όλα αυτά τα δεδομένα.

Ένα ακόμη ζήτημα που προκύπτει στο IoT είναι αυτό της φορητότητας των δεδομένων. Η φορητότητα των δεδομένων συμφώνα με την παράγραφο 1 του άρθρου 20 αναφέρεται στο δικαίωμα «*να διαβιβάζει τα εν λόγω δεδομένα σε άλλον υπεύθυνο επεξεργασίας χωρίς αντίρρηση από τον υπεύθυνο επεξεργασίας στον οποίο παρασχέθηκαν τα δεδομένα προσωπικού χαρακτήρα, σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο* ». Έτσι, το πρόσωπο, στο οποίο αναφέρονται τα δεδομένα, δικαιούται, να λάβει αντίγραφο από τον υπεύθυνο επεξεργασίας, ο οποίος επιτρέπει την περαιτέρω χρήση και διαβίβαση σε άλλον των δεδομένων αυτών από το πρόσωπο στο οποίο αναφέρονται τα δεδομένα. Οι ενέργειες αυτές αποκτούν μάλιστα ακόμα μεγαλύτερη σημασία, αν ληφθεί υπόψη ότι σκοπός του επονομαζόμενου «δικαιώματος φορητότητας», είναι να σταματήσουν οριστικά οι καταστάσεις εγκλωβισμού και εξάρτησης των χρηστών από μία μόνο υπηρεσία. Σκοπός εν προκειμένω είναι η άρση των εμποδίων στον ανταγωνισμό και η στήριξη νέων παραγόντων ώστε να καινοτομήσουν σε αυτή την αγορά.[69]

Καθοριστικής σημασίας αποτελεί το άρθρο 25 που αναφέρεται στην προστασία των δεδομένων ήδη από τον σχεδιασμό ενός συστήματος ή μιας συσκευής. Οι απαιτήσεις απορρήτου και ασφάλειας θα πρέπει να ενσωματωθούν στην αρχική διαδικασία σχεδιασμού μιας συσκευής ή ενός δικτύου (privacy by design) με αποτέλεσμα η ιδιωτικότητα και η ασφάλεια των δεδομένων να είναι δυνατή σε συσκευές IoT. Δηλαδή οι κατασκευαστές συσκευών πρέπει να ακολουθούν διαδικασία ασφάλειας ήδη από το στάδιο του σχεδιασμού και να διαθέτουν ορισμένα εξαρτήματα για τα προκαταρκτικά συστήματα κρυπτογράφησης κλειδιού.

Επιπρόσθετα τα άρθρα 27 και 28 καθορίζουν του υπευθύνους επεξεργασίας. Το άρθρο 27 ορίζει εκπρόσωπους των υπεύθυνων επεξεργασίας ή αυτών που εκτελούν την επεξεργασία όταν δεν

[69] https://ec.europa.eu/info/law/law-topic/data-protection_en

είναι εγκατεστημένοι στην ευρωπαϊκή ένωση. Το άρθρο 28 αναφέρεται στην περίπτωση όπου η επεξεργασία πρόκειται να διενεργηθεί για λογαριασμό υπευθύνου επεξεργασίας, ο υπεύθυνος επεξεργασίας χρησιμοποιεί μόνο εκτελούντες την επεξεργασία που παρέχουν επαρκείς διαβεβαιώσεις για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων, κατά τρόπο ώστε η επεξεργασία να πληροί τις απαιτήσεις του παρόντος κανονισμού και να διασφαλίζεται η προστασία των δικαιωμάτων του υποκειμένου των δεδομένων.

Για παράδειγμα , μια εταιρεία Χ θέλει να καταγράφει τις ώρες που έρχονται και αποχωρούν οι εργαζόμενοι της .Οι εργαζόμενοι μέσω μιας ετικέτας RFID «δηλώνουν» πότε μπήκαν και πότε αποχώρησαν, ενώ σε περίπτωση που οι εργαζόμενοι παρατείνουν το ωράριο τους καταγράφονται οι υπερωρίες τους. Έτσι οι εργαζόμενοι μπορούν να αποκτήσουν πρόσβαση στα δεδομένα που καταγράφονται από τον μετρητή των ωρών εργασίας τους, για να βλέπουν τις επιπλέον ώρες που δούλεψαν. Οι συσκευές αυτές (rfid tags και readers) ανήκουν σε μία άλλη εταιρεία Ψ , η οποία διαθέτει επίσης πρόσβαση στα δεδομένα των πελατών της. Στο πλαίσιο αυτό, οι εργαζόμενοι πρέπει να θεωρούνται ως πρόσωπα στα οποία αναφέρονται τα δεδομένα- «υποκείμενα των δεδομένων» και πρέπει να τους χορηγείται πρόσβαση στον ατομικό λογαριασμό τους στην εφαρμογή της μέτρησης ωρών , ενώ η εταιρεία Χ θεωρείται ο «υπεύθυνος της επεξεργασίας. Ταυτόχρονα όμως η εταιρεία Ψ είναι «ο εκτελών την επεξεργασία» ,αφού συλλέγει και επεξεργάζεται τις ώρες των εργαζομένων.

Ιδιαιτέρα σημαντικό είναι το άρθρο 33 του Κανονισμού που αναφέρεται στη γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή . Στην ίδια κατεύθυνση το άρθρο 34 σχετίζεται με την ανακοίνωση παραβίασης των δεδομένων στο υποκείμενο των δεδομένων. *«Το υποκείμενο των δεδομένων έχει το δικαίωμα να γνωρίζει ότι παραβιάστηκαν τα δεδομένα του αποφεύγοντας καταστάσεις υψηλού κινδύνου όπως να θέσει σε κίνδυνο δικαιώματα και ελευθερίες φυσικών προσώπων.»* Τέλος τα άρθρα 37,38,39 ορίζουν τον υπεύθυνο προστασίας των δεδομένων και ποιες προϋποθέσεις πρέπει να πληροί ,τα καθήκοντα που πρέπει να αναλάβει και τη θέση του δηλαδή *«ότι συμμετέχει, δεόντως και εγκαίρως, σε όλα τα ζητήματα τα οποία σχετίζονται με την προστασία δεδομένων προσωπικού χαρακτήρα»*.

Τα προβλήματα που θα αντιμετωπίσουν οι κατασκευαστές-προμηθευτές IoT, στην περίπτωση που αγνοήσουν τις εφαρμογές ιδιωτικότητας και προστασίας προσωπικών δεδομένων είναι αρκετά και σε πολλές περιπτώσεις μπορεί γίνουν καταστροφικά. Συγκεκριμένα, με το νέο

Κανονισμό εισάγονται επιπλέον στάδια ελέγχου των υπευθύνων της επεξεργασίας και μεγαλύτερες εγγυήσεις προστασίας για τα προσωπικά δεδομένα. Καθιερώνεται και το δικαίωμα προσφυγής των υποκειμένων των δεδομένων, δηλαδή δικαίωμα καταγγελίας σε εποπτική αρχή, επιφυλασσόμενο το δικαίωμα δικαστικής προσφυγής κατά νομικά δεσμευτικής απόφασης εποπτικής αρχής που το αφορά. Ο Νέος Κανονισμός παρέχει στον χρήστη το δικαίωμα αποζημίωσης από τον υπεύθυνο της επεξεργασίας, εφόσον ζημιώθηκε από την επεξεργασία των δεδομένων κατά παράβαση των διατάξεων του Κανονισμού. Συνεπώς το IoT έρχεται σε σύγκρουση με τον Κανονισμό καθώς η βασική προϋπόθεση για τη λειτουργία του IoT είναι η προσβασιμότητα σε δεδομένα . Ωστόσο όμως η εφαρμογή του ΓΚΠΔ στο IoT θα επιβάλει αλλαγές που ήταν αναγκαίες ως προς τη διαφύλαξη των δεδομένων που συλλέγονται και επεξεργάζονται.

Ο Κανονισμός (ΕΕ) 2016/679 παρουσιάζει σοβαρές προκλήσεις για το Διαδίκτυο των Πραγμάτων, αλλά δεν είναι ανυπέρβλητες. Στην πραγματικότητα, ο ΓΚΠΔ ήρθε στην καλύτερη χρονική στιγμή για την εξέλιξη του IoT. Αυτή είναι μια τεράστια ευκαιρία για τους κατασκευαστές και τους φορείς εκμετάλλευσης δικτύων να συνεργαστούν για την οικοδόμηση της ιδιωτικότητας στον κόσμο του Διαδικτύου των Πραγμάτων.

9.1.3 Οδηγία 2002/58/ΕΚ όπως τροποποιήθηκε από την οδηγία 2009/136/ΕΚ.

Η οδηγία 2002/58/ΕΚ, γνωστή και ως e-Privacy Οδηγία ή Cookie Law, επικεντρώνεται στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών. Με άλλα λόγια, θέτει κάποιους περιορισμούς στους παρόχους τηλεπικοινωνιακών υπηρεσιών, σχετικά με την ανωνυμία των δεδομένων που διακινούνται. [70] Πιο συγκεκριμένα, η εν λόγω οδηγία αναφέρεται σε :

[70] Οδηγία 2002/58/εκ του Ευρωπαϊκού κοινοβουλίου και του συμβουλίου της 12ης Ιουλίου 2002 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες)

Ασφάλεια της επεξεργασίας

Ο πάροχος υπηρεσιών οφείλει να ορίζει εξουσιοδοτημένο προσωπικό για την πρόσβαση σε προσωπικά δεδομένα ηλεκτρονικών επικοινωνιών διατηρώντας πάντα την ασφάλεια των υπηρεσιών και ,προστατεύοντας τα δεδομένα προσωπικού χαρακτήρα από τυχαία καταστροφή, τυχαία απώλεια ή αλλοίωση και άλλες παράνομες επεξεργασίες. Ταυτόχρονα εξασφαλίζεται η εφαρμογή πολιτικής ασφάλειας, σε σχέση με την επεξεργασία προσωπικών δεδομένων.

Απόρρητο των επικοινωνιών

Τα κράτη μέλη οφείλουν να εγγυώνται το απόρρητο των επικοινωνιών, που πραγματοποιούνται μέσω δημόσιου δικτύου . Οφείλουν, ειδικότερα, να απαγορεύουν σε κάθε άλλο πρόσωπο εκτός των χρηστών την υποκλοπή, την αποθήκευση των επικοινωνιών και των δεδομένων κίνησης, χωρίς τη συγκατάθεση των ενδιαφερόμενων χρηστών, εκτός εάν το εν λόγω πρόσωπο είναι νομίμως εγκεκριμένο.[71]

Επεξεργασία δεδομένων κίνησης ή θέσης

Τα δεδομένα κίνησης που αφορούν συνδρομητές και χρήστες, τα οποία υποβάλλονται σε επεξεργασία και αποθηκεύονται από τον πάροχο δημόσιου δικτύου, πρέπει να απαλείφονται ή να καθίστανται ανώνυμα, όταν δεν είναι πλέον απαραίτητα Όσον αφορά τα δεδομένα θέσης, , αυτά είναι δυνατό να υποστούν επεξεργασία, μόνο όταν καθίστανται ανώνυμα ή με τη ρητή συγκατάθεση των χρηστών Επιπλέον στην οδηγία αναφέρεται το δικαίωμα της ανάκλησης της συγκατάθεσης, όσον αφορά την επεξεργασία δεδομένων, που σχετίζονται με την κίνηση ή τη θέση.

Cookies

Η οδηγία προβλέπει ότι οι χρήστες πρέπει να δίνουν τη συγκατάθεσή τους για την αποθήκευση πληροφοριών στον τερματικό εξοπλισμό τους ή για να επιτευχθεί η πρόσβαση σε τέτοιες πληροφορίες. Για τον σκοπό αυτόν, πρέπει να παρέχονται στους χρήστες σαφείς και ακριβείς πληροφορίες, για τους σκοπούς της αποθήκευσης ή της πρόσβασης.

[71] https://lawandtech.eu/2014/09/02/confidentiality-of-communications/

Επιπρόσθετα ,σύμφωνα με το άρθρο 5 παρ. 3 της Οδηγίας 2002/58/ ΕΚ, τα κράτη μέλη μεριμνούν, ώστε η αποθήκευση πληροφοριών ή η απόκτηση προσβάσεως σε ήδη αποθηκευμένες πληροφορίες στον τερματικό εξοπλισμό συνδρομητή ή χρήστη επιτρέπεται μόνον εάν ο συγκεκριμένος συνδρομητής ή χρήστης έχει δώσει τη συγκατάθεσή του με βάση σαφείς και εκτενείς πληροφορίες, σύμφωνα με την Οδηγία 95/46/ΕΚ, μεταξύ άλλων για το σκοπό της επεξεργασίας. Αυτό δεν εμποδίζει οποιαδήποτε τεχνικής φύσεως αποθήκευση ή πρόσβαση, αποκλειστικός σκοπός της οποίας είναι η διενέργεια της διαβιβάσεως μιας επικοινωνίας μέσω δικτύου ηλεκτρονικών επικοινωνιών ή που είναι απολύτως αναγκαία για να μπορεί ο πάροχος υπηρεσίας της κοινωνίας της πληροφορίας την οποία έχει ζητήσει ρητά ο συνδρομητής ή ο χρήστης να παρέχει τη συγκεκριμένη υπηρεσία. Το ζήτημα που ανακύπτει με τις συσκευές IoT είναι ότι ο χρήστης των συσκευών που συγκατατέθηκε στην επεξεργασία των δεδομένων του δεν είναι ο μόνος του οποίου τα δεδομένα επεξεργάζονται. Για παράδειγμα, μέσω των google glasses είναι δυνατή η βιντεοσκόπηση άλλων χρηστών χωρίς την προηγούμενη συγκατάθεσή τους. Η λήψη συγκαταθέσεως σε αυτές τις περιπτώσεις καθίσταται προβληματική. [72]

9.1.4 Γνωμοδότηση 2018/C 440/02 (INT/846) της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής (EESC)

Μία ενδιαφέρουσα γνωμοδότηση σχετικά με την εμπιστοσύνη, την ιδιωτικότητα και την ασφάλεια των καταναλωτών και των επιχειρήσεων στο Διαδίκτυο των πραγμάτων (Internet of Things) εξέδωσε η Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή (EESC).

Όπως αναφέρεται στη γνωμοδότηση η οποία υιοθετήθηκε από την ολομέλεια στις 19 Σεπτεμβρίου το 2018 , κατά τα τελευταία δεκαπέντε έτη η εμφάνιση του Διαδικτύου έχει επιφέρει αλλαγές σε όλους τους τομείς της καθημερινής ζωής, επηρεάζοντας τις διάφορες καταναλωτικές συνήθειες. Συγκεκριμένα προβλέπεται ότι εντός της επόμενης δεκαετίας η επανάσταση το Διαδικτύου των πραγμάτων θα επηρεάσει τους τομείς της ενέργειας, της γεωργίας και των μεταφορών, όπως επίσης και τους πιο παραδοσιακούς τομείς της οικονομίας και της κοινωνίας.

[72] Διαδίκτυο των πραγμάτων (Internet of Things-IoT): Αποικισμός της καθημερινής ζωής ή νέα τεχνολογική πρόκληση; Φ. ΠΑΝΑΓΟΠΟΥΛΟΥ-ΚΟΥΤΝΑΤΖΗ, ΔΙΜΕΕ 3/2014-Έτος 11ο

Οι τεράστιες νομικές προκλήσεις που αντιμετωπίζουν η ΕΕ και τα κράτη μέλη της μπορούν να εξηγηθούν από το γεγονός ότι πολλά από τα ειδικά χαρακτηριστικά του IoT (υψηλά επίπεδα πολυπλοκότητας και ισχυρή αλληλεξάρτηση, το στοιχείο της αυτονομίας, οι συνιστώσες της δημιουργίας και/ή επεξεργασίας δεδομένων και μια ανοιχτή διάσταση) διακρίνουν και άλλες αναδυόμενες ψηφιακές τεχνολογίες, όπως τα blockchain και το υπολογιστικό νέφος.[73]

Το IoT αποτελεί ένα πολυσύνθετο οικοσύστημα που επιτρέπει τη διασύνδεση συσκευών διαφορετικών κατασκευαστών, διανομέων ή παραγωγών λογισμικού, , ώστε να είναι δυνατή η αυτοματοποίηση όλων των διαφορετικών διαλειτουργικών διαδικασιών. Αυτό δημιουργεί δυσκολίες στην απόδοση ευθυνών σε περιπτώσεις μη συμμόρφωσης με τη νομοθεσία .

Από την πλευρά της, η Ευρωπαϊκή Ένωση προετοιμάζεται για να αντιμετωπίσει την ψηφιακή σύγκλιση και τις νέες προκλήσεις του IoT, ξεκινώντας από τη δρομολόγηση του σχεδίου «Η στρατηγική i2010 – Ευρωπαϊκή κοινωνία της πληροφορίας για την ανάπτυξη και την απασχόληση», μέχρι και το πρόσφατο Σχέδιο Δράσης IoT (βλ. έγγραφο «Η πρόοδος στο Διαδίκτυο των Πραγμάτων στην Ευρώπη», που αποτέλεσε μέρος της ανακοίνωσης του 2016 «Ψηφιοποίηση της ευρωπαϊκής βιομηχανίας. Τα πλήρη οφέλη από την ψηφιακή ενιαία αγορά»[74]

Η διασυνδεσιμότητα των συσκευών που χαρακτηρίζει το οικοσύστημα του IoT μπορεί να ενθαρρύνει τη διαμόρφωση παράνομων ή ανεπιθύμητων τεχνολογικών πρακτικών και να το μετατρέψει σε ένα περιβάλλον με δεδομένα εύκολα προσπελάσιμα και ταχύτατα διαδιδόμενα. Για τον λόγο αυτόν απαιτείται να εδραιωθεί με ολοκληρωμένο τρόπο η ασφάλεια, σε καθένα ξεχωριστά και σε όλα μαζί τα στοιχεία του συστήματος.

Οι εφαρμογές του IoT προσφέρουν ήδη οικονομικά και κοινωνικά οφέλη στο πλαίσιο της παγκοσμιοποίησης. Οι νομικές προκλήσεις που αντιμετωπίζουν η ΕΕ και τα κράτη μέλη της βασίζονται από το γεγονός ότι πολλά από τα ειδικά χαρακτηριστικά του IoT διακρίνουν και άλλες ψηφιακές τεχνολογίες, όπως τα blockchain, η εκτύπωση σε 3D και το υπολογιστικό νέφος.
Στην συγκεκριμένη γνωμοδότηση αναλύει μια νέα προσέγγιση όσον αφορά τις ευθύνες, με στόχο να διασφαλιστεί ότι τόσο οι καταναλωτές όσο και οι επιχειρήσεις που υιοθετούν εφαρμογές του

[73] Internet of Things: Ιδιωτικότητα και ασφάλεια καταναλωτών και επιχειρήσεων στο Διαδίκτυο των πραγμάτων https://www.lawspot.gr

[74] [74] https://www.lawspot.gr/nomika-nea/internet-things-idiotikotita-kai-asfaleia-katanaloton-kai-epiheiriseon-sto-diadiktyo-ton

IoT, προστατεύονται σε περιπτώσεις που προϊόντα με ενδεδειγμένες ρυθμίσεις μπορεί να αποδειχθούν ελαττωματικές ή μη ασφαλείς, λόγω συμβάντων ψηφιακής ασφάλειας ή λόγω μη εξουσιοδοτημένης αθέμιτης χρήσης (π.χ. από hackers).Το περιβάλλον αυτό πρέπει να δίνει τη δυνατότητα για πρόβλεψη, πρόληψη και προστασία από εκείνες τις αυτοματοποιημένες αποφάσεις που μπορεί παραβιάζουν τις ηθικές αξίες και τα παγκοσμίως αναγνωρισμένα ανθρώπινα δικαιώματα. Οι καταναλωτές πλέον ασκούν έλεγχο επί των προσωπικών τους δεδομένων βάσει του νέου Γενικού Κανονισμού για την Προστασία Δεδομένων (ΓΚΠΔ).Ο χρήστης μιας συσκευής πρέπει να ελέγχει τον τρόπο με τον οποίο γίνεται χρήση των δεδομένων που παράγει και το ποιος έχει τη δυνατότητα πρόσβασης σε αυτά, λαμβανομένου υπόψη ότι η ποικιλία των δεδομένων, καθώς και η συγκέντρωση και η σύνδεσή τους με άλλα δεδομένα, συνεπάγονται σοβαρό κίνδυνο για την ιδιωτικότητα στο οικοσύστημα του IoT. Οι νομικές εγγυήσεις θα πρέπει να διασφαλίζουν την απόλυτη δυνατότητα των χρηστών να ασκούν τα δικαιώματα τους και της προστασίας των δεδομένων τους προσωπικού χαρακτήρα χωρίς περιορισμό Παράλληλα πτυχές και επιπτώσεις της ιδιωτικότητας πρέπει να αξιολογούνται σε όλη τη διαδικασία σχεδιασμού και ανάπτυξης ενός συνδεδεμένου προϊόντος, Ως εκ τούτου, οι αρχές της προστασίας της ιδιωτικότητας εκ σχεδιασμού και της ιδιωτικότητας εξ ορισμού πρέπει να εφαρμόζονται με συνέπεια όσον αφορά το IoT.

Λαμβάνοντας υπόψη τα παραπάνω και με στόχο την επίτευξη ισορροπίας μεταξύ των διαφόρων ενδιαφερόμενων μερών, η **Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή εξέδωσε την παρακάτω γνωμοδότηση 2018/C 440/02 «Εμπιστοσύνη, ιδιωτικότητα και ασφάλεια των καταναλωτών και των επιχειρήσεων στο Διαδίκτυο των πραγμάτων»**[75] μεταξύ των οποίων προτείνει μία σειρά δράσεων μεταξύ των οποίων:

- Τη δημιουργία περιβαλλόντων δοκιμών (sand boxes) που θα αποσκοπούν όχι μόνο στην απλή δοκιμή τεχνολογιών, αλλά και στη δοκιμή κανονιστικών προτύπων.
- Τον ορισμό ιδρυμάτων και ανεξαρτήτων αρχών ως παράγοντες διευκόλυνσης και εποπτείας των έργων του IoT
- Προώθηση συμπράξεων και πλατφόρμων συνεργασίας δημόσιου και ιδιωτικού τομέα, με τη συμμετοχή της επιστημονικής κοινότητας, της βιομηχανίας και των καταναλωτών

[75] https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=OJ:C:2018:440:FULL&from=RO

- Προώθηση εκστρατειών ευαισθητοποίησης και εκπαιδευτικών προγραμμάτων για την ευκολότερη υιοθέτηση του IoT από τις επιχειρήσεις και τους καταναλωτές
- Αξιολόγηση από την Ευρωπαϊκή Επιτροπή της νομοθεσίας που συνδέεται με το IoT και, βελτίωση των ισχυόντων νομοθετικών πράξεων .[76]

Για να δείχνουν εμπιστοσύνη οι καταναλωτές πρέπει αφενός να τηρείται αυστηρά η σχετική νομοθεσία και αφετέρου να κοινοποιείται ότι ακολουθούνται βέλτιστες επιχειρηματικές πρακτικές όσον αφορά την ιδιωτικότητα και την ασφάλεια, ενώ είναι καθήκον των θεσμικών οργάνων η σύνδεσή τους με τις στρατηγικές εταιρικής κοινωνικής ευθύνης και τις κοινωνικά υπεύθυνες επενδύσεις. Ο κοινωνικός και οικονομικός αντίκτυπος του IoT θα είναι περισσότερο θετικός εφόσον συνδεθεί κατάλληλα με την ανάπτυξη κοινωνικών και περιβαλλοντικών πολιτικών στο πλαίσιο της συνεργατικής οικονομίας, της κυκλικής οικονομίας και της λειτουργικής οικονομίας.[77]

9.1.5 Ανακοίνωση COM/2007/0096 σχετικά με τη ραδιοσυχνική αναγνώριση (RFID) στην Ευρώπη

Η επιτροπή των ευρωπαϊκών κοινοτήτων εξέδωσε ανακοίνωση στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών, με θέμα : *Η ραδιοσυχνική αναγνώριση (RFID) στην Ευρώπη: βήματα προς την κατεύθυνση χάραξης πλαισίου πολιτικής {SEC(2007) 312}*.Με την συγκεκριμένη ανακοίνωση καθίστανται σαφείς οι τεχνικές προδιαγραφές, σύμφωνα με τις οποίες θα μπορούν οι χρήστες να αξιοποιούν την τεχνολογία RFID. Επιπλέον γίνεται αναφορά στην ανάγκη προστασίας της ιδιωτικής ζωής και παροχής ασφάλειας· την διαχείριση των βάσεων δεδομένων RFID που αφορούν τις ταυτότητες ,τη διάθεση ραδιοφάσματος, την καθιέρωση εναρμονισμένων διεθνών προτύπων, καθώς και τις ανησυχίες σχετικά με τις επιπτώσεις στην υγεία και το περιβάλλον.

[76] Trust, privacy and consumer security in the Internet of Things (IoT) (own-initiative opinion) https://www.eesc.europa.eu/el/node/59507?fbclid=IwAR28bSm9c9gZzskz_Q_F11CTKsXXhDsSeHOEWnBcZ_6wJNWHis6A8lnqdRM

[77] Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης C 440 - 61ο έτος -6 Δεκεμβρίου 2018 2018/C 440/02 Γνωμοδότηση της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής με θέμα «Εμπιστοσύνη, ιδιωτικότητα και ασφάλεια των καταναλωτών και των επιχειρήσεων στο Διαδίκτυο των πραγμάτων» (γνωμοδότηση πρωτοβουλίας)

[78]Ενώ παράλληλα στην παράγραφο 3.3 γίνεται ειδική αναφορά στη «***Διαχείριση των πόρων στο μελλοντικό «Ίντερνετ των πραγμάτων».***[79]

9.1.6 Η ομάδα εργασίας του άρθρου 29: Σχετικό Γνωμοδοτικό πλαίσιο

Η ομάδα εργασίας που συστάθηκε βάσει του άρθρου 29 της οδηγίας 95/46/ΕΚ προτείνει τις παρακάτω χρήσιμες σχετικές γνώμες , αναφορικά με την προστασία των δεδομένων σε εφαρμογές RFID και σε συσκευές IoT. Συγκεκριμένα :

<u>Γνώμη 5/2010:</u>

Σχετικά με την πρόταση του κλάδου για ένα πλαίσιο εκπόνησης εκτιμήσεων των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων για τις εφαρμογές RFID.[80]

Η γνώμη αυτή τονίζει την ανάγκη αναδείξεως και αξιολογήσεως των κινδύνων για την ιδιωτική ζωή που συνδέονται με μία εφαρμογή RFID από τον ίδιο τον φορέα εκμεταλλεύσεως RFID. Σύμφωνα με τη γνώμη της ομάδας εργασίας του άρθρου 29 το προτεινόμενο πλαίσιο ταξινομεί την εφαρμογή της αξιολόγησης κινδύνου, που πρέπει να εφαρμόζεται για την προστασία των δεδομένων στις εφαρμογές RFID σε τέσσερα δυνητικά επίπεδα :

- *«Επίπεδο 0»: εφαρμογές οι οποίες περιλαμβάνουν ουσιαστικά εφαρμογές RFID που δεν επεξεργάζονται δεδομένα προσωπικού χαρακτήρα και στις οποίες τις ετικέτες χειρίζονται μόνον Χρήστες, αποκλείονται από την εκπόνηση εκτιμήσεων επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων.*
- *«Επίπεδο 1»: εφαρμογές στις οποίες δεν πραγματοποιείται επεξεργασία δεδομένων προσωπικού*

---

[78] Αλεξανδροπούλου - Αιγυπτιάδου, Ε. - Μαυρίδης, Ι., Η προστασία των προσωπικών δεδομένων ενόψει της εφαρμογής της νέας τεχνολογίας της ταυτοποίησης με ραδιοσυχνότητες (R.F.I.D) - Νομική και τεχνολογική προσέγγιση, Αρμενόπουλος, τομ. 61, σελ. 493-504, 2007

[79] ***ΑΝΑΚΟΙΝΩΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΣΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ, ΤΟ ΣΥΜΒΟΥΛΙΟ, ΤΗΝ ΕΥΡΩΠΑΪΚΗ ΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΚΟΙΝΩΝΙΚΗ ΕΠΙΤΡΟΠΗ ΚΑΙ ΤΗΝ ΕΠΙΤΡΟΠΗ ΤΩΝ ΠΕΡΙΦΕΡΕΙΩΝ :Η ραδιοσυχνική αναγνώριση (RFID) στην Ευρώπη: βήματα προς την κατεύθυνση χάραξης πλαισίου πολιτικής***

https://eur-lex.europa.eu/legal content/EL/TXT/HTML/?uri=CELEX:52007DC0096&from=EL

[80] Βλ. Ομάδα Εργασίας Άρθρου 29, Γνώμη 5/2010, σχετικά με την πρόταση του κλάδου για ένα πλαίσιο εκπόνησης εκτιμήσεων των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων για τις εφαρμογές RFID.

χαρακτήρα, όμως τις ετικέτες φέρουν Φυσικά Πρόσωπα.

- *«Επίπεδο 2»: είναι εφαρμογές που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα, αλλά στις οποίες οι ίδιες οι ετικέτες δεν περιέχουν δεδομένα προσωπικού χαρακτήρα.*
- *«Επίπεδο 3»: είναι εφαρμογές στις οποίες οι ετικέτες περιέχουν δεδομένα προσωπικού χαρακτήρα.*[81]

Γνώμη 9/2011:

Σχετικά με την αναθεωρημένη πρόταση της βιομηχανίας για ένα πλαίσιο αξιολόγησης αντικτύπου και προστασίας δεδομένων για εφαρμογές RFID.

Η παρούσα γνώμη αντικατέστησε την γνώμη 5/2010, η οποία αναφέρει ότι εκτός από την αξιολόγηση κινδύνου (risk assessment) που πρέπει να εφαρμόζεται για την προστασία των δεδομένων στις εφαρμογές RFID και αναλύεται σε τέσσερα επίπεδα , θα πρέπει να εφαρμόζεται μια φάση προ-αξιολόγησης που ταξινομεί μια εφαρμογή RFID σύμφωνα με μια κλίμακα 4 επιπέδων, με βάση ένα δέντρο απόφασης (decision tree).

Γνώμη 13/2011:

Σχετικά με τις υπηρεσίες εντοπισμού γεωγραφικής θέσης που παρέχονται μέσω έξυπνων κινητών συσκευών. [82]

Η συγκεκριμένη γνώμη, διακρίνει τους υπεύθυνους επεξεργασίας δεδομένων:

- σε υπεύθυνους των υποδομών εντοπισμού γεωγραφικής θέσεως
- σε παρόχους εφαρμογών και υπηρεσιών εντοπισμού γεωγραφικής θέσεως
- σε σχεδιαστές λειτουργικών συστημάτων έξυπνων κινητών συσκευών

Παράλληλα στην εν λόγω Γνώμη θεσπίζονται οι θεμιτοί λόγοι επεξεργασίας, βασισμένων στην έγκυρη συγκατάθεση. Η συγκατάθεση πρέπει να αφορά στον εκάστοτε συγκεκριμένο σκοπό επεξεργασίας των δεδομένων από τον υπεύθυνο της επεξεργασίας, όπως για παράδειγμα την κατάρτιση προφίλ. Σε περίπτωση που οι σκοποί της επεξεργασίας τροποποιηθούν κατά τρόπο ουσιώδη, ο υπεύθυνος της επεξεργασίας πρέπει να ζητήσει την εκ νέου συγκατάθεση. Τέλος τονίζεται ότι κατά την αγορά της συσκευής, οι υπηρεσίες εντοπισμού θέσεως πρέπει να είναι απενεργοποιημένες.

---

[81] https://docplayer.gr/7334775-Oma-a-ergasias-toy-arthroy-29-gia-tin-prostasia-ton-e-omenon.html

[82] Βλ. Ομάδα Εργασίας Άρθρου 29, Γνώμη 13/2011 σχετικά με τις υπηρεσίες εντοπισμού γεωγραφικής θέσης που παρέχονται μέσω έξυπνων κινητών συσκευών

Γνώμη 12/2011:

Σχετικά για την προστασία των δεδομένων σχετικά με τα ευφυή συστήματα μέτρησης

Η σχετική Γνώμη αναφέρει ότι τα ευφυή συστήματα μέτρησης ενδέχεται να επεξεργάζονται δεδομένα με πολλούς και καινοτόμους τρόπους επεξεργασίας. Τονίζεται ότι ανεξάρτητα από το είδος της επεξεργασίας που υπόκεινται τα δεδομένα, πρέπει να προσδιορίζονται με σαφήνεια οι υπεύθυνοι της επεξεργασίας δεδομένων και οι υποχρεώσεις τους. Επιπλέον επισημαίνεται η προστασία της ιδιωτικής ζωής ήδη από τον σχεδιασμό και η προστασία της ασφάλειας και των δικαιωμάτων των υποκειμένων των δεδομένων. Τα υποκείμενα των δεδομένων πρέπει να είναι ενημερωμένα σχετικά με την επεξεργασία των δεδομένων τους και να έχουν επίγνωση των θεμελιωδών διαφορών στον τρόπο επεξεργασίας των δεδομένων τους, έτσι ώστε να διασφαλίζεται η εγκυρότητα της συγκαταθέσεώς τους κάθε φορά.[83]

Γνώμη 02/2013:

Σχετικά για τις εφαρμογές των έξυπνων συσκευών.

Σύμφωνα με την εν λόγω Γνώμη, η οποία εφαρμόζεται απόλυτα στην περίπτωση του IoT, ο πολύπλοκος χαρακτήρας του οικοσυστήματος εφαρμογών, η δυνατότητα πρόσβασης σε δεδομένα που αποθηκεύονται σε κινητές συσκευές και η έλλειψη νομικής ευαισθητοποίησης των σχεδιαστών των εφαρμογών δημιουργούν ορισμένους σοβαρούς κινδύνους όσον αφορά την προστασία των δεδομένων των χρηστών εφαρμογών. Οι κίνδυνοι αυτοί κυμαίνονται από έλλειψη διαφάνειας μέχρι ανεπαρκή μέτρα ασφαλείας, έλλειψη συγκατάθεσης και ελαστικότητα των σκοπών επεξεργασίας των δεδομένων. Η Γνώμη θέτει πολλές υποχρεώσεις στους σχεδιαστές των εν λόγω συσκευών, οι οποίοι, μεταξύ άλλων, οφείλουν

α) να γνωρίζουν και να συμμορφώνονται με τις υποχρεώσεις που υπέχουν ως υπεύθυνοι επεξεργασίας, όταν επεξεργάζονται δεδομένα που έχουν λάβει από ή που αφορούν τους τελικούς χρήστες και όταν συνεργάζονται με εκτελούντες επεξεργασία δεδομένων,

β) να ζητούν συγκατάθεση προτού η εφαρμογή αρχίσει να ανακτά ή να τοποθετεί πληροφορίες στη συσκευή, και για κάθε κατηγορία δεδομένων, στην οποία θα αποκτήσει πρόσβαση η εφαρμογή,

[83] Βλ. Ομάδα Εργασίας Άρθρου 29, Γνώμη 12/2011 σχετικά με τα ευφυή συστήματα μέτρησης

γ) να έχουν επίγνωση του ότι η συγκατάθεση δεν νομιμοποιεί την υπερβολική ή δυσανάλογη επεξεργασία δεδομένων·

δ) να γνωστοποιούν κατά τρόπο συγκεκριμένο και κατανοητό τους σκοπούς της επεξεργασίας δεδομένων πριν από την εγκατάσταση της εφαρμογής και να επιτρέπουν στους χρήστες την ανάκληση της συγκατάθεσή τους

ε) να τηρούν την αρχή της ελαχιστοποιήσεως δεδομένων και να συλλέγουν μόνο τα δεδομένα που είναι απολύτως απαραίτητα για την εκτέλεση της επιθυμητής λειτουργικής δυνατότητας

στ) να λαμβάνουν τα αναγκαία οργανωτικά και τεχνικά μέτρα προκειμένου να εξασφαλίζουν την προστασία των δεδομένων προσωπικού χαρακτήρα που επεξεργάζονται

ζ) να παρέχουν ευανάγνωστη, κατανοητή και ευχερώς προσπελάσιμη πολιτική προστασίας της ιδιωτικής ζωής (πολιτική απορρήτου)

η) να επιτρέπεται στους χρήστες των εφαρμογών να ασκούν τα δικαιώματα τους

θ) να καθορίζεται ο χρόνος διατηρήσεως των δεδομένων που συλλέγονται [84]

Γνώμη 04/2013:

Σχετικά με το υπόδειγμα για την εκτίμηση των επιπτώσεων της προστασίας δεδομένων όσον αφορά τα ευφυή δίκτυα και τα ευφυή συστήματα μέτρησης .

Η Γνώμη τονίζει την ανάγκη εκτενέστερης καθοδηγήσεως όσον αφορά την επιλογή νομικής βάσεως για την επεξεργασία και την επιλογή που πρέπει να διαθέτουν τα πρόσωπα, στα οποία αναφέρονται τα δεδομένα. Ειδικότερα, θα πρέπει να υπάρχει σαφής καθοδήγηση σχετικά με το τι μπορεί να γίνει χωρίς συγκατάθεση του χρήστη και το τι απαιτεί συγκατάθεση του χρήστη. Ιδιαίτερη προσοχή πρέπει να δοθεί στην εφαρμογή εξ αποστάσεως διακοπής και μεμονωμένων ενδείξεων. Επισημαίνεται ότι για να είναι έγκυρη η συγκατάθεση, οι καταναλωτές πρέπει να κατανοούν τι θα συμβεί στα δεδομένα τους. Είναι ιδιαίτερα σημαντικό, σε περίπτωση αναλύσεως των χαρακτηριστικών, να έχουν το δικαίωμα να γνωρίζουν τα ατομικά χαρακτηριστικά τους και τη λογική τυχόν αλγορίθμων που χρησιμοποιούνται για τη συγκέντρωση δεδομένων. Οι

[84] Διαδίκτυο των πραγμάτων (Internet of Things-IoT): Αποικισμός της καθημερινής ζωής ή νέα τεχνολογική πρόκληση; Φ. ΠΑΝΑΓΟΠΟΥΛΟΥ-ΚΟΥΤΝΑΤΖΗ, ΔΙΜΜΕ 3/2014-Έτος 11ο

πληροφορίες για τις εξ αποστάσεως λειτουργίες διακοπής/επαναλήψεως είναι εξίσου σημαντικές: οι πελάτες πρέπει να γνωρίζουν ποια περιστατικά μπορούν να οδηγήσουν σε διακοπή.[85]

Γνώμη 07/2013:

Η οποία είναι η αναθεώρηση της γνώμης 04/2013 στην οποία τονίζεται ότι πρέπει να εφαρμοστούν μηχανισμοί, ώστε να διασφαλίζεται ότι, εξ ορισμού, υποβάλλονται σε επεξεργασία μόνον εκείνα τα δεδομένα προσωπικού χαρακτήρα, τα οποία είναι αναγκαία για κάθε συγκεκριμένο σκοπό επεξεργασίας και ότι τα εν λόγω δεδομένα δεν συλλέγονται ούτε διατηρούνται πέραν του ελάχιστου απαραίτητου ορίου για τους σκοπούς αυτούς, από την άποψη τόσο της ποσότητας των δεδομένων όσο και του χρόνου της αποθηκεύσεώς τους.[86]

Γνώμη 8/2014:

Σχετικά με τις πρόσφατες εξελίξεις στο διαδίκτυο των πραγμάτων

Η σχετική γνώμη αναλύθηκε εκτενώς ανωτέρω.

[85] https://ec.europa.eu/justice/article-29/documentation/opinion recommendation/files/2013/wp205_en.pdf

[86] Διαδίκτυο των πραγμάτων (Internet of Things-IoT): Αποικισμός της καθημερινής ζωής ή νέα τεχνολογική πρόκληση; Φ. ΠΑΝΑΓΟΠΟΥΛΟΥ-ΚΟΥΤΝΑΤΖΗ, ΔΙΜΜΕ 3/2014-Έτος 11ο

9.2 Νομικό Πλαίσιο στην Ελλάδα

Νόμος 2472/1997

Προστασία του Ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Το πρώτο μεγάλο βήμα της Ε.Ε προς της κατεύθυνση της προστασίας των προσωπικών δεδομένων ήταν η Οδηγία 95/46/ΕΚ, η οποία ενσωματώθηκε στην ελληνική έννομη τάξη με τον Ν. 2472/1997 που αφορά στην προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Ο νόμος Ν. 2472/1997 έχει ισχύ και σήμερα. Αντικείμενο του νόμου είναι η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα, ενώ ο σκοπός του είναι η προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και της ιδιωτικής ζωής. Ακόμη, πρόκειται για το νόμο που συγκρότησε την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και τις έδωσε αυξημένες αρμοδιότητες και δικαιώματα. Το IoT εμπίπτει στο προστατευτικό πεδίο της Οδηγίας όταν τα δεδομένα αναφέρονται και μπορούν να οδηγήσουν στην ταυτοποίηση ενός φυσικού προσώπου. Το άρθρο 4 του Νόμου περί προσωπικών δεδομένων, προβλέπει ότι τα δεδομένα που επεξεργάζονται πρέπει να είναι να είναι κατάλληλα, συναφή, ακριβή και πρόσφορα και όχι υπερβολικά σε σχέση με τους σκοπούς για τους οποίους συλλέγονται και υφίστανται επεξεργασία.[87] Επιπρόσθετα το άρθρο 10 του Νόμου επικεντρώνεται στο απόρρητο και την ασφάλεια της επεξεργασίας, ενώ το άρθρο 8 αναλύει την διασύνδεση των αρχείων ,προσδιορίζοντας :

α) Τον σκοπό για τον οποίο η διασύνδεση θεωρείται αναγκαία.

β) Το είδος των δεδομένων προσωπικού χαρακτήρα που αφορά η διασύνδεση.

γ) Το χρονικό διάστημα για το οποίο επιτρέπεται η διασύνδεση.

δ) Τους τυχόν όρους και προϋποθέσεις για την αποτελεσματικότερη προστασία των δικαιωμάτων και ελευθεριών και ιδίως του δικαιώματος ιδιωτικής ζωής των υποκειμένων ή τρίτων.[88]

Νόμος 3471/2006

Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του Ν. 2472/97

[87] Νόμος 2472/1997 Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα

[88] Άρθρο 8 του 2472/97 περί διασύνδεσης αρχείων.

Η διαδικασία επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και η ιδιωτικότητα των ηλεκτρονικών τηλεπικοινωνιών περιέχεται στην η οδηγία 2002/58/EC, γνωστή και ως e-Privacy Directive ή Cookie Law, η οποία ενσωματώθηκε στην ελληνική έννομη τάξη με τον Ν. 3471/2006.

Ο νόμος αυτός έχει πεδίο εφαρμογής την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τη διασφάλιση του απορρήτου των διαθέσιμων, στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, σε δημόσια δίκτυα. Σχετικά με την προστασία του απορρήτου, απαγορεύει την ακρόαση, την υποκλοπή, την αποθήκευση ή παρακολούθηση των επικοινωνιών από άλλα πρόσωπα πλην των χρηστών, χωρίς τη συγκατάθεσή τους. Απαγορεύει επίσης την εγκατάσταση κατασκοπευτικών λογισμικών (spyware) και κρυφών αναγνωριστικών στοιχείων. Αναφορικά με τα δεδομένα κίνησης/θέσης, υποχρεώνει τους παρόχους στη διαγραφή ή ανωνυμοποίησή τους, μετά την εκπλήρωση του σκοπού επεξεργασίας. Τέλος, οι φορείς παροχής υπηρεσιών και δικτύου ηλεκτρονικών επικοινωνιών (ISPs), υποχρεώνονται να λαμβάνουν ενδεδειγμένα προς τον κίνδυνο τεχνικά και οργανωτικά μέτρα ασφαλείας, με παράλληλη ενημέρωση των συνδρομητών.[89]

Νόμος 3917/2011

Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις.

Με το νόμο 3917/2011 ενσωματώθηκε στην έννομη τάξη της Ελλάδας η Οδηγία 2006/24/ΕΚ για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία, σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών. Ο νόμος αυτός αφορά όλους τους Παρόχους διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιου δικτύου επικοινωνιών. Οι συγκεκριμένοι πάροχοι οφείλουν να διατηρούν για συγκεκριμένο χρονικό διάστημα τα δεδομένα του άρθρου 5 του

[89] Νόμος 3471/2006 Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών

προαναφερθέντος νόμου, που παράγονται ή υποβάλλονται σε επεξεργασία από αυτούς, προκειμένου τα δεδομένα αυτά να καθίστανται διαθέσιμα στις αρμόδιες αρχές για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων (τα εγκλήματα αυτά ορίζονται περιοριστικά στο άρθρο 4 του ν. 2225/1994). Το άρθρο 7 του συγκεκριμένου νόμου παρουσιάζει ιδιαίτερο ενδιαφέρον καθώς αναφέρεται στις υποχρεώσεις των Παρόχων για την προστασία και την ασφάλεια των δεδομένων καθ΄ όλη τη διάρκεια της διατήρησής τους. Έτσι, χωρίς να θίγονται οι διατάξεις για την προστασία των προσωπικών δεδομένων και του απορρήτου της επικοινωνίας, πρέπει να ακολουθούνται οι ακόλουθες αρχές ασφαλείας:

α) Τα διατηρούμενα δεδομένα πρέπει να είναι της ίδιας ποιότητας και να έχουν την ίδια προστασία και ασφάλεια με τα δεδομένα που περιέχει το δίκτυο.

β) Θα πρέπει να λαμβάνονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας των δεδομένων κατά τυχαίας ή παράνομης καταστροφής τους ή τυχαίας απώλειας, αλλοίωσης, μη εξουσιοδοτημένης ή παράνομης αποθήκευσης, επεξεργασίας, πρόσβασης ή αποκάλυψης.

γ) Θα πρέπει να λαμβάνονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλισθεί ότι στα δεδομένα έχει πρόσβαση μόνον ειδικά εξουσιοδοτημένο προσωπικό.[90]

[90] https://www.itsecuritypro.gr/diatirisi-ton-dedomenon-ton-ilektronikon-epikinonion-ti-lei-o-n-39172011/

ΣΥΜΠΕΡΑΣΜΑΤΑ

Το Διαδίκτυο των πραγμάτων (IoT) έχει αναδειχθεί ως η πιο σύγχρονη και έξυπνη τεχνολογία με εφαρμογές σε πολλούς τομείς. Το Internet of Things είναι μία έννοια που αφορά τα αντικείμενα της καθημερινότητας μας ,όπως βιομηχανικές μηχανές και wearable συσκευές που χρησιμοποιούν ενσωματωμένους αισθητήρες για τη συλλογή δεδομένων και την ανάληψη κάποιας δράσης σε αυτά μέσα σε ένα δίκτυο. Κάπως έτσι λειτουργεί ένα έξυπνο σπίτι που χρησιμοποιεί αισθητήρες (sensors) για την αυτόματη ρύθμιση της θέρμανσης ή του φωτισμού. Με απλά λόγια το Internet of Things είναι το τεχνολογικό μέλλον που θα κάνει τη ζωή μας πιο εύκολη.

Ωστόσο παρά τα πολλά πλεονεκτήματα του διαδικτύου των πραγμάτων στις ζωές των ανθρώπων, αναδύονται στην επιφάνεια πολλοί κίνδυνοι και προκλήσεις ως αναφορά την προστασία των προσωπικών δεδομένων των χρηστών. Ο τεράστιος όγκος δεδομένων που θα δημιουργείται από τον συνεχώς αυξανόμενο αριθμό συνδεδεμένων συσκευών θα αποτελεί πιθανότατα μία από τις βασικότερες μεθόδους αποκόμισης κερδών από το IoT, αλλά και μία από τις βασικότερες ανησυχίες ως προς την ασφάλεια των χρηστών και την προστασία των δεδομένων τους.

Δυστυχώς λόγω ευπαθειών των IoT συσκευών · όπως κενά ασφαλείας στο υλικό, ελλιπώς σχεδιασμένα λογισμικά με μια σειρά από τρωτά σημεία, προεπιλεγμένοι κωδικοί πρόσβασης ,αδυναμία υποστήριξης νέων πρωτοκόλλων ασφαλείας ,σφάλματα σχεδίασης ή και ελλείψεων από τους κατασκευαστές τους -προκειμένου να κρατηθεί το κόστος χαμηλά- , η ασφάλεια των δεδομένων των χρηστών τίθεται σε κίνδυνο.

Κακόβουλοι χρήστες εκμεταλλεύονται τις αδυναμίες των συστημάτων και μπορούν πολύ εύκολα να διεισδύσουν και να υποκλέψουν προσωπικές πληροφορίες των χρηστών. Επιπλέον ένας ακόμη σοβαρός κίνδυνος ,σχετίζεται με τους φορείς παροχής υπηρεσιών του διαδικτύου των πραγμάτων. Οι ίδιοι μπορούν να αποκτήσουν πρόσβαση σε μεγάλο πλήθος δεδομένων των χρηστών , καθώς οι περισσότεροι δεν τίθενται υπό έλεγχο, με αποτέλεσμα να μπορούν να διεισδύουν σε οποιαδήποτε πληροφορία αφορά τους χρήστες .

Η ασφάλεια έχει τελικά αναγνωριστεί ως η βασική απαίτηση για όλους τους τύπους συστημάτων πληροφορικής, συμπεριλαμβανομένων των συστημάτων IoT. Τα προβλήματα ασφάλειας του

IoT σε συνδυασμό με την έλλειψη ενημέρωσης των χρηστών υποδαυλίζουν την ιδιωτικότητα και το απόρρητο.

Το απόρρητο σχετίζεται με την ασφάλεια, αλλά απαιτεί συγκεκριμένα μέτρα στα επίπεδα εφαρμογής, δικτύου και συσκευών. Όχι μόνο τα δεδομένα των χρηστών πρέπει να προστατεύονται από την απροκάλυπτη κλοπή, αλλά το δίκτυο πρέπει να σχεδιαστεί έτσι ώστε να μην μπορούν εύκολα να χρησιμοποιηθούν τα προσωπικά δεδομένα για την επεξεργασία και εξαγωγή περισσότερων και αναλυτικότερων δεδομένων. Οι απλοί χρήστες δεν έχουν αντιληφθεί την σοβαρότητα των κινδύνων που διατρέχουν. Άλλωστε αυτό φαίνεται και από την ευκολία που οι περισσότεροι χρήστες αναρτούν στα κοινωνικά μέσα, ευαίσθητες πληροφορίες, όπως τηλέφωνα, διευθύνσεις και προσωπικές στιγμές με τις οικογένειες τους. Οι επιστήμονες όμως της πληροφορικής προειδοποιούν για την ανάγκη αύξησης της ασφάλειας των συστημάτων που μπορούν να συνδέονται στο IoT ,καθώς οι χρήστες των IoT συστημάτων θα είναι οι στόχοι των επίδοξων εισβολέων.

Γενικότερα, η εκτεταμένη συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα από τις IoT συσκευές κρύβει πολλούς κίνδυνους. Οι περιπτώσεις παραβιάσεων της ιδιωτικότητας είναι πάρα πολλές , με αποτέλεσμα να οδηγούμαστε σε κοινωνίες συνεχούς παρακολούθησης. Τα δεδομένα που συλλέγονται, ακόμη και αν δεν είναι προσωπικού χαρακτήρα ,μπορούν να σκιαγραφήσουν ένα χρήστη ,δημιουργώντας ένα προφίλ για αυτόν .Δεδομένα κίνησης, θέσης , επιλογών του χρήστη, είναι ικανά σε συνδυασμό μαζί να ταυτοποιήσουν και να εντοπίσουν ένα φυσικό πρόσωπο. Οι χρήστες χωρίς να το γνωρίζουν ,μπορούν να πέσουν θύματα της επεξεργασίας των δεδομένων τους σε τέτοιο βαθμό , ώστε οι πληροφορίες που παράγονται από την επεξεργασία των δεδομένων τους ,να χρησιμοποιηθούν για δευτερεύοντες σκοπούς ,πέρα του αρχικού σκοπού της συλλογής και επεξεργασίας τους. Παράλληλα ,οι ίδιοι πρέπει να είναι ενήμεροι για την συλλογή και επεξεργασία των δεδομένων τους ,γνωρίζοντας το σκοπό και το χρονικό διάστημα της επεξεργασίας ,έχοντας δώσει πρώτα φυσικά τη ρητή συγκατάθεση τους.

Επομένως με βάση τα ανωτέρω , οι κατασκευαστές και οι φορείς παροχής υπηρεσιών του διαδικτύου των πραγμάτων, οφείλουν να λαμβάνουν τεχνικά και οργανωτικά μέτρα για την εύρυθμη λειτουργία των IoT συσκευών, προστατεύοντας έτσι την ιδιωτικότητα των χρηστών. Βάσει της Ευρωπαϊκής νομοθεσίας που ορίζει κανόνες για τη σωστή χρήση και επεξεργασία των προσωπικών δεδομένων στο Διαδίκτυο των Πραγμάτων ,θεσπίζεται η τήρηση της ιδιωτικότητας σε αυτές τις συσκευές. Ωστόσο οι χρήστες των IoT συστημάτων, θα πρέπει να είναι ιδιαίτερα

προσεκτικοί με τα δεδομένα που διαθέτουν για επεξεργασία και να γνωρίζουν πολύ καλά τα δικαιώματά τους σχετικά με την παράνομη συλλογή και επεξεργασία των δεδομένων τους. Όπως είδαμε και στο 7ο κεφάλαιο σχετικά με τις Smart Cities , στις περισσότερες, δεν έχουν ληφθεί μέτρα προώθησης της υπεύθυνης χρήσης των δεδομένων. Ήδη οι πρώτες IoT συσκευές έχουν αντιμετωπίσει περιστατικά διαρροής και απώλειας δεδομένων εξαιτίας των τρωτών τους σημείων, θέτοντας σε κίνδυνο την ιδιωτικότητα. Συνεπώς είναι επιτακτική η ανάγκη ενημέρωσης των IoT συστημάτων με ειδικούς κατάλληλους μηχανισμούς ασφαλείας.

Τέλος οι Ευρωπαϊκές Αρχές Προστασίας Δεδομένων οφείλουν να ελέγχουν πιο αυστηρά τους κατασκευαστές και τους φορείς των υπηρεσιών του Διαδικτύου των Πραγμάτων ως προς την τήρηση της νομιμότητας της επεξεργασίας των δεδομένων που συλλέγονται από τις συσκευές. Η εφαρμογή του νέου Γενικού Κανονισμού για την προστασία των προσωπικών δεδομένων ,αν και καλύπτει σχεδόν στο μέγιστο την ασφάλεια των Προσωπικών Δεδομένων από την παράνομη επεξεργασία τους , δεν είναι δυνατόν να συμβαδίζει με τις νέες μορφές της τεχνολογίας, η οποία αλλάζει σε τόσο μικρό χρονικό διάστημα.

Συμπερασματικά ο όρος του Διαδικτύου των Πραγμάτων δεν αναφέρεται μόνο στη διασύνδεση των συσκευών, αλλά στην πραγματικότητα το IoT είναι κάτι πολύ περισσότερο από συσκευές που συνδέονται μέσω έξυπνων δικτύων. Υπάρχουν σοβαρές ανησυχίες σχετικά με την ασφάλεια των πληροφοριών που ανταλλάσσονται κατά τη σύνδεση, καθώς η δημιουργία όλο και περισσότερων νέων σημείων πρόσβασης, αυξάνει τα σημεία επίθεσης. Οι προκλήσεις που δημιουργούνται στο πλαίσιο της ανάπτυξης των τεχνολογιών IoT είναι σαφώς πολλές αλλά και σύνθετες . Το ζητούμενο σε κάθε περίπτωση είναι η τήρηση πρωτοκόλλων ασφαλείας για την προστασία των προσωπικών δεδομένων και η τήρηση των νομικών πλαισίων από τους κατασκευαστές των IoT συσκευών, εξασφαλίζοντας τα δικαιώματα των χρηστών ,επιτρέποντας φυσικά την επέκταση του Διαδικτύου των Πραγμάτων στις ζωές μας.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- Angelakis, V., Tragos, E., Pohls, H., Kapovits, A., & Bassi, A. (2017). Designing, Developing, and Facilitating Smart Cities: Urban Design to IoT Solutions. Switzerland: Springer
- Barrie Sosinsky, (2011), Cloud Computing Bible, Wiley Publishing
- Behmann, F. & Wu, K. (2015). Collaborative Internet of Things (C-IoT). For Future Smart Connected Life and Business. U.K.: John Wiley & Sons Ltd.
- BK Tripathy, J Anuradha, (2018). Internet of Things (IoT): Technologies, Applications, Challenges and Solutions, U.S.A.: CRC Press, Taylor & Francis.
- Bolic M., Simplot-Ryl D., & Stojmenovic I. (2010). RFID Systems. Research Trends and Challenges. U.K.: John Wiley & Sons.
- Boo, Y., Stirling, D., Chi, L., Liu, L., Ong, K. & Williams, G. (2017). Data Mining. Singapore: Springer
- Chen, M., & Chen, S. (2016). RFID Technologies for Internet of Things. Switzerland: Springer International Publishing AG.
- Duffy Marsan C., (2015) "IAB Releases Guidelines for Internet-of-Things Developers." IETF Journal 11.1, Internet Engineering Task Force.
- Finkenzeller, K., & Müller, D. (2010). RFID Handbook. Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication. U.K.: John Wiley & Sons, Ltd.
- Fox, R., & Hao, W. (2018). Internet Infrastructure_ Networking, Web Services, and Cloud Computing. U.S.A.: CRC Press
- Kale, V. (2018). Creating Smart Enterprises. Leveraging Cloud, Big Data, Web, Social Media, Mobile and IoT Technologies. N.Y.: CRC Press.
- Khattab, A., Jeddi, Z., Amini, E., & Bayoumi, M. (2017). RFID Security. A Lightweight Paradigm. U.S.A.: Springer International Publishing.
- Konstantinou, & Spanos, 2015, Materializing the Web of Linked Data, Springer
- Li, S., & Xu, L. (2017). Securing the Internet of Things. U.S.A.: Syngress

- Liu, A., Li, K., Shahzad, M., & Liu, X. (2017). RFID Protocol Design, Optimization and Security for the Internet of Things. U.K.: CPI Group.
- Macaulay, T. (2017). RIoT Control. Understanding and Managing Risks and the Internet of Things. U.K.: Morgan Kaufmann.
- Mavromoustakis, C., Mastorakis, G., & Dobre, C. (2017). Advances in Mobile Cloud Computing and Big Data in the 5G. U.K.: Springer.
- Migga Kizza, J. (2017). Guide to Computer Network Security. N.Y.: Springer International Publishing
- Nilanjan, D., Hassanien, A., Bhatt, C., Ashour, A., & Satapathy, S., (2018). Internet of Things and Big Data Analytics toward Next-Generation Intelligence. Switzerland: Springer.
- Oreku, G., & Pazynyuk, T. (2016). Security in Wireless Sensor Networks. Switzerland: Springer International Publishing.
- Rankl, W, & Effing, W. (2010). the Smart Card Handbook. U.K.: John Wiley & Sons, Ltd.
- Reynolds, G., & Stair, R., (2018). Principles of information systems. USA: Cengage Learning
- Russell, B., & Duren, D. (2016). Practical internet of things security. U.K.: Packt Publishing.
- Sakr, S, Wylot, M., Mutharaju, R., Phuoc, D., & Fundulaki, I., (2018). Linked Data. Storing, Querying, and Reasoning. U.S.A.: Springer International Publishing).
- Samuel Greengard (2015). The Internet of Things (The MIT Press Essential Knowledge series)
- Skilton, Mark, Hovsepian, Felix (2018) The 4th Industrial Revolution Responding to the Impact of Artificial Intelligence on Business, Palgrave Macmillan
- Soro, A., Brereton, M., & Roe, P. (2018). Social Internet of Things. Switzerland: Springer.
- Tschofenig, H., et. al., (2015) “Architectural Considerations in Smart Object Networking. Tech”, Internet Architecture Board

- Weber, R. H., & Studer, E. (2016). Cybersecurity in the Internet of Things: Legal aspects. Computer Law & Security Review, 715-728
- Αλεξανδροπούλου – Αιγυπτιάδου Ευγενία, (2016), Προσωπικά Δεδομένα σελ.93-94, Νομική Βιβλιοθήκη
- Δουληγέρης, Χ., Μητρόπουλος, Σ., (2015). Πληροφοριακά συστήματα στο διαδίκτυο. [ηλεκτρ. βιβλ.] Αθήνα: Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών.
- Κοτσαλής Λεωνίδας , Κωνσταντίνος Μενουδάκος, (2018) .Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (GDPR), Νομική Βιβλιοθήκη
- Μήτρου Λίλιαν (2017). Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων, νέο δίκαιο-νέες υποχρεώσεις-νέα δικαιώματα ,Εκδόσεις Σακκουλάς
- Παρασκευάς, Μ., Ασημακόπουλος, Γ., & Τριανταφύλλου, Β. (2015). Κοινωνία της Πληροφορίας. Αθήνα: Σύνδεσμος Ελληνικών ακαδημαϊκών βιβλιοθηκών.
- Τζώρτη Βιργινία (2018), Προστασία Δεδομένων Προσωπικού Χαρακτήρα στον Χώρο Ελευθερίας, Ασφαλείας & Δικαιοσύνης, Νομική Βιβλιοθήκη
- Φερενίκη Παναγοπούλου-Κουτνατζή (2017), Ο Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων 679/2016/ΕΕ, Εκδόσεις Σακκουλάς
- Φουληράς, Π., (2015). Ανάπτυξη και διαχείριση δικτύων υπολογιστών. [ηλεκτρ. βιβλ.] Αθήνα: Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών.

Επιστημονικά Άρθρα & Περιοδικά

- A Framework for Privacy Protection and Usage Control of Personal Data in a Smart City Scenario, Gianmarco Baldini, Ioannis Kounelis, Igor Nai Fovino, Ricardo Neisse, (2015)
- A potential weakness in RFID-based Internet-of-things systems, Volume 20, (2015), Pages 115-126
- A Survey on Internet of Things: Security and Privacy Issues, International Journal of Computer Applications (0975 – 8887) Volume 90 – No 11, March 2014
- Architecture for security monitoring in IoT environments, Christos Stergiou, Kostas E. Psannis, Andreas P., Plageras, Giorgos Kokkonis, Yutaka Ishibashi (2017), Research Gate

- Building the Internet of Things Using RFID: The RFID Ecosystem Experience, Frédéric Thiesse, Florian Michahelles, Published by the IEEE Computer Society
- Data Security in Smart Cities: Challenges and Solutions, Informatica Economică vol. 20, no. 1/2016, Daniela POPESCUL, Laura Diana RADU, Alexandru Ioan Cuza, University Iaș
- Internet of Things (IoT): A Literature Review, Journal of Computer and Communications 2015, 3, 164-173 Published Online May 2015 in SciRes
- Internet of Things and Big Data Analytics for Smart and Connected Communities, Y. Sun et al.: IoT and Big Data Analytics for SCCs
- Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment, P. Gope et al. / Future Generation Computer Systems
- Performance Evaluation of Routing Protocols for BIG Data application, Evangelos Balasas, Kostas E. Psannis, Manos Roumeliotis, (2018), Research Gate
- Privacy concerns in smart cities, L. van Zoonen / Government Information Quarterly 33 (2016) 472–480
- Scalable RFID security framework and protocol supporting Internet of Things, Computer Networks, Computer Networks 67 (2014) 89–103
- Secure integration of IoT and Cloud Computing, Christos Stergiou, Kostas E. Psannis, Byung-Gyu Kim, Brij Gupta, 78 (2018) 964–975
- Security, Privacy & Efficiency of Sustainable Cloud Computing for Big Data & IoT, Christos Stergiou, Kostas E. Psannis, Brij B. Gupta, Yutaka Ishibashi (2018), Research Gate
- Smart Cities, Nicos Komninos (2018), Research Gate
- Special section on emerging multimedia technology for smart surveillance system with IoT environment, Brian Kim, Kostas Psannis & Harish Bhaskar,Springer (2017), Research Gate

- Transferring Wireless High Update Rate Supermedia Streams Over IoT, George Kokkonis, Kostas E. Psannis, Manos Roumeliotis, Yutaka Ishibashi, Byung-Gyu Kim and Anthony G. Constantinides, (2017), Research Gate
- The Pursuit of Citizens' Privacy: A Privacy-Aware Smart City Is Possible, Antoni Martínez-Ballesté, Pablo A. Pérez-Martínez, and Agusti Solanas, Universitat Rovira i Virgili
- The role of internet of things in developing smart cities, Andreea-Maria Tirziu, Catalin Vrabie
- Toward efficient smartification of the Internet of Things (IoT) services,Oladayo Bello Sherali Zeadally, Future Generation Computer Systems
- Will the GDPR slow down development of Smart Cities?, Goran Vojković, Ph.D,(2018)1496-1497
- Η προστασία των προσωπικών δεδομένων ενόψει της εφαρμογής της νέας τεχνολογίας της ταυτοποίησης με ραδιοσυχνότητες (R.F.I.D) - Νομική και τεχνολογική προσέγγιση, Αλεξανδροπούλου - Αιγυπτιάδου, Ε. - Μαυρίδης, Ι., Αρμενόπουλος, τομ. 61, σελ. 493-504, 2007

Διαδίκτυο

- https://www.quora.com/What-is-the-difference-between-network-and-Networking What is the difference between network and Networking? (Πρόσβαση 22.6.2018).
- http://www.rfidjournal.com/articles/view?4986 That 'Internet of Things', (πρόσβαση 28.6.2018).
- https://www.explainthatstuff.com/analog-and-digital.html Analog and digital, (πρόσβαση 2.8.2018).
- https://riot-os.org/#features RIOT: The friendly Operating System for the Internet of Things, (πρόσβαση 3.8.2018).
- http://www.rfidjournal.com/articles/view?2481 Gen 2 EPC Protocol Approved as ISO 18000-6C, (πρόσβαση 3.8.2018).
- https://computer.howstuffworks.com/rom.htm How ROM Works, (πρόσβαση 3.8.2018).

- https://www.computer-automation.de/steuerungsebene/steuern-regeln/artikel/93559/0/ Industrie 4.0, (πρόσβαση 4.8.2018).
- https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503286 Cyber-Physical Systems (CPS), (πρόσβαση 4.8.2018).
- https://www.zdnet.com/article/5-nightmarish-attacks-that-show-the-risks-of-iot-security/ Five nightmarish attacks that show the risks of IoT security, (πρόσβαση 5.8.2018).
- https://www.digitalattackmap.com/understanding-ddos/ (πρόσβαση 5.8.2018).
- https://www.cbc.ca/news/technology/brickerbot-malware-breaks-smart-devices-1.4065557 what is Brickerbot, (πρόσβαση 5.8.2018).
- https://www.digitalattackmap.com/understanding-ddos/ Botnet, (πρόσβαση 5.8.2018).
- https://www.technocracy.news/chinas-cctv-surveillance-network-took-just-7-minutes-capture-bbc-reporter/ China's CCTV Surveillance Network Took Just 7 Minutes To 'Capture' BBC Reporter, (πρόσβαση 7.8.2018).
- https://blogs.sap.com/2015/06/30/industry-40-fourth-industrial-revolution/ Βιομηχανία 4.0 - τέταρτη βιομηχανική επανάσταση, (πρόσβαση 20.8.2018).
- https://www.iso.org/standard/73599.html ISO/IEC 14443-4:2018 Cards and security devices for personal identification -- Contactless proximity objects -- Part 4: Transmission protocol, (πρόσβαση 23.8.2018).
- https://www.piraeusbank.gr/el/idiwtes/trapezikes-ypiresies/e-banking/mobile-apps/winbank-wallet/winbank-wallet-app winbank wallet App, πληρωμή μέσω κινητού τηλεφώνου, (πρόσβαση 23.8.2018).
- https://www.uzelf.org/wp-content/uploads/2017/12/R2G-mHealth-Developer-Economics-2017-Status-And-Trends.pdf m Health App Economics 2017. Current Status and Future Trends in Mobile Health, (πρόσβαση 25.8.2018)
- https://www.mordorintelligence.com/industry-reports/internet-of-things-in-healthcare-market?gclid=Cj0KCQjww8jcBRDZARIsAJGCSGtbNCBJ1biTerQ28e7zLYIRNri54cZpSvTfu2KqGIFt_2NPnii6axMaAuKoEALw_wcB Internet of Things (IoT) in Healthcare Market - Segmented by Type, Application, Component, End-users, and Geography - Growth, Trends, and Forecast (2018 - 2023), (πρόσβαση 25.8.2018).
- http://autocaat.org/Technologies/Automated_and_Connected_Vehicles/ Συνδεδεμένα και αυτοματοποιημένα οχήματα, (πρόσβαση 29.8.2018).

- https://www.sae.org/standards/content/j3016_201401/ Ταξινόμηση και ορισμοί όρων που σχετίζονται με αυτοματοποιημένα συστήματα οδήγησης οδικών μηχανοκίνητων οχημάτων, (πρόσβαση 29.8.2018).

- https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046 Οδηγία 95/46/EC, της Ε.Ε., (πρόσβαση 31.8.2018).

- http://www.sev.org.gr/Uploads/Documents/50953/SPECIAL%20REPORT_14_3_2018.pdf Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR): ευκαιρίες και προκλήσεις για τις επιχειρήσεις στην εποχή της ψηφιοποίησης, (πρόσβαση 31.8.2018).

- file:///C:/Users/top1/Downloads/MEMO-18-387_EN.pdf Questions and Answers – General Data Protection Regulation, (πρόσβαση 31.8.2018).

- https://www.ft.com/content/50bb4830-6a4c-11e6-ae5b-a7cc5dd5a28c Yuval Noah Harari on big data, Google and the end of free will, (πρόσβαση 31.8.2018).

- https://www.statista.com/statistics

- Meet the Nest Thermostat | Nest." (2015) Nest Labs https://nest.com/thermostats/nest-learning-thermostat/overview/ , (πρόσβαση 15.9.2018).

- Communication Models in Internet of Things: A Survey (πρόσβαση 20 .9.2018). http://www.ijste.org/articles/IJSTEV3I11049.pdf

- https://hal.inria.fr/file/index/docid/945122/filename/2013-riot_os.pdf RIOT OS: Towards an OS for the Internet of Things, (πρόσβαση 3.10.2018).

- https://www.iec.ch/whitepaper/pdf/iecWP-internetofthings-LR-en.pdf Internet of Things: Wireless Sensor Networks (πρόσβαση 10.10.2018).

- https://royalsociety.org/~/media/events/2017/10/tof-iot/iot-conference%20report-final.pdf The Internet of Things: opportunities and threats, (πρόσβαση 15.10.2018).

- http://www.dpa.gr/portal/page?_pageid=33,19052&_dad=portal&_schema=PORTAL#5 (πρόσβαση 10.11.2018).

- https://ec.europa.eu/info/news/smart-city-matchmaking-barcelona-2018-nov-12_en (πρόσβαση 19.1.2019).

- http://www.urban-hub.com/cities/smart-city-3-0-ask-barcelona-about-the-next-generation-of-smart-cities/ (πρόσβαση 19.1.2019).

- http://www.barcinno.com/barcelona-smart-city-technologies/ (πρόσβαση 19.1.2019).
- https://www.hackerearth.com/blog/internet-of-things/barcelona-smart-city/ (πρόσβαση 19.1.2019).
- https://www.mobypark.com/en/parking-amsterdam (πρόσβαση 19.1.2019).
- https://amsterdamsmartcity.com/projects/flexible-street-lighting (πρόσβαση 19.1.2019).
- http://iotlivinglab.com/ (πρόσβαση 20.1.2019).
- http://www.copcap.com/newslist/2014/copenhagen-is-the-worlds-smartest-city (πρόσβαση 20.1.2019).
- https://www.decidim.barcelona/ (πρόσβαση 20.1.2019).
- Γνώμη 8/2014 σχετικά με τις πρόσφατες εξελίξεις στο διαδίκτυο των πραγμάτων https://www.dataprotection.ro/servlet/ViewDocument?id=1088 (πρόσβαση 20.1.2019)