ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ

ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ

ΤΜΗΜΑ ΝΟΜΙΚΗΣ

ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

«Προστασία Προσωπικών Δεδομένων και Διαδίκτυο των πραγμάτων»

Διπλωματική Εργασία
του
Ιωαννίδη Θ. Ιωάννη

Θεσσαλονίκη, 02/2022

«ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ»

Ιωαννίδης Θ. Ιωάννης

Πτυχίο Νομικής Σχολής, Δημοκρίτειο Πανεπιστήμιο Θράκης, 2013

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΟ ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέποντες Καθηγητές
Κομνηνός Κόμνιος
Κωνσταντίνος Ψάννης

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 01/03/2022

Ονοματεπώνυμο 1	Ονοματεπώνυμο 2	Ονοματεπώνυμο 3
Κωνσταντίνος Ψάννης	Κομνηνός Κόμνιος	Μαρία Μυλώση
.....	.....	.....

Ιωαννίδης Θ. Ιωάννης

Περίληψη

Η παρούσα μελέτη πραγματεύεται τη ραγδαία ανάπτυξη της τεχνολογίας του Διαδικτύου των Πραγμάτων (IoT) και τις επιπτώσεις που έχει αυτή στον τομέα της προστασίας της ιδιωτικότητας και του απορρητου. Το Διαδίκτυο των Πραγμάτων αποτελεί μια ταχέως εξελισσόμενη τεχνολογία,η οποία έχει καταφέρει να διεισδύσει στην καθημερινή ζωή των ανθρώπων χάριν των ωφελειών που προσφέρουν οι εφαρμογές του σε πολλούς τομείς της.

Με τη διασύνδεση συσκευών που περιέχουν αισθητήρες επιτυγχάνουν τη συλλογή, επεξεργασία και τον διαμοιρασμό δεδομένων των χρηστών και του περιβάλλοντος τους. Συλλέγουν τεράστιες ποσότητες δεδομένων, που με την κατάλληλη επεξεργασία παράγουν πληροφορίες χρήσιμες για τους χρήστες και τους φορείς παροχής των υπηρεσιών τους. Με αυτόν τον τρόπο καταφέρνουν να μεγιστοποιούν την απόδοση μειώνοντας το κόστος και προσφέροντας υπηρεσίες υψηλότερου επιπέδου από αυτές που προσφέρουν οι σύγχρονες παραδοσιακές συσκευές. Οι τομείς εφαρμογής της τεχνολογίας του Διαδικτύου των Πραγμάτων είναι πολλοί και ποικίλοι και ενδέχεται να αφορούν οικιακές συσκευές, κινητά τηλέφωνα, φορετές συσκευές (ρολόγια, γυαλιά, παπούτσια κ.ο.κ.), συσκευές ρύθμισης της οδικής κυκλοφορίας, συσκευές μέτρησης των περιβαλλοντικών συνθηκών, ιατρικές συσκευές και βιομηχανικές και γεωργικές μηχανές. Οι συσκευές αυτές τείνουν να χαρακτηρίζονται «έξυπνες» και είναι ικανές να διαμοιράζουν δεδομένα μεταξύ τους βελτιώνοντας ουσιαστικά την ποιότητα της ζωής μας.

Βέβαια, το Διαδίκτυο των Πραγμάτων εκτός από οφέλη για την καθημερινότητα των χρηστών του κρύβει και κινδύνους για την προστασία της ιδιωτικότητας και των προσωπικών τους δεδομένων. Οι κίνδυνοι αυτοί είναι αποτέλεσμα των διαφόρων κενών ασφαλείας που παρουσιάζουν οι διασυνδεδεμένες συσκευές και μπορεί να οδηγήσουν σε παραβιάσεις δεδομένων από κακόβουλες επιθέσεις. Επιθέσεις που μπορεί να προκαλέσουν μη εξουσιοδοτημένη πρόσβαση, κοινοποίηση, καταστροφή ή/και αλλοίωση των προσωπικών δεδομένων των χρηστών. Επίσης, έχει παρατηρηθεί η χρήση δεδομένων από τους παρόχους των υπηρεσιών του Διαδικτύου των Πραγμάτων για σκοπούς διαφορετικούς από τον αρχικό σκοπό της επεξεργασίας χωρίς ο χρήστης να έχει ενημερωθεί και χωρίς να έχει δώσει τη συναίνεση του.

Η παρούσα διπλωματική αποσκοπεί να καταδείξει την αναγκαιότητα υιοθέτησης κατάλληλων πρακτικών και μηχανισμών ασφαλείας στο Διαδίκτυο των Πραγμάτων για να

επιτευχθεί η προστασία της ιδιωτικότητας και του απορρήτου των χρηστών του. Προς αυτή την κατεύθυνση κινείται και η ισχύουσα ελληνική και ευρωπαϊκή νομοθεσία για την προστασία των δεδομένων προσωπικού χαρακτήρα προεξέχοντος του Κανονισμού της ΕΕ 2016/679 για την Προστασία Δεδομένων (ΓΚΠΔ), ο οποίος ορίζει τα νομικά πλαίσια μέσα στα οποία έχουν τη δυνατότητα να καινοτομούν οι σχεδιαστές, οι κατασκευαστές και πάροχοι των υπηρεσιών του Διαδικτύου των Πραγμάτων.

Λέξεις Κλειδιά: Διαδίκτυο των Πραγμάτων (ΔτΠ), Προσωπικά Δεδομένα, Δεδομένα Προσωπικού Χαρακτήρα, Ασφάλεια, Απόρρητο, Ιδιωτικότητα.

Abstract

This study focuses on the increasing importance and rapid growth of the so-called “Internet of Things” (IoT) technology and its consequences on the field of privacy and confidentiality protection. The Internet of Things represents a rapidly evolving technology, which has managed to penetrate into our daily lives as its applications offer unique value and benefits in a plethora of aspects of people’s everyday life.

By connecting devices with built-in sensors, such IoT applications achieve the collection, processing, and sharing not only of users’ data but also of data derived from the environment in which they are embedded. Huge amounts of data are collected and when these are properly and effectively processed, they have the potential to produce useful and meaningful information for both the users and their service providers.

In this way, they maximize efficiency by simultaneously reducing costs and offering high-quality services than those offered by traditional legacy technologies and outdated devices used in everyday life. IoT Applications are several, can vary, and can be related to many devices, such as home appliances, mobile phones, wearable devices (smart watches, glasses, shoes, etc.), devices for road traffic regulation, devices for providing information and assessing environmental conditions, medical devices, and industrial and agricultural machinery. These devices tend to be characterized as "smart" and have the capability to share data with each other, improving our daily lives in an effective and meaning manner. However, the IoT offers not only benefits for the users, but also entails latent risks regarding the protection of their privacy and personal data. These risks emerge from security gaps and the inherent vulnerabilities from which such interconnected devices are inflicted and consequently, may lead to detrimental data breaches by malicious online ‘attacks’. Such attacks may allow unauthorized access and cause disclosure, destruction and/or significant and undesirable alteration of users' personal data. Further, it has recently been realized that providers of IoT services may make use of user’s data for purposes other than the original ones, without the users being informed and without having given their consent. Against this background, this study highlights the importance of protecting users’ privacy and it underlines the pressing need for adopting appropriate security mechanisms in the context of IoT.

This study aims to demonstrate the need to adopt appropriate practices and security mechanisms on the Internet of Things in order to achieve the protection of the privacy and privacy of its users. The current Greek and European legislation for the protection of personal data, in line with the EU Regulation on Data Protection 2016/679, which sets the legal framework within which the designers, manufacturers and service providers of the Internet of Things could innovate.

Keywords: Internet of Things, IoT, Personal Data, Privacy, Confidentiality.

Περιεχόμενα

ΚΕΦΑΛΑΙΟ 4ο

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Συμβολισμοί

ΑΠΔΠΧ :	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
αριθ.:	αριθμός
Αρ.:	Άρθρο
βλ.:	βλέπε
ΓΚΠΔ :	Γενικός Κανονισμός Προστασίας Δεδομένων
ΔΕΕ :	Δικαστήριο της Ευρωπαϊκής Ένωσης
ΔΙΜΕΕ:	Δίκαιο Μέσων Ενημέρωσης και Επικοινωνίας
ΔτΠ :	Διαδίκτυο των Πραγμάτων
ΕΑΠΔ :	Εκτίμηση Αντικτύπου για την Προστασία των Δεδομένων
εδ.:	εδάφιο
εκδ.:	εκδόσεις
επ.:	επόμενα
ΕΕ :	Ευρωπαϊκή Ένωση
ΕΚ:	Ευρωπαϊκό Κοινοβούλιο
επ:	επόμενα
ΕΣΠΔ :	Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων
ΕΟΚΕ :	Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή
Η/Υ :	Ηλεκτρονικός Υπολογιστής
Κ :	Κανονισμός
κλπ. :	και τα λοιπά
κ.ο.κ. :	και ούτω καθεξής
λ.χ. :	λόγου χάρη
Ν. :	Νόμος
ΟΕ29 :	Ομάδα εργασίας του άρθρου 29
Ο.Η.Ε. :	Οργανισμός Ηνωμένων Εθνών

ο.π.:	όπως παραπάνω
παρ.:	παράγραφος
ΠΔ :	Προσωπικά Δεδομένα
Π.Χ. :	Προσωπικού Χαρακτήρα
σελ. :	σελίδα
στοιχ. :	στοιχείο
ΤΠΕ :	Τεχνολογίες των Πληροφοριών και της Επικοινωνίας
Σύντ. :	Σύνταγμα
σχ :	σχετικά
ΥΠΔ :	Υπεύθυνος Προστασίας Δεδομένων
AI :	Artificial Intelligence
Art. :	Article
Big Data :	Μεγάλα Δεδομένα
GDPR :	General Data Protection Regulation
ICT :	Information and communication Technology
DPIA :	Data Protection Impact Assessment
DPO :	Data Protection Officer
DoS :	Αδυναμία εξυπηρέτησης
DdoS :	Διάχυτη αδυναμία εξυπηρέτησης
GPS :	Global Positioning System
IP :	Interner Protocol
MCC:	Mobile Cloud Computing
ML :	Machine Learning
RDF :	Radio Frequency Identification
WSN :	Wireless Sensor Network

Προστασία Προσωπικών Δεδομένων και Διαδίκτυο των Πραγμάτων

Κεφάλαιο 1ο

1.1 Ο Ορισμός του Διαδικτύου των Πραγμάτων

Το «Διαδίκτυο των Πραγμάτων ή Ίντερνετ των πραγμάτων» (“Internet of Things”) είναι μία έννοια που σήμερα περιλαμβάνει την πλειονότητα των αντικειμένων της καθημερινότητας μας- από βιομηχανικές μηχανές μέχρι και φερόμενες/wearable συσκευές- τα οποία με τη χρήση ενσωματωμένων αισθητήρων/sensors συλλέγουν κάθε φύσης δεδομένα και την ανάληψη κάποιας δράσης σε αυτά μέσα σε ένα δίκτυο.

Η ιδέα πίσω από το «Διαδίκτυο των Πραγμάτων» (ΔτΠ) είναι η σύνδεση όλων των ηλεκτρονικών συσκευών μεταξύ τους ή/και με το Διαδίκτυο. Με λίγα λόγια το Διαδίκτυο των Πραγμάτων εφαρμόζεται σε ένα εξάρτημα που αποτελείται από αισθητήρες και μία σύνδεση δικτύου. Με αυτόν τον τρόπο μπορεί κάποιος να ελέγξει, να παρακολουθήσει, να διαχειριστεί ή και να επιβλέψει από το σπίτι, την εργασία του ή το αυτοκίνητο, αντικείμενα της καθημερινής του ζωής. Παρότι το «Διαδίκτυο των Πραγμάτων» είναι μια ευρέως διαδεδομένη έννοια που συναντάται σε πολλούς και διαφορετικούς τομείς του επιστημονικού πεδίου, δεν υπάρχει κοινά αποδεκτός ορισμός, καθώς συναντώνται πολλοί διαφορετικοί τρόποι ορισμού του.

Ένας ιδιαίτερα ευρύς και κοινά αποδεκτός ορισμός του «Διαδικτύου των Πραγμάτων», ο οποίος καταφέρνει να συνοψίζει τη βασική ιδέα του, είναι ο εξής: Ως Διαδίκτυο των Πραγμάτων ορίζεται «η διάχυτη παρουσία μιας ποικιλίας πραγμάτων ή αντικείμενων (π.χ. αισθητήρες, ενεργοποιητές, κινητά τηλέφωνα, tablets κλπ) τα οποία είναι σε θέση να αλληλεπιδρούν μεταξύ τους και να συνεργάζονται για να επιτύχουν κοινούς στόχους»[1].

Σε γενικές γραμμές το ΔτΠ ορίζεται ως ένα παγκόσμια κατανεμημένο δίκτυο (ή δίκτυα) φυσικών αντικειμένων, τα οποία είναι ικανά να αισθάνονται ή να δρουν στο περιβάλλον τους και να επικοινωνούν μεταξύ τους, μ' άλλες μηχανές ή υπολογιστές.

Βέβαια, έχουν αναπτυχθεί κι άλλοι ορισμοί για το «Διαδίκτυο των Πραγμάτων»:

- Σύμφωνα με τον Forrester, το ΔτΠ ορίζεται ως ένα «έξυπνο περιβάλλον, το οποίο χρησιμοποιεί πληροφορίες και τεχνολογίες επικοινωνιών για να δημιουργήσει κρίσιμα

[1] βλ. σχετικά Zhang M., Yu T., Zhai G.F. (2011), Smart Transport System Based on -The Internet of Things, σελ. 1073–1076.

στοιχεία υποδομής και υπηρεσίες διοίκησης μιας πόλης, εκπαίδευσης, υγειονομικής περίθαλψης, δημόσιας ασφάλειας, πραγματικής περιουσίας, μεταφοράς, όπως και επιχειρήσεις κοινής ωφέλειας μεγαλύτερης επίγνωσης, πιο διαδραστικές και αποτελεσματικές»[2].

- Το Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (‘”IEEE”) σε αναφορά που εξέδωσε (2014) ορίζει το «Διαδίκτυο των Πραγμάτων» ως ένα δίκτυο από αντικείμενα, που το καθένα έχει ενσωματωμένους αισθητήρες, οι οποίοι έχουν τη δυνατότητα να συνδέονται στο Διαδίκτυο.
- Σύμφωνα με τη Διεθνή Ένωση Τηλεπικοινωνιών (“ITU Telecommunication Standardization Sector/ITU-T”) το «Διαδίκτυο των Πραγμάτων» αποτελεί μια παγκόσμια υποδομή για την κοινωνία της πληροφορίας, που ενεργοποιεί προηγμένες υπηρεσίες από διασυνδεδεμένα αντικείμενα, τα οποία βασίζονται στις ήδη υπάρχουσες τεχνολογίες επικοινωνιών[3].
- Η διεθνής κοινότητα IETF στην έκθεση της “Internet of Things 2010” αναφέρει ότι το ΔτΠ συνδέει αντικείμενα που βρίσκονται γύρω μας (ηλεκτρικά και μη) με σκοπό τη συνεχεία επικοινωνία μεταξύ τους. Η εξέλιξη των RFID ετικετών, αισθητήρων, έξυπνων κινητών τηλεφώνων (smart phones) καθιστούν δυνατή την υλοποίηση του Δτπ. Στο ΔτΠ τα αντικείμενα αλληλεπιδρούν μεταξύ τους για να κάνουν τις υπηρεσίες καλύτερες και προσβάσιμες πάντα και παντού.

Οι παραπάνω ορισμοί δεν αντηχούν επαρκώς τη βιομηχανική σκοπιά του Δτπ, καθώς ανάμεσα στα οφέλη χρήσης της τεχνολογίας είναι και η βελτίωση της βιομηχανικής παραγωγής με ταυτόχρονη μείωση της κατανάλωσης των πόρων. Αυτός είναι και ο λόγος που πολλές από τις εταιρίες κολοσσούς πραγματοποιούν σημαντικές επενδύσεις στις τεχνολογίες του ΔτΠ. Μάλιστα πολλές από τις εταιρίες αυτές κάνουν χρήση διαφορετικών όρων για να περιγράψουν το ΔτΠ, όπως ο όρος «Διαδίκτυο των πάντων» (“Internet of Everything”) της εταιρίας Cisco, ο όρος «Εξυπνότερος Πλανητης» (“Smarter Planet”) της εταιρίας IBM και ο όρος «Βιομηχανικό Διαδίκτυο» (“Industrial Internet”) της εταιρίας GE, οι οποίοι δίνουν στις τεχνολογίες του ΔτΠ μια πιο διευρυμένη έννοια.

---

[2] βλ. Gubbi J., Buyya R., Marusi S, Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions, Technical Report CLOUDS-TR-2012-2 (2012), Palaniswamia M.The University of Melbourne,διαθέσιμο στον διαδικτυακό σύνδεσμο:https://arxiv.org/ftp/arxiv/papers/1207/1207.0203.pdf

[3] βλ. και σχετικά International Telecomunication Union - Internet Reports 2005: *The Internet of Things (2005)*, 7η Έκδοση, διαθέσιμο στον διαδικτυακό σύνδεσμο: http://handle.itu.int/11.1002/pub/800eae6f-en

Αρκετά διευρυμένη είναι και η έννοια των «πραγμάτων» στο ΔτΠ, καθώς περιλαμβάνει προσωπικά αντικείμενα της καθημερινότητας μας, όπως τηλέφωνα, ρολόγια και γυαλιά ηλίου. Επίσης, περιλαμβάνει στοιχεία του ευρύτερου καθημερινού περιβάλλοντος του ανθρώπου, όπως λ.χ. το όχημα του, αλλά και βιομηχανικές μηχανές, όπως προαναφέρθηκε. Όλα αυτά τα «πράγματα», μέσω της σύνδεσης στο Διαδίκτυο παρέχουν πληροφορίες , δεδομένα ακόμα και υπηρεσίες.[4]

1.2. Η ιστορία του Διαδικτύου των Πραγμάτων

Ως πρόδρομος του ΔτΠ θεωρείται ο πρώτος ηλεκτρομαγνητικός τηλέγραφος, που δημιουργήθηκε το έτος 1832 από τους Άγγλους εφευρέτες William Forthergil Cooke και Charles Wheatstone. Η δημιουργία του πρώτου ηλεκτρομαγνητικού τηλέγραφου συντέλεσε ουσιαστικά στη σύνδεση συσκευών μεταξύ τους για πρώτη φορά επιτρέποντας την εξ αποστάσεως επικοινωνία των σταθμών τρένων του Camden Town και του London Euston[5]. Βέβαια, η ιστορία του «Διαδικτύου των Πραγμάτων» ξεκινάει ουσιαστικά από την εφεύρεση του Διαδικτύου στα τέλη της δεκαετίας του 1960.

Η σύνδεση υπολογιστών και δικτύων με σκοπό τον έλεγχο συσκευών-αντικειμένων πρωτοεμφανίστηκε στα τέλη της δεκαετίας του 1970 με τη δημιουργία συστημάτων που επέτρεπαν την εξ αποστάσεως παρακολούθηση μετρητών του ηλεκτρικού δικτύου μέσω τηλεφωνικών γραμμών.

Ως η πρώτη συσκευή του ΔτΠ θεωρείται ο αυτόματος πωλητής προϊόντων της εταιρείας “Coca Cola”, που κατασκευάστηκε από προγραμματιστές του Πίτσμπουργκ της Πενσυλβάνια των Η.Π.Α στις αρχές της δεκαετίας του 1980 και τοποθετήθηκε στο Πανεπιστήμιο Carnegie Melon της πόλης. Ο αυτόματος πωλητής διέθετε ειδικούς αισθητήρες, οι οποίοι μέσω της σύνδεσης στο Διαδίκτυο παρείχαν τη δυνατότητα στους χειριστές να γνωρίζουν ανά πάσα στιγμή τον αριθμό των προϊόντων που υπήρχαν στον αυτόματο πωλητή και αν αυτά βρίσκονταν στην κατάλληλη

[4] βλ.σχετικά Mohammad Abdur Razzaque, Marija Milojevic Andrei Palade, Siobhán Clarke (2015) Middleware for Internet of Things: A Survey ,*IEEE Internet of Things Journal,*σ.σ. 70-95, σε σελ.74 επ.

[5] βλ. *The first electric telegraph in 1837 revolutionised communications* (2016,2 Φεβρουαρίου), Ανάκτηση από Telegram.co.uk 15 Φεβρουαρίου 2021 στον διαδικτυακό τόπο: https://www.telegraph.co.uk/technology/connecting-britain/first-electric-telegraph

θερμοκρασία. Όπως γίνεται εύκολα αντιληπτό, η άκρως καινοτόμα αυτή εφεύρεση αποτέλεσε το έναυσμα για περαιτέρω έρευνες στο χώρο των διασυνδεδεμένων συσκευών και αποτέλεσε ορόσημο για τις συσκευές του ΔτΠ[6].

Η βασική ιδέα του ΔτΠ είναι η διασύνδεση συσκευών μέσω ενός πρωτοκόλλου του Διαδικτύου (IP), του οποίου η χρήση πρωτοεμφανίστηκε στις αρχές τις δεκαετίας του 1970[7]. Βέβαια, μέχρι το έτος 1990 η χρήση του πρωτοκόλλου του Διαδικτύου (IP) αφορούσε αποκλειστικά τη σύνδεση ηλεκτρονικών υπολογιστών στο Διαδίκτυο. Το 1990 ήταν η χρονιά κατά την οποία έγινε χρήση του για τη σύνδεση άλλων συσκευών πλην των ηλεκτρονικών υπολογιστών στο Διαδίκτυο. Συγκεκριμένα, ο John Romkey κατασκεύασε μια τοστίερα ("The Internet Toaster"), η οποία είχε τη δυνατότητα να συνδεθεί στο Διαδίκτυο μέσω ενός IP Πρωτοκόλλου[8].

Βέβαια, ο όρος "Internet of Things" («Διαδίκτυο των Πραγμάτων») χρησιμοποιήθηκε για πρώτη φορά πολύ αργότερα. Το έτος 1999 ο επιχειρηματίας Kevin Ashton συμμετέχοντας σε μια ερευνητική ομάδα κατάφερε να συνδέσει αντικείμενα με το Διαδίκτυο με τη χρήση μιας ετικέτας τύπου "RFID" και ήταν αυτός που χρησιμοποίησε για πρώτη φορά τον όρο.[9]

Τα επόμενα χρόνια έγιναν μεγάλα βήματα εξέλιξης των τεχνολογιών διασύνδεσης, ενώ η μεγάλη άνθιση του ΔτΠ τοποθετείται στα τέλη της δεκαετίας του 2000 (2008-2009). Υπολογίζεται, μάλιστα, ότι το 2010, για πρώτη φορά στα χρονικά, σε κάθε άνθρωπο αντιστοιχούσαν περισσότερες από μία συνδεδεμένες συσκευές. Πιο συγκεκριμένα, ο αριθμός των διασυνδεδεμένων συσκευών ανά άτομο αυξήθηκε από το 0,08 που ήταν το 2003 σε 1,84.[10]

Η αναθεώρηση του πρωτοκόλλου επικοινωνίας του Διαδικτύου από IPv4 σε IPv6 το έτος 2011 ("Internet Protocol version 6") έδωσε ακόμα περισσότερες επιλογές σύνδεσης αντικειμένων στο Διαδίκτυο, ενώ το ετήσιο Συμπόσιο της Gartner έδειξε τις κατευθύνσεις ανάπτυξης του ΔτΠ για τα χρόνια που ακολούθησαν μέχρι και σήμερα.

---

[6] βλ. Jordan Teciher (2018), *The little-known story of the first IoT device*, IBM, διαθέσιμο στον διαδικτυακό σύνδεσμο: https://www.ibm.com/blogs/industries/little-known-story-first-iot-device

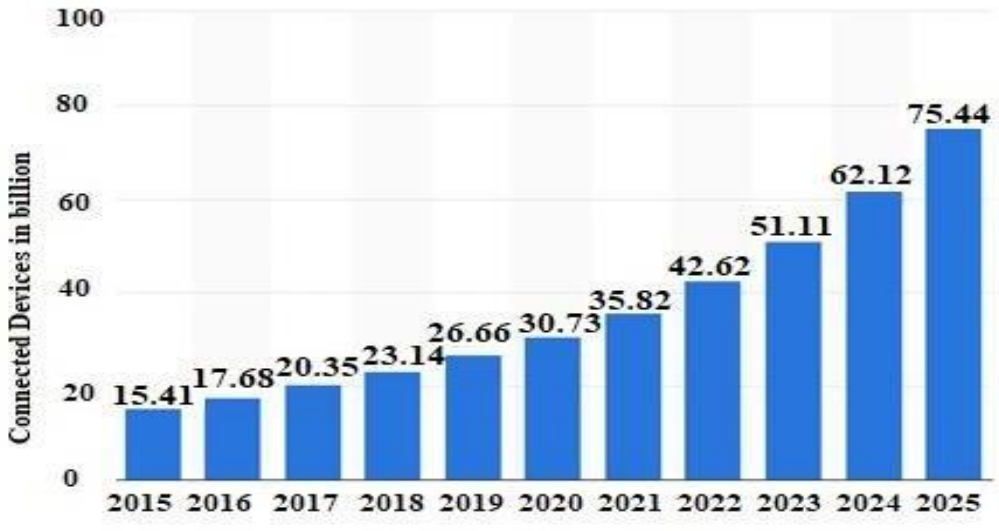
[7] βλ. Evan Andrews (2013,18 Δεκεμβρίου), *Who invented Internet*?, Ανάκτηση από history.com στις 16 Φεβρουαρίου 2021, διαθέσιμο στον διαδικτυακό σύνδεσμο: https://www.history.com/news/who-invented-the-internet

[8] Διεξοδικότερα για τη «Διαδικτυακή Τοστιέρα» βλ. John Romkey (2016), Toast of the IoT: The 1990 Interop Internet Toaste, *IEEE Consumer Eletronics Magazine* , σ.σ. 116-119

[9] βλ. Kevin Ashton (2009,Ιούνιος),In the real world, things matter more than ideas, *RFID Journal*, διαθέσιμο στον διαδικτυακό σύνδεσμο:https://www.rfidjournal.com/articles/view?4986

[10] βλ. Dave Evans (2011, Απρίλιος),The Internet of Things: How the Next Evolution of the Internet Is Changing Everything, *Cisco Internet Business Solutions Group* , σελ. 2-4, *διαθέσιμο στον διαδικτυακό σύνδεσμο:* https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

Σήμερα, σύμφωνα με το Statistica οι διασυνδεδεμένες συσκευές ξεπερνούν τα 50 δισεκατομμύρια, αριθμός που το έτος 2025 θα φτάσει τις 75,44 δισεκατομμύρια συσκευές.



Εικόνα 1: Αριθμός διασυνδεδεμένων συσκευών από το 2015 έως το 2025.
Πηγή: Statistica.com

Συνακόλουθα, η Mordor Intelligence σε έκθεσή της[11] προβλέπει ότι η παγκόσμια αγορά του ΔτΠ, η οποία αποτιμήθηκε σε 761,4 δισεκατομμύρια δολάρια το 2020, θα ξεπεράσει τα 1,38 τρισεκατομμύρια δολάρια (1.386,06 δισεκατομμύρια δολάρια) μέχρι το 2026.

1.3 Η Τεχνολογία του Διαδικτύου των Πραγμάτων

Το ΔτΠ, όπως έχει προαναφερθεί, αποτελεί κατά βάση συστήματα από διάφορες συσκευές, αντικείμενα ή αισθητήρες, που μέσω της μεταξύ τους διασύνδεσης και της σύνδεσης στο Διαδίκτυο επιτυγχάνουν την προσφορά υπηρεσιών βέλτιστης ποιότητας. Το ΔτΠ αποτελείται από τρία κύρια μέρη: 1) Τα "πράγματα" (αντικείμενα), 2) Τα δίκτυα επικοινωνίας που συνδέουν τα αντικείμενα και (3) Τα υπολογιστικά συστήματα, που χρησιμοποιούν τη ροή δεδομένων από και προς τα αντικείμενα.[12]

[11] βλ. Mordor Inteligence, *Internet of things (iot) market - growth, trends, covid-19 impact, and forecasts* (2021 – 2026), σελ. 4-5

[12] βλ. Konstantinos Psannis, Christos Stergiou (2016, Ιούνιος), Recent advances delivered by mobile cloud computing and Internet of Things for Big data applications: A Survey, Special Issue: Management of the Internet of things and big data, *International Journal of Network Management,* (Volume 27, Issue 3)

Το Διαδίκτυο αποτελεί το βασικό πυλώνα της λειτουργίας της τεχνολογίας του ΔτΠ, όπως γίνεται εύκολα αντιληπτό και από την ίδια την ονομασία που της έχει δοθεί. Βέβαια, δεν είναι πάντα απαραίτητο όλες διασυνδεδεμένες οι συσκευές του ΔτΠ να έχουν απευθείας πρόσβαση στο Διαδίκτυο, αλλά αρκεί η διασύνδεση τους μέσω πρωτοκόλλων επικοινωνίας (π.χ. Bluetooth), η οποία τελικώς οδηγεί σε μια σύνδεση με ένα ηλεκτρονικό υπολογιστή ή φορητή συσκευή (π.χ. tablet,smartphone) η οποία είναι συνδεδεμένη στο Διαδίκτυο.

Γενεσιουργός δύναμη, όμως, του ΔτΠ αποτελούν τα δεδομένα και η διαχείριση της ροής τους. Το Διαδίκτυο των πραγμάτων παράγει, αποθηκεύει και κατευθύνει δεδομένα συνεχώς, ενώ η αξιοποίηση των αυξανόμενων ροών των δεδομένων αυτών, η εξαγωγή ουσιαστικών συμπερασμάτων και ο εντοπισμός μοτίβων συμπεριφοράς αποτελούν βασικό τρόπο λειτουργίας ενός συστήματος του ΔτΠ.

Όσον αφορά τη διασύνδεση των συσκευών μεταξύ τους, αυτή επιτυγχάνεται με τη χρήση συγκεκριμένων πρωτοκόλλων επικοινωνίας, τα οποία ποικίλουν ανάλογα με την αρχιτεκτονική του μοντέλου επικοινωνίας που χρησιμοποιεί κάθε σύστημα του ΔτΠ. Το γενικό πλαίσιο της αρχιτεκτονικής μοντέλων επικοινωνίας που χρησιμοποιούν τα συστήματα του Δτπ αποτυπώνεται αναλυτικά από το συμβούλιο αρχιτεκτονικής του Διαδικτύου “Internet Architecture Board” (IAB) στον κατευθυντήριο οδηγό για την διασύνδεση των έξυπνων συσκευών. Τα μοντέλα επικοινωνίας σύμφωνα με το IAB είναι τα παρακάτω:

1. Μοντέλο “Device-to-Device”: Άμεση σύνδεση και επικοινωνία μεταξύ δύο συσκευών μέσω πολλών τύπων δικτύων IP ή του Διαδικτύου, χωρίς τη χρήση κάποιου ενδιάμεσου διακομιστή-server εφαρμογών.
2. Μοντέλο “Device-to-Cloud”: Σύνδεση των συσκευών μέσα από μια διαδικτυακή υπηρεσία υπολογιστικού νέφους (Cloud), η οποία επιβλέπει την ανταλλαγή δεδομένων και ελέγχει την ροή των μηνυμάτων επιτρέποντας στον χρήστη αλλά και στις άλλες συσκευές απομακρυσμένη πρόσβαση.
3. Μοντέλο “Device-to-application-layer gateway”: Οι συσκευές συνδέονται σε μια ενδιάμεση τοπική πύλη-συσκευή (π.χ. ένα smartphone) αποκτώντας πρόσβαση σε μια υπηρεσία υπολογιστικού νέφους (Cloud).
4. Μοντέλο “Back-End Data Sharing”: Επιτρέπει τα δεδομένα που συλλέγονται από μια συσκευή να συγκεντρώνονται και να αναλύονται, ώστε κάθε χρήστη να είναι σε θέση να εξάγει και

να αναλύει δεδομένα έξυπνων αντικειμένων από μια υπηρεσία υπολογιστικού νέφους (Cloud) σε συνδυασμό με δεδομένα από άλλες πηγές. [13]

1.3.1 RFID Systems

Όπως αναφέρθηκε παραπάνω, η λειτουργία του ΔτΠ προϋποθέτει την ύπαρξη συγκεκριμένων αναγνωρίσιμων αντικειμένων-πραγμάτων και την εικονική τους παρουσίαση στην αρχιτεκτονική τους συστήματος του ΔτΠ. Για να είναι, όμως, ένα αντικείμενο αναγνωρίσιμο με διακριτό ρόλο εντός του συστήματος του ΔτΠ εκμεταλλεύεται την αναγνώριση τους μέσω ραδιοσυχνοτήτων με τη χρήση ετικετών τύπου "RFID"(Radio Frequency Identification).

Η αναγνώριση μέσω ραδιοσυχνοτήτων αποτελεί μια αυτορυθμιζόμενη τεχνολογία που χρησιμοποιείται σε διάφορα συστήματα για την αναγνώριση αντικειμένων και την εκτέλεση των λειτουργιών τους, όπως είναι η συλλογή δεδομένων και διάφοροι έλεγχοι λειτουργίας. Ένα σύστημα RFID απαρτίζεται από έναν μεγάλο αριθμό ετικετών, έναν ή περισσότερους αναγνώστες RFID και έναν διακομιστή back-end. Οι σύγχρονες ετικέτες ταξινομούνται ως εξής:

1. Παθητικές ετικέτες: Τροφοδοτούνται από ραδιοκύματα του αναγνώστη RFID και επικοινωνούν με τον αναγνώστη μέσω της ανάστροφης κατανομής,
2. Ενεργές ετικέτες: Τροφοδοτούνται από τις δικές τους πηγές ενέργειας και
3. Ημιενεργές ετικέτες: Περιέχουν εσωτερικές πηγές ενέργειας, ενώ επικοινωνούν με τον αναγνώστη μέσω οπίσθιας σάρωσης[14].

Κάθε ετικέτα περιέχει ένα μικροτσίπ, το οποίο είναι προσαρτημένο σε κάθε αντικείμενο-πράγμα του ΔτΠ και λειτουργεί ως το αναγνωριστικό του. Παράλληλα, προβαίνει σε ανταλλαγές πληροφοριών μεταξύ των αντικειμένων χρησιμοποιώντας ραδιοκύματα, ενώ το μεγαλύτερο πλεονέκτημα έναντι άλλων τεχνολογιών είναι η αυτοματοποίηση στην αναγνώριση των αντικειμένων, που οδηγεί σε μείωση κόστους σε πολλούς τομείς της επιχειρηματικής δραστηριότητας[15].

---

[13] βλ. αναλυτικότερα Karen Rose, Scott Eldridge, Lyman Chapin (2015, Οκτώβριος) The Internet of Things: An Overview Understanding the Issues and Challenges of a More Connected World, Internet Society, σελ. 13-18

[14] βλ. αναλυτικότερα Chen M., & Chen S (2016), RFID Technologies for Internet of Things, Switzerland: Springer International Publishing AG, σελ. 11-13

[15] βλ. Aman Ullah (2018), IoT: Applications of RFID and Issues, International Journal of Internet of Things and Web Services,Volume 3, σελ 1-2

Η χρήση της τεχνολογίας αναγνώρισης μέσω ραδιοκυμάτων (“RFID”) συναντάται σε όλο και περισσότερες εφαρμογές, όπως η είσπραξη διοδίων, η αλυσίδα εφοδιασμού, η κτηνοτροφία, η παρακολούθηση προϊόντων κ.α. .

1.4 Νέες Τεχνολογίες και Διαδίκτυο των Πραγματων

Με βάση τις παραπάνω αναφορές σε διαμοιρασμό μεγάλου αριθμού δεδομένων (Big Data), χρήση υπηρεσιών υπολογιστικού νέφους (Cloud Computing) και εντοπισμού μοτίβων συμπεριφοράς (Artificial Intelligence), γίνεται εύκολα αντιληπτό ότι το ΔτΠ συνδέεται άμεσα και με άλλες σύγχρονες και ραγδαία εξελισσόμενες ψηφιακές τεχνολογίες.

1.4.1 Τεχνολογία Υπολογιστικού Νέφους (Cloud Computing)

Σύμφωνα με το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) των Ηνωμένων Πολιτειών Αμερικής, το «Υπολογιστικό Νέφος» (“Cloud Computing”) είναι ένα τεχνολογικό μοντέλο, που επιτρέπει την πανταχού παρούσα, βολική και κατ’ απαίτηση διαδικτυακή πρόσβαση σε μια δεξαμενή κοινόχρηστων υπολογιστικών πόρων (π.χ. δίκτυα, διακομιστές, αποθηκευτικές μονάδες, εφαρμογές και υπηρεσίες), που προσφέρεται γρήγορα και με την ελάχιστη δυνατή προσπάθεια ή αλληλεπίδραση άλλου παρόχου υπηρεσιών[16].

Με απλούστερα λόγια, το «Υπολογιστικό Νέφος» είναι η αποθήκευση, η επεξεργασία και η χρήση δεδομένων από απομακρυσμένους υπολογιστές στους οποίους εξασφαλίζεται πρόσβαση μέσω του Διαδικτύου, γεγονός που δημιουργεί μεγάλη ευελιξία αναφορικά με τις ανάγκες υπολογιστικής ισχύος. Η τεχνολογία βασίζεται σε τεράστιας χωρητικότητας κέντρα δεδομένα που εξασφαλίζουν επεξεργαστική ισχύ και είναι προσβάσιμα από σχεδόν οποιουδήποτε τύπου λογισμικό υπολογιστή[17].

---

[16] βλ. αναλυτικότερα για τον ορισμό του «Υπολογιστικού Νέφους» στο *Final Version of NIST Cloud Computing Definition Published* (2011,25 Οκτωβρίου), Ανάκτηση από nist.gov.com 20 Φεβρουαρίου 2021, στον διαδικτυακό τόπο: https://www.nist.gov/news-events/news/2011/10/final-version-nist-cloud-computing-definition-published

[17] βλ. και *Εκμετάλλευση των δυνατοτήτων του υπολογιστικού νέφους (Cloud Computing) στην Ευρώπη – τι είναι και τι σημαίνει αυτό για μένα;*(2012, 27 Σεπτεμβρίου), Ανάκτηση 21 Φεβρουαρίου 2021, διαθέσιμο στον διαδικτυακό τόπο της Ευρωπαϊκής Επιτροπής:https://ec.europa.eu/commission/presscorner/detail/el/MEMO_12_713

Με βάση την ανωτέρω τεχνολογία έχει αναπτυχθεί τα τελευταία χρόνια η τεχνολογία του «Κινητού Υπολογιστικού Νέφους» (“Mobile Cloud Computing”), η οποία ως σκοπό έχει την παροχή πρόσβασης σε πληροφορίες και δεδομένα από οποιοδήποτε μέρος ανά πάσα στιγμή, περιορίζοντας ή εξαλείφοντας την ανάγκη για εξοπλισμό υλικού. Η δυνατότητα του αυτή την καθιστά μια πρωτεύουσα τεχνολογία στη χρήση της τεχνολογίας του ΔτΠ. Πιο συγκεκριμένα, το “Mobile Cloud Computing” (“MCC”) ορίζεται ως ενοποίηση της τεχνολογίας “Cloud Computing” με κινητές συσκευές για να κάνουν τις κινητές συσκευές επινοητικές από άποψη υπολογιστικής ισχύος, μνήμης, αποθήκευσης, ενέργειας και συνειδητοποίησης περιβάλλοντος[18].

Η χρήση της τεχνολογίας του “MCC” σε εφαρμογές του ΔτΠ μπορεί να καλύψει ορισμένα κενά της τεχνολογίας του ΔτΠ, όπως είναι η περιορισμένη δυνατότητα αποθήκευσης και της απαιτούμενης σύνδεσης των εφαρμογών στο Διαδίκτυο. Από την άλλη πλευρά, το ΔτΠ καταφέρνει να διευρύνει σημαντικά το πεδίο εφαρμογής της τεχνολογίας του CC, το οποίο αποτελούσε και ένα μεγάλο ζητούμενο για την τεχνολογία αυτή.

Βέβαια, η ενσωμάτωση του Υπολογιστικού Νέφους στο ΔτΠ δεν λύνει μόνο προβλήματα αλλά δημιουργεί και νέα. Πιο συγκεκριμένα, γεννώνται βασικά ζητήματα ασφάλειας κατά τη χρήση του από τις εφαρμογές του ΔτΠ λόγω της έλλειψης εμπιστοσύνης στον πάροχο υπηρεσιών ή τις γνώσεις σχετικά με συμφωνίες επιπέδου υπηρεσίας (SLA) και γνώσεις σχετικά με τη φυσική θέση των δεδομένων[19].

1.4.2 Μεγάλα Δεδομένα (Big Data)

Τα «Μεγάλα Δεδομένα» (“Big Data”) είναι ένας ευρέως διαδεδομένος όρος, ο οποίος χρησιμοποιείται για να περιγράψει την ταχύτατη αύξηση του όγκου των διακινούμενων δεδομένων σε δομημένη και μη δομημένη μορφή. Ο αριθμός αυτός των δεδομένων είναι τόσο μεγάλος ή/και πολύπλοκος που τον καθιστά μη αξιοποιήσιμο από τις παραδοσιακές εφαρμογές επεξεργασίας δεδομένων. Η τεχνολογία των «Μεγάλων Δεδομένων» καθιστά τον μεγάλο αυτό όγκο δεδομένων

[18] βλ. Psannis, Stergiou (2016, Ιούνιος), ο.π. σελ. 3

[19] βλ. Brij B. Gupta, Gregorio Martinez Perez, Dharma P. Agrawal & Deepak Gupta (2020), Handbook of computer networks and cyber security, (chapter 21). Στο Christos Stergiou, Andreas P. Plageras, Konstantinos E. Psannis & Brij B. Gupta, *Secure Machine Learning scenario from Big Data in Cloud Computing via Internet of Things network*(σ.σ. 525-554), σελ. 543-544

αξιοποιήσιμο οδηγώντας σε πιο σίγουρη και εμπεριστατωμένη λήψη αποφάσεων και ως εκ τούτου σε μεγαλύτερη λειτουργική αποδοτικότητα, μείωση κόστους και μειωμένο κίνδυνο[20].

Το ΔτΠ καθιστά δυνατή τη σύνδεση συσκευών ή/και αισθητήρων μεταξύ τους αλλά και με το Διαδίκτυο μεταδίδοντας δεδομένα μέσω των συσκευών και των αισθητήρων. Τα δεδομένα που συλλέγονται αφορούν ποικίλους τύπους δεδομένων, "θόρυβο" ακόμα και ορισμένα μη αξιοποιήσιμα και περιττά δεδομένα[21]. Η συλλογή τόσου μεγάλου όγκου δεδομένων πραγματοποιείται από πολλούς και διάφορους κόμβους τεχνολογίας, οι οποίοι δημιουργούν διάφορα δίκτυα, τα οποία καθορίζουν τη λειτουργία των συσκευών του ΔτΠ. Με δεδομένο ότι οι αισθητήρες και οι διάφορες άλλες συσκευές του ΔτΠ υποβαθμίζονται με την πάροδο του χρόνου, η χρήση της τεχνολογίας των "Μεγάλων Δεδομένων" μειώνει τον κίνδυνο των σφαλμάτων και διατηρεί την ακρίβεια στη λήψη αποφάσεων, καθώς προσφέρει τη δυνατότητα αυτόματης διόρθωσης σφαλμάτων.

Παραδοσιακά, τα «Μεγάλα δεδομένα» αναπτύσσονται σε τέσσερις διαστάσεις, οι οποίες είναι:

α) Όγκος των δεδομένων: Οι συσκευές του ΔτΠ αποθηκεύουν τεράστιο αριθμό δεδομένων, τα οποία μπορεί να αφορούν δεδομένα εργαζομένων δεδομένα όπως τα αρχεία των εργαζομένων, πληροφορίες και ιστορικό αγοράς πελατών, ιατρικά δεδομένα χρηστών κ.α. . Αυτές οι πρόσθετες πληροφορίες ονομάζονται «μετα-δεδομένα» ("metadata") που συντελούν στην εξαγωγή συγκεκριμένων συμπερασμάτων. Η μεγάλη ποσότητα των δεδομένων που δημιουργούνται και συλλέγονται από συσκευές του ΔτΠ είναι σημαντική για τη λειτουργία τους, καθώς όλα τα δεδομένα πρέπει να μετρηθούν, να αποθηκευτούν ή να μεταδοθούν σε άλλους κόμβους, αποτελώντας παράλληλα σημαντική πρόκληση καθώς οι παραδοσιακές τεχνολογίες αποθήκευσης δεν μπορούν να διαχειριστούν αποτελεσματικά τόσο μεγάλο όγκο δεδομένων.

β) Ποικιλία των δεδομένων: Οι συσκευές του ΔτΠ συλλέγουν πολλούς και διαφορετικούς τύπους δομημένων και μη δομημένων δεδομένων. Τα «Μεγάλα Δεδομένα» συνεπάγονται την ταυτόχρονη συγκέντρωση δεδομένων στόχου από ένα μεγάλο εύρος πηγών, ενώ τα δεδομένα που συλλέγονται κατά τη λειτουργία της τεχνολογίας του ΔτΠ μπορεί να περιλαμβάνουν δεδομένα από ποικίλα είδη αισθητήρων και μη αριθμητικά δεδομένα (λ.χ. δεδομένα τύπου mp3, mp4, ραδιοφωνικά σήματα).

---

[20] βλ. αναλυτικότερα Psannis, Stergiou (2016, Ιούνιος),ο.π., σελ. 2 επ.

[21] βλ. Shivanjali Khare and Michael Totaro (2019, Ιούλιος), Big Data in IoT, *IEEE Internet of Things Journal*, *Conference Paper- 10th ICCCNT 2019,* σελ. 2 επ.

γ) Ταχύτητα επεξεργασίας των δεδομένων: Η παραγωγή και συλλογή δεδομένων από τους αισθητήρες ή τις άλλες συσκευές εισόδου του ΔτΠ συντελείται με εξαιρετικά υψηλή ταχύτητα, μιας και τα δεδομένα πρέπει να επεξεργάζονται άμεσα για να παραχθούν τα επόμενα. Επιπλέον, η ταχύτητα της παραγωγής δεδομένων δεν είναι πάντα συνεχής, αλλά αλλάζει με την πάροδο του χρόνου.

δ) Αλήθεια των δεδομένων: Τα δεδομένα που παράγονται από τις συσκευές εισόδου του ΔτΠ, θα πρέπει να είναι απόλυτα ακριβή, καθώς δεν υπάρχουν περιθώρια σφάλματος στη μέτρηση. Είναι δεδομένο ότι οι ασύρματοι αισθητήρες ενδέχεται να αντιμετωπίσουν σφάλματα επικοινωνίας και αποτυχία υλικού λόγω πολλών παραγόντων που αφορούν το εξωτερικό περιβάλλον, δυσλειτουργία του δικτύου κτλ. Ως εκ τούτου, είναι απαραίτητο τα δεδομένα που αποθηκεύονται να είναι ακριβή και πλήρη, ενώ η κατηγοριοποίηση σε αξιόπιστα και μη αξιόπιστα δεδομένα καθίσταται επιβεβλημένη[22].

Όπως γίνεται εύκολα αντιληπτό, τα (Μεγάλα) δεδομένα και το ΔτΠ συνδέονται πολύ στενά μεταξύ τους και παρότι αποτελούν ξεχωριστές τεχνολογίες είναι πολύ δύσκολο να μιλήσουμε για το ένα χωρίς να αναφέρουμε και το άλλο. Οι εφαρμογές του ΔτΠ παράγουν τεράστια ροή δεδομένων, τα οποία συλλέγονται σε πραγματικό χρόνο και υποβάλλονται σε επεξεργασία και ανάλυση παράγοντας αποτελέσματα άμεσα. Τα εργαλεία Ανάλυσης των Μεγάλων Δεδομένων (“Big Data Analytics”) έχουν την ικανότητα να χειρίζονται τη συνεχή αυτή ροή δεδομένων εξάγοντας χρήσιμες πληροφορίες, οι οποίες εξάγουν τα επιθυμητά αποτελέσματα για τις εφαρμογές του ΔτΠ. Τελικά, ο συνδυασμός αυτός των πληροφοριών από το ΔτΠ και η ανάλυση των «Μεγάλων δεδομένων» οδηγεί σε εξοικονόμηση κόστους, βελτιωμένη απόδοση και κατανάλωση των απολύτως απαραίτητων πόρων. Το ΔτΠ και τα «Μεγάλα δεδομένα» έχουν μια πολύ σημαντική αλληλένδετη σχέση, η οποία θα συνεχίσει να αναπτύσσεται καθώς εξελίσσονται και οι τεχνολογίες αυτές.

1.4.3 Η αξία των δεδομένων

Τα δεδομένα αποτελούν ακατέργαστα στοιχεία, τα οποία μόνο όταν συνδυαστούν κατάλληλα παράγουν πληροφορίες. Η μορφή τους μπορεί να είναι διαφορετικής φύσης και μια από τις βασικές λειτουργίες κάθε λογισμικού είναι η επεξεργασία αυτών και η παρουσίαση τους στο χρήστη με τρόπο «ευανάγνωστο». Η πληροφορία αποτελείται από πολλά δεδομένα, τα οποία έχουν

[22] ibid

οργανωθεί με τρόπο που τους προδίδει πρόσθετη αξία και οδηγεί σε γνώση. Γίνεται εύκολα αντιληπτό, ότι η αξία της πληροφορίας που δημιουργείται εξαρτάται από την αξία και την ποσότητα των δεδομένων που υφίστανται επεξεργασία. Όσο μεγαλύτερος ο αριθμός των «αξιόπιστων» δεδομένων που υφίστανται επεξεργασία, τόσο πιθανό είναι η πληροφορία που έχει εξαχθεί να οδηγεί σε ασφαλή συμπεράσματα.

Το Διαδίκτυο και η συνεχώς αυξανόμενη χρήση του, έχει οδηγήσει σε έναν τεράστιο αριθμό δημοσιευμένων πληροφοριών. Οι πληροφορίες αυτές ενδέχεται να είναι ετερογενείς, διασκορπισμένες και αλληλοκαλυπτόμενες. Έτσι, καθίσταται πολύ δύσκολη η προσπέλασή τους και η αποτελεσματική τους αξιοποίηση. Αποτελεί, λοιπόν, βασικό ζητούμενο η εκμετάλλευση αυτών με την παραγωγή γνώσης. Ο σύγχρονος Παγκόσμιος Ιστός αποτελείται από ημίδομημένα έγγραφα και συνδέσμους, των οποίων η σημασιολογία δεν είναι πάντα φανερή, καθώς το περιεχόμενο τους καθίσταται αντιληπτό από τον άνθρωπο, αλλά όχι από τις μηχανές[23].

Τα «πράγματα» στο ΔτΠ παράγουν τεράστιες ποσότητες δεδομένων σε πραγματικό χρόνο. Δεδομένης της κλίμακας των δεδομένων που δημιουργούνται, τίθεται σοβαρό ζήτημα για την επεξεργασία αυτών των τεράστιων ποσοτήτων δεδομένων. Σε αυτό το πλαίσιο, οι σημασιολογικές τεχνολογίες, όπως τα «Διασυνδεδεμένα δεδομένα» (“Linked Data”), που αποσκοπούν στη διευκόλυνση επικοινωνίας μηχανής προς μηχανή, παίζουν όλο και πιο σημαντικό ρόλο. Τα διασυνδεδεμένα δεδομένα αποτελούν μέρος μιας αυξανόμενης τάσης προς πολύ κατανεμημένα συστήματα, με χιλιάδες ή δυνητικά εκατομμύρια ανεξάρτητες πηγές που παρέχουν δομημένα δεδομένα[24].

Ο σύγχρονος Παγκόσμιος Ιστός έχει τη μορφή ενός «Ιστού Εγγράφων», καθώς ο μεγαλύτερος όγκος των δημοσιευθέντων στοιχείων είναι έγγραφα με δεσμούς μεταξύ τους. Η νέα τάση και η υιοθέτηση σημασιολογικών τεχνολογιών, όπως τα «Διασυνδεδεμένα Δεδομένα», επεκτείνουν τα όρια του σύγχρονου Ιστού σε έναν παγκόσμιο χώρο όπου τμήματα δεδομένων από διαφορετικές πηγές συνδέονται σημασιολογικά δημιουργώντας νέες προοπτικές για τις σύγχρονες αναπτυσσόμενες τεχνολογίες, όπως το ΔτΠ και τα «Μεγάλα Δεδομένα»[25]. Το νέο αυτό τμήμα του Παγκόσμιου Ιστού ονομάζεται «Σημασιολογικός Ιστός» (“Web 3.0”) και στόχος του είναι μεταξύ

---

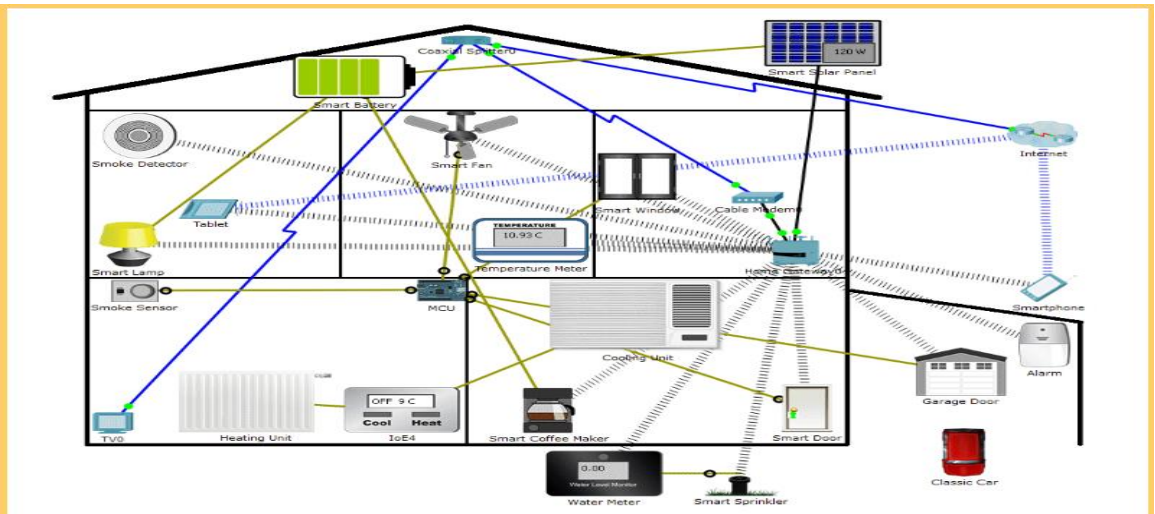
[23] βλ. C. Bizer, R. Cyganiak (2007), How to publish Linked Data on the Web, *T. Heath*, Workshop at the 17th International World Wide Web Conference Beijing, China, April 22, 2008*, σελ.1 επ.*

[24] βλ. Qin Y., Sheng Q.Z., Edward Curry (2015), Matching Over Linked Data Streams in the Internet of Things, *IEEE Internet Computing*, σελ 2-4

[25] βλ.Sakr S, Wylot M., Mutharaju, R.,Le Phuoc, D.,Fundulaki, I (2018), Linked Data, *Springer International Publishing, σελ. 5-7*

άλλων να προσδώσουν μεγαλύτερη αξία στα δεδομένα και να παράγονται πιο έμπιστες πληροφορίες, γεγονός που θα έχει πολλαπλά οφέλη σε τομείς όπως η υγεία, η εκπαίδευση, ο επιχειρηματικός τομέας κ.α. [26].

Το ΔτΠ αποτελεί ουσιαστικά ένα «σύστημα συστημάτων» (“system of systems”), όπου η λειτουργικότητά του πραγματώνεται μέσω αλυσίδων επεξεργασίας κατά τη λειτουργία των οποίων ανταλλάσσονται τεράστιες ποσότητες δεδομένων.



Εικόνα 2: Συλλογή και διαμοιρασμός δεδομένων σε ένα «Έξυπνο» σπίτι.

Πηγή εικόνας: Accountability in the Internet of Things (IoT): Systems, law & ways forward, Jatinder Singh, Christopher Millard, Chris Reed, Jennifer Cobbe, Jon Crowcroft

Στην Εικόνα 2 δίδεται ένα παράδειγμα επεξεργασίας δεδομένων από ένα σύστημα του ΔτΠ (ένα «έξυπνο» σπίτι), όπου οι αισθητήρες (π.χ. δεδομένα θέσης και θερμοκρασίας) σε μια κινητή συσκευή ενεργοποιούν ένα σύστημα θέρμανσης στο σπίτι. Η λειτουργικότητα προκύπτει από ενορχήστρωση μιας γκάμας στοιχείων του συστήματος, μέσω μιας σειράς ανταλλαγής μεγάλης κλίμακας δεδομένων, όπου κάθε στοιχείο είναι δυνητικά διαχειρίσιμο από διαφορετικούς οργανισμούς ή χρήστες[27].

1.4.4 Εξόρυξη Δεδομένων (Data Mining)

[26] βλ. αναλυτικότερα για την έννοια του «Σημασιολογικού Ιστού» στο *Σημασιολογικός Ιστός*. Ανάκτηση από el.wikipedia.org στις 25 Φεβρουαρίου 2021, στον διαδικτυακό σύνδεσμο: https://el.wikipedia.org/wiki/%CE%A3%CE%B7%CE%BC%CE%B1%CF%83%CE%B9%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CE%BA%CF%8C%CF%82_%CE%99%CF%83%CF%84%CF%8C%CF%82

[27] βλ. Jatinder Singh Christopher Millard, Chris Reed, Jennifer Cobbe & Jon Crowcroft(2018), Accountability in the Internet of Things (IoT): Systems, law & ways forward, vol.51, σελίδες 54-65

Η «Εξόρυξη Δεδομένων» (“Data Mining”) είναι μία έννοια που συνήθως παραπέμπει σε κάθε είδος φόρμα με μεγάλη ποσότητα δεδομένων ή επεξεργασία δεδομένων, αλλά επίσης αναφέρεται σε κάθε είδος συστήματος υποστήριξης αποφάσεων, όπως η τεχνητή νοημοσύνη (“Artificial Intelligence”), η εκμάθηση μηχανής-ML (“Machine Learning”) και η επιχειρηματική ευφυΐα. Ο όρος αναφέρεται στη διαδικασία εξεύρεσης μιας πληροφορίας ή χρήσιμων μοτίβων από μεγάλες βάσεις δεδομένων[28].

Αποτελεί μια διαδικασία που χρησιμοποιούν οι εταιρείες για να μετατρέψουν τα ακατέργαστα δεδομένα σε χρήσιμες πληροφορίες. Πιο συγκεκριμένα, με τη χρήση κατάλληλου λογισμικού αντλούν πληροφορίες για τους πελάτες τους βελτιώνοντας με αυτόν τον τρόπο τις στρατηγικές διαφήμισης τους και αυξάνοντας τις πωλήσεις τους.[29]

Το ΔτΠ δημιουργεί συνεχώς τεράστιας κλίμακας δεδομένα αναγκάζοντας τις εταιρίες να αναπτύξουν τις τεχνολογίες των «Μεγάλων Δεδομένων» για να ανταπεξέλθουν με αυτόν τον συνεχώς αυξανόμενο όγκο δεδομένων και να μεγιστοποιήσουν τα οφέλη της τεχνολογίας του ΔτΠ, καθώς ο όγκος των δεδομένων που δημιουργεί το ΔτΠ θα ήταν άχρηστος χωρίς την αναλυτική ισχύ των «Μεγάλων δεδομένων».

1.4.5 Τεχνητή Νοημοσύνη

Η ραγδαία ανάπτυξη του ΔτΠ με όλο και περισσότερες συσκευές και αισθητήρες να διαρρέουν συνεχώς δεδομένα, ενδέχεται σύντομα να μην μπορεί να καλυφθεί επαρκώς από την ικανότητα του Διαδικτύου. Παράλληλα, η τεχνολογία της «Τεχνητής Νοημοσύνης» (“Artificial Intelligence”) αναπτύσσεται με ταχείς ρυθμούς και στις εφαρμογές του ΔτΠ, έχοντας μάλιστα το ψευδώνυμο της «Τεχνητής Νοημοσύνης αιχμής» (“Edge AI”).[30]

---

[28] βλ. αναλυτικότερα για τον όρο της «εξόρυξης δεδομένων» στο *Εξόρυξη Δεδομένων*. Ανάκτηση σπό el.wikipedia.org στις 25 Φεβρουαρίου 2021, στο:https://el.wikipedia.org/wiki/%CE%95%CE%BE%CF%8C%CF%81%CF%85%CE%BE%CE%B7_%CE%B4%CE%B5%CE%B4%CE%BF%CE%BC%CE%AD%CE%BD%CF%89%CE%BD

[29] βλ. Boo, Y.L., Stirling, D., Chi, L., Liu, L., Ong, K.-L. & Williams, G. (2018), Data Mining, *Springer, Volume 845, 15th Australasian Conference, AusDM 2017, Melbourne, VIC, Australia, August 19-20*

[30] βλ. Xi Lin Jun Wu, Haoran Liang & Wu Yang Jianhua Li (2019, Μάϊος), Making Knowledge Tradable in Edge-AI Enabled IOT: A Consortium Blockchain-based Efficient and Incentive Approach, *IEEE Internet of Things Journal*, *Student Member,* σελ. 1-2

Σύμφωνα με το Ευρωπαϊκό Κοινοβούλιο, ως «Τεχνητή Νοημοσύνη» ορίζεται «η ικανότητα μιας μηχανής να αναπαράγει τις γνωστικές λειτουργίες ενός ανθρώπου, όπως είναι η μάθηση, ο σχεδιασμός και η δημιουργικότητα». Με τη χρήση της η κάθε είδους μηχανή καθίσταται ικανή να αντιλαμβάνεται το περιβάλλον της, να επιλύει προβλήματα και να επιτυγχάνει προκαθορισμένους στόχους, αναλύοντας μεγάλο όγκο δεδομένων και λαμβάνοντας αποφάσεις με βάση αυτά.[31]

Με τη χρήση, λοιπόν, της «Τεχνητής Νοημοσύνης» στις εφαρμογές του ΔτΠ ο τεράστιος όγκος των διακινούμενων δεδομένων καθίσταται ευκολότερα διαχειρίσιμος, καθώς συμβάλει στην εξαγωγή ασφαλέστερων συμπερασμάτων και στη λήψη αποφάσεων. Έχει οδηγήσει επίσης στην μετατροπή της τεχνολογίας του ΔτΠ από "Data-As-Aservice" («Τα δεδομένα ως Υπηρεσία») σε "Knowledge-As-Aservice" («Η γνώση ως Υπηρεσία»)[32], καθώς το ΔτΠ καθίσταται πια ικανό να εξάγει ασφαλή συμπεράσματα από τα δεδομένα που διακινεί και αναλύει, ανιχνεύοντας τα διάφορα μοτίβα συμπεριφοράς. Επιπλέον, μέσω της «Μηχανικής Εκμάθησης» ("ML") καθίσταται δυνατό να προβλεφθούν οι συνθήκες λειτουργίας μιας συσκευής και να εντοπιστούν οι παράμετροι που θα πρέπει να τροποποιηθούν για να εξασφαλιστούν τα ιδανικά αποτελέσματα. Ως εκ τούτου, η σύζευξη του ΔτΠ και της «Τεχνητής Νοημοσύνης» προσφέρει, μεταξύ άλλων, μια εικόνα για το ποίες διαδικασίες είναι περιττές και χρονοβόρες και ποιες απαιτούν βελτιωτικές παρεμβάσεις, ενώ μας δίνει τη δυνατότητα να προβλέψουμε τυχόν βλάβες ή αστοχίες του εξοπλισμού και να προγραμματίσουμε τακτικές διαδικασίες συντήρησης τους[33]. Συνολικά, η σύζευξη του ΔτΠ με την «Τεχνητή Νοημοσύνη» οδηγεί σε προηγμένο επίπεδο λύσεων και μετατρέπει ουσιαστικά τις συσκευές του ΔτΠ σε «έξυπνες συσκευές» με τη δυνατότητα εξαγωγής συπερασμάτων από έναν τεράστιο όγκο δεδομένων.

---

[31] βλ. *Τι είναι η τεχνητή νοημοσύνη και πώς χρησιμοποιείται;* (2020, 9 Σεπτεμβρίου) .Ανάκτηση στις 30 Φεβρουαρίου 2021 από την επίσημη ιστοσελίδα της Ευρωπαϊκής Επιτροπής:https://www.europarl.europa.eu/news/el/headlines/society/20200827STO85804/ti-einai-i-techniti-noimosuni-kai-pos-chrisimopoieitai

[32] βλ. Xi Lin Jun Wu, Haoran Liang & Wu Yang Jianhua Li (2019, Μάϊος), ο.π.

[33] βλ. Yinong Chen (2020, Ιούλιος), IoT, cloud, big data and AI in interdisciplinary domains, *Simulation Modeling Practice and Theory*, Article 102070*,* σελ 2-3

Κεφάλαιο 2ο

2. Τομείς Εφαρμογής του ΔτΠ

2.1 Οι «έξυπνες» πόλεις

Οι πόλεις είναι οι βασικοί πυλώνες της οικονομίας κάθε χώρας, καθώς καταλαμβάνουν σχεδόν το 80% του παγκοσμίου ΑΕΠ. Παράλληλα, στις πόλεις καταναλώνονται τα 2/3 της παγκοσμίως παραχθείσας ενέργειας και ευθύνονται για την παραγωγή του 70% των παγκόσμιων εκπομπών διοξειδίου του άνθρακα (CO2).[34] Συνακόλουθα, ο πληθυσμός των πόλεων αναμένεται να αυξηθεί από το 55,3% του συνολικού πληθυσμού που ήταν το 2018 σε 60% έως το έτος 2030, σύμφωνα με έκθεση του Οργανισμού Ηνωμένων Εθνών[35].

Με βάση τα ανωτέρω, γίνεται εύκολα αντιληπτή η κεντρική θέση που κατέχει η πόλη στην παγκόσμια οικονομία, αλλά και στην καθημερινότητα των πολιτών του κόσμου. Αυτός είναι και ο λόγος που βρίσκεται στο επίκεντρο του ενδιαφέροντος των κέντρων λήψεων αποφάσεων αλλά και των σχεδιαστών και παραγωγών τεχνολογιών με σκοπό τη δημιουργία «έξυπνων πόλεων»(“smart cities”), οι οποίες με την υιοθέτηση-χρήση της τεχνολογίας του ΔτΠ καταφέρνουν να προωθούν την καινοτομία, να επιδιώκουν τη βιώσιμη αστική ανάπτυξη και να ενθαρρύνουν τη συμμετοχή των πολιτών, επιχειρήσεων και άλλων συντελεστών στη διαδικασία λήψης αποφάσεων[36].

Σύμφωνα με τον ορισμό του D. Torppeta, «Έξυπνη» είναι η πόλη που συνδυάζει τις Τεχνολογίες των Πληροφοριών και της Επικοινωνίας (ΤΠΕ) και το Διαδίκτυο (“Web 2.0”) με άλλες οργανωτικές και σχεδιαστικές προσπάθειες για τον εκσυγχρονισμό και την επιτάχυνση των

---

[34] βλ. Huawei and IDC (2017,27 Ιουλίου), Huawei Smart City White Paper, σελ.5 επ.

[35] βλ. *Έκθεση του Οργανισμού Ηνωμένων Εθνών για τις πόλεις Παγκοσμίως κατά το έτος 2018* (2019).Ανάκτηση από un.org 30 Φεβρουαρίου 2021,στον διαδικτυακό σύνδεσμο:https://www.un.org/en/events/citiesday/assets/pdf/the_worlds_cities_in_2018_data_booklet.pdf

[36] βλ. Μαρία Παναγιωτοπούλου, Αναστασία Στρατηγέα, Γιώργος Σωμαρακάκης (2014, Ιούνιος), Έξυπνες Πόλεις και Βιώσιμη Αστική Ανάπτυξη – Παραδείγματα από τη

Μεσογειακή και την Ελληνική Εμπειρία,, Conference Paper : Conference: ΕΛΛΗΝΙΚΟ ΤΜΗΜΑ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΚΑΙ ΔΙΕΘΝΟΥΣ ΕΤΑΙΡΕΙΑΣ ΠΕΡΙΦΕΡΕΙΑΚΗΣ ΕΠΙΣΤΗΜΗΣ, 12ο ΕΠΙΣΤΗΜΟΝΙΚΟ ΣΥΝΕΔΡΙΟ «Αστική και Περιφερειακή Ανάπτυξη: σύγχρονες προκλήσεις» at: Athens Greece, σελ. 4

γραφειοκρατικών διαδικασιών και τον προσδιορισμό νέων, καινοτόμων λύσεων για τη διαχείριση της πολυπλοκότητας του αστικού χώρου και την επιδίωξη της βιώσιμης αστικής ανάπτυξης[37].

Σε μια «έξυπνη πόλη» χρησιμοποιούνται διαφορετικοί τύποι ηλεκτρονικών αισθητήρων συλλογής δεδομένων για την παροχή πληροφοριών. Η ιδέα ενσωματώνει την τεχνολογία πληροφοριών και επικοινωνιών (ΤΠΕ) και διασυνδεόμενες συσκευές του ΔτΠ με σκοπό την βελτιστοποίηση των λειτουργιών των πόλεων.

Οι τομείς των λειτουργιών και των υπηρεσιών των πόλεων τους οποίους επιχειρεί να βελτιώσει η ιδέα της «έξυπνης πόλης» με τη χρήση των ανάλογων τεχνολογιών έχει ως εξής:

Πίνακας 1

Τομέας	Εφαρμοζόμενες Τεχνολογίες
Διακυβέρνηση	Συστήματα ηλεκτρονικής διακυβέρνησης (e-government), διαδικτυακές συναλλαγές, λειτουργικά συστήματα πόλεων, συστήματα διαχείρισης απόδοσης.
Μεταφορές	Ευφυή συστήματα μεταφορών, ολοκληρωμένο σύστημα έκδοσης εισιτηρίων.
Ενέργεια	Έξυπνα πλέγματα, έξυπνοι μετρητές, εφαρμογές χρήσης ενέργειας, έξυπνος φωτισμός.
Ασφάλεια και διαχείριση περιστατικών έκτακτης ανάγκης	Κεντρικοί θάλαμοι ελέγχου. ψηφιακή παρακολούθηση, προγνωστική αστυνόμευση, συντονισμένη αντίδραση έκτακτης ανάγκης.
Αστικά απόβλητα	Κάδοι συμπίεσης απορριμμάτων και δυναμική δρομολόγηση / συλλογή τους.
Ρύπανση περιβάλλοντος	Δίκτυα αισθητήρων (π.χ. ρύπανσης, θορύβου, καιρού, κίνησης εδάφους, διαχείρισης πλημμυρών).
Κτίρια	Συστήματα διαχείρισης κτιρίων, δίκτυα

[37] βλ. Torppeta D. (2010), The Smart City Vision: How Innovation and ICT Can Build Smart, Livable, Sustainable Cities, *Think! The Innovation Knowledge Foundation,* Report 5/2010

Τομέας	Εφαρμοζόμενες Τεχνολογίες
	αισθητήρων.
Σπίτια	Έξυπνοι μετρητές, έξυπνες συσκευές ελεγχόμενες από εφαρμογή.

Παρότι στην πράξη κάθε «έξυπνη πόλη» έχει τα δικά της συγκεκριμένα χαρακτηριστικά λόγω των ιδιαιτεροτήτων κάθε επιμέρους πόλης, η ιδέα και οι στόχοι είναι παντού οι ίδιοι. Η προσδοκία όλων είναι η δημιουργία πόλεων, όπου όλες οι λειτουργίες και οι υπηρεσίες τους θα είναι διασυνδεδεμένες με σκοπό την αντιμετώπιση και την βελτιστοποίηση των καθημερινών αστικών ζητημάτων. Συγκεκριμένα, όπως προκύπτει και από τον Πίνακα 1 μια «έξυπνη» πόλη επιχειρεί τη δημιουργία: α) «Έξυπνης» οικονομίας με την προώθηση της επιχειρηματικότητας, της καινοτομίας, της παραγωγικότητας, και ανταγωνιστικότητας· β) «Έξυπνης» κυβέρνησης, επιτρέποντας νέες μορφές και νέους τρόπους λειτουργίας ηλεκτρονικής διακυβέρνησης, βελτιωμένα μοντέλα και προσομοιώσεις για την καθοδήγηση της μελλοντικής ανάπτυξης, αποδεικτικά στοιχεία λήψης αποφάσεων, καλύτερη παράδοση υπηρεσιών, και να κάνει την κυβέρνηση περισσότερο διαφανή, συμμετοχική και υπεύθυνη· γ) «Έξυπνων» πολιτών, δημιουργώντας έναν πιο ενημερωμένο πολίτη και προωθώντας τη δημιουργικότητα, την επαγρύπνηση και τη μεγαλύτερη συμμετοχικότητα· δ) «Έξυπνες» μεταφορές με τη δημιουργία ευφυών συστημάτων μεταφορών και λειτουργικότερων συστημάτων δημόσιων συγκοινωνιών· ε) «Έξυπνο» περιβάλλον προωθώντας τη βιωσιμότητα και την ανάπτυξη της πράσινης ενέργειας με την αποτελεσματικότερη διαχείριση των αστικών αποβλήτων και την αντιμετώπιση των αστικών ρύπων· στ) «Έξυπνη» διαβίωση βελτιώνοντας την ποιότητα ζωής, αυξάνοντας την ασφάλεια και τη διαχείριση των περιστατικών έκτακτης ανάγκης. Εν ολίγοις, η παραγωγή «έξυπνων» πόλεων υπόσχεται να λύσει θεμελιώδη σύγχρονα αστικά ζητήματα μειώνοντας το κόστος και δημιουργώντας οικονομική ανάπτυξη ταυτόχρονα με τη βελτίωση των υπηρεσιών και την αύξηση της συμμετοχής και πρωτευόντως της ποιότητας ζωής.

Κεντρικό στοιχείο της δημιουργίας των «έξυπνων» πόλεων είναι η δημιουργία, συλλογή, επεξεργασία, ανάλυση και κοινή χρήση τεραστίων ποσοτήτων δεδομένων σχετικά με την υποδομή, τις υπηρεσίες και τους πολίτες της πόλης. Πράγματι, οι τεχνολογίες των «έξυπνων» πόλεων αφορούν ακριβώς τη δημιουργία πόλεων στη βάση των δεδομένων, επιτρέποντας δηλαδή στα συστήματα και στις υπηρεσίες των πόλεων να ανταποκρίνονται και να ενεργούν βάσει δεδομένων,

κατά προτίμηση δεδομένων σε πραγματικό χρόνο. Επομένως, δεν είναι σύμπτωση ότι η προσπάθεια δημιουργίας έξυπνων πόλεων συνδυάζεται με την επερχόμενη επανάσταση δεδομένων.

Οι «έξυπνες» πόλεις κινούνται και αναπτύσσονται από έναν κατακλυσμό από «Μεγάλα» και ανοιχτά δεδομένα ("open data") που προέρχονται από:

- εταιρίες κοινής ωφέλειας (εταιρίες ηλεκτρικής ενέργειας, φυσικού αερίου, νερού, φωτισμού),
- παρόχους μεταφορών (δεδομένα τοποθεσίας/κίνησης, ροής κυκλοφορίας),
- χρήστες κινητών συσκευών/τηλεφώνων/tablets/smartwatches (δεδομένα τοποθεσίας/ κίνησης, χρήσης εφαρμογών, συμπεριφορικά δεδομένα),
- ιστότοπους ταξιδιών και καταλυμάτων (κριτικές, σχόλια, δεδομένα τοποθεσίας/μετακίνησης, κατανάλωση προϊόντων),
- μέσα κοινωνικής δικτύωσης (απόψεις, φωτογραφίες, προσωπικές πληροφορίες, δεδομένα τοποθεσίας/μετακίνησης),
- πληθοπορισμός ("crowdsourcing") και επιστήμη πολιτών , χάρτες (π.χ. OpenStreetMap),τοπικές γνώσεις-βασισμένες στην εμπειρία (π.χ. Wikipedia), καιρός.
- κυβερνητικοί φορείς και δημόσια διοίκηση (υπηρεσίες, έρευνες).
- βιβλιοθήκες, μουσεία, ραδιοτηλεοπτικοί οργανισμοί, αρχεία (ιστορία ανθρώπων, πολιτισμών και τόπων),
- χρηματοπιστωτικά ιδρύματα και αλυσίδες λιανικής (κατανάλωση, τοποθεσία),
- ιδιωτικές εταιρείες επιτήρησης και ασφάλειας (δεδομένα τοποθεσίας, συμπεριφορικά δεδομένα),
- υπηρεσίες έκτακτης ανάγκης (ασφάλεια, εγκληματικότητα, αστυνόμευση) και
- οικιακές συσκευές και συστήματα ψυχαγωγίας (συμπεριφορικά δεδομένα, στοιχεία κατανάλωσης).

Ενώ πολλά από αυτά τα δεδομένα είναι μη διαθέσιμα και μη προσπελάσιμα, ορισμένα από αυτά είναι σε κοινή χρήση με τρίτους προμηθευτές και ορισμένα είναι ανοιχτά (μέσω υποδομών δεδομένων ή APIs) με σκοπό να αξιοποιηθούν για όλους τους τομείς της «έξυπνης» πόλης. Πρωτοβουλίες έξυπνων πόλεων ανά τον κόσμο όπως αστικά λειτουργικά συστήματα επιδιώκουν να

συνδέσουν πολλαπλές τεχνολογίες «έξυπνων» πόλεων για να επιτρέψουν μεγαλύτερο συντονισμό των συστημάτων της πόλης. Ομοίως, τα αστικά λειτουργικά κέντρα και οι αστικοί πίνακες ελέγχου προσπαθούν να σχεδιάσουν και να συνδέσουν όσο περισσότερα από τα δεδομένα τους μαζί για να παρέχουν «νοημοσύνη πόλης». Η αφθονία δεδομένων και οι νέες αναλύσεις ("data analytics") βοηθούν επίσης στη δημιουργία νέων αναλυτικών πεδίων όπως η αστική πληροφορική (μια προσέγγιση πληροφόρησης και αλληλεπίδρασης ανθρώπου-υπολογιστή για την εξέταση και επικοινωνία αστικών διαδικασιών) και η αστική επιστήμη (μια υπολογιστική προσέγγιση μοντελοποίησης και προσομοίωσης στην κατανόηση, την εξήγηση και την πρόβλεψη των διαδικασιών της πόλης)[38].

2.2 Το «έξυπνο» σπίτι

Εξέχουσα θέση στην ανάπτυξη των τεχνολογιών του ΔτΠ κατέχει η «έξυπνη» κατοικία, μιας και το σπίτι αποτελεί ένα χώρο στον οποίο ο σύγχρονος άνθρωπος περνάει σημαντικό μέρος της καθημερινότητας του. Η ιδέα βασίζεται σε εφαρμογές που μέσω διασυνδεδεμένων συσκευών και αισθητήρων που ασχολούνται με την εν γένει παρακολούθηση και ρύθμιση των πόρων και των συνθηκών στο περιβάλλον της οικείας με δυνατότητα ελέγχου και αλληλεπίδρασης αυτόματα ή εξ' αποστάσεως σε πραγματικό χρόνο. Οι εφαρμογές αυτές καλύπτουν όλο το φάσμα των αναγκών μιας κατοικίας, όπως η ασφάλεια, η διατροφή των ενοίκων και των κατοικίδιων αλλά και η ρύθμιση των συνθηκών εντός και εκτός της κατοικίας.

Πιο συγκεκριμένα, οι αισθητήρες συλλέγουν δεδομένα από τους εσωτερικούς και τους εξωτερικούς χώρους της κατοικίας, όπως θερμοκρασία, φωτισμό, υγρασία, θόρυβο και ατμοσφαιρική πίεση, ενώ συλλέγει δεδομένα που αφορούν τους ενοίκους του, όπως οι διατροφικές τους επιλογές, οι συνήθειες τους (π.χ. παρακολούθηση προγραμμάτων σε μια smart-τηλεόραση ή πότε επιστρέφουν στην κατοικία τους) και διάφορα δεδομένα υγείας[39]. Οι χρήστες των εφαρμογών της «έξυπνης» κατοικίας μέσω του οικιακού δικτύου Wi-fi τους, διαφόρων διασυνδεδεμένων

[38] βλ. Rob Kitchin (2016, Ιανουάριος), Getting smarter about smart cities: Improving data privacy and data security, *Data Protection Unit, Department of Taoiseach, Dublin Ireland*, σελ. 19-20

[39] βλ. National Institute of Standards and Technology -NIST (2013), Foundations for Innovation in Cyber-Physical Systems, Workshop report, σελ. 1 επ., διαθέσιμο στον διαδικτυακό σύνδεσμο: https://www.nist.gov/system/files/documents/el/CPS-WorkshopReport-1-30-13-Final.pdf

οικιακών ηλεκτρικών συσκευών (τηλεοράσεις, δέκτες AV, κινητές συσκευές, ψυγείο κ.ο.κ.) και με μια σειρά από μεθόδους πρόσβασης (όπως λ.χ. smart speakers, οθόνες αφής, κινητά τηλέφωνα, tablets) αλληλεπιδρούν με το περιβάλλον τους και το ρυθμίζουν- ακόμα και απομακρυσμένα και σε πραγματικό χρόνο- ανάλογα με τις προτιμήσεις και τις ανάγκες τους[40].

Εικόνα 3: Παράδειγμα ενός «έξυπνου» σπιτιού

πηγή εικόνας: Hesham Bahram.com

Για να κατανοήσουμε το μέγεθος των πληροφοριών που συλλέγονται σε ένα «έξυπνο» σπίτι, αρκεί να φανταστούμε ένα πλήρως εξοπλισμένο σπίτι με «έξυπνες» συσκευές στην κουζίνα, το υπνοδωμάτιο, το μπάνιο, το γκαράζ και τον κήπο (όπως αυτό της Εικόνας υπ'αριθμ. 3), τα οποία ελέγχονται με φωνητικές εντολές μέσω ενός «έξυπνου» μικροφώνου (“Smart Speakers”, όπως λ.χ. Amazon Echo, Google Home). Οι συσκευές του υπνοδωματίου, συλλέγουν δεδομένα για την ώρα που οι ένοικοι του σπιτιού σηκώνονται από το κρεβάτι τους, η «έξυπνη» καφετιέρα για το πως και πότε καταναλώνουν τον καφέ τους και οι αισθητήρες της εξώπορτας γα την ώρα που αναχωρούν για την εργασία τους. Εν συνεχεία, συλλέγονται από τους αισθητήρες της πόρτας του γκαράζ δεδομένα για το το χρόνο που επιστρέφουν από την εργασία τους, ενώ το «έξυπνο» ψυγείο «γνωρίζει» ποια τρόφιμα καταναλώνονται ως μεσημεριανό γεύμα. Αποθηκεύονται, επίσης, οι προτιμήσεις θερμοστάτη και φωτισμού, ενώ και οι υπόλοιπες «έξυπνες» συσκευές συλλέγουν σχεδόν όλες τις συνήθειες των ενοίκων μέχρι τη στιγμή που θα αποχωρήσουν πάλι από την κατοικία τους, ενώ τα «έξυπνα» μικρόφωνα καταγράφουν κάθε φωνητική εντολή και ενδεχόμενα κάθε άλλον

[40] βλ. Dr. Ovidiu Vermesan & Dr. Peter Friess (2013), Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, Rivers Publishers Series in Communication, σελ. 55 επ.

ήχο εντός της οικείας[41]. Τέλος, τα συλλεγόμενα δεδομένα από κάθε συσκευή και αισθητήρα ενδέχεται να διαμοιράζονται και στις άλλες συσκευές του «έξυπνου» σπιτιού, με γνώμονα ότι όσο μεγαλύτερος ο όγκος των επεξεργαζόμενων δεδομένων τόσο βελτιστοποιημένη θα είναι η προσφερόμενη υπηρεσία της τεχνολογίας του ΔτΠ στην κατοικία.

2.3 Ηλεκτρονική Υγεία και « Έξυπνο» Νοσοκομείο

Η ηλεκτρονική υγεία (“e-health”) αποτελεί μία διαδικασία με την οποία τροφοδοτείται, αφενός το σύστημα υγείας με ιατρικές πληροφορίες μέσω ηλεκτρονικών μέσων και αφετέρου καθίσταται εφικτή η σύνδεση μεταξύ ασθενούς και γιατρών ή συστημάτων υγείας σε ολόκληρο τον κόσμο. Αυτό επιτυγχάνεται με τη χρήση του Διαδικτύου, που παρέχει τις υποδομές για την κοινή αποδοχή της ηλεκτρονικής υγείας παγκοσμίως, καθώς και την εφαρμογή και ανάπτυξη ηλεκτρονικών εφαρμογών υγείας (“e-health applications”). Μέσω της υιοθέτησης αυτής, προωθείται ένα εκσυγχρονισμένο σύστημα υγείας, που ενδεχομένως να προσφέρει μία πληθώρα καινοτομιών, με ενιαίο στόχο τους την εξοικονόμηση χρόνου αλλά και πόρων οικονομικού και περιβαλλοντικού περιεχομένου[42], εφόσον πρωτίστως, δεν θα είναι απαραίτητη η εγγύτητα ανάμεσα σε ασθενή και ιατρικό προσωπικό και επομένως θα δύναται να εξυπηρετείται ο ασθενής άμεσα χωρίς την παρουσία του, ενώ δευτερευόντως, μέσω υπηρεσιών διαδικτυακού φακέλου ασθενούς, δεν θα είναι πλέον απαραίτητη η κατανάλωση χαρτιού για την τύπωση πολλών εκατοντάδων χιλιάδων φωτοτυπιών για την πληθώρα των ιατρικών εγγράφων των ασθενών ούτε και, συνεπώς, η αυτοπρόσωπη εμφάνιση του ασθενούς σε διάφορες υπηρεσίες για τη λήψη αντιγράφων του ιατρικού ιστορικού του, των εξετάσεων του και άλλων χρήσιμων αρχείων.

Η υιοθέτηση του ηλεκτρονικού φακέλου του ασθενή, απαιτεί και την εφαρμογή της τεχνολογίας του «Υπολογιστικού Νέφους» στα νοσοκομεία, σε κλινικές καθώς και σε ιδιωτικά ιατρεία. Με την εφαρμογή του διευκολύνεται η πρόσβαση στα ιατρικά αρχεία ενός ασθενούς από τον ιατρό του και συνεπώς η αντιμετώπιση διαφόρων προβλημάτων υγείας που δεν απαιτούν την αυτοπρόσωπη παρουσία του ασθενούς. Με τη λειτουργία του θεσμού αυτού, προωθείται ένας

[41] βλ. αναλυτικότερα Matthew Day (2019, 19 Φεβρουαρίου), *Your Smart Light Can Tell Amazon and Google When You Go to Bed.* Ανάκτηση από bloombergquint.com στις 15 Απριλίου 2021, διαθέσιμο στον διαδικτυακό σύνδεσμο:https://www.bloombergquint.com/pursuits/your-smart-light-can-tell-amazon-and-google-when-you-go-to-bed

[42] βλ. Sofia Ouhbi, José Luis Fernández-Alemán, Juan Manuel Carrillo-de-Gea, Ambrosio Toval & Ali Idri (2017), E-health internationalization requirements for audit purposes, *Journal, Elsevier North-Holland, Inc. New York, NY, USAComputer Methods and Programs in Biomedicine archive*, σ.σ. 49-60, σελ. 51 επ.

οικονομικότερος και αποτελεσματικότερος τρόπος επίλυσης ιατρικών προβλημάτων, κυρίως για ασθενείς που δεν έχουν εύκολη πρόσβαση σε ιατρικά κέντρα.

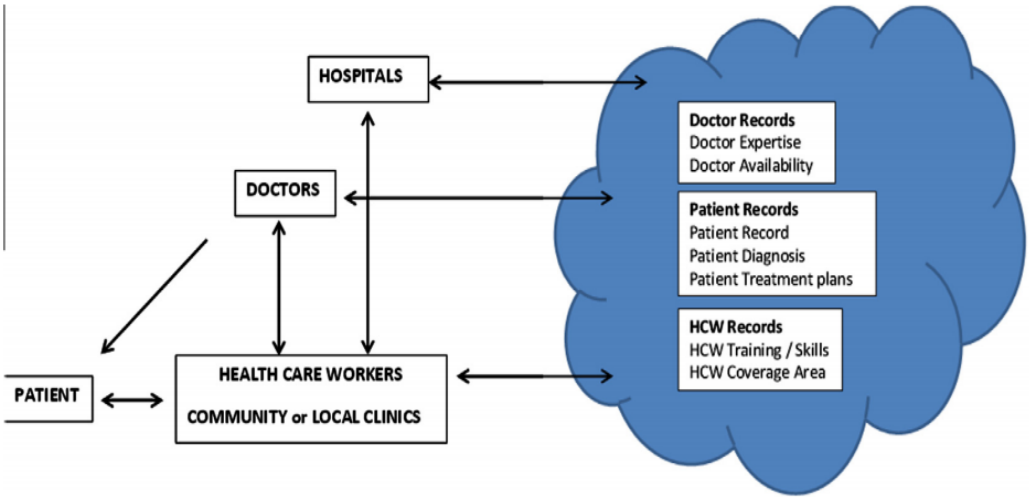


Fig. 1. Working components of the ensemble e-health artefact architecture.

Εικόνα 4: Επεξεργασία δεδομένων ασθενούς κατά τη χρήση του e-health

Πηγή: Shah J. Miah , Jahidul Hasan, John G. Gammack (2017), On-Cloud Healthcare Clinic: An e-health consultancy approach for remote communities in a developing country

Στην παραπάνω εικόνα (εικόνα υπ' αριθμ. 4) δίνεται ένα παράδειγμα χρησιμότητας των ηλεκτρονικών φακέλων υγείας: Αρχικά, ο ασθενής ξεκινάει τη διαδικασία εγγραφής του με έναν υπεύθυνο του συγκεκριμένου συστήματος υγείας (είτε κλινική είτε δημόσιο νοσοκομείο είτε ιδιωτικός ιατρός) και στη συνέχεια, αφού ο ασθενής έχει λάβει στοιχεία εισόδου του σε έναν ιστότοπο, ακολουθεί μια διαδικασία μεταφοράς των ιατρικών αρχείων του ασθενούς στο «σύννεφο»(“cloud”), η συσχέτιση του προβλήματός του με αντίστοιχα ήδη υπάρχοντα ιατρικά προβλήματα στη βάση δεδομένων, ώστε να κατανεμηθούν ορθώς. Επιπλέον, αφού ανιχνευθεί το είδος του προβλήματος, η υπόθεση του ασθενούς συνδέεται με κάποιον ιατρό βάσει ειδικότητάς του και αυτός, καθίσταται υπεύθυνος στην αρχική διάγνωση του προβλήματος και τελικώς, στην

προώθηση των στοιχείων αυτών στο αρμόδιο νοσοκομείο/κλινική. Εφ' εξής, μπορεί είτε να γίνει συνταγογράφηση για την λήψη φαρμάκων είτε καθοδήγηση για την αντιμετώπιση της ασθένειας[43].

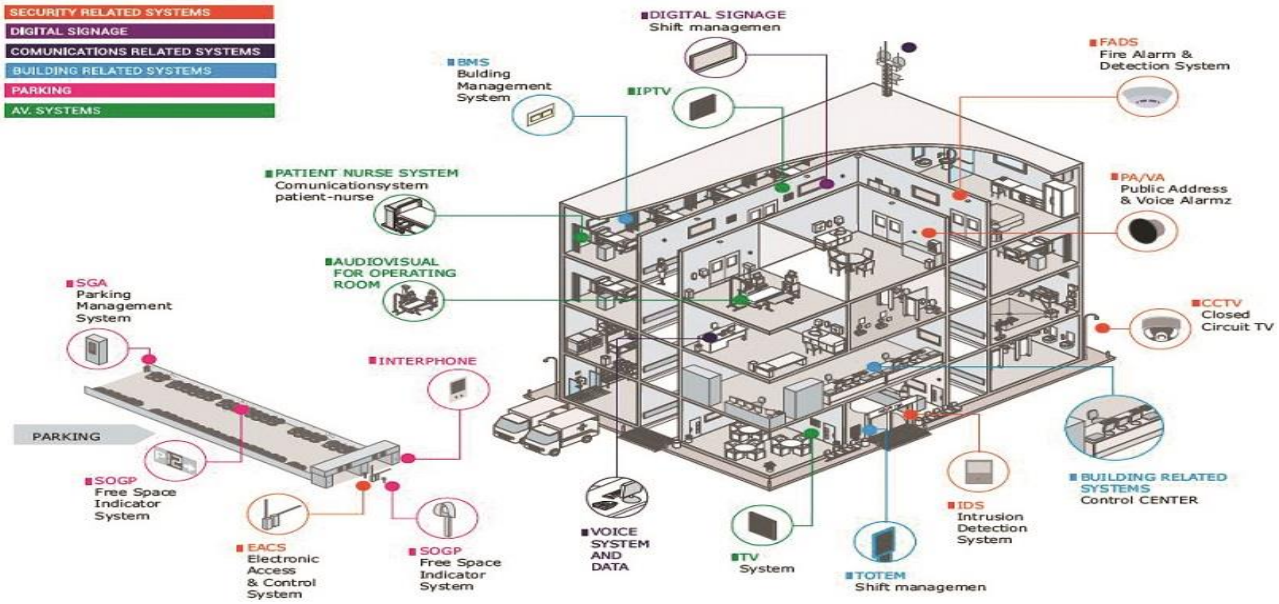
«Έξυπνο» νοσοκομείο ("Smart" hospital) μπορεί να χαρακτηριστεί ένα νοσοκομείο που λειτουργεί με αυτοματοποιημένες και ιδανικές διαδικασίες, χτισμένο σε ένα περιβάλλον τεχνολογιών πληροφοριών και επικοινωνιών βασισμένο στις τεχνολογίες του ΔτΠ, έτσι ώστε να βελτιώσει τη φροντίδα των ασθενών και να προωθήσει και να εφαρμόσει καινοτομίες στον τομέα της υγείας[44]. Στόχος, λοιπόν, των «έξυπνων» νοσοκομείων, είναι συλλέγοντας όλα τα απαραίτητα δεδομένα να βελτιώσει τη διάγνωση των ασθενειών, την μείωση του χρόνου αναμονής στα νοσοκομεία και συνεπώς να επιτύχει στη μεγαλύτερη άνεση και γρηγορότερη εξυπηρέτηση των ασθενών χωρίς μεγάλους χρόνους αναμονής, στην εξ' αποστάσεως ιατρική φροντίδα μέσω προώθησης του θεσμού του ΔτΠ. Δηλαδή, να δύναται να επιλυθεί ή να διαγνωσθεί το ιατρικό θέμα του ασθενούς ακόμη και αν βρίσκεται στην οικία του, με τη χρήση κάποιων συσκευών του ΔτΠ που θα πραγματοποιούν λ.χ. μετρήσεις σακχάρου ή καρδιακών παλμών με τη χρήση συσκευών ιχνηλάτησης δραστηριότητας ("activity trackers") ή ακόμη και βηματοδότη.

Τέλος, στην παρακάτω εικόνα (Εικόνα υπ' αριθμ. 5), δίνεται ένα παράδειγμα ενός «έξυπνου» νοσοκομείου, όπου όπως γίνεται αντιληπτό, υπάρχει πλήρης αυτοματοποίηση όλων των διαδικασιών εντός του νοσοκομείου. Τούτο βέβαια, δεν αποτελεί ένα απλό ζήτημα, καθώς η κατασκευή ενός τέτοιου κτίσματος καθώς και η συντήρηση του αποτελεί ένα μεγάλου οικονομικού κόστους έργο. Παρόλα αυτά, με την χρήση των υποδομών αυτών, επιτυγχάνεται ο σκοπός λειτουργίας ενός έξυπνου νοσοκομείου, αφού πληρούνται οι προαναφερθέντες στόχοι και συνεπώς η εξυπηρέτηση των ασθενών είναι κατά έναν μεγάλο βαθμό βελτιωμένη.

---

[43] βλ. Shah J. Miah, Jahidul Hasan, John G. Gammack (2017) On-Cloud Healthcare Clinic: An e-health consultancy approach for remote communities in a developing country, *Telematics and Informatics*, σ.σ. 311-322 (volume 34, issue 1), σελ. 314 επ.

[44] βλ. ENISA (2016, Νοέμβριος), Smart Hospitals- Security and Resilience for Smart Health Service and Infrastructures, *European Union Agency For Network And Information Security,* σελ.9, διαθέσιμο στον διαδικτυακό σύνδεσμο:https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals/at_download/fullReport



Εικόνα 5: Έξυπνο Νοσοκομείο

Πηγή: www.coolingindia.in

Κεφάλαιο 3ο

3.1 Κίνδυνοι και Ασφάλεια στο ΔτΠ

Το ΔτΠ εκτός από τις τεχνολογικές προκλήσεις και τους οικονομικούς ορίζοντες που ανοίγει για τον επιχειρηματικό κόσμο και την απαιτούμενη άνεση που προσφέρει σε κάθε πολίτη/καταναλωτή, κρύβει και κινδύνους για την ασφάλεια των ανθρώπων και της ιδιωτικότητας τους.

Η εξάπλωση του Διαδικτύου και η όλο και πιο ευρεία χρήση του σε πολλούς τομείς της καθημερινότητας αλλά και σε κρίσιμες εργασίες της επιχειρηματικής δραστηριότητας, οδήγησε και στην αύξηση των κρουσμάτων ασφαλείας. Η εισαγωγή της ασύρματης επικοινωνίας και η σχεδόν καθολική χρήση των «έξυπνων» τηλεφώνων από την πλειοψηφία του παγκόσμιου πληθυσμού δημιούργησε μια παγκόσμια ψηφιακή κοινότητα χωρίς σύνολα, η οποία είναι εκτεθειμένη σε κακόβουλες επιθέσεις. Όσο, λοιπόν, το Δτπ εξαπλώνεται με τη χρήση δισεκατομμυρίων συσκευών, από τους απλούς αισθητήρες καταγραφής θερμοκρασίας μέχρι και πολύπλοκες συσκευές ελέγχου βιομηχανικών μονάδων, ιατρικών μηχανημάτων και στρατιωτικών όπλων, τόσο μεγαλώνουν και οι φόβοι για την ασφάλεια τους και την προστασία του ανθρώπου και της ιδιωτικότητας του.

Οι κίνδυνοι που σχετίζονται με τις συσκευές του ΔτΠ είναι πολυάριθμοι και ποικίλοι και σχετίζονται με τους τομείς εφαρμογής της τεχνολογίας. Ως τεχνολογία στην οποία δεδομένα και

πληροφορίες διακινούνται συνεχώς και προς πάσα κατεύθυνση, ελοχεύει ο κίνδυνος οι πληροφορίες να καταχραστούν ή να αποκτηθεί μη εξουσιοδοτημένη πρόσβαση στις συσκευές με σκοπό τον έλεγχο της λειτουργίας τους ή την καταστροφή τους. Οι κίνδυνοι αυτοί,βέβαια, εμφανίζονται και σε κάθε παραδοσιακό δίκτυο υπολογιστών. Στο ΔτΠ, όμως, ελλοχεύουν κίνδυνοι που δεν συναντώνται στα παραδοσιακά δίκτυα, όπως είναι ο κίνδυνος καταστροφής των συσκευών, αλλά και κινδύνους για τη σωματική ακεραιότητα και τη ζωή των χρηστών. Αυτό μπορεί να γίνει καλύτερα κατανοητό, εάν αναλογιστούμε ένα δίκτυο 10 εκατομμυρίων αυτοκινούμενων οχημάτων να κυκλοφορούν στους δρόμους. Αν τέτοιες συσκευές πέσουν θύμα κακόβουλης επίθεσης, όχι μόνο η οδική ασφάλεια θα επηρεαστεί, αλλά και οι ζωές των χρηστών - επιβαινόντων σ' αυτά. Επιπλέον, οι συσκευές του ιατρικού ΔτΠ, όπως οι βηματοδότες είναι ένα άλλο καλό παράδειγμα των σοβαρών σωματικών απειλών που δημιουργούνται από μη ασφαλείς συνδεδεμένες συσκευές.

Ο κίνδυνος έγκειται όχι μόνο στη δυνατότητα των επιτιθέμενων να λαμβάνουν τον έλεγχο των συσκευών αλλά και σε σχέση με τη μαζική και συνεχή αποθήκευση «Μεγάλων Δεδομένων» που παράγονται από τα «έξυπνα» αντικείμενα. Μάλιστα, οι συσκευές με εκτεταμένες δυνατότητες συλλογής δεδομένων είναι βρίσκονται όλο και περισσότερο σε χώρους που συνήθως θεωρούνται ιδιωτικοί (π.χ. σπίτια, αυτοκίνητα, ακόμα και στο σώμα μας). Οι συσκευές αυτές παράγουν κολοσσιαία ποσά δεδομένων, συμπεριλαμβανομένων των απόρρητων πληροφοριών και των ευαίσθητων δεδομένων. Ο τεράστιος όγκος και η αξία των δεδομένων αυτών δημιουργεί μεγάλη δυναμική για κακόβουλες ενέργειες και κακή χρήση τους[45].

3.2 Ευπάθειες του ΔτΠ

Ένα δίκτυο του ΔτΠ αποτελείται κατά κύριο από ασύρματα δίκτυα αισθητήρων ("WSN") και συνδεόμενων συσκευών, οι οποίες εποπτεύουν αντικείμενα ή/και συλλέγουν δεδομένα. Σε ένα τέτοιο ασύρματο δίκτυο οι συσκευές φέρουν έναν ή περισσότερους αισθητήρες και διαθέτουν χαμηλή επεξεργαστική ισχύ, καταναλώνουν ελάχιστη ενέργεια υλοποιώντας αδόμητα ή δομημένα δίκτυα. Στα δομημένα δίκτυα οι αισθητήρες συνδέονται με έναν κεντρικό σταθμό, ενώ στα αδόμητα είναι περισσότεροι και αλληλοσυνδέονται υλοποιώντας αλγόριθμους δρομολόγησης πληροφορίας

[45] βλ.. Rolf H. Weber και Evelyne Studer (2016), Cybersecurity in the Internet of Things: Legal aspects, *Elsevier, Computer law & Security review 32*, σ.σ. 715-728, σελ. 719 ε.π.

με βάση τη βέλτιστη διαχείριση ενέργειας. Η ασφάλεια των δεδομένων ενός ασύρματου δικτύου αισθητήρων αντιμετωπίζει διάφορες προκλήσεις.

Συγκεκριμένα, οι μηχανισμοί διασφάλισης θα πρέπει να λαμβάνουν υπόψιν τους τη χαμηλή επεξεργαστική ισχύ και την περιορισμένη κατανάλωση ενέργειας των συσκευών, μιας και τα δεδομένα εκπέμπονται μέσω ενός κοινού μέσου (αέρας)[46]. Οι περιορισμένες δυνατότητες των συσκευών, καθιστούν λοιπόν πολλές παραδοσιακές μεθοδολογίες ασφάλειας αδύνατο να χρησιμοποιηθούν, δημιουργώντας σημαντικό ζήτημα στην ασφάλεια τους[47]. Μια βλάβη στην υποδομή του δικτύου από διαδικτυακή επίθεση ή φυσική καταστροφή μπορεί να οδηγήσει σε σημαντικά προβλήματα, το μέγεθος των οποίων γίνεται ακόμη πιο ορατό αν συνυπολογίσουμε την άμεση σύνδεση των συσκευών και των αισθητήρων με τα διακινούμενα δεδομένα. Μάλιστα, τα ασύρματα δίκτυα αισθητήρων μπορεί να είναι πιο εκτεθειμένα σε κακόβουλες επιθέσεις από άλλα δίκτυα, ενώ και η μορφή και η πολυπλοκότητα των επιθέσεων αυτών παρουσιάζει σχεδόν καθημερινές αλλαγές[48].

Επιπλέον, έχει υποστηριχθεί ότι η διασφάλιση του ΔτΠ έχει καταστεί ένα δύσκολο εκπόνημα, καθώς τα τρωτά σημεία του είναι δυσκολότερο να εντοπιστούν και να ασφαλιστούν επειδή τα μέτρα ασφαλείας αναπτύσσονται (μόνο μετά από επιθέσεις), το εύρος των επιθέσεων είναι μεγάλο (π.χ. επιθέσεις σε υλισμικό, λογισμικό, πρωτόκολλα επικοινωνίας κ.λπ.), ενώ κάθε προκληθείσα βλάβη περιουσιακή ή μη είναι σημαντική λόγω της φύσης των υπηρεσιών που προσφέρονται και των δεδομένων που διακινούνται[49].Συνακόλουθα, όσο επεκτείνεται το ΔτΠ με ταχύτατους ρυθμούς αυξάνοντας τα δίκτυα συνδεδεμένων συσκευών με το Διαδίκτυο, δημιουργεί εκθετικά περισσότερους φορείς κυβερνοεπιθέσεων γεγονός που με τη σειρά του εισάγει εκθετικά μεγαλύτερο αριθμό κινδύνων ασφαλείας[50].

---

[46] βλ. Ιωάννης Μαυρίδης (2015), Ασφάλεια Πληροφοριών στο Διαδίκτυο, Ελληνικά Ακαδημαϊκά Ηλεκτρονικά Συγγράμματα και Βοηθήματα, σελ. 45-46

[47] βλ. Oreku, G., & Pazynyuk, T (2016), Security in Wireless Sensor Networks,, Springer International Publishing, σελ.11

[48] βλ. αναλυτικότερα Internet of Things: Wireless Sensor Networks (2014, 26 Νοεμβρίου), *International Electrotechnical Commission, White Paper*, σελ. 39-40, διαθέσιμο στον διαδικτυακό σύνδεσμο:https://storage-iecwebsite-prd-iec-ch.s3.eu-west-1.amazonaws.com/2019-09/content/media/files/iec_wp_internet_of_things_en.pdf

[49] βλ. Dr Lachlan Urquhart και Dr Lachlan Urquhart, *Avoiding the Internet of Insecure Industrial Things*, Computer Law and Security Review, σ.σ. 450-466, σελ 453 επ. (Volume 34, Issue 3)

[50] βλ. Rolf H. Weber και Evelyne Studer, ο.π., σελ. 715 επ.

Η ταχύτητα με την οποία αναπτύσσεται το ΔτΠ έχει βάλει τον τομέα της ασφάλειας σε δεύτερη μοίρα, καθιστώντας ως επί το πλείστον τις «έξυπνες» συσκευές μη ασφαλείς. Σύμφωνα με έρευνα της εταιρίας Hewlett Packard, το έτος 2015 το 70 % των συσκευών του ΔτΠ έχουν ευπάθειες ασφαλείας, που αφορούν μη ισχυρούς κωδικούς πρόσβασης, ελλειπή κρυπτογράφηση και γενικότερη έλλειψη έλεγχου πρόσβασης των χρηστών. Μάλιστα, σύμφωνα πάντα με την ίδια έρευνα, κάθε συσκευή του ΔτΠ είχε κατά μέσο όρο 25 ευπάθειες ασφαλείας[51].

Χαρακτηριστικά θα μπορούσαμε να αναφέρουμε ότι οι κύριες ευπάθειες ασφαλείας των συσκευών του Δτπ αφορούν:

• Έλλειψη κρυπτογράφησης στη μεταφορά δεδομένων: Πολλές συσκευές του ΔτΠ είναι απλές "μονάδες εργασιών", ενώ όλες οι συσκευές διαθέτουν χαμηλή επεξεργαστική ισχύ για μείωση του κόστους. Αυτό έχει ως αποτέλεσμα ότι οι περισσότερες συσκευές δεν είναι σε θέση την ισχύ επεξεργασίας που απαιτείται για ισχυρά μέτρα ασφαλείας και ασφαλή επικοινωνία μεταξύ των συσκευών, όπως λ.χ. είναι η κρυπτογράφηση. Αυτό είναι, φυσικά, ιδιαίτερα προβληματικό συνυπολογίζοντας τις τεράστιες ποσότητες δεδομένων που μεταδίδονται μεταξύ των «έξυπνων» συσκευών, του υπολογιστικού νέφους και των κινητών εφαρμογών (Mobile apps).

• Ανεπαρκής έλεγχος ταυτότητας και εξουσιοδότησης: Ο έλεγχος ταυτότητας/εξουσιοδότησης μπορεί να είναι ανεπαρκής λόγω της μη χρήσης ισχυρών κωδικών πρόσβασης ή της εν γένει μη χρήσης κωδικών, καθώς και της έλλειψης επαλήθευσης ταυτότητας στις περιπτώσεις συλλογής ευαίσθητων δεδομένων.

• Μη ασφαλής διεπαφή ιστού: Τα ζητήματα ασφαλείας που αφορούν τη διεπαφή ιστού περιλαμβάνουν συνεχείς δέσμες ενεργειών μεταξύ ιστοτόπων (cross-site scripting) και αδύναμα ή προεπιλεγμένα (by default) διαπιστευτήρια.

• Μη ασφαλές λογισμικό και υλικολογισμικό: Λόγω περιορισμών πόρων, οι περισσότερες συσκευές του ΔτΠ έχουν σχεδιαστεί χωρίς τη δυνατότητα λήψης ενημερώσεων λογισμικού ή υλικολογισμικού (που θα ανέβαζε αισθητά το κόστος κατασκευής). Αυτό είναι, φυσικά, προβληματικό καθώς θεωρείται ουσιαστικά αδύνατο να κατασκευαστεί ένα λογισμικό ή υλικολογισμικό χωρίς ευπάθειες. Ακολούθως, η αδυναμία διόρθωσης αυτών των ευπαθειών μέσω μιας αναβάθμισης και ενημέρωσης λογισμικού καθιστά τις συσκευές μη ασφαλείς. Επιπλέον, ακόμα και στις συσκευές

[51] βλ. αναλυτικότερα τα αποτελέσματα της έρευνας της HP στον διαδικτυακό σύνδεσμο: https://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.YH7th-gzbDe

όπου έχει προβλεφθεί η λήψη ενημερώσεων, δεν γίνεται χρήση της κρυπτογράφησης για τις λήψεις ενημερώσεων λογισμικού[52].

Γίνεται, λοιπόν, εύκολα αντιληπτό ότι οι κατασκευαστές των εφαρμογών του ΔτΠ θέτοντας ως πρωταρχικούς στόχους την καινοτομία, τη λειτουργικότητα και τη μείωση του κόστους παραγωγής παραβλέπουν την πολυπόθητη ασφάλεια των συσκευών καθιστώντας το ΔτΠ χώρο δράσης των επίδοξων hackers.

3.3 Ασφάλεια Δεδομένων στο ΔτΠ

Για να καταφέρουμε να αναλογιστούμε, πόσο σημαντική είναι η ασφάλεια στο Διαδίκτυο αρκεί απλά να υπολογίσουμε τις επιπτώσεις που δημιουργούν οι διάφορες κυβερνοεπιθέσεις. Οι επιπτώσεις μια επιτυχημένης επίθεσης αξιολογούνται κυρίως με βάση τη μείωση της αξίας των αγαθών ή/και τη πρόκληση προσωρινής δυσλειτουργίας ή διακοπής της λειτουργίας του εκάστοτε συστήματος. Οι επιθέσεις αυτές μπορεί να προκαλέσουν αποκάλυψη ή αλλοίωση πληροφοριών,άρνηση εξυπηρέτησης, δυσφήμιση και επιπλέον κόστος.

Η αποκάλυψη ή αλλοίωση των πληροφοριών αναφέρεται στην απώλεια της εμπιστευτικότητας (αποκάλυψη) ή της ακεραιότητας (αλλοίωση) μέρους ή του συνόλου μιας διαβαθμισμένης ή ευαίσθητης πληροφορίας που τηρείται σε ένα πληροφοριακό σύστημα και προκαλείται από μη εξουσιοδοτημένη ενέργεια.

Η πρόκληση άρνησης εξυπηρέτησης στις υπηρεσίες του Διαδικτύου προκαλεί την απώλεια της διαθεσιμότητας του συστήματος στους νόμιμους χρήστες του και εμφανίζεται ως ολική αδυναμία προσφοράς της υπηρεσίας ή ως αλλοίωση των ποιοτικών χαρακτηριστικών της (λ.χ. μεγάλος χρόνος απόκρισης). Επιπλέον, τέτοια περιστατικά αλλοίωσης των χαρακτηριστικών μιας διαδικτυακής υπηρεσίας ή κάθε άλλης φύσεως συμβάντα μπορεί να προκαλέσουν αρνητική φήμη γι’ αυτήν με άμεσο αποτέλεσμα την απώλεια δυνητικών ή παρόντων χρηστών. Συνακόλουθα, κάθε περιστατικό ασφαλείας που επιφέρει απώλεια χρηστών λόγω άρνησης εξυπηρέτησης ή δυσφήμισης, επιφέρει αύξηση του κόστους είτε μέσω της απώλειας εσόδων είτε μέσω των

[52] βλ. Rolf H. Weber και Evelyne Studer (2016), ο.π.

ενεργειών για την αποκατάσταση της οιασδήποτε φύσης ζημιάς είτε ακόμα και μέσω δυνητικών ποινών που μπορεί να επιβληθούν από αρχές, όπως τα δικαστήρια[53].

Στο σημείο αυτό, αξίζει να αναφέρουμε μια έρευνα[54] της CSO για τα σημαντικότερα περιστατικά ασφάλειας, και πιο συγκεκριμένα, περιστατικά παραβίασης δεδομένων, που συνέβησαν κατά τον 21ο αιώνα. Σύμφωνα με την οποία έχουν συμβεί 15 σημαντικά περιστατικά παραβίασης δεδομένων μέχρι και το τέλος του έτους 2020, τα οποία αφορούσαν συνολικά δεδομένα 3,5 δισεκατομμυρίων ανθρώπων. Σημαντικότερη όλων, μέχρι σήμερα, κρίνεται η παραβίαση δεδομένων 3 δισεκατομμυρίων χρηστών των εφαρμογών της εταιρίας "Yahoo" το έτος 2013, η οποία μάλιστα και έχει φέρει την εταιρία σε σημαντικό οικονομικό τέλμα[55].

Μάλιστα για μερικές από τις παραπάνω παραβιάσεις δεδομένων οι υπεύθυνες εταιρίες κλήθηκαν από τις αρμόδιες αρχές να πληρώσουν πρόστιμα πολλών εκατομμυρίων ευρώ. Για παράδειγμα, η εταιρία "Marriott" δέχθηκε πρόστιμο ύψους 124 εκατομμυρίων δολαρίων, το οποίο αργότερα μειώθηκε, ενώ η εταιρία "Equifax" συμφώνησε να πληρώσει τουλάχιστον 575 εκατομμύρια δολάρια για την παραβίαση δεδομένων χρηστών που τελέστηκε το έτος 2017. Στις αρχές του 2020 η ρυθμιστική αρχή επέβαλε πρόστιμο στις εταιρίες της "DSG Retail Limited "(DSG) το πρόστιμο μετά την ανακάλυψη κακόβουλου λογισμικού σημείου πώλησης σε πάνω από 5.000 μηχανήματα στα καταστήματα "Currys PC World" και "Dixons Travel" το πρόστιμο των 500.000 αγγλικών λυρών (£), ενώ ρεκόρ αποτελεί το πρόστιμο των 5 δισεκατομμυρίων δολαρίων ($) που κλήθηκε να καταβάλει η εταιρία "Facebook Inc." για παραβιάσεις στις οποίες υπέπεσε η ίδια σχετικά με τη παράνομη χρήση των προσωπικών δεδομένων 87 εκ. χρηστών των εφαρμογών της από την εταιρία "Cambridge Analytica" (σκάνδαλο Cambrige Analytica)[56] .

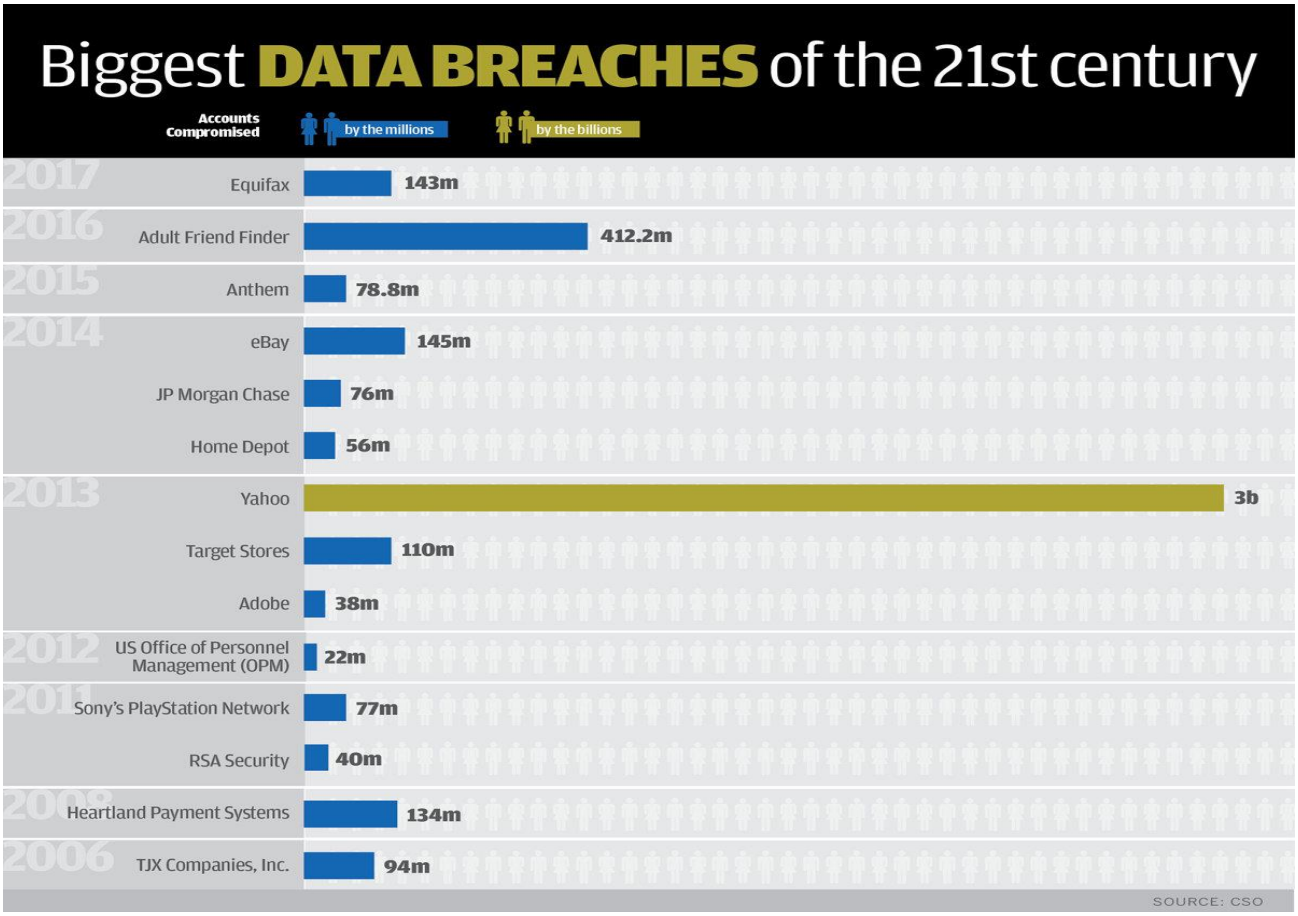
---

[53] βλ. Ιωάννης Μαυρίδης (2015), Ασφάλεια Πληροφοριών στο Διαδίκτυο, Ελληνικά Ακαδημαϊκά Ηλεκτρονικά Συγγράμματα και Βοηθήματα, σελ. 19-22

[54] βλ. Michael Hill & Dan Swinhoe (2021, 16 Ιουλίου), *The 15 biggest data breaches of the 21st century*. Ανάκτηση από csoonline.com στις 20 Απριλίου 2021, διαθέσιμο στον διαδικτυακό σύνδεσμο: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

[55] βλ. *Yahoo triples likely scoope of 2013 hack to 3 billion users* (2017, 03 Μαρτίου). Ανάκτηση από bloomberg.com στις 20 Απριλίου 2021,στον διαδικτυακό σύνδεσμο: https://www.bloomberg.com/news/articles/2017-10-03/yahoo-says-all-3-billion-users-probably-affected-by-2013-breach

[56] βλ. *Πρόστιμο 5 δισ. δολάρια στο Facebook για το σκάνδαλο της Cambridge Analytica* (2019, 13 Ιουλίου). *Ανάκτηση από tovima.gr στις 20 Απριλίου 2021, στον διαδικτυακό σύνδεσμο:* https://www.tovima.gr/2019/07/13/science/prostimo-5-dis-dolaria-sto-facebook-gia-to-skandalo-tis-cambridge-analytica/



Εικόνα 6: Οι σημαντικότερες παραβιάσεις δεδομένων του 21ου αιώνα

Πηγή: IoEBusiness

Όσον αφορά το εξεταζόμενο πεδίο του Δτπ, οι ευπάθειες των συσκευών του έχουν δώσει πρόσφορο έδαφος για κακόβουλες επιθέσεις, οι οποίες έχουν οδηγήσει σε σημαντικά περιστατικά ασφαλείας. Υπάρχει σημαντικός αριθμός περιστατικών ασφαλείας, που ενισχύουν τα επιχειρήματα όσων θεωρούν το ΔτΠ μη ασφαλές.

Αρκετά τέτοια περιστατικά παρατηρήθηκαν κατά τα πρώιμα χρόνια της ευρείας χρήσης των τεχνολογιών του ΔτΠ (2013 και έπειτα), όπου οι κατασκευαστές της τεχνολογίας έδειχναν ενδιαφέρον μόνο για την καινοτομία, αγνοώντας πόσο σημαντικός είναι ο τομέας της ασφάλειας των συσκευών. Ως τέτοια, για παράδειγμα, αξίζει να αναφερθούν τα κενά ασφαλείας που εντόπισε ο ερευνητής κυβερνοασφάλειας Billy Rios σε νοσοκομειακές αντλίες, τα οποία θα μπορούσαν να εκμετταλευτούν οι επίδοξοι χάκερς ώστε δυνητικά να χορηγήσουν θανατηφόρες δόσεις φαρμάκων σε ασθενείς[57].

[57] βλ. Fergal Gallagher (2015, 09 Ιουνίου), *Hackers Could Remotely Send Fatal Doses To Patients Via Flawed Hospital Pumps.* Ανάκτηση από techtimes.com στις 20 Απριλίου 2021, διαθέσιμο στο:

Παραμένοντας στο χώρο των «έξυπνων» ιατρικών συσκευών, θα αναφέρουμε την έρευνα που δημοσίευσε ο ερευνητής της εταιρίας ασφαλείας "IOActive", Barnaby Jack, τον Φεβρουάριο του 2013. Αφορμή για την έρευνα αποτέλεσε ένα επεισόδιο της τηλεοπτικής εκπομπής "Heartland", στο οποίο κάποιος κατάφερε να σκοτώσει τον αντιπρόεδρο των Ηνωμένων Πολιτειών Αμερικής αποκτώντας τον έλεγχο του βηματοδότη του. Ο ερευνητής, εξετάζοντας όλα τα στοιχεία του τηλεοπτικού σχεδίου, απέδειξε ότι μια τέτοια επίθεση ήταν ουσιαστικά εφικτή για κάποιον ο οποίος θα μπορούσε να λάβει τον έλεγχο του βηματοδότη, ενώ βρισκόταν σε απόσταση 15 μέτρων από το στόχο[58].

Άξια αναφοράς είναι, επίσης, δυο περιστατικά που αφορούν ευπάθειες συσκευών που χρησιμοποιούσαν οι γονείς για να βελτιώσουν την καθημερινότητα των παιδιών τους. Συγκεκριμένα, η πρώτη αναφορά μας σχετίζεται με πολλαπλά περιστατικά ασφαλείας, τα οποία συνέβησαν και αφορούσαν κάμερες απομακρυσμένης φύλαξης μωρών, τον έλεγχο των οποίων κατάφεραν να πάρουν χακερς απενεργοποιώντας τις οθόνες τους[59], κάνοντας χρήση των ηχείων τους με σκοπό τον εκφοβισμό[60] και αποκτώντας πρόσβαση στις κάμερες των συσκευών με σκοπό να κατασκοπεύουν τους χρήστες τους[61]. Επιπλέον, περιστατικά ασφαλείας είχαμε και στα παιδικά παιχνίδια της εταρίας με την επωνυμία "VTECH", όπου ένας χάκερ κατάφερε να αποσπάσει τα δεδομένα των συσκευών (ονόματα των παιδιών, διευθύνσεις, δεδομένα ήχου από τα μικρόφωνα κτλ) που αφορούσαν 6,3 εκατομμύρια παιδιά με σκοπό να εκθέσει τα σημαντικά ζητήματα ασφαλείας των συσκευών αυτών και να αναγκάσει την εταιρία κατασκευής να τα διορθώσει.

---

https://www.techtimes.com/articles/59180/20150609/hackers-remotely-send-fatal-doses-patients-via-flawed-hospital-pumps.htm

[58] βλ. Charles P.A., Shari Lawrence Pfleeger και Jonathan Margulies (2018), Ασφάλεια Πληροφοριακών Συστημάτων, Εκδόσεις Τζιόλα, Έκδοση 5η, σελ. 657-658

[59] βλ. Darlene Storm (2015, 2 Φεβρουαρίου), *Hacker hijacks wireless Foscam baby monitor, talks and freaks out nanny.* Ανάκτηση από computerworld.com στις 20 Απριλίου 2021, διαθέσιμο στον διαδικτυακό σύνδεσμο: https://www.computerworld.com/article/2878741/hacker-hijacks-wireless-foscam-baby-monitor-talks-and-freaks-out-nanny.html

[60] βλ. Chenda Ngak (2013, 13 Αυγούστου), *Baby monitor hacked, spies on Texas child.* Ανάκτηση από cbsnews.com στις 21 Απριλίου 2021, διαθέσιμο στον διαδικτυακό σύνδεσμο: https://www.cbsnews.com/news/baby-monitor-hacked-spies-on-texas-child/

[61] βλ. *US parents warned on hacked baby webcams* (2016, 28 Ιανουαρίου). Ανάκτηση από bbc.com στις 21 Απριλίου 2021,στον διαδικτυακό σύνδεσμο: https://www.bbc.com/news/technology-35427586

Βέβαια, ακόμα και σήμερα και παρά τα άλματα που έχουν κάνει η τεχνολογία του ΔτΠ παρατηρούνται σημαντικά ζητήματα ασφάλειας στις διασυνδεδεμένες συσκευές και στις υπηρεσίες του. Χαρακτηριστικά μπορούμε να αναφέρουμε ότι μόνο κατά το έτος 2020 είχαμε 10 σημαντικά (δημοσιευμένα) περιστατικά ασφαλείας στον χώρο του ΔτΠ[62]. Μερικά από αυτά τα περιστατικά είναι τα εξής:

- Κακόβουλο λογισμικό εκμεταλλεύτηκε την έλλειψη ενημερώσεων σε συσκευές ΔτΠ που χρησιμοποιούν το λειτουργικό σύστημα των "Windows 7" της εταιρίας "Microsoft", το οποίο εξέθεσε περίπου 200 εκατομμύρια συσκευές σε σοβαρούς κινδύνους ασφαλείας. Το περιστατικό ασφαλείας συνέβη για πρώτη φορά τον Ιανουάριο του 2020 θέτοντας σε κίνδυνο την ασφάλεια των εργαζομένων, διαφόρων συστημάτων παραγωγής και, σε ορισμένες περιπτώσεις, ευαίσθητων δεδομένων[63].
- Οι ευπάθειες μιας «έξυπνης» σκούπας αποτέλεσαν το έναυσμα για απομακρυσμένες κακόβουλες επιθέσεις, οι οποίες μεταξύ άλλων προκάλεσαν πλήρη αδυναμία εξυπηρέτηση και έδωσε στους επιτιθέμενους πλήρη πρόσβαση στις συσκευές εικόνας-κάμερες των συσκευών των χρηστών. Το περιστατικό έγινε γνωστό κατά την πραγματοποίηση του Παγκοσμίου Συνεδρίου Κυβερνοασφάλειας ("RSA Conference") τον Ιούλιο του 2020, οπού παρουσιάστηκαν τα κενά ασφαλείας της εν λόγω συσκευής. Αυτό είχε σημαντικές επιπτώσεις στη φήμη της εταιρίας κατασκευής, αλλά και εν γένει στις πωλήσεις των προϊόντων της κατηγορίας των «έξυπνων» οικιακών συσκευών[64].
- Τον Μάιο του 2019, ερευνητές της εταιρίας κυβρενοασφάλειας "Applied Risk" παρουσίασαν μια έκθεση σύμφωνα με την οποία τα συστήματα ελέγχου εισόδου πολλών «έξυπνων» κτιρίων της εταιρίας "NSC Linear eMerge" είχαν συγκεκριμένες, 10 στον αριθμό, ευπάθειες ασφαλείας, οι οποίες τα καθιστούσαν πιθανούς στόχους κυβερνοεπιθέσεων. Η εταιρία κατασκευής αγνοώντας την

---

[62] βλ. Roman Golubov (2020, 24 Μαρτίου), *There Are No Winter Breaks on the Darknet: Our Top 10 IoT Cyber Stories of Q1 2020.* Ανάκτηση από firedome.io στις 23 Απριλίου 2021, διαθέσιμο στον διαδικτυακό σύνδεσμο: https://firedome.io/blog/top-10-iot-cyber-stories-of-q1-2020/

[63] βλ. Alison DeNisco Rayome (2020, 5 Φεβρουαρίου), *Beware Windows 7 users: Malware campaign targeting IoT devices.* Ανάκτηση από cnet.com στις 23 Απριλίου 2021, διαθέσιμο στον διαδικτυακό σύνδεσμο: https://www.cnet.com/news/beware-windows-7-users-malware-campaign-targeting-iot-devices/

[64] βλ. Lindsey O'Donnell (2020, 27 Φεβρουαρίου), *IoT Insecurity: When Your Vacuum Turns on You.* Ανάκτηση από threatpost.com στις 23 Απριλίου 2021, διαθέσιμο στον διαδικτυακό σύνδεσμο: https://threatpost.com/vacuum-cleaners-baby-monitors-and-other-vulnerable-iot-devices/153294/

παραπάνω έκθεση, δεν φρόντισε να παρέχει ενημερώσεις λογισμικού, που θα βελτίωναν αυτές τις ευπάθειες. Έτσι, τον Φεβρουάριο του 2020 περισσότερα από 2.300 «έξυπνα» κτίρια έπεσαν θύμα κακόβουλων επιθέσεων, με την αδυναμία εξυπηρέτησης των συστημάτων εισόδου να καθιστά αδύνατη την είσοδο και την έξοδο στα κτίρια δημιουργώντας σημαντικά προβλήματα σε δημόσιες υπηρεσίες, ιδιωτικές επιχειρήσεις, εργοστάσια και κατοικίες[65].

- Το έτος 2019 παρατηρήθηκε σημαντικός αριθμός κακόβουλων επιθέσεων στις πολύ δημοφιλείς συσκευές φωνητικών εντολών σε «έξυπνα» σπίτια των εταιριών "Amazon" (Alexa) και "Google" (Google Home Smart). Οι επιτιθέμενοι, εκμεταλλευόμενοι διάφορα κενά ασφαλείας των συσκευών αυτών, αποκτούσαν απομακρυσμένη πρόσβαση στον έλεγχο των «έξυπνων» συσκευών του σπιτιού και στα διάφορα δεδομένα που συνέλεγαν (λ.χ. αποκτούσαν πρόσβαση στα μικρόφωνα και τις κάμερες των συσκευών ή ενεργοποιούσαν άλλες συσκευές που ήταν συνδεδεμένες στο οικιακό δίκτυο Wi-Fi). Ήδη από τον Απρίλιο του 2018 πολλοί ερευνητές κυβερνοασφάλειας είχαν επισημάνει τα κενά ασφαλείας των συσκευών, αλλά οι εταιρίες κατασκευής δεν κατάφεραν να αποτρέψουν τις επιθέσεις αυτές, με αποτέλεσμα οι χρήστες να βιώσουν πολύ δυσάρεστα περιστατικά ανασφάλειας εντός της οικείας τους[66].

Ο αριθμός των περιστατικών ασφαλείας στις συσκευές του ΔτΠ έχει δημιουργήσει σκεπτικισμό στο καταναλωτικό κοινό/χρήστες του ΔτΠ, πεποίθηση που καταδεικνύεται από διάφορες έρευνες που έχουν γίνει τα τελευταία χρόνια. Συγκεκριμένα, έρευνα της "Juniper Networks" σε πάνω από 4.000 χρήστες κινητών συσκευών το έτος 2012 είχε τα εξής αποτελέσματα: Πάνω απο το 76% των ερωτηθέντων δήλωσε ότι έχει κάνει χρήση του κινητού του τηλεφώνου για πρόσβαση σε υπηρεσίες που απαιτούν την συλλογή ευαίσθητων δεδομένων, όπως τα ιατρικά δεδομένα. Από αυτούς, το 41% δήλωσαν ότι δεν παρείχαν ποτέ κάποιου είδους άδεια για τη χρήση τους. Επίσης, οι χρήστες εμφανίστηκαν αναποφάσιστοι σχετικά με το πόση ασφαλή θεωρούν τη συσκευή του κινητού τους τηλεφώνου, καθώς μόνο το 15% έδειχνε να την εμπιστεύεται, το 18%

---

[65] βλ. Catalin Cimpanu (2020, 2 Φεβρουαρίου), *Hackers are hijacking smart building access systems to launch DDoS attacks.* Ανάκτηση από zdnet.com στις 23 Απριλίου 2021, διαθέσιμο στον διαδικτυακό σύνδεσμο: https://www.zdnet.com/article/hackers-are-hijacking-smart-building-access-systems-to-launch-ddos-attacks/

[66] βλ. Catalin Cimpanu (2019, 20 Οκτωβρίου), *Alexa and Google Home devices leveraged to phish and eavesdrop on users, again.* Ανάκτηση από zdnet.com στις 23 Απριλίου 2021, διαθέσιμο στον διαδικτυακό σύνδεσμο: https://www.zdnet.com/article/alexa-and-google-home-devices-leveraged-to-phish-and-eavesdrop-on-users-again/ και Jane Wakefield (2018, 14 Απριλίου), *TED 2018: The smart home that spied on its owner.* Ανάκτηση από bbc.com στις 21 Απριλίου 2021, διαθέσιμο στον διαδικτυακό σύνδεσμο: https://www.bbc.com/news/technology-43747421

δήλωνε ελάχιστη εμπιστοσύνη και το 63% δεν είχε ακόμη διαμορφώσει άποψη. Βέβαια, αυτό δεν έχει εμποδίσει τους χρήστες να κατέχουν πάνω από μια διασυνδεδεμένη συσκευή. Μάλιστα, το 18% των ερωτηθέντων κατείχαν 5 ή και παραπάνω «έξυπνες» συσκευές[67].

Μάλιστα, μεταγενέστερη έρευνα (2019) καταδεικνύει πως τα χρόνια της γιγάντωσης του Δτπ μεγάλωσε και η δυσπιστία των χρηστών του για την ασφάλεια του. Συγκεκριμένα, σε έρευνα που έγινε σε καταναλωτές στην Αυστραλία, τον Καναδά, τη Γαλλία, την Ιαπωνία, τη Μεγάλη Βρετανία και τις Η.Π.Α. το 63% των συμμετεχόντων θεωρεί τις διασυνδεδεμένες συσκευές «ανατριχιαστικές/μυστηριώδεις» σχετικά με τον τρόπο που συλλέγουν δεδομένα από τους χρήστες τους. Μάλιστα, σύμφωνα πάντα με την ίδια έρευνα, οι υπόνοιες αυτές ελλιπούς ασφάλειας έχει αποτρέψει σχεδόν έναν στους τρεις συμμετέχοντες (28%) από το να κατέχουν μια «έξυπνη» συσκευή[68].

3.4 Προκλήσεις και Κίνδυνοι Ασφαλείας στο ΔτΠ

Κάθε συσκευή του ΔτΠ συσκευή θα μπορούσε δυνητικά να αποτελέσει πόρτα για πιθανή κακόβουλη επίθεση. Γι' αυτόν ακριβώς το λόγο η ασφάλεια θα πρέπει να εξασφαλίζεται σε όλη τη διάρκεια λειτουργίας της υποδομής του ΔτΠ. Οι προκλήσεις που αντιμετωπίζει κάθε κατασκευαστής της τεχνολογίας του ΔτΠ αφορούν:

• Εμπιστευτικότητα, για να αποφευχθεί η αποκάλυψη των απόρρητων πληροφοριών (συμπεριλαμβανομένων και των ευαίσθητων προσωπικών δεδομένων) σε μη εξουσιοδοτημένα άτομα ή συστήματα.

• Ακεραιότητα, για να διασφαλιστεί ότι τα δεδομένα που διαχειρίζεται το σύστημα του ΔτΠ δεν έχουν υποστεί οιαδήποτε τροποποίηση από μη εξουσιοδοτημένα μέρη.

• Διαθεσιμότητα, για να διασφαλιστεί ότι οι υπηρεσίες που παρέχονται από τις πλατφόρμες του ΔτΠ ή οι πόροι που προσφέρονται από τις συσκευές λειτουργούν σωστά και χωρίς διακοπές.

• Αυθεντικότητα, για να επαληθευτεί ότι όλες οι διαδικασίες (επεξεργασία δεδομένων, συναλλαγές και οι επικοινωνίες) είναι γνήσιες και παράγονται/επεξεργάζονται από αξιόπιστα μέρη[69].

---

[67] βλ. Charles P.A., Shari Lawrence Pfleeger & Jonathan Margulies (2018), ο.π., σελ. 659-660.

[68] βλ. Ipsos Mori (2019, 1 Μαΐου), *The Trust Opportunity: Exploring Consumer Attitudes to the Internet of Things.* Ανάκτηση από internetsociety.org στις 23 Απριλίου 2021, στο: https://www.internetsociety.org/resources/doc/2019/trust-opportunity-exploring-consumer-attitudes-to-iot/

[69] βλ. Sebastien Ziegler (2019), Internet of Things Security and Data Protection, Springer, σελ. 21 επ.

Οι κάθε είδους κακόβουλες επιθέσεις έχουν συνήθως κοινά χαρακτηριστικά και ακολουθούν συγκεκριμένη μεθοδολογία, η οποία σε γενικές γραμμές ακολουθεί τα εξής βήματα:

Αρχικά ο επιτιθέμενος προσπαθεί να συγκεντρώσει επαρκείς πληροφορίες για το σύστημα-στόχο. Οι πληροφορίες αυτές τον βοηθούν να ανακαλύψει πιθανές ευπάθειες στο σύστημα και μπορεί να αφορούν την έκδοση του λειτουργικού συστήματος, τις εκδόσεις λογισμικού, την τοπολογία του δικτύου, τα διαθέσιμα ασύρματα δίκτυα κ.α. Σε δεύτερο στάδιο, ο επιτιθέμενος προσπαθεί να εκμεταλλευτεί τις ευπάθειες του συστήματος αποκτώντας πρόσβαση στο δίκτυο. Έχοντας αποκτήσει πρόσβαση, προβαίνει σε τροποποίηση των ρυθμίσεων πρόσβασης με σκοπό να διευκολύνει οποιαδήποτε μελλοντική του πρόσβαση στο σύστημα και να αποτρέψει τον εντοπισμό του από τους διαχειριστές του. Αφού ολοκληρώσει την εισβολή του, φροντίζει να καλύψει οποιαδήποτε ίχνη του από το σύστημα-στόχο, ενώ παράλληλα προσπαθεί να εντοπίσει περισσότερα συστήματα στο δίκτυο, την εισβολή στα οποία διευκολύνει η προηγούμενη του εισβολή στα συστήματα του δικτύου. Τέλος, συνηθίζεται να επιχειρεί να προκαλέσει ζημία στις ρυθμίσεις του δικτύου αλλά και στα δεδομένα του, προβαίνοντας σε αποκάλυψη, αλλοίωση ή και ολική διαγραφή τους[70].

Η συγκεκριμένη δομή των συστημάτων του ΔτΠ μας βοηθάει να κατηγοριοποιήσουμε τους κινδύνους ασφαλείας του ανάλογα με το επίπεδο της υποδομής που στοχεύει κάθε επίθεση, προβαίνοντας σε διάκριση σε φυσικό επίπεδο, επίπεδο δικτύου και επίπεδο εφαρμογής. Στους παρακάτω πίνακες παρουσιάζονται οι κίνδυνοι ασφαλείας και η περιγραφή τους ανά επίπεδο:

Πίνακας 2

1. Κίνδυνοι ασφάλειας του φυσικού επιπέδου:

Κίνδυνος ασφάλειας	**Περιγραφή**
Φυσική επίθεση (Physical Attack)	Η επίθεση, η οποία κυρίως αναφέρεται στη υλικές ζημιές στους κόμβους

[70] βλ. Μαυρίδης (2015), ο.π., σελ. 50-51

Κίνδυνος ασφάλειας	Περιγραφή
Αποτυχία εξοπλισμού	Η απόδοση του εξοπλισμού μειώνεται ή χάνεται ολικώς που οφείλεται σε εξωτερικούς παράγοντες, στο περιβάλλον του εξοπλισμού ή στην πάροδο του χρόνου
Αποτυχία γραμμής (Line Fault)	Είναι η αποτυχία παροχής ενέργειας στους κόμβους
Ηλεκτρομαγνητική διαρροή (Electromagnetic Leakage)	Με την εκπομπή ηλεκτρομαγνητικών σημάτων στον εξοπλισμό του ΔτΠ, οι επιτιθέμενοι μπορούν να ανακτήσουν τα αρχικά δεδομένα
Ηλεκτρομαγνητική παρεμβολή (Electromagnetic interference)	Τα ανεπιθύμητα ηλεκτρομαγνητικά σήματα ή θόρυβο, που αφού δημιουργώντας παρεμβολές στα σήματα που λαμβάνουν οι συσκευές δημιουργώντας πρόβλημα στην απόδοση του συστήματος
Αδυναμία εξυπηρέτησης (DoS)	Ο επιτιθέμενος καθιστά το σύστημα ανίκανο να παρέχει τις υπηρεσίες του μέσω της κατανάλωσης του εύρους ζώνης του δικτύου
Μπλοκάρισμα καναλιών	Τα δεδομένα δεν μπορούν να διακινηθούν ανάμεσα στις συσκευές (κανάλι), επειδή το κανάλι είναι κατειλημμένο για μεγάλο χρονικό διάστημα
Sibyl Attack	Ο επιτιθέμενος καταφέρνει να πάρει τον έλεγχο των κόμβων του συστήματος, αναπαριστώντας πολλαπλές ταυτότητες των κόμβων του συστήματος
Επαναλαμβανόμενη επίθεση	Ο επιτιθέμενος αποστέλλει ξανά και ξανά τα δεδομένα του συστήματος που είχε καταφέρει να υποκλέψει νωρίτερα ξεγελώντας το σύστημα
Καταστροφή δεδομένων αντίληψης (Perception data destruction)	Η μη εξουσιοδοτημένη εισαγωγή, διαγραφή και επεξεργασία των δεδομένων αντίληψης
Υποκλοπή δεδομένων	Παράνομη πρόσβαση στα δεδομένα του συστήματος μέσω παρεμβολής στο κανάλι επικοινωνίας των κόμβων
Παραβίαση δεδομένων	Ο επιτιθέμενος παρακολουθεί και τροποποιεί τα δεδομένα και στη συνέχεια στέλνει τροποποιημένα δεδομένα στον παραλήπτη
Μη εξουσιοδοτημένη πρόσβαση	Μη εξουσιοδοτημένοι χρήστες αποκτούν πρόσβαση στα δεδομένα του συστήματος

Κίνδυνος ασφάλειας	Περιγραφή
Παθητική επίθεση (Passive Attack)	Ο επιτιθέμενος συλλέγει παθητικά δεδομένα μέσω παρακολούθησης των πακέτων του δικτύου (sniffing) και συλλογής πληροφοριών
Παραβίαση Κόμβου (Node capture)	Ο κόμβος πύλης ή ο κεντρικός κόμβος ελέγχεται από τους εισβολείς

Πίνακας 3

2.Κίνδυνοι ασφάλειας σε επίπεδο δικτύου:

Κίνδυνος ασφάλειας	Περιγραφή
Διάχυτη αδυναμία εξυπηρέτησης (DDoS)	Πολλαπλοί κακόβουλοι κόμβοι επιτίθενται ταυτόχρονα στον διακομιστή-στόχο με σκοπό να προκαλέσουν αδυναμία εξυπηρέτησης (DoS)
Δρομολόγηση επίθεσης	Ο εισβολέας παρεμβαίνει στην κανονική διαδικασία δρομολόγησης στέλνοντας πλαστά πληροφορίες δρομολόγησης
Επίθεση κόμβου νεροχύτη	Διακοπή της μετάδοσης δεδομένων μεταξύ φυσικού επιπέδου και επιπέδου δικτύου επιτίθεται στον κόμβο του νεροχύτη
Παραπλανητική επίθεση κατεύθυνσης (Direction misleading attack)	Κακόβουλος κόμβος τροποποιεί τις διευθύνσεις προέλευσης και προορισμού των πακέτων δεδομένων και στη συνέχεια το στέλνει σε λάθος διαδρομή, με αποτέλεσμα σύγχυση δρομολόγησης δικτύου
Επίθεση Blackhole	Ο κακόβουλος κόμβος εξαπατά άλλους κόμβους του συστήματος για τη δημιουργία δρομολόγησης μαζί του και στη συνέχεια απορρίπτει κάθε πακέτο που πρέπει να προωθηθεί, προκαλώντας απώλεια πακέτου
Flooding Attack	Εξάντληση των πόρων των διακομιστών του δικτύου επίπεδο δικτύου από επίθεση άρνησης εξυπηρέτησης-Smurf και DDoS
Trapdoor	Επιτρέπεται η παράκαμψη της πολιτικής ασφαλείας όταν αποστέλλονται συγκεκριμένα δεδομένα
Sybil Attack	Ο κακόβουλος κόμβος αποκτώντας πολλές ταυτότητες συγχρόνως καταφέρνει να ελέγχει τους περισσότερους από τους κόμβους του συστήματος με σκοπό να

Κίνδυνος ασφάλειας	Περιγραφή
	εμποδίσει τη μετάδοση δεδομένων
Sinkhole attack	Ο κακόβουλος κόμβος προσελκύει τους κόμβους του συστήματος ως κανονικό σημείο στη διαδρομή δρομολόγησης, έτσι ώστε όλα τα δεδομένα να ρέουν μέσω αυτού
Wormhole attack	Ο επιτιθέμενος μεταδίδει μέσω σύνδεσης χαμηλής ταχύτητας πληροφορίες που αποστέλλονται σε ένα συγκεκριμένο μέρος του δικτύου και τα επαναλαμβάνει σε διαφορετικό μέρος του
Επίθεση βρόχου δρομολόγησης	Κακόβουλος κόμβος τροποποιεί τη διαδρομή δεδομένων για να προκαλέσει έναν άπειρο βρόχο δρομολόγησης
Hello flooding attack	Ο κακόβουλος κόμβος ξεγελάει τους κόμβους στο δίκτυο, ο οποίοι θεωρούν ότι είναι οι άμεσοι γείτονές του, χρησιμοποιώντας ένα ισχυρό σήμα για τη μετάδοση πληροφοριών δρομολόγησης
Επίθεση πλαστογράφησης (Spoofing)	Ο κακόβουλος κόμβος εξαπατά τους κόμβους του δικτύου ώστε να αποστέλλουν δεδομένα μέσω μιας αναποτελεσματικής διαδρομής ή ενός λάθους κόμβου
Επιλεκτική προώθηση	Ο κακόβουλος κόμβος χάνει σκόπιμα μερικές ή όλες τις βασικές πληροφορίες κατά την προώθηση
Tunnel attack	Οι κακόβουλοι κόμβοι κρύβουν την πραγματική απόσταση σύνδεσης μεταξύ τους εξαπατώντας δελεάστε τους άλλους κόμβους ώστε να δημιουργήσουν διαδρομή δρομολόγησης μέσω αυτών
Ψευδή δρομολόγηση πληροφοριών	Ο κακόβουλος κόμβος επιτίθεται σε επίπεδο δικτύου αλλοιώνοντας τη δρομολόγηση των πληροφοριών

Πίνακας 4

3. <u>Κίνδυνοι ασφαλείας σε επίπεδο εφαρμογής:</u>

Κίνδυνος ασφάλειας	Περιγραφή
Διαρροή απόρρητων δεδομένων	Διαρροή απόρρητο δεδομένων των χρηστών εξαιτίας μη ασφαλούς μεταφοράς, αποθήκευσης και παρουσίασης δεδομένων

Κίνδυνος ασφάλειας	Περιγραφή
Μη εξουσιοδοτημένη πρόσβαση	Παράνομη πρόσβαση στο δίκτυο και στα δεδομένα συστήματος
Κακόβουλος κώδικας	Κώδικας στο σύστημα χωρίς άμεσες συνέπειες, ο οποίος όμως μπορεί κρύβει περαιτέρω κινδύνους ασφαλείας
Forged control commands	Οι επιτιθέμενοι χρησιμοποιούν κακόβουλα ή καταστρέφουν το σύστημα δημιουργώντας εντολές ελέγχου
Loophole	Επίθεση στο σύστημα χρησιμοποιώντας τα κενά των εφαρμογών στο επίπεδο της διεπαφής εφαρμογής
Ιοί και δούρειοι ίπποι (Trojan horses)	Οι ιοί και οι δούρειοι ίπποι είναι γενικά απειλές ασφαλείας των εφαρμογών στο επίπεδο εφαρμογής
SQL injection attack	Είναι ένας κοινός τρόπος επίθεσης στη βάση δεδομένων του συστήματος

3.5 Εμπιστευτικότητα και ακεραιότητα προσωπικών δεδομένων

Όπως αναφέρθηκε παραπάνω, η εξασφάλιση της εμπιστευτικότητας και της ακεραιότητας των προσωπικών δεδομένων αποτελεί ένα από τα βασικά σημεία της ασφάλειας των συσκευών του ΔτΠ. Η προστασία των προσωπικών δεδομένων είναι μια βασική παράμετρος, η οποία θα πρέπει να εξετάζεται κατά τη διαδικασία σχεδι'ασης και κατασκευής μιας υπηρεσίας ΔτΠ. Η εξασφάλιση της εμπιστευτικότητας των δεδομένων καθιστά τα δεδομένα που διακινούνται σε ένα σύστημα αναγνώσιμα και επεξεργάσιμα μόνο από εξουσιοδοτημένους χρήστες. Η ακεραιτότητα των δεδομένων με τη σειρά της, αναφέρεται στη διασφάλιση της τροποποίησης ή επεξεργασίας των δεδομένων μόνο από εξουσιοδοτημένους χρήστες[71].

Η ραγδαία εξέλιξη του ΔτΠ έχει επιτρέψει την απομακρυσμένη πρόσβαση σε πληροφορίες οποιαδήποτε στιγμή και από οποιαδήποτε συσκευή του συστήματος. Οι πληροφορίες αυτές μπορεί να αφορούν δεδομένα του περιβάλλοντος των συσκευών (όπως λ.χ. η θερμοκρασία στους κοινόχρηστους χώρους μια πολυκατοικίας), δεδομένα που αφορούν την ίδια την κατάσταση των συσκευών (όπως λ.χ. το επίπεδο αυτονομίας ενός «έξυπνου» αυτοκινήτου), μέχρι και προσωπικά

[71] βλ. Μαυρίδης (2015), ο.π., σελ. 90 επ.

δεδομένα των χρηστών των συσκευών (όπως λ.χ. η διάρκεια και η ύπνου του χρήστη ενός «έξυπνου» ρολογιού και άλλα δεδομένα που αφορούν την υγεία του).

Είναι φυσικό, οι χρήστες των εφαρμογών του ΔτΠ να επιθυμούν τα δεδομένα τους να μην είναι προσβάσιμα σε μη εξουσιοδοτημένους παράγοντες. Πολλώ δε μάλλον, όταν ο κίνδυνος της διάθεσης μπορεί να αφορά δεδομένα που χρησιμοποιούνται για να σχηματιστούν διάφορα προφίλ χρηστών, όπως δεδομένα για τις τροφές που προτιμούν να καταναλώνουν, τα ρούχα που αγοράζουν, τις προτιμήσεις στα ταξίδια τους κ.ο.κ. Είναι λογικό, λοιπόν, να υπάρχει ανησυχία για την προστασία αυτών των δεδομένων, καθώς ο συνδυασμός και η επεξεργασία τους ενδέχεται να αποδώσει πληροφορίες, οι οποίες μπορούν δυνητικά να χρησιμοποιηθούν για να τον βλάψουν.

3.6 Διαθεσιμότητα και Αυθεντικότητα ΔτΠ

Όπως αναφέρθηκε και παραπάνω, η διαθεσιμότητα των δεδομένων έχει να κάνει με τη διαφύλαξη της εξουσιοδοτημένης πρόσβασης στα δεδομένα ενός συστήματος χωρίς καθυστερήσεις και εμπόδια. Το ΔτΠ έχει διεισδύσει σε ποικίλες εφαρμογές, συστήματα και υπηρεσίες κρίσιμης σημασίας, όπως η βιομηχανία, η ιατρική και η ασφάλεια των ανθρώπων και των αγαθών. Αυτό έχει οδηγήσει σε πάγια απαίτηση αξιοπιστίας και διαθεσιμότητας και η λειτουργία κάθε πράγματος του ΔτΠ θα πρέπει να διασφαλίζεται από αυθεκτικότητα και διαθεσιμότητα, όροι που χρησιμοποιούνται κατά κύριο λόγο από μηχανικούς βιομηχανικών συστημάτων και κατασκευαστές συστημάτων πληροφορικής.

Αναλυτικότερα, κάθε σύστημα του ΔτΠ θα πρέπει να διασφαλίζει την αυθεκτικότητα και την ευστάθεια/διαθεσιμότητα. Θα πρέπει, δηλαδή, κάθε σύστημα ΔτΠ να είναι σε θέσει να παράσχει απρόσκοπτα τις υπηρεσίες του παρά τις οποιασδήποτε εξωτερικές διαταραχές ή επιθέσεις (ευστάθεια), αλλά και να έχει τη δυνατότητα να προσαρμόζεται σ' αυτές τις αλλαγές και να διαμορφώνει αναλόγως τις προσφερόμενες υπηρεσίες[72].

[72] βλ. Macaulay Tyson & Morgan Kaufmann (2016),RIoT Control-Understanding and Managing Risks and the Internet of Things (Chapter 8). Στο Macaulay Tyson, Availability and Reliability Requierements in the IoT, σ.σ. 141-155, σελ 141 επ. (1st Edition)

Κεφάλαιο 4ο

4. Προσωπικά Δεδομένα στο Διαδίκτυο των Πραγμάτων

4.1. Εισαγωγή στα Προσωπικά Δεδομένα

Ως «Προσωπικό δεδομένο» ή «δεδομένο προσωπικού χαρακτήρα» ορίζεται[73] «κάθε πληροφορία που αναφέρεται σε συγκεκριμένο φυσικό πρόσωπο, ανεξαρτήτως πληροφοριακής αξίας και βαρύτητας». Σημαντικό στοιχείο για τον χαρακτηρισμό μιας πληροφορίας ως «προσωπικό δεδομένο» είναι η άμεση ή έμμεση σύνδεση του με εν ζωή φυσικό πρόσωπο. Μάλιστα, η πληροφορία αυτή δεν αρκεί να συνδέεται με το πρόσωπο αυτό, αλλά πρέπει το πρόσωπο αυτό να ταυτοποιείται άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε κάποιο αναγνωριστικό στοιχείο ταυτότητας, όπως για παράδειγμα όνομα, αριθμός ταυτότητας, δεδομένα θέσης κ.ο.κ.. Με βάση τα ανωτέρω ως προσωπικό δεδομένο μπορεί, ενδεικτικά και όχι περιοριστικά, να χαρακτηριστεί η ημερομηνία γέννησης, το ονομεπώνυμο, η διεύθυνση κατοικίας, ο αριθμός τηλεφώνου, το φύλο, η εθνικότητα, τα στοιχεία εκπαίδευσης, η επαγγελματική σταδιοδρομία, η οικογενειακή κατάσταση, η διεύθυνση IP (Internet Protocol). Δεν λογίζονται ως προσωπικά δεδομένα τα στατιστικής φύσης συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν να προσδιοριστούν πια τα πρόσωπα στα οποία αναφέρονται.

Τα προσωπικά δεδομένα διακρίνονται σε «απλά» και «ευαίσθητα». Κριτήριο για τη διάκριση αυτή είναι η πληροφοριακή βαρύτητα τους σε σχέση με το δικαίωμα στην ιδιωτικότητα[74]. Στην κατηγορία των ευαίσθητων δεδομένων (ή «των δεδομένων ειδικών κατηγοριών») ανήκουν τα δεδομένα που συναποτελούν τον πυρήνα της ιδιωτικής ζωής του ανθρώπου και τα οποία απαριθμούνται στο άρθρο 9 του Κανονισμού (ΕΕ) 2016/679 (ΓΚΠΔ ή GDPR) ως εξής: δεδομένα που αποκαλύπτουν την εθνοτική ή φυλετική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, τη συμμετοχή σε συνδικαλιστική οργάνωση, τα γενετικά και βιομετρικά δεδομένα, δεδομένα που αφορούν την υγεία και δεδομένα που αφορούν τη σεξουαλική ζωή ή τον γενετήσιο προσανατολισμό ενός προσώπου.

---

[73] βλ. Αλεξανδροπούλου-Αιγυπτιάδου (2016), Προσωπικά Δεδομένα, Νομική Βιβλιοθήκη, σελ. 43 επ.

[74] βλ. Αλεξανδροπούλου-Αιγυπτιάδου (2016), ο.π., σελ 45 επ.

Τα προσωπικά δεδομένα που δεν ανήκουν στις ειδικές κατηγορίες του άρθρου 9 του Κανονισμού (ΕΕ) 2016/679, αποτελούν απλά (ή μη ευαίσθητα) προσωπικά δεδομένα. Η ειδοποιός διαφορά μεταξύ των δύο βασικών κατηγοριών προσωπικών δεδομένων είναι ότι για τα ευαίσθητα το επίπεδο προστασίας είναι υψηλότερο, η επεξεργασία τους επιτρέπεται μόνο κατ' εξαίρεση και οι όροι της νόμιμης επεξεργασίας τους ορίζονται ειδικώς στις διατάξεις του άρθρου 9 του Κανονισμού (ΕΕ) 2016/679.

Όσον αφορά τα δεδομένα που διακινούνται στα συστήματα του ΔτΠ, μεγάλο μέρος αυτών αποτελούν προσωπικά δεδομένα. Ορισμένα εξ αυτών ενδέχεται να είναι αυστηρά προσωπικά και να αποτελούν ευαίσθητα προσωπικά δεδομένα (όπως λ.χ. δεδομένα ήχου και εικόνας από συστήματα παρακολούθησης, δεδομένα υγείας από «έξυπνα» ρολόγια), ενώ άλλα λιγότερο και να αποτελούν απλά προσωπικά δεδομένα (λ.χ. ονοματεπώνυμο και αριθμός τηλεφώνου από ένα «έξυπνο» κινητό τηλέφωνο).

Στο πλαίσιο του ΔτΠ, η δυνατότητα ταυτοποίησης ενός ατόμου βάσει δεδομένων που προκύπτουν από «έξυπνες» συσκευές αποτελεί συχνό φαινόμενο. Σε πολλές περιπτώσεις, μάλιστα, αποτελεί και ένα βασικό ζητούμενο για τη λειτουργία του συστήματος του ΔτΠ. Πιο συγκεκριμένα, σε εφαρμογές όπως ένα «έξυπνο» σύστημα εισόδου ενός ιδιωτικού χώρου η δυνατότητα ταυτοποίησης του ιδιοκτήτη του χώρου (λ.χ. μέσω δακτυλικού αποτυπώματος) αποτελεί σημαντική προϋπόθεση για τη σωστή λειτουργία του και την προσφορά της υπηρεσίας για την οποία κατασκευάστηκε.

Επιπλέον, ως προσωπικά δεδομένα μπορούν να χαρακτηρίζονται ακόμα και εκείνα τα δεδομένα που υφίστανται επεξεργασία μετά τη ψευδωνυμοποίηση τους. Πιο συγκεκριμένα, κάθε χρήστης συσκευής του ΔτΠ αποκτά επιγραμμικά αναγνωριστικά στοιχεία ταυτότητας,που αποκτά από τα πρωτόκολλά των συσκευών και των εφαρμογών τους, όπως είναι τα διάφορα αναγνωριστικά cookies και οι ετικέτες αναγνώρισης. Τα ίχνη που αφήνουν αυτά σε συνδυασμό με άλλες πληροφορίες που συλλέγουν οι συσκευές, συντελούν στη δημιουργία του προφίλ του χρήστη-φυσικού προσώπου και στην αναγνώρισή του. Μάλιστα η Ομάδα του άρθρου 29 στη γνώμη υπ' αριθμ. 2/2002 αναγνωρίζει τη διεύθυνση IP (Internet Protocol) ως προσωπικό δεδομένο, καθώς μπορεί έμμεσα και σε συνδυασμό με άλλες πληροφορίες να φανερώσει την ταυτότητα του φυσικού προσώπου που προβαίνει σε χρήση μιας συσκευής.

Σημαντική, επίσης, είναι η έννοια του «υπεύθυνου επεξεργασίας», ο οποίος ορίζεται ως «οποιοσδήποτε καθορίζει, μόνος του ή από κοινού με άλλους, τον σκοπό και τον τρόπο επεξεργασίας των προσωπικών δεδομένων και συνακόλουθα φέρει και την ευθύνη για την

πραγματοποιούμενη επεξεργασία, ανεξάρτητα αν αυτή πραγματοποιείται από τον ίδιο ή από άλλο πρόσωπο.». Αυτό σημαίνει ότι «υπεύθυνος επεξεργασίας» μπορεί να είναι οποιοδήποτε φυσικό ή νομικό πρόσωπο, όπως ένας έμπορος, ένας ελεύθερος επαγγελματίας, μια εταιρία, ένα σωματείο, ένα ίδρυμα, ένας δημόσιος οργανισμός, το ίδιο το Κράτος. Στην περίπτωση του ΔτΠ ως «υπεύθυνος της επεξεργασίας» των δεδομένων που σχετίζονται με τους χρήστες του ενδέχεται να είναι η εταιρία κατασκευής του συστήματος, ο ιδιοκτήτης μιας διαδικτυακής πλατφόρμας ή και το ίδιο το Κράτος σε περιπτώσεις όπως π.χ. συστημάτων μιας «έξυπνης» πόλης, ενός δημόσιου «έξυπνου» νοσοκομείου ή της ηλεκτρονικής διακυβέρνησης.

Ο έλεγχος της επεξεργασίας των δεδομένων ενδέχεται να ασκείται από δύο η περισσότερους υπεύθυνους από κοινο, οι οποίοι ορίζονται από το άρθρο 26 του ΓΚΠΔ ως «από κοινού υπεύθυνοι επεξεργασίας». Σύμφωνα με πρόσφατη νομολογία του Δικαστηρίου της Ευρωπαϊκής Ένωσης («ΔΕΕ») η έννοια του από κοινού υπεύθυνου πρέπει να ερμηνεύεται ευρέως. Μάλιστα, ενδέχεται να προσλάβει διάφορες μορφές με την ευθύνου του καθενός από τους από κοινού υπεύθυνους να περιορίζεται μόνος στις πράξεις για τις οποίες ο καθένας από αυτούς ορίζει τους σκοπούς της επεξεργασίας[75].

Σύμφωνα, μάλιστα, με την από 05.06.2018 απόφασή του ΔΕΕ στην υπόθεση C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig–Holstein (ULD) κατά Wirtschaftsakademie Schleswig-Holstein GmbH έκρινε ότι ο διαχειριστής σελίδας “fan page” στο Facebook είναι από κοινού υπεύθυνος με την εταιρία του Facebook για την επεξεργασία των δεδομένων των επισκεπτών της σελίδας του. Το ΔΕΕ έκρινε ότι η ύπαρξη από κοινού ευθύνης δε σημαίνει απαραίτητα ότι η ευθύνη κατανέμεται ισομερώς και ισοδύναμα, αλλά καθίσταται δυνατή η συμμετοχής τους σε επεξεργασία προσωπικών δεδομένων σε διαφορετικά στάδια και σε διαφορετικούς βαθμούς[76].

Στο σημείο αυτό αξίζει να αναφέρουμε τους διάφορους ορισμούς[77] των όρων που χρησιμοποιούνται για την προστασία των προσωπικών δεδομένων:

- Υποκείμενο Δεδομένων ή Υποκείμενο: «Το φυσικό πρόσωπο, στο οποίο αναφέρονται τα δεδομένα και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί, δηλαδή μπορεί να προσδιοριστεί άμεσα ή εμμέσως, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός

[75] βλ. Κομνηνός Γ. Κόμνιος (2021), Ζητήματα από την εφαρμογή το κανονισμού για την προστασία δεδομένων στη διεθνή διαιτησία, εκδόσεις Σάκκουλα, 1η έκδοση, σελ. 3 επ.
[76] βλ. Κομνηνός Γ. Κόμνιος (2018), Από κοινού υπεύθυνοι επεξεργασίας δεδομένων – Η περίπτωση του διαχειριστή σελίδας fan page στο Facebook, *Δίκαιο Τεχνολογίας & Επικοινωνίας, σελ. 298 επ.*
[77] βλ. Αλεξανδροπούλου-Αιγυπτιάδου (2016), ο.π., σελ. 60 επ.

περισσότερων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική ή κοινωνική».

- Επεξεργασία προσωπικών δεδομένων: «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».
- Συγκατάθεση (συναίνεση) του υποκειμένου των δεδομένων: «Κάθε ελεύθερη, ρητή και ειδική δήλωση βουλήσεως που εκφράζεται με τρόπο σαφή και εν πλήρη επίγνωση, με την οποία το υποκείμενο των δεδομένων, αφού έχει προηγουμένως ενημερωθεί, δέχεται να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν».
- Αποδέκτης των δεδομένων: «Το φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός, στον οποίο ανακοινώνονται τα δεδομένα, ανεξαρτήτως εάν πρόκειται για τρίτο μέρος ή όχι».
- Τρίτος: «Κάθε φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός, εκτός από το υποκείμενο των δεδομένων, τον υπεύθυνο Επεξεργασίας και τα πρόσωπα που είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα, εφόσον αυτά ενεργούν υπό την άμεση εποπτεία ή για λογαριασμό του υπεύθυνου επεξεργασίας».
- Εκτελών την Επεξεργασία: «Οποιοσδήποτε επεξεργάζεται προσωπικά δεδομενα για λογαριασμό του υπεύθυνου επεξεργασίας, όπως φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός».

4.2 Κίνδυνοι κατά την επεξεργασία Προσωπικών Δεδομένων στο ΔτΠ

Η επεξεργασία προσωπικών δεδομένων αποτελεί μια από τις βασικότερες λειτουργίες των εφαρμογών της τεχνολογίας του ΔτΠ, όπως λεπτομερώς αναλύθηκε σε προηγούμενα κεφάλαια.

Βέβαια, κατά την επεξεργασία των δεδομένων αυτών προκύπτουν σοβαρά ζητήματα που αφορούν την ιδιωτικότητα των χρηστών-υποκειμένων των προσωπικών δεδομένων και γενικότερα την ασφάλεια των υπολογιστικών συστημάτων. Πιο συγκεκριμένα, οι κίνδυνοι από την επεξεργασία προσωπικών δεδομένων στο ΔτΠ συνοψίζονται ως εξής:

α) Παρακολούθηση υποκειμένων- δεδομένα θέσης

Μεγάλος αριθμός των συσκευών του ΔτΠ, όπως λ.χ. «έξυπνα» κινητά τηλέφωνα και «έξυπνα» ρολόγια, διαθέτουν αισθητήρες εντοπισμού θέσης, οι οποίες μπορούν ανά πάσα να καταδείξουν την τοποθεσία που βρίσκεται ο χρήστης της συκευής αλλά και τη διαδρομή που έχει ακολουθήσει. Η υπηρεσία εντοπισμού θέσης χρησιμοποιεί τη γεωγραφική θέση μιας φορητής συσκευής για να παρέχει διάφορες υπηρεσίες διαφήμισης και ενημερώσεις τον καιρό, για την κίνηση στους κ.ο.κ. Τα δεδομένα θέσης (GPS) και η διεύθυνση IP θεωρούνται προσωπικά δεδομένα, μιας και μπορούν άμεσα ή έμμεσα να ταυτοποιήσουν το άτομο στο οποίο ανναφέρονται. Η προβληματική έγκειται στον ανά πάσα στιγμή εντοπισμό του χρήστη και στην αποθήκευση της τοποθεσίας του για απροσδιόριστο χρονικό διάστημα. Αυτό μπορεί να οδηγήσει σε μια αέναη παρακολούθηση του χρήστη εν αγνοία του και τη χρήση αυτών των δεδομένων για διαφορετικούς σκοπούς άλλους από τους σκοπούς προσφοράς της υπηρεσίας[78].

β) Χρήση των δεδομένων για διαφορετικούς σκοπούς

Στο ΔτΠ εγείρονται ανησυχίες σχετικά με τον τεράστιο όγκο προσωπικών δεδομένων που συλλέγονται νόμιμα για ένα συγκεκριμένο σκοπό και υφίστανται επεξεργασία από τρίτους για σκοπούς διαφορετικούς από τους αρχικούς σκοπούς επεξεργασίας. Γίνεται, δηλαδή, χρήση δεδομένων, που έχουν συλλεγεί για την παροχή των υπηρεσιών της εφαρμογής του ΔτΠ, για σκοπούς εμπορικούς ή για σκοπούς δημοσίου συμφέροντος κατά τρόπο ασυμβίβαστο με τον αρχικό σκοπό συλλογής. Πιο συγκεκριμένα, έχει παρατηρηθεί χρήση τέτοιων δεδομένων από ασφαλιστικές εταιρίες, εργοδότες και αστυνομικές αρχές, ενώ κάτι τέτοιο θα ήταν επιτρεπτό από τις αστυνομικές αρχές μόνο σε πολύ συγκεκριμένες περιπτώσεις διάπραξης σοβαρών εγκλημάτων[79].

γ) Εξαγωγή πληροφοριών μέσω διασύνδεσης συστημάτων

Είναι σύνηθης διαδικασία στο ΔτΠ να συντελείται διασύνδεση δύο ή περισσότερων διαφορετικών συστημάτων, τα οποία λειτουργούν ξεχωριστά. Ο συνδυασμός των δεδομένων αυτών που προέρχονται από διαφορετικές πηγές, ενδέχεται να εξάγει πληροφορίες, τις οποίες ο χρήστης

[78] βλ. Φ. Παναγοπούλου-Κουτνατζή (2014), Διαδίκτυο των πραγμάτων (Internet of Things-IoT): Αποικισμός της καθημερινής ζωής ή νέα τεχνολογική πρόκληση;, *ΔιΜΕΕ 3/2014- έτος 11ο,σ.σ. 343-358*, σελ. 350 επ.
[79] Ibid, σελ 351 επ.

δεν είχε καμία πρόθεση να αποκαλύψει με τη χρήση καθενός από τα ξεχωριστά συστήματα. Σύμφωνα με τον προϊσχύοντα Ν. 2472/97, το παραπάνω αποτελεί ειδική μορφή επεξεργασίας δεδομένων. Συγκεκριμένα στο άρθρο 8 του Ν.2472/97 γίνεται αναφορά στη «διασύνδεση αρχείων» ως πράξη επεξεργασίας δεδομένων. Αντίθετα, στον Κανονισμό (ΕΕ) 2016/679, δεν υπάρχει ειδική αναφορά στην συσχέτιση των δεδομένων.

δ) Κατάρτιση προφίλ χρήστη και λήψη αυτοματοποιημένων αποφάσεων

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».*

Παρατηρείται η δημιουργία συγκεκριμένων προτύπων συμπεριφοράς από εφαρμογές του ΔτΠ, οι οποίες είναι σε θέση να δημιουργούν συγκεκριμένα μοτίβα συμπεριφοράς των χρηστών τους, κάνοντας την ταξινόμηση των πολιτών σε διάφορες κατηγορίες (καταναλωτικοί, σπάταλοι, επικίνδυνοι κτλ) ευκολότερη. Αυτό έχει προεκτάσεις και στη «διανοητική ιδιωτικότητα» του ατόμου, καθώς η ελευθερία σκέψης του κάθε ατόμου, που αποτελεί το θεμέλιο κάθε ελεύθερης κοινωνίας, μπορεί να επηρεαστεί αρνητικά από την έμμεση επιρροή στη λήψη συγκεκριμένων αποφάσεων μέσω των κατάλληλων μηχανισμών που δημιουργούνται από τα μοτίβα συμπεριφοράς κάθε ατόμου. Για παράδειγμα, ένα ατόμο που η γενικότερη συμπεριφορά και δραστηριότητα του μπορεί να το καταττάσει στο μοτίβο συμπεριφοράς του «σπάταλου» ανθρώπου, μπορεί μέσω της προβολής των κατάλληλων διαφημίσεων (στοχευμένη διαφήμιση) κατά την χρήστη των εφαρμογών του ΔτΠ να πειστεί να προβεί σε αγορές συγκεκριμένων προϊόντων.

Συνακόλουθα, και σε συνδυασμό με το αναφερόμενο στοιχείο β' (χρήση δεδομένων για διαφορετικούς σκοπούς), η δημιουργία προφίλ χρήστη και η χρήση των δεδομένων για διαφορετικούς σκοπούς από τους αρχικούς σκοπούς συλλογής τους, μπορεί να οδηγήσει στην απαγορευμένων λήψη αυτοματοποιημένων αποφάσεων. Για παράδειγμα, μια ασφαλιστική εταιρία θα μπορούσε να κάνει χρήση των δεδομένων που έχουν συλλεγεί από ένα «έξυπνο» ρολόι, δεδομένα που οδήγησαν στη δημιουργία ενός προφίλ χρήστη ενός ατόμου που δεν διάγει υγιεινό τρόπο ζωής και να αποφασίσει την αυτόματη άρνηση της ασφάλισης ζωής του συγκεκριμένου

ατόμου[80].

Παρότι οι χρήστες αναζητούν τη βέλτιστη δυνατή λειτουργικότητα από τα συστήματα του ΔτΠ, είναι δύσκολο γι'αυτούς να εμπιστευτούν πλήρως τις εφαρμογές του λόγω της πολυπλοκότητάς τους. Τα άτομα, που μοιράζονται τα προσωπικά τους δεδομένα μέσω του ΔτΠ συνήθως δεν έχουν πλήρη κατανόηση του τρόπου με τον οποίο η τεχνολογία αυτή λειτουργεί, πώς εφαρμόζονται τα μέτρα ασφαλείας και ποιος έχει πρόσβαση στα δεδομένα τους. Αυτό υπογραμμίζει μια σημαντική πρόκληση για το ΔτΠ: την «ασυμμετρία πληροφόρησης»("asymmetric information")[81]. Η «ασυμμετρία πληροφόρησης»[82], μπορεί να εγκυμονεί σημαντικούς κινδύνους για τους χρήστες, οι οποίοι ενδεχομένως να μην προέβαιναν στη χρήση μιας υπηρεσίας ή μιας συσκευής του ΔτΠ αν είχαν όλες τις πληροφορίες που αφορούν την επεξεργασία των δεδομένων τους, ενώ σε κάθε περίπτωση μπορεί να ενισχύσει τη δυσπιστία τους απέναντι στο ΔτΠ.

4.3 Νομοθετικό καθεστώς προστασίας

Το δικαίωμα προστασίας της ιδιωτικότητας κατοχυρώθηκε συνταγματικά με τη διάταξη του άρθρου 9 Α, που ορίζει ότι «καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα των προσωπικών δεδομένων, όπως νόμος ορίζει». Κατοχυρώθηκε, λοιπόν, το ατομικό δικαίωμα προστασίας απέναντι στη συλλογή, επεξεργασία και χρήση των προσωπικών δεδομένων με συμβατικό ή ηλεκτρονικό τρόπο, προσδιορίζοντας το δικαίωμα κάθε ανθρώπου να ορίζει ο ίδιος αν και σε μέχρι ποιο σημείο θα καταστεί πληροφοριακό αντικείμενο.

Στην ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων συμπεριλαμβάνονται το άρθρο 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, το άρθρο ΣΤ' της Συνθήκης για την Ευρωπαϊκή Ένωση, το άρθρο 8 της Ευρωπαϊκής Σύμβασης των Δικαιωμάτων του Ανθρώπου, η Σύμβαση 108 του Συμβουλίου της Ευρώπης και η επικαιροποίηση αυτής.

Στα πλαίσια του ενωσιακού δικαίου εφαρμόζεται και ο Κανονισμός της ΕΕ 679/2016-Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ), ο οποίος τέθηκε σε εφαρμογή από τις 25-05-

[80] ibid,σελ. 350-351
[81] βλ. Ziegler (2019), ο.π., σελ. 130 επ.
[82] Για περισσότερες πληροφορίες σχετικά με την «ασυμμετρία πληροφόρησης» βλ. *Information asymmetry* (2022). Ανάκτηση από en.wikipedia.org στις 20 Ιανουαρίου 2022, στον διαδικτυακό σύνδεσμο: https://en.wikipedia.org/wiki/Information_asymmetry

2018 σύμφωνα με το άρθρο 99 παρ. 2 αυτού και κατήργησε την Οδηγία 95/46/ΕΚ. Σύμφωνα με το άρθρο 288 της Συνθήκης για τη Λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ), ο ΓΚΠΔ έχει άμεση εφαρμογή σε όλα τα κράτη μέλη της ΕΕ, τα οποία υποχρεούνται να λάβουν τα αναγκαία μέτρα για την προσαρμογή της εθνικής νομοθεσίας τους. Με την κατάργηση της Οδηγίας, επιλέχθηκε η μορφή του Κανονισμού, προκειμένου το κείμενο των εφαρμοστέων κανόνων να χαίρει άμεσης, ομοιόμορφης και πιο συνεκτικής εφαρμογής από τα κράτη μέλη, καθώς το γεγονός που οτι οι Οδηγίες απαιτούσαν και μεταγενέστερη διαδικασία ενσωμάτωσής τους στην εθνική νομοθεσία οδηγούσε σε μη ενιαία και ανομοιομορφή εφαρμογή των επιταγών της στα κράτη μέλη[83].
Στη χώρα μας αυτό συνέβη με τον Ν. 4624/2019 (ΦΕΚ Α΄137), στον οποίο ορίστηκαν τα μέτρα εφαρμογής του ΓΚΠΔ και ενσωματώθηκε στην εθνική νομοθεσία η Οδηγία (ΕΕ) 2016/680. Ο προισχύων Ν. 2472/1997 καταργήθηκε, εκτός των διατάξεων που αναφέρονται ρητά στο άρθρο 84 του Ν. 4624/2019.

Ο ν. 3471/2006, ο οποίος ενσωματώνει την Οδηγία 2002/58/ΕΚ (Οδηγία "e-Privacy"), όπως έχει τροποποιηθεί με την Οδηγία 2009/136/ΕΚ, αποτελεί συμπλήρωση και εξειδίκευση του θεσμικού πλαισίου της προστασίας των δεδομένων προσωπικού χαρακτήρα στον τομέα των ηλεκτρονικών επικοινωνιών.

4.3.1 Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ) στο πλαίσιο του ΔτΠ

Ο ΓΚΠΔ από την πρώτη ημέρα εφαρμογής του, ήτοι την 25η Μαΐου του 2018, έχει δημιουργήσει ένα νέο και αρκετά αυστηρότερο σε σχέση με το προισχύον νομικό καθεστώς πλαίσο δαιχείρισης και επεξεργασία των προσωπικών δεδομένων. Ο κόσμος του ΔτΠ και των συγγενικών του τεχνολογιών («Μεγάλα Δεδομένα», AI κ.ο.κ.) είχε ραγδαία εξέλιξη αρκετά χρόνια νωρίτερα από την ψήφιση του ΓΚΠΔ. Η ραγδαία αυτή εξέλιξη των τεχνολογιών αυτών, που έχουν ως κεντρικό πυλώνα της λειτουργίας του την επεξεργασία δεδομένων, και η ασύδωτη και χωρίς όρια επεξεργασία τεράστιας κλίμακας δεδομένων από τους κατασκευαστές και τους διαχειριστές των εφαρμογών των τεχνολογιών αυτών οδήγησε στην ανάγκη δημιουργίας νέου νομικού πλαισίου για την προστασία της ιδιωτικότητας.

Η ανάγκη, λοιπόν, για τη δημιουργία νέου νομικού καθεστώτος για την προστασία των

[83] βλ. και επιμέλεια Λ.Κοτσαλής -Κ. Μενουδάκος (2018), Γενικος Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (GDPR) Νομική διάσταση και πρακτική εφαρμογή,σελ.5

δεδομένων δημιουργήθηκε πολύ νωρίτερα από την ημέρα ψήσισης του ΓΚΠΔ. Από την άλλη πλευρά, ο κόσμος του Διαδικτύου έχει φέρει την άμεση και καθολική πληροφόρηση και τη διάχυτη υπολογιστική δύναμη, γενονός που έρχεται σε άμεση σύγκρουση με τις αυστηρές επιταγές του ΓΚΠΔ, ο οποίος ως έχει ως κύριο μέλημα την προστασία της ιδιωτικότητας και των προσωπικών δεδομένων. Εϊναι, λοιπόν, πολύ σημαντικός ο συγκερασμός της αδιάκοπης τεχνολογικής εξέλιξης που επιφέρει η ανάπτυξη του Διαδικτύου και της ανάγκης για διαφύλαξη της ιδιωτικότητας του ατόμου.

Ο ΓΚΠΔ έχει επιχειρήσει να καλύψει ένα ευρύ φάσμα πράξεων επεξεργασίας δεδομένων της σύγχρονης τεχνολογικής και μη πραγματικότητας. Βέβαια, οι προκλήσεις που δημιουργούν η συνεχώς εξελισσόμενη τεχνολογία του ΔτΠ, αλλά και οι τεχνολογίες των «Μεγάλων Δεδομένων», της «Υπολογιστικής Νέφους» και της «Τεχνητής Νοημοσύνης» δεν έχουν αντιμετωπιστεί συγκεκριμένα, καθώς δεν υπάρχουν ειδικές αναφορές στις τεχνολογίες αυτές [84].

Προκύπτει, βέβαια, έντονος προβληματισμός για το αν και κατά πόσο είναι σε θέση οι κατασκευαστές του ΔτΠ να επιτύχουν τη συμμόρφωση με τις επιταγές του ΓΚΠΔ χωρίς να επηρεαστεί ουσιωδώς η λειτουργία των συστημάτων τους και η προσφερόμενες υπηρεσίες. Επιπλέον, ο ΓΚΠΔ επιτρέπει στους εθνικούς νομοθέτες να επιβάλλουν πρόσθετες και ειδικότερες υποχρεώσεις σε εθνικό επίπεδο. Αυτο δημιουργεί σοβαρό ζήτημα για του υπεύθυνους επεξεργασίας στο ΔτΠ, καθώς θα πρέπει να λαμβάνουν ταυτόχρονα υπόψιν τους τις υποχρεώσεις που προκύπτουν από διάφορες εθνικές νομοθεσίες, καθώς είναι σύνηθες στο ΔτΠ τα δεδομένα να σύλλεγονται από συσκευές που βρίσκονται εγκατεστημένες σε μια χώρα και να αποθηκεύονται ή/και να υφίστανται επεξεργασία σε τερματικούς που είναι εγκατεστημένοι σε διαφορετικές χώρες[85]. Γίνεται, λοιπόν, εύκολα κατανοητό ότι η συμμόρφωση των συστημάτων του ΔτΠ με την ισχύουσα νομοθεσία για την προστασία των δεδομένων αποτελεί μια πραγματική πρόκληση, δεδομένης της φύσης των συσκευών του ΔτΠ και της επεξεργασίας των δεδομένων.

4.3.2 Αρχές που διέπουν την επεξεργασία των προσωπικών δεδομένων

Σύμφωνα με το άρθρο 5 του ΓΚΠΔ προβλέπονται ορισμένες αρχές βάσει των οποίων θα πρέπει να γίνεται η επεξεργασία των δεδομένων. Οι αρχές αυτές είναι οι εξής:

[84] βλ. Κομνηνός Γ. Κόμνιος (2020), Η αξιολόγηση το Γενικού Κανονισμού για την Προστασία Δεδομένων. Διαδικασία-Γνώμες – Προτάσεις, *Περιοδικό Αρμενόπουλος*, σ.σ. 1129-1140, σελ. 1129-1130 (Τεύχος 7)
[85] βλ. Ziegler (2019), ο.π., σελ. 119-120

- Η επεξεργασία των δεδομένων πρέπει να γίνεται με τρόπο σύννομο και θεμιτό και να είναι διαφανής ως προς το υποκείμενο των δεδομένων («αρχή της νομιμότητας, της αντικειμενικότητας και της διαφάνειας»).
- Η επεξεργασία πρέπει να πραγματοποιείται για καθορισμένους, νόμιμους και ρητούς σκοπούς («αρχή του περιορισμού του σκοπού»).
- Τα υπό επεξεργασία δεδομένα πρέπει να είναι κατάλληλα, συναφή και να περιορίζονται στο απαραίτητο μέτρο για την εξυπηρέτηση των σκοπών της επεξεργασίας («αρχή της ελαχιστοποίησης των δεδομένων»).
- Τα υπό επεξεργασία δεδομένα πρέπει να είναι ακριβή και να επικαιροποιούνται κατά το αναγκαίο μέτρο. Πρέπει να επιδιώκεται άμεση διαγραφή των δεδομένων εκείνων τα οποία είναι ανακριβή σε σχέση με τους σκοπούς της επεξεργασίας («αρχή της ακρίβειας»).
- Τα υπό επεξεργασία δεδομένα πρέπει να τηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων τους μόνο για το διάστημα που απαιτείται για την επίτευξη των σκοπών της επεξεργασίας («αρχή του περιορισμού της περιόδου αποθήκευσης»).
- Πρέπει να γίνεται χρήση κατάλληλων τεχνικών και οργανωτικών μέτρων προκειμένου να εξασφαλίζεται η επεξεργασία των δεδομένων κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλειά τους («αρχή της ακεραιότητας και της εμπιστευτικότητας»).
- Τέλος, σε συνέχεια των ανωτέρω υποχρεώσεων που απορρέουν από τις γενικές αρχές του άρθρου 5 του Γενικού Κανονισμού, η παράγραφος 2 του ίδιου άρθρου προβλέπει, περαιτέρω, ότι ο υπεύθυνος επεξεργασίας φέρει ευθύνη και έχει την υποχρέωση να μπορεί να αποδείξει ανά πάσα στιγμή τη συμμόρφωσή του με τις γενικές αρχές της παραγράφου 1 («αρχή της λογοδοσίας»).

Πρώτη αναφέρεται «η αρχή της νομιμότητας του σκοπού και του τρόπου επεξεργασίας», σύμφωνα με την οποία η επεξεργασία των προσωπικών δεδομένων θα πρέπει να εξυπηρετεί έναν σκοπό, έστω και μελλοντικό, ο οποίος θα πρέπει να επιλέγεται στα πλαίσια της συνταγματικής νομιμότητας και της νομιμότητας που επιβάλλει ο κοινός νομοθέτης και να είναι συγκεκριμένος. Τα όρια της νομιμότητας καλύπτουν εκτός από τον σκοπό της επεξεργασίας και την ίδια τη μέθοδο της επεξεργασίας, η οποία θα πρέπει να διενεργείται με τρόπο που δεν παραβιάζει τις ελευθερίες και τα δικαιώματα του υποκειμένου[86].

Εξαιρετικά σημαντική θεωρείται η «αρχή της αναλογικότητας/ελαχιστοποίησης των δεδομένων», στην οποία έχει στηριχθεί πολλές φορές η ΑΠΠΔ για να εκφέρει κρίση σε διάφορα

[86] βλ. Αλεξανδροπούλου-Αιγυπτιάδου (2016), ο.π., σελ. 69-71

ζητήματα προστασίας δεδομένων προσωπικού χαρακτήρα. Με βάση αυτή, τα προς επεξεργασία δεδομένα πρέπει να είναι συναφή, πρόσφορα και όχι περισσότερα από όσα απαιτείται για το σκοπό της επεξεργασίας. Θα πρέπει , δηλαδή, να υπάρχει αυστηρή σύνδεση μεταξύ του επιδιωκόμενου σκοπού με τα υπό επεξεργασία προσωπικά δεδομένα , να είναι κατάλληλα για την επίτευξη του και να είναι τα απολύτως απαραίτητα (όχι περισσότερα) για να φτάσουμε στο επιδιωκόμενο αποτέλεσμα. Ορίζει, λοιπόν, δύο κριτήρια για τον έλεγχο νομιμότητας της επεξεργασίας, το ποσοτικό κριτήριο, που απαιτεί συνάφεια και προσφορότητα ως προς το σκοπό της επεξεργασίας και το ποιοτικό, που απαιτεί τα δεδομένα να είναι «όχι περισσότερα από όσα κάθε φορά απαιτείται»[87].

Βασικές αρχές της επεξεργασίας είναι, επίσης, η «αρχή της ακρίβειας», η οποία επιτάσσει τα δεδομένα να ανταποκρίνονται στην πραγματικότητα, να είναι επίκαιρα και ακριβή, και η «αρχή της καθορισμένης χρονικής διάρκειας διατήρησης των προσωπικών δεδομένων» , σύμφωνα με την οποία τα δεδομένα θα πρέπει να τηρούνται στη μορφή που επιτρέπει τον προσδιορισμό της ταυτότητας του υποκειμένου τους μόνο για όσο διάστημα απαιτείται για την πραγματοποίηση των σκοπών της συλλογής και της επεξεργασίας τους. Το χρονικό διάστημα της επεξεργασίας κρίνεται κατά περίπτωση από την Αρχή, που είναι υπεύθυνη για την προστασία των δεδομένων προσωπικού χαρακτήρα, και η διατήρηση τους για ιστορικούς, επιστημονικούς ή στατιστικούς λόγους μετά την πάροδο του ορισμένου χρονικού διαστήματος επιτρέπεται μόνο με άδεια της[88].

Στις παραπάνω αρχές ήρθαν να προστεθούν με τον Κανονισμό 2016/679 και άλλες δύο σημαντικές αρχές που αφορούν την επεξεργασία των προσωπικών δεδομένων , κατ' επέκταση και των βιομετρικών δεδομένων. Η διάταξη του άρθρου 5 του Κανονισμού εισάγει ,συμπληρωματικά με τις ήδη γνωστές παραπάνω αρχές, και την «Αρχή της ακεραιότητας και της εμπιστευτικότητας», σύμφωνα με την οποία η επεξεργασία των προσωπικών δεδομένων πρέπει να γίνεται με τέτοιο τρόπο που εξασφαλίζει την ασφάλεια των δεδομένων, την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών και οργανωτικών μέτρων ακολουθώντας την προσέγγιση με βάση τον κίνδυνο ("risk-based approach") για τα δικαιώματα και τις ελευθερίες των υποκειμένων διασφαλίζοντας το κατάλληλο επίπεδο ασφάλειας των δεδομένων. Σύμφωνα με το άρθρο 32 παρ. 2 του ΓΚΠΔ για να εκτιμηθεί το ενδεδειγμένο επίπεδο ασφαλείας ενός συστήματος πρέπει να

[87] ibid, σελ. 72-73
[88] Ibid, σελ 79 επ.

λαμβάνονται υπόψιν οι κίνδυνοι που απορρέουν από την επεξεργασία με γνώμονα την ακεραιότητα και την εμπιστευτικότητα των δεδομένων [89].

Με το άρθρο 5 του Κανονισμού εισάγεται και η «αρχή της λογοδοσίας», η οποία επιβάλλει στον υπεύθυνο επεξεργασίας των προσωπικών δεδομένων την υποχρέωση απόδειξης της συμμόρφωσης στις παραπάνω Αρχές επεξεργασίας.

4.3.3 Νομιμότητα της επεξεργασίας Προσωπικών Δεδομένων στο ΔτΠ

Κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα για να είναι συνταγματικά αποδεκτή και σύνομμη, θα πρέπει αφενός να είναι σύμφωνη με τις ορισθείσες αρχές της επεξεργασίας και αφετέρου να θεμελιώνεται σε μια από τις βάσεις νομιμότητας που ορίζει ο ΓΚΠΔ για κάθε κατηγορία δεδομένων.

Όπως αναφέρθηκε και παραπάνω είναι αρκετά σύνηθες οι εφαρμογές του ΔτΠ να προβαίνουν σε πράξεις επεξεργασίας προσωπικών δεδομένων που ανήκουν στους χρήστες του. Τις περιπτώσεις κατά τις οποίες η επεξεργασία αυτή είναι νόμιμη ορίζει ο ΓΚΠΔ στο άρθρο 6 για τα «μη ευαίσθητα» δεδομένα (απλά προσωπικά δεδομένα) και στο άρθρο 9 για τα δεδομένα ειδικών κατηγοριών (ευαίσθητα προσωπικά δεδομένα). Συγκεκριμένα, σύμφωνα με το άρθρο 6 παρ.1 του ΓΚΠΔ η επεξεργασία των (μη ευαίσθητων) προσωπικών δεδομένων είναι σύννομη όταν:

α) Το υποκείμενο έχει παράσχει τη συναίνεσή του για την επεξεργασία των προσωπικών του δεδομένων για έναν ή περισσότερους σκοπούς.

β) 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.

γ) Η επεξεργασία είναι αναγκαία για την εκπλήρωση έννομης υποχρεώσεως του υπεύθυνου επεξεργασίας.

δ) Η επεξεργασία είναι αναγκαία για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου ή άλλου φυσικού προσώπου.

ε) 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.

[89] βλ. Κόμνιος (2021) ο.π., σελ. 50 επ.

στ) Η επεξεργασία είναι απαραίτητη για τους σκοπούς των εννόμων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος υπό τον όρο ότι τούτο υπερέχει προφανώς των θεμελιωδών δικαιωμάτων και συμφερόντων του υποκειμένου των δεδομένων, ιδίως αυτό είναι παιδί.

Σχετικά με την επεξεργασία των δεδομένων των ειδικών κατηγοριών του άρθρου 9 του ΓΚΠΔ, αυτή θεωρείται επιτρεπτή μόνο κατ' εξαίρεση. Πιο συγκεκριμένα, επιτρέπεται η επεξεργασία των δεδομένων αυτών αποκλειστικά στις ακόλουθες περιπτώσεις:

α) Το υποκείμενο των δεδομένων έχει παράσχει ρητή συγκατάθεση για την επεξεργασία για έναν ή περισσότερους συγκεκριμένους σκοπούς, εκτός εάν το δίκαιο της Ένωσης ή κράτους μέλους προβλέπει ότι η απαγόρευση που αναφέρεται στην παράγραφο 1 δεν μπορεί να αρθεί από το υποκείμενο των δεδομένων.

β) Η επεξεργασία είναι απαραίτητη για την εκτέλεση των υποχρεώσεων και την άσκηση συγκεκριμένων δικαιωμάτων του υπευθύνου επεξεργασίας ή του υποκειμένου των δεδομένων στον τομέα του εργατικού δικαίου και του δικαίου κοινωνικής ασφάλισης και κοινωνικής προστασίας, εφόσον επιτρέπεται από το δίκαιο της Ένωσης ή κράτους μέλους ή από συλλογική συμφωνία σύμφωνα με το εθνικό δίκαιο παρέχοντας κατάλληλες εγγυήσεις για τα θεμελιώδη δικαιώματα και τα συμφέροντα του υποκειμένου των δεδομένων.

γ) 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.

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

στ) Η επεξεργασία είναι απαραίτητη για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων ή όταν τα δικαστήρια ενεργούν υπό τη δικαιοδοτική τους ιδιότητα.

ζ) Η επεξεργασία είναι απαραίτητη για λόγους ουσιαστικού δημόσιου συμφέροντος, βάσει του δικαίου της Ένωσης ή κράτους μέλους, το οποίο είναι ανάλογο προς τον επιδιωκόμενο στόχο, σέβεται την ουσία του δικαιώματος στην προστασία των δεδομένων και προβλέπει κατάλληλα και

συγκεκριμένα μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων του υποκειμένου των δεδομένων,

η) Η επεξεργασία είναι απαραίτητη για σκοπούς προληπτικής ή επαγγελματικής ιατρικής, εκτίμησης της ικανότητας προς εργασία του εργαζομένου, ιατρικής διάγνωσης, παροχής υγειονομικής ή κοινωνικής περίθαλψης ή θεραπείας ή διαχείρισης υγειονομικών και κοινωνικών συστημάτων και υπηρεσιών βάσει του ενωσιακού δικαίου ή του δικαίου κράτους μέλους ή δυνάμει σύμβασης με επαγγελματία του τομέα της υγείας και με την επιφύλαξη των προϋποθέσεων και των εγγυήσεων που αναφέρονται στην παράγραφο 3.

θ) 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 και ασφάλειας της υγειονομικής περίθαλψης και των φαρμάκων ή των ιατροτεχνολογικών προϊόντων, βάσει του δικαίου της Ένωσης ή του δικαίου κράτους μέλους, το οποίο προβλέπει κατάλληλα και συγκεκριμένα μέτρα για την προστασία των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων, ειδικότερα δε του επαγγελματικού απορρήτου.

ι) Η επεξεργασία είναι απαραίτητη για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς σύμφωνα με το άρθρο 89 παράγραφος 1 βάσει του δικαίουτης Ένωσης ή κράτους μέλους, οι οποίοι είναι ανάλογοι προς τον επιδιωκόμενο στόχο, σέβονται την ουσία του δικαιώματος στην προστασία των δεδομένων και προβλέπουν κατάλληλα και συγκεκριμένα μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων του υποκειμένου των δεδομένων.

Όπως προκύπτει από την ανωτερω ανάλυση, όταν εξετάζουμε αν μια πράξη επεξεργασίας είναι νόμιμη ανάλογα πάντα με την κατηγορία των δεδομένων προσωπικού χαρακτήρα που υφίστανται επεξεργασία, εξετάζουμε αν εμπίπτει στους ως άνω επιτρεπτούς λόγους επεξεργασίας που ορίζονται στην παρ.1 β',γ',δ',ε',στ' του άρθρου 6 για τα «απλά» και στην παρ. 2 β',γ',δ',ε',στ',ζ'η',θ'ι' του άρθρου 9 του ΓΚΠΔ για τα «ευαίσθητα». Αυτές οι βάσεις επεξεργασίας αντανακλούν τη φύση του δικαιώματος προστασίας των προσωπικών δεδομένων. Όπως αναφέρεται και στη Γνώμη 6/2014 της Ομάδας του Άρθρου 29, οι λόγοι αυτοί επιτρέπουν την επεξεργασία σε καταστάσεις, όπου η επεξεργασία κρίνεται σκόπιμη και αναγκαία, ανεξαρτήτως της συγκατάθεσης[90].

[90] βλ. Λίλιαν Μήτρου (2017), ο γενικός κανονισμός προστασίας προσωπικών δεδομένων, εκδόσεις Σάκκουλας, σελ. 81 επ.

Αν η υπό κρίση πράξη επεξεργασίας δεν καλύπτεται από αυτές τις βάσεις επεξεργασίας, εξετάζουμε αν το υποκείμενο έχει δώσει τη συγκατάθεσή του για την επεξεργασία αυτή ως ορίζεται στην παρ. 1 α' του άρθρου 6 και στην παρ.2 α' του άρθρου 9 του ΓΚΠΔ. Η συγκατάθεση ως νόμιμη βάση επεξεργασίας έχει θεωρηθεί ως ο «σκληρός» πυρήνας και η τελευταία «γραμμή αμύνης» ενάντια στην απώλεια του ελέγχου επί των δεδομένων[91].

Το γεγονός ότι μια πράξη βασίζεται πράγματι στα θεμέλια που έχει ορίσει ο ΓΚΠΔ, δεν σημαίνει ότι ο υπεύθυνος της επεξεργασίας των δεδομένων απαλλάσσεται από την υποχρέωση τήρησης των αρχών που ορίζονται για την επεξεργασία των δεδομένων.Στις ως άνω περιπτώσεις κατ' εξαίρεση επιτρεπτής επεξεργασίας δεδομένων ειδικων κατηγοριών, ως ειδικότερη περίπτωση επεξεργασίας προσωπικών δεδομένων, θα πρέπει να τηρούνται απαραιτήτως συγκεκριμένοι κανόνες επεξεργασίας, που αναφέρονται στο άρθρο 5 του ΓΚΠΔ και ανάγονται σε Αρχές επεξεργασίας προσωπικών δεδομένων[92].

Η πολυπλοκότητα του ΔτΠ καθιστά αρκετά δύσκολη την εξεύρεση της κατάλληλης νομικής βάσης επεξεργασίας και κάθε ξεχωριστή πράξη. Όπως θα αναλυθεί εκτενώς και κατωτέρω, είναι αρκετά δύσκολο να ληφθεί νόμιμη συγκατάθεσή για όλες τις επιμέρους πράξεις επεξεργασίας του ΔτΠ και η νομική βάση-ειδικά στον τομέα των «έξυπνων» πόλεων-μπορεί να εξαρτάται από έναν περίπλοκο συνδυασμό νομικών βάσεων σε διάφορα επίπεδα.[93]

4.3.4 Η συγκατάθεση

Η συγκατάθεση αποτελεί τη νομική βάση που χρησιμοποιείται στις περιπτώσεις , που οι σκοποί της επεξεργασίας των δεδομένων των εφαρμογών του ΔτΠ δεν καλύπτονται από τις άλλες βάσεις επεξεργασίας του άρθρου 6 παρ.1 και του άρθρου 9 παρ.2 του ΓΚΠΔ. Οι εφαρμογές αυτές αφορούν κυρίως κατασκευαστές συσκευών, πλατφόρμες κοινωνικής δικτύωσης ή πλατφόρμες δεδομένων, φορείς που διαθέτουν συσκευές προς δανεισμό.

Όπως και στην Οδηγία 95/46/ΕΚ και τον ν. 2472/1997, έτσι και στον ισχύοντα Κανονισμό (ΕΕ) 2016/679 και τον ν. 4624/2019 η συναίνεση-συγκατάθεση του υποκειμένου διαδραματίζει σημαίνοντα ρόλο για τη νομιμότητα της επεξεργασίας των προσωπικών δεδομένων. Σύμφωνα με το άρθρο 6 παρ.1 α' και το άρθρο 9 παρ. 2 α' του ΓΚΠΔ, η επεξεργασία των δεδομένων προσωπικού

[91] ibid σελ. 77 επ.
[92] ibid σελ. 71-72
[93] βλ. Ziegler (2019), ο.π., σελ. 123-124

χαρακτήρα είναι νόμιμη, αν νωρίτερα έχει ληφθεί η συγκατάθεση του υποκειμένου των δεδομένων για τους συγκεκριμένους σκοπούς επεξεργασίας. Η συγκατάθεση δίδεται με βάση τις διατυπώσεις του άρθρου 7 του Κανονισμού (ΕΕ) 2016/679, σύμφωνα με το οποίο η συγκατάθεση του υποκειμένου θα πρέπει να δίδεται μετά από πλήρη ενημέρωση του υποκειμένου και να είναι ειδική, ρητή και ελεύθερη.

Η Ομάδα εργασίας του άρθρου 29 στις κατευθυντήριες γραμμές σχετικά με τη συγκατάθεση βάσει του Κανονισμού 2016/679, όπως τελικώς αναθεωρήθηκαν και εκδόθηκαν στις 10 Απριλίου 2018, ορίζει ως «ελεύθερη» τη συγκατάθεση που δόθηκε από τα υποκείμενα των δεδομένων έχοντας πραγματική επιλογή και έλεγχο. Η συγκατάθεση δεν θεωρείται ελεύθερη εάν το υποκείμενο των δεδομένων δεν είναι σε θέση να αρνηθεί ή να αποσύρει τη συγκατάθεσή του χωρίς να ζημιωθεί.

Στην αιτιολογική σκέψη με αριθμό 43 του ΓΚΠΔ καταδεικνύεται ότι η συγκατάθεση δεν θα πρέπει να θεωρείται νόμιμη βάση επεξεργασίας, όταν υπάρχει ζήτημα ανισορροπίας ισχύος μεταξύ του υποκειμένου των δεδομένων και του υπεύθυνου επεξεργασίας, καθώς σε τέτοιες περιπτώσεις είναι σαφές πως το υποκείμενο δεν έχει ρεαλιστικές εναλλακτικές δυνατότητες πέραν της αποδοχής των όρων της επεξεργασίας. Παραδείγματα τέτοιων περιπτώσεων είναι η επεξεργασία των δεδομένων του εργαζόμενου από τον εργοδότη του ή του πολίτη από δημόσιες αρχές. Κατά κανόνα, η συγκατάθεση δεν παρέχεται ελεύθερα στις περιπτώσεις στις οποίες υπάρχει οποιοδήποτε στοιχείο καταναγκασμού, πίεσης ή αδυναμίας άσκησης της ελεύθερης βούλησης και ο χρήστης των εφαρμογών του ΔτΠ νιώθει ότι εξαναγκάζεται να συγκατατεθεί ή ότι θα υποστεί αρνητικές συνέπειες εάν δεν συγκατατεθεί. Εντός των ανωτέρω πλαισίων κινείται και η με αριθμ. 115/2001 Οδηγία της Αρχής Προστασίας Προσωπικών Δεδομένων για την επεξεργασία των δεδομένων στο πλαίσιο των εργασιακών σχέσεων, η οποία σκιαγραφεί με λεπτομέρεια τα όρια της νομιμότητας της επεξεργασίας.

Ακόμη μια προϋπόθεση για την έγκυρη συγκατάθεση είναι να προηγείται πλήρης ενημέρωση του υποκειμένων, όπως αυτή ορίζεται στο άρθρο 7 του ΓΚΠΔ, ώστε να θεωρηθεί πως αυτή δόθηκε «εν πλήρει επιγνώσει». Η ενημέρωση αυτή, η οποία στα πλαίσια του ΔτΠ συνηθίζεται να γίνεται με αναδυόμενα (pop-up) κείμενα, θα πρέπει, μεταξύ άλλων, να πληροφορεί το υποκείμενο για το σκοπό της επεξεργασίας, τις κατηγορίες δεδομένων που υφίστανται επεξεργασία κατά τη χρήση της εφαρμογής, τους αποδέκτες των δεδομένων, τα δικαιώματα των χρηστών ως υποκειμένων των δεδομένων και τα στοιχεία του υπευθύνου επεξεργασίας και του τυχόν εκπροσώπου του. Για να είναι, όμως, «ειδική» η συγκατάθεση θα πρέπει να μην αναφέρεται σε κάθε μελλοντική επεξεργασία, αλλά να αφορά μόνο την επεξεργασία για την οποία έχει παρασχεθεί

η ενημέρωση. Σε περίπτωση, που τα δεδομένα χρησιμοποιηθούν για διαφορετικούς σκοπούς, απαιτείται νέα λήψη συγκατάθεσης[94].

Η συγκατάθεση δίδεται ρητά, όταν από τα μέσα με τα οποία εκδηλώνεται (λ.χ. προφορικά, γραπτώς, ηλεκτρονικά) οδηγούν στο άμεσο συμπέρασμα για τη σχετική βούληση του υποκειμένου. Μάλιστα, έχει κριθεί ότι η συγκατάθεση μπορεί να δίδεται και σιωπηρά, αρκεί να προκύπτει σαφώς ότι άμεσος σκοπός είναι η εξωτερίκευση της βούλησης του υποκειμένου για συγκατάθεση. Βέβαια, η σιωπηρή συγκατάθεση δεν νομιμοποιεί την επεξεργασία των δεδομένων ειδικών κατηγοριών (ευαίσθητων), για την επεξεργασία των οποίων απαιτείται η συγκατάθεση να είναι όχι μόνο ρητή, αλλά και έγγραφη[95].

Πάρα ταύτα, η λήψη της συγκατάθεσης ενός χρήστη-υποκειμένου για συγκεκριμένη πράξη δεν σημαίνει την εσαεί δέσμευση του ως προς τις αποδεχθείσες πράξεις επεξεργασίας. Κι αυτό γιατί, ο ΓΚΠΔ υποχρεώνει τους υπεύθυνους επεξεργασίας να παρέχουν τη δυνατότητα για ανάκληση της συγκατάθεσης ανά πάσα στιγμή, χωρίς όμως ανασταλτικό χαρακτήρα. Συνεπώς, οι κατασκευαστές των εφαρμογών του ΔτΠ θα πρέπει να καθιστούν τεχνικά εφικτή την ανάκληση της συγκατάθεσης του χρήστη σε κάθε στιγμή χρήσης των εφαρμογών του ΔτΠ και παροχής των υπηρεσιών τους.

Αξίζει να υπογραμμίσουμε πως η παροχή συγκατάθεσης εκ μέρους του υποκειμένου των δεδομένων δεν συνεπάγεται παραίτηση από το δικαίωμα προστασίας των προσωπικών δεδομένων και απαλλαγή του υπεύθυνου επεξεργασίας από τις υποχρεώσεις του[96].

Συνεπώς, ο χρήστης των εφαρμογών ΔτΠ θα πρέπει να συγκατατίθεται στην επεξεργασία δεδομένων του έχοντας πλήρη γνώση και επαρκή ενημέρωση για την επεξεργασία αυτή.

4.3.5 Η χρήση της συγκατάθεσης ως βάση επεξεργασίας στο ΔτΠ

Η λήψη της συγκατάθεσης από τους χρήστες του ΔτΠ αποτελεί, όπως προαναφέρθηκε, μια από τις κύριες βάσεις επεξεργασίας. Η χρήση της, όμως, ειδικά σε ψηφιακά περιβάλλοντα έχει αμφισβητηθεί έντονα είτε λόγω της αναντιστοιχίας της απαίτησης με την πραγματικότητα της διαδικτυακής συλλογής είτε επειδή θεωρείται ότι αποτελεί παγίδα και δημιουργεί την ψευδαίσθηση συνειδητής επιλογής. Κι αυτό, διότι οι άνθρωποι ως χρήστες τείνουν να συγκατατίθενται εύκολα και απερίσκεπτα, ακόμα κι αν είναι πράγματι ευαίσθητοι ως προς τις

[94] βλ. Αλεξανδροπούλου-Αιγυπτιάδου (2016), ο.π., σελ. 92 επ.
[95] ibid σελ. 91-92

[96] βλ. Μήτρου (2017), ο.π., σελ. 71 επ.

απειλές για την ιδιωτικότητά τους. Δίδουν, λοιπόν, τη συγκατάθεσή τους επειδή επιθυμούν τη χρήση μιας υπηρεσίας ή διαδικτυακής εφαρμογής, γεγονός που δυστυχώς μπορεί να οδηγήσει ακόμα και στο λεγόμενο "online tracking profiling".[97]Το ψηφιακό περιβάλλον, όμως, και η ποικιλομορφία των τρόπων χρήσης των δεδομένων στο ΔτΠ δημιουργεί την ανάγκη αυξημένης προσοχής από πλευράς των υπεύθυνων επεξεργασίας κατά τη χρήση της ως βάσης επεξεργασίας.

Σύμφωνα με το άρθρο 7 παρ. 1 και την αιτιολογική σκέψη με αριθμ. 42 του ΓΚΠΔ αποτελεί ρητή υποχρέωση του υπεύθυνου επεξεργασίας να αποδεικνύει τη συγκατάθεση του υποκειμένου των δεδομένων. Δεν αρκεί, λοιπόν, να λαμβάνει με έγκυρο τρόπο τη συγκατάθεση, αλλά να είναι ανά πάσα στιγμή σε θέση να την αποδείξει. Αυτό με τη σειρά του σημαίνει, ότι οι κατασκευαστές της τεχνολογίας του ΔτΠ θα πρέπει να διασφαλίσουν ότι η συγκατάθεση που δίδεται, κατά κύριο λόγο, με ψηφιακά μέσα είναι και έγκυρη βάσει των ανωτέρω προϋποθέσεων που θέτει ο ΓΚΠΔ και τεχνικά αποδείξιμη.

Βέβαια, η ανάγκη απόδειξης της συγκατάθεσης δεν θα πρέπει να οδηγεί σε επεξεργασία υπερβολικών ποσοτήτων πρόσθετων δεδομένων. Σύμφωνα με τις Κατευθυντήριες γραμμές με αριθμ. 5/2020 για την συγκατάθεση στα πλαίσια του ΓΚΠΔ που εξέδωσε το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (εφεξής «ΕΣΠΔ»), που διαδέχθηκε την «Ομάδα εργασίας του άρθρου 29» (ΟΕ29), οι υπεύθυνοι επεξεργασίας θα πρέπει να έχουν αναπτύξει τους κατάλληλους μηχανισμούς, ώστε να είναι σε θέση να διαθέτουν επαρκή δεδομένα, για να αποδεικνύουν την ύπαρξη συνδέσμου με την επεξεργασία, αλλά δεν θα πρέπει να οδηγούνται στη συλλογή περισσότερων πληροφοριών από όσες είναι αναγκαίες[98].

Στις ανωτέρω κατευθυντήριες γραμμές του ΕΣΠΔ αναφέρεται, επιπροσθέτως, ότι ο υπεύθυνος επεξεργασίας οφείλει να έχει προσαρμόσει τις παραμέτρους της εφαρμογής του ΔτΠ, ώστε να είναι σε θέση να αποδείξει ότι το υποκείμενο ενημερώθηκε και ότι όλη η ροή των εργασιών και των πράξεων επεξεργασίας των δεδομένων κινήθηκε εντός των πλαισίων της έγκυρης συγκατάθεσης.

Προβληματική, επίσης, μπορεί να αποδειχθεί η ανάκληση της δοθείσας συγκατάθεσης στις πράξεις επεξεργασίας δεδομένων από τον χρήστη του ΔτΠ λόγω του ψηφιακού τρόπου

[97] Ibid, σελ. 77 επ.

[98] βλ. και Κατευθυντήριες γραμμές 5/2020 σχετικά με τη συγκατάθεση βάσει του κανονισμού 2016/679, Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2020, 4 Μαΐου), έκδοση 1.1., σελ. 27 επ. . Ανάκτηση στις 20 Ιανουαρίου 2022 από την επίσημη ιστοσελίδα της Ευρωπαϊκής Επιτροπής.

εξασφάλισης της και των ενδεχόμενων πολλών διαφορετικών σκοπών επεξεργασίας των δεδομένων κατά τη χρήση των τεχνολογιών του ΔτΠ.

Όπως προαναφέρθηκε, ο ΓΚΠΔ στο άρθρο 7 παρ. 3 ορίζει ότι ο υπεύθυνος επεξεργασίας οφείλει να λάβει όλα τα κατάλληλα μέτρα, ώστε το υποκείμενο των δεδομένων να είναι σε θέση να ανακαλέσει τη συγκατάθεση σε κάθε στιγμή και με την ίδια ευκολία που την έδωσε. Δεν προβλέπει, όμως, ότι η παροχή και η ανάκληση της συγκατάθεσης πρέπει να γίνονται με τον ίδιο τρόπο.

Στο υπ' αριθμ. 5/2020 κείμενο των κατευθυντήριων γραμμών του ΕΣΠΔ αναφέρεται χαρακτηριστικά: «Όταν η συγκατάθεση εξασφαλίζεται με τη χρήση ειδικής για υπηρεσία διεπαφής χρήστη (για παράδειγμα, μέσω ιστότοπου, εφαρμογής, λογαριασμού σύνδεσης, διεπαφής συσκευής του διαδικτύου των πραγμάτων ή ηλεκτρονικού ταχυδρομείου), το υποκείμενο των δεδομένων πρέπει αναμφίβολα να είναι σε θέση να ανακαλέσει τη συγκατάθεση μέσω της ίδιας ηλεκτρονικής διεπαφής, καθώς η μετάβαση σε άλλη διεπαφή μόνο για τον λόγο της ανάκλησης της συγκατάθεσης θα απαιτούσε αδικαιολόγητη προσπάθεια». Αναφέρεται επιπρόσθετα ότι η οποιαδήποτε ανάκληση της συγκατάθεσης δεν θα πρέπει να επιφέρει μείωση του επιπέδου της υπηρεσίας ή να απαιτεί επιπλέον χρέωση[99]. Αντιλαμβανόμαστε, λοιπόν, ότι στις περιπτώσεις όπου η επεξεργασία των δεδομένων αποτελεί απαραίτητη προϋπόθεση για την παροχή της υπηρεσίας είναι ιδιαίτερα προβληματικό να βασίσουμε τη νομιμότητα της επεξεργασίας των δεδομένων στη συγκατάθεση. Επιπλέον, είναι συνήθης πρακτική των κατασκευαστών των τεχνολογιών του ΔτΠ να κάνουν χρήση της μεγάλης κλίμακας δεδομένων που υφίστανται επεξεργασία για πολλαπλούς σκοπούς (παροχή υπηρεσίας, διαφημιστικοί σκοποί, δημιουργία προφίλ χρήστη κ.ο.κ.).

Η ανάλυση των δεδομένων μεγάλης κλίμακας καθιστά εξίσου σύνηθη για την τεχνολογία του ΔτΠ την κατάρτιση πορφίλ χρήστη και την αυτοματοποιημένη ατομική λήψη αποφάσεων με σκοπό τη βελτίωση των υπηρεσιών και την εξοικονόμηση πόρων. Η διαδικασία κατάρτισης προφίλ συχνά λαμβάνει χώρα εν αγνοία του χρήστη-υποκειμένου των δεδομένων και παρότι η συγκατάθεση αποτελεί μια από τις εξαιρέσεις από την απαγόρευση της αυτοματοποιημένης λήψης αποφάσεων και κατάρτισης προφίλ του άρθρου 22 παρ. 1 του ΓΚΠΔ, η χρήση της ως βάση επεξεργασίας για τις ανωτέρω πράξεις επεξεργασίας στο ΔτΠ θα πρέπει να γίνεται με ιδιαίτερη προσοχή. Πιο συγκεκριμένα, με βάση και τις Κατευθυντήριες γραμμές της Ομάδας του Άρθρου 29 για την αυτοματοποιημένη λήψη αποφάσεων και την κατάρτιση προφίλ για τους σκοπούς του Κανονισμού

[99] ibid

2016/679 οι υπεύθυνοι επεξεργασίας θα πρέπει να αποδεικνύουν ότι τα υποκείμενα των δεδομένων κατανοούν επακριβώς το αντικείμενο της επεξεργασίας και τους εφιστά την προσοχή ότι η συγκατάθεση δεν αποτελεί πάντα την κατάλληλη βάση για την επεξεργασία[100].

Καταλήγοντας, οι κατασκευαστές των τεχνολογιών του ΔτΠ θα πρέπει να είναι ίδιατερα προσεκτικοί όταν κάνουν χρήση της συγκατάθεσης ως βάσης επεξεργασίας των δεδομένων των χρηστών των τεχνολογιών του ΔτΠ, καθώς, όπως αναλύθηκε ανωτέρω, η λήψη νόμιμης βάσει των επιταγών του ΓΚΠΔ συγκατάθεσης για τους πολλαπλούς σκοπούς επεξεργασίας της μεγάλης κλίμακας δεδομένων που χρησιμοποιούνται για την παροχή των υπηρεσιών τους, μπορεί να αποδειχθεί ιδιαίτερα προβληματική. Θα ήταν, λοιπόν, ασφαλέστερο να επιχειρηθεί να χρησιμοποιηθεί ως βάση νομιμοποίησης των πράξεων επεξεργασίας στο ΔτΠ κάποια από τις άλλες βάσεις επεξεργασίας του άρθρου 6 και του άρθρου 9 του ΓΚΠΔ, και κυριώς η βάση επεξεργασίας του άρθρου 6 παρ.1 στ', δηλαδή ως πράξη απαραίτητη για τους σκοπούς των εννόμων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας, οι οποίοι συχνά είναι η παροχή της συγκεκριμένης υπηρεσίας του ΔτΠ στον χρήστη και η διασφάλιση της εύρυθμης λειτουργίας του συστήματος του ΔτΠ.

4.3.6 Τα δικαιώματα των υποκειμένων

Ποια είναι τα δικαιώματα του υποκειμένου των δεδομένων που πρέπει να λάβει υπόψιν ο υπεύθυνος επεξεργασίας;

Σύμφωνα με το κεφάλαιο III του ΓΚΠΔ (άρθρα 12-22) το υποκείμενο των δεδομένων έχει τα εξής δικαιώματα αναφορικά με την επεξεργασία των δεδομένων του:

1. Δικαίωμα στη διαφανή ενημέρωση: ο υπεύθυνος επεξεργασίας οφείλει να λαμβάνει κατάλληλα μέτρα για να ενημερώνει το υποκείμενο των δεδομένων σχετικά με την επεξεργασία των δεδομένων του και την άσκηση των δικαιωμάτων του. Σε κάθε περίπτωση πρέπει να παρέχονται στο υποκείμενο των δεδομένων επαρκείς πληροφορίες για την ταυτοποίηση του υπευθύνου επεξεργασίας και τα δικαιώματά του σε σχέση με αυτή.

[100] βλ. τις Κατευθυντήριες γραμμές της Ομάδας του Άρθρου 29 για την αυτοματοποιημένη λήψη αποφάσεων και την κατάρτιση προφίλ για τους σκοπούς του Κανονισμού 2016/679 (2018,6 Φεβρουαρίου), Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, έκδοση 1.1., σελ. 14-15. Ανάκτηση στις 20 Ιανουαρίου 2022 από την επίσημη ιστοσελίδα της Ευρωπαϊκής Επιτροπής

2. Δικαίωμα πρόσβασης του υποκειμένου των δεδομένων στα δεδομένα του που υφίστανται επεξεργασία και δυνατότητα λήψης αντιγράφου αυτών.

3. Δικαίωμα διόρθωσης: Το υποκείμενο των δεδομένων μπορεί να απαιτήσει τη διόρθωση ανακριβών δεδομένων.

4. Δικαίωμα διαγραφής («δικαίωμα στη λήθη»): διαγραφή δεδομένων που δεν είναι πλέον απαραίτητα για τους σκοπούς της επεξεργασίας ή έχουν συλλεγεί χωρίς τη συγκατάθεση του υποκειμένου ή εν γένει με τρόπο παράνομο.

5. Δικαίωμα στον περιορισμό της επεξεργασίας: το υποκείμενο των δεδομένων δικαιούται να ζητήσει τον περιορισμό των υπό επεξεργασία δεδομένων του για λόγους όπως η ανακρίβεια των δεδομένων, η παράνομη επεξεργασία των δεδομένων και εν γένει για κάθε περίπτωση που τα δεδομένα δεν είναι πλέον απαραίτητα για τους σκοπούς της επεξεργασίας ή το υποκείμενο των δεδομένων αντιτίθεται σε αυτή.

6. Δικαίωμα στη φορητότητα: το υποκείμενο των δεδομένων μπορεί να λαμβάνει από τον υπεύθυνο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα του και να τα διαβιβάζει περαιτέρω σε άλλον υπεύθυνο επεξεργασίας, χωρίς την αντίρρηση του προηγούμενου, ή μπορεί να αιτηθεί την απευθείας διαβίβαση των δεδομένων του από τον υπεύθυνο επεξεργασίας σε άλλον υπεύθυνο.

7. Δικαίωμα εναντίωσης: το υποκείμενο των δεδομένων μπορεί ανά πάσα στιγμή να εναντιωθεί στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του,περιλαμβανομένης της κατάρτισης προφίλ και ιδίως σε περιπτώσεις όπου η επεξεργασία των δεδομένων προσωπικού χαρακτήρα γίνεται για σκοπούς απευθείας εμπορικής προώθησης.

8. Δικαίωμα να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας: το υποκείμενο των δεδομένων έχει το δικαίωμα να μην υπόκειται σε απόφαση η οποία λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ. Σε κάθε περίπτωση όπου βάσει σύμβασης, νόμου ή ρητής συγκατάθεσης του υποκειμένου των δεδομένων η λήψη αυτοματοποιημένων αποφάσεων και η κατάρτιση προφίλ επιτρέπονται, το υποκείμενο των δεδομένων δικαιούται και ο υπεύθυνος επεξεργασίας υποχρεούται να εξασφαλίσει τουλάχιστον τη δυνατότητα ανθρώπινης παρέμβασης του υποκειμένου στην απόφαση, καθώς και τη δυνατότητα αμφισβήτησης της τελευταίας.

Τα ανωτέρω δικαιώματα έχουν προφανώς και οι χρήστες των συσκεών του ΔτΠ. Παράλληλα, ο ΓΚΠΔ κάνει ορισμένες ειδικές προβλεψεις για διαδικασίες και μηχανισμούς για την άσκηση αυτών των δικαιωμάτων των υποκειμένων των δεδομένων. Πιο συγκεκριμένα, γίνεται ειδική μνεία, μεταξύ άλλων, σε μέσα για την υποβολή των αιτημάτων άσκησης των δικαιωμάτων με ηλεκτρονικό τρόπο

στις περιπτώσεις που έχουμε επεξεργασία δεδομένων με αυτοματοποιημένα μέσα. Γεγονός που φαντάζει εύλογο και επιβεβλημένο όσον αφορά την προστασίας της ιδιωτικότητας του ατόμου, αλλά όταν πρόκειται για εφαρμογές του ΔτΠ, η υλοποίηση του παρουσιάζει σημαντικές προκλήσεις.

Σύμφωνα με το άρθρο 15 του ΓΚΠΔ, το υποκείμενο των δεδομένων έχει το δικαίωμα πρόσβασης στα δεδομένα τα οποία επεξεργάζεται ο καθε υπεύθυνος επεεργασίας και τον αφορούν, το οποίο του παρέχει πρόσβαση 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.»*

Βέβαια, όταν αναφερόμαστε σε πολύπλοκα συστήματα του ΔτΠ η άσκηση του δικαιώματος πρόσβασης δημιουργεί ιδιαίτερους προβληματισμούς. Σε ένα σύστημα του ΔτΠ ένα μεγάλο μέρος των δεδομένων που αποθηκεύονται και διαμοιράζονται στα συστήματα του ΔτΠ είναι «ακατέργαστα δεδομένα»[101]. Αποτελεί, λοιπόν, σύνηθες φανόμενο οι τελικοί χρήστες των εφαρμογών αυτών να μην έχουν τη δυνατότητα πρόσβασης στα ακατέργαστα δεδομένα των συσκευών του ΔτΠ. Βέβαια, είναι εύλογο να επιδεικνύουν μεγαλύτερο ενδιαφέρον για τα επεξεργασμένα δεδομένα, καθώς τα ακατέργαστα μπορεί να μην είναι κατανοητά γι' αυτούς. Έχοντας, όμως, πρόσβαση μόνο στα επεξεργασένα δεδομένα δεν θεωρείται ικανοποιητική άσκηση του δικαιώματος πρόσβασης, καθώς τα υποκείμενα δεν αποκτούν πλήρη εικόνα για την επεξεργασία που υφίστανται τα δεδομένα τους, καθώς η πρόσβαση σε ακατέργαστα δεδομένα ενδέχεται να τους δώσει πληροφορίες, οι οποίες δεν προκύπτουν από τα επεξεργασμένα δεδομένα.

Ζήτημα προκύπτει, επίσης, σχετικά με τη φορητότητα των δεδομένων στο ΔτΠ. Συμφώνα με την παράγραφο 1 του άρθρου 20, το υποκείμενο των δεδομένων έχει το δικαίωμα να λάβει αντίγραφο των δεδομένων που τον αφορούν από τον υπεύθυνο επεξεργασίας και *«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».* Αφορμή της ανωτέρω ρύθμισης αποτέλεσε η ανάγκη για απεξαρτητοποίηση των χρηστών από υπηρεσίες συγκεκριμένων εταιριών κατασκευαστών με σκοπό την άρση των εμποδίων στον ανταγωνισμό και την καινοτομία.

Σύμφωνα με το άρθρο 17 του ΓΚΠΔ, ο υπεύθυνος επεξεργασίας οφείλει να διαγράψει τα

[101] Για περισσότερες πληροφορίες για τα «ακατέργαστα δεδομένα» βλ. *Raw* Data (23 Ιανουαρίου 2022,. Ανάκτηση από en.wikipedia.org στις 25 Ιανουαρίου 2022, στο διαδικτυακό σύνδεσμο: https://en.wikipedia.org/wiki/Raw_data

δεδομένα ενός υποκείμενου που αιτηθεί τη διαγραφή των δεδομένων του *«χωρίς αδικαιολόγητη καθυστέρηση και ο υπεύθυνος επεξεργασίας υποχρεούται να διαγράψει δεδομένα προσωπικού χαρακτήρα χωρίς αδικαιολόγητη καθυστέρηση. Αποφεύγοντας την δημιουργία προφίλ του υποκειμένου τω δεδομένων.»* Σε μεγάλο αριθμό εφαρμογών του ΔτΠ η αποθήκευση των ήδη επεξεργασμένων δεδομένων με σκοπό τη δημιουργία προφίλ χρήστη αποτελεί σημαντικό παράγοντα της λειτουργίας τους και της προσφοράς της βέλτιστης υπηρεσίας στο χρήστη. Στις εφαρμογές αυτές θα πρέπει να δίδεται στο χρήση άμεσα και χωρίς ιδιαίτερο κόπο η δυνατότητα να διαγράψει οριστικά τα δεδομένα του, καθώς δεν μπορεί να θεωρηθει νόμιμη η διατήρηση τους με μόνο σκοπό τη διατήρηση της ιστορικής μνήμης και της βέλτιστης λειτουργίας της εφαρμογής[102].

4.3.7 Υποχρεώσεις του υπεύθυνου επεξεργασίας στο ΔτΠ

Στο κεφάλαιο IV του ΓΚΠΔ, που περιέχονται τα άρθρα 24-43, γίνεται αναφορά στις υποχρεώσεις των υπευθύνων επεξεργασίας. Συγκεκριμένα ο υπεύθυνος επεξεργασίας:

- Έχει υποχρέωση λαμβάνοντας υπόψιν τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων να εφαρμόζει τα κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζει. ώστε να είναι ανά πάσα στιγμή σε θέση να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τις απαιτήσεις του ΓΚΠΔ (άρθρο 24) και να προσταστεύονται επαρκώς τα προσωπικά δεδομένα και τα δικαιώματα των υποκειμένων (άρθρο 25), και να φροντίζει ώστε τα μέτρα αυτά να επικαιροποιούνται. Συνίσταται, επίσης, η τήρηση Κωδίκων Δεοντολογίας του άρθρου 40 του ΓΚΠΔ ή εγκεκριμένου μηχανισμού πιστοποίησης του άρθρου 42 .
- Έχει υποχρέωση να τηρεί «αρχείο δραστηριοτήτων» για ορισμένες πράξεις επεξεργασίας δεδομένων, στο οποίο γίνεται αναφορά σε όλες τις πράξεις επεξεργασίας δεδομένων, στη φύση των δεδομέμων, στο σκοπό επεξεργασίας τους, καθώς και στα κατάλληλα μέτρα που έχουν παρθεί για την προστασία τους (άρθρο 30).
- Στις περιπτώσεις όπου έχει τελεστεί κάποια παραβίαση δεδομένων που ενδέχεται να προκαλέσει κίνδυνο στα δικαιώματα και τις ελευθερίες των υποκειμένων, οφείλει εντός 72 ωρών από τη στιγμή που αποκτά γνώση της παραβιάσης να γνωστοποιεί κάθε παραβίαση προσωπικών

[102] βλ. αναλυτικότερα και Κανέλλος Λεωνίδας (2020), The GDPR Handbook, Για DPOs, Επιχειρήσεις & Οργανισμούς, Νομική Βιβλιοθήκη, σελ. 150 επ.

δεδομένων στην αρμόδια εποπτική αρχή και να την ανακοινώνει στο υποκείμενο των δεδομένων (άρθρο 33).

- Στις περιπτώσεις που η επεξεργασία ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων υποχρεούται να προβεί σε εκτίμηση αντικτύπου για την προστασία των Δεδομένων (ΕΑΠΔ-DPIA) των πράξεων επεξεργασίας πριν από την επεξεργασία (άρθρο 35) και όταν η εκτίμηση αυτή καταδεικνύει πράγματι μεγάλο κίνδυνο για τα συμφέροντα των υποκειμένων οφείλει να προχωρήσει σε προηγούμενη διαβούλευση με την αρμόδια εποπτική Αρχή (ΑΠΔΠΧ) πριν προχωρήσει στην τέλεση των πράξεων επεξεργασίας (άρθρο 36).
- Εάν η επεξεργασία γίνεται από δημόσια αρχή ή φορέα ή συνίσταται σε τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε «μεγάλη κλίμακα»[103] ή αφορά σε επεξεργασία σε «μεγάλη κλίμακα» ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα και δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα οφείλει να διορίζει Υπεύθυνο Προστασίας Δεδομένων (ΥΠΔ-DPO).

Στο σημείο αυτό αξίζει να γίνει ιδιαίτερη μνεία στο άρθρο 25 του ΓΚΠΔ που αναφέρεται στην προστασία των δεδομένων «ήδη από τον σχεδιασμό και εξ ορισμού» (“privacy by design”). Αυτό σημαίνει ότι οι απαιτήσεις απορρήτου και ασφάλειας θα πρέπει να ενσωματωθούν στην αρχική διαδικασία σχεδιασμού ενός συστήματος ή μιας συσκευής του ΔτΠ και όχι να αφήνονται για μεταγενέστερο στάδιο. Αυτή η απαίτηση του ΓΚΠΔ έρχεται με σκοπό να αλλάξει μια συνήθη πρακτική των κατασκευαστών των εφαρμογών του ΔτΠ να σχεδιάζουν ένα σύστημα ή μια συσκευή χωρίς να λάβουν ως παράμετρο την προστασία των δεδομένων και εν γένει του συστήματος. Αυτή η πρακτική είχε ως αποτέλεσμα, όπως αναφέρθηκε και σε προηγούμενα κεφάλαια, να δημιουργούνται συστήματα και συσκευές ευάλωτες σε κακόβουλες επιθέσεις, γεγονός που με τη σειρά του έχει οδηγήσει σε πολλά περιστατικά παραβίασης δεδομένων τα χρόνια της ανάπτυξης της τεχνολογίας του ΔτΠ.

Ένα ακόμα ζήτημα που ρυθμίζεται στο κεφάλαιο IV του ΓΚΠΔ είναι η περίπτωση, όπου ο υπεύθυνος επεξεργασίας χρησιμοποιεί κάποιο τρίτο φυσικό πρόσωπο ή οργανισμό («εκτελούντες την επεξεργασία») για να επιτελέσει για λογαριασμό του πράξεις επεξεργασίας δεδομένων.

[103] Η επεξεργασία «μεγάλης κλίμακας» ορίζεται στο σημείο υπ' αριθμ. 91 της αιτιολογικής έκθεσης του ΓΚΠΔ από τους εξης παράγοντες: Τον αριθμό των εμπλεκόμενων υποκειμένων των δεδομένων, είτε ως συγκεκριμένος αριθμός είτε ως ποσοστό επί του συναφούς πληθυσμού, τον όγκο των δεδομένων και/ή το εύρος των διαφόρων στοιχείων δεδομένων που υφίστανται επεξεργασία, τη διάρκεια ή το μόνιμο χαρακτήρα της δραστηριότητας επεξεργασίας δεδομένων και τη γεωγραφική έκταση της δραστηριότητας επεξεργασίας.

Σύμφωνα με το άρθρο 28 ο υπεύθυνος επεξεργασίας οφείλει να επιλέγει μόνο εκτελούντες την επεξεργασία που παρέχουν επαρκείς διαβεβαιώσεις για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων. Ενδείκνυται, επίσης, να δεσμεύει συμβατικά τους εκτελούντες την επεξεργασία στην τήρηση των ανωτέρω δεσμεύσεων πάντα με γνώμονα τον ΓΚΠΔ και να ελέγχει συστηματικά την τήρηση τους από τους εκτελούντες.

Όπως γίνεται εύκολα κατανοητό οι κατασκευαστές των εφαρμογών του ΔτΠ ενδέχεται να αντιμετωπίσουν σοβαρές προκλήσεις στην προσπάθεια τους να συμμορφωθούν με τον Κανονισμό (ΕΕ) 2016/679. Τα πρόστιμα που προβλέπονται στις περιπτώσεις που αγνοήσουν τις υποχρεώσεις τους ως υπεύθυνοι επεξεργασίας είναι σημαντικά και τσουχτερά. Συγκεκριμένα, βάσει της παρ. 6 του άρθρου 83 η μη συμμόρφωση με τις επιταγές του ΓΚΠΔ και με εντολές της αρμόδιας εποπτικής Αρχής επισύρει διοικητικά πρόστιμα ύψους έως 20.000.000 € ή σε περίπτωση επιχειρήσεων έως το 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους (ανάλογα ποιο από τα δύο είναι υψηλότερο). Επιπρόσθετα, με τον ΓΚΠΔ εισάγονται περισσότερα στάδια ελέγχου των υπευθύνων της επεξεργασίας και μεγαλύτερες εγγυήσεις προστασίας για τα προσωπικά δεδομένα και εδραιώνεται το δικαίωμα των υποκειμένων για καταγγελία στην αρμόδια εποπτική Αρχή, ενώ με βάση την «αρχή της λογοδοσίας» που εισάγεται πρώτη φορά με τον ΓΚΠΔ ο υπεύθυνος επεξεργασίας είναι διαρκώς υπόλογος στα άτομα και στις Αρχές. Οφείλει, όχι απλώς να εφαρμόζει τον Κανονισμό, αλλά και να είναι κάθε στιγμή σε θέση να αποδείξει ότι συμμορφώνεται με όλες τις απαιτήσεις του, ενώ δίδει και τη δυνατότητα στις αρμόδιες εποπτικές Αρχές να προβούν σε έλεγχο στους υπεύθυνους επεξεργασίας χωρίς να έχει προηγηθεί σχετική καταγγελία των υποκειμένων.

Με βάση, λοιπόν, τα ανωτέρω γίνεται αντιληπτό ότι η εφαρμογή του ΓΚΠΔ στο ΔτΠ επιβάλει σημαντικές αλλαγές ως προς τη διασφάλιση της ιδιωτικότητας των ατόμων και των δεδομένων τους.

4.4 Αντιμετωπίζοντας τις προκλήσεις ιδιωτικότητας στο ΔτΠ

Το ΔτΠ ανθεί και διευρύνει συνεχώς τους τομείς της καθημερινότητας στους οποίους εισέρχεται. Αυτή η συνεχής εξέλιξη του καθιστά το ΔτΠ αβέβαιο και δυναμικό και κάνει τις παραδοσιακές προκλήσεις κυβερνοασφάλειας να κλιμακώνονται και να πολλαπλασιάζονται. Το ΔτΠ βασίζεται σε αλληλεπιδράσεις ετερογενών στοιχείων, τα οποία σε μερικά συστήματα μπορεί να περιλαμβάνουν εξοπλισμούς δικτύωσης, αισθητήρες, υποδομές υπολογιστικού νέφους, ακόμα και

ανθρώπινη παρέμβαση[104]. Το ανωτέρω καθιστά ιδιαίτερα δύσκολο για τους υπεύθυνους επεξεργασίας να εφαρμώσουν ουσιαστικό έλεγχο στα δεδομένα και συμμορφωθούν με τις απαιτήσεις του ΓΚΠΔ και των διαφόρων εθνικών νομοθεσιών, λόγω των πολλαπλών πηγών δεδομένων, τον διάσπαρτο αριθμό δεδομένων και των διαφόρων οντοτήτων που εμπλέκονται.

Στο δύσκολο πόνημα της συμμόρφωσης με την ισχύουσα νομοθεσία για την προστασία των προσωπικών δεδομένων, το πρώτο βήμα για κάθε υπεύθυνο επεξεργασίας στο ΔτΠ θα πρέπει να είναι ο έλεγχος και ο εντοπισμός σημείων μη συμμόρφωσης και στη συνέχεια η προσπάθεια να καλυφθούν τα σημεία αυτά. Μια λογική σειρά αντιμετώπισης των προκλήσεων ασφαλείας στο ΔτΠ είναι η ακόλουθη:

1. Αρχικά, θα πρέπει να προβεί στον προσδιορισμό της εκάστοτε ισχύουσας εθνικής και κοινοτικής νομοθεσίας με κριτήριο την τοποθεσία της ανάπτυξης των συστημάτων του ΔτΠ και της συλλογής και επεξεργασίας των δεδομένων τους.
2. Το δεύτερο βήμα στοχεύει στον εντοπισμό των κατηγοριών των προσωπικών δεδομένων που ενδέχεται να συλλεχθούν και/ ή υποβάλλονται σε επεξεργασία από το σύστημα του ΔτΠ.
3. Παρέχεται πλήρης ενημέρωση στα υποκείμενα των δεδομένων σύμφωνα με όσα ορίζονται στα άρθρα 13-14 του ΓΚΠΔ, και εξασφαλίζεται η εύκολη επικοινωνία τους με τον υπεύθυνο προστασίας δεδομένων (DPO) του υπεύθυνου επεξεργασίας.
4. Στις περιπτώσεις, όπου ορίζεται από το άρθρο 35 του ΓΚΠΔ, διενεργείται Εκτίμηση Αντικτύπου σχετικά με την Προστασία των Δεδομένων (ΕΑΠΔ-DPIA), η σκοπεύει να αξιολογήσει τους πιθανούς κινδύνους που προκύπτουν από την επεξεργασία δεδομένων για τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων. Η DPIA Θα πρέπει να εκτελείται πριν από τη συλλογή των δεδομένων. Χρησιμοποιείται, επίσης, ως αποδεικτικό έγγραφο απόδειξης της συμμόρφωσης με την ισχύουσα νομοθεσία για την προστασία των δεδομένων.
5. Θα πρέπει να διενεργείται συστηματικά ανάλυση κενών (Gap analysis), κατά προτίμηση από τρίτους, για να εντοπιστεί οποιαδήποτε πιθανή μη συμμόρφωση με την ΓΚΠΔ. Η ανάλυση κενών θα πρέπει να είναι όσο το δυνατόν πιο συστηματική και να βασίζεται σε σαφή μεθοδολογία.
6. Όλες οι διαπιστωθείσες περιπτώσεις μη συμμόρφωσης αντιμετωπίζονται άμεσα με την υποστήριξη της ανώτατης διοίκησης του κάθε οργανισμού και κατά περίπτωση με νομικούς και τεχνικούς εμπειρογνώμονες.
7. Από τη στιγμή που έχουν επιλυθεί όλα τα ζητήματα μη συμμόρφωσης, συνίσταται η

[104] βλ. Ziegler (2019), ο.π., σελ. 129 επ.

αξιολόγηση από καποιο τρίτο μέρος και η λήψη ειδικής πιστοποίησης.

8. Τέλος, θα πρέπει να δημιουργηθεί ένας μηχανισμός ελέγχου και αναθεώρησης της συμμόρφωσης [105].

Όπως τονίστηκε ανωτέρω, για τη δημιουργία ενός ασφαλούς συστήματος ΔτΠ ο υπεύθυνος επεξεργασίας οφείλει να εφαρμόζει τα κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας των προσωπικών δεδομένων που υφίστανται επεξεργασία. Ο πάροχος, λοιπόν, ενός ασφαλούς συστήματος του ΔτΠ οφείλει να να εφαρμόζει ελαχιστοποίηση δεδομένων, απαιτώντας τους χρήστες μόνο τα απαραίτητα δεδομένα για τη διαδικασία και πρέπει να αποθηκεύσει αυτά τα δεδομένα για τον ελάχιστο απαιτούμενο χρόνο[106]. Η αρχή του περιορισμού της αποθήκευσης υποχρεώνει τους υπευθύνους επεξεργασίας δεδομένων να μην αποθηκεύουν προσωπικά δεδομένα για «περισσότερο από όσο είναι απαραίτητο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία τα δεδομένα προσωπικού χαρακτήρα». Στο ΔτΠ η χρησιμότητα των αποθηκευμένων δεδομένων για τον επιδιωκόμενο σκοπό ενός συγκεκριμένου προϊόντος ή υπηρεσίας θα πρέπει να επανεξετάζεται περιοδικά. Βέβαια, επιτρέπεται επίσης η αποθήκευση χωρίς να προκύπτει σύνδεση με συγκεκριμένο σκοπό επεξεργασίας όταν δεδομένα «θα υποβληθούν σε επεξεργασία αποκλειστικά για σκοπούς αρχειοθέτησης για λόγους δημόσιου συμφέροντος, επιστημονικούς ή ιστορικούς ερευνητικούς σκοπούς ή στατιστικούς σκοπούς». Αυτό μπορεί να έρχεται σε σύγκρουση με τα συμφέροντα και τα δικαιώματα των υποκειμένων των δεδομένων ή άλλες υποχρεώσεις των υπεύθυνων επεξεργασίας σύμφωνα με τη νομοθεσία των κρατών μελών που ενδέχεται να απαιτούν μεγαλύτερες ή μικρότερες περιόδους αποθήκευσης δεδομένων (π.χ. το άρθρο 23 του ΓΚΠΔ αφορά την πρόσβαση σε ιστορικά δεδομένα για ποινικές έρευνες).[107]

Επιπλέον, ο πάροχος οφείλει να ορίσει ποιος έχει πρόσβαση σε αυτά προσωπικά δεδομένα και θα πρέπει να βρεί τον τρόπο να ενσωματώσει στο σύστημα του ΔτΠ έναν τρόπο ώστε ο χρήστης να μπορεί να δώσει ή να αποσύρει τη συγκατάθεσή του/της διαδικασία προσωπικών δεδομένων, όπως αναλύθηκε ανωτέρω. Το σύστημα ΔτΠ θα πρέπει, επίσης, να ενσωματώσει έναν εύκολο τρόπο για τα υποκείμενα για να ασκήσουν τα δικαιώματα τους, όπως αυτά ορίζονται από τον ΓΚΠΔ, και κυρίως αυτά της διόρθωσης και της διαγραφής.

Επιπλέον, το σύστημα του ΔτΠ θα πρέπει να εξασφαλίζει την προστασία των προσωπικών

---

[105] Ibid σελ. 122-123

[106] βλ. Metallidou Chrysi, Konstantinos E. Psannis & Eugenia Alexandropoulou-Egyptiadou (2020), An Efficient IoT System Respecting the GDPR, *The 3rd World Symposium on Communication Engineering*, σελ. 81-82

[107] βλ. Wachter Sandra (2018, 28 Σεπτεμβρίου), The GDPR and the IoT:a three-step transparecy model, *Law, Innovation and Technology, Taylor and Francis Group*, σελ. 9 επ.

δεδομένων και την ασφάλεια της επεξεργασίας τους με την εφαρμογή των τεχνικών της ψευδωνυμοποίησης, ανωνυμοποίσης και κρυπτογράφησης, διασφαλίζοντας την εμπιστευτικότητα και της ακεραιότητας τους[108].

Βέβαια, όταν εξετάζουμε υπό κατασκευή συστήματα του ΔτΠ θα πρέπει πάντα να διασφαλίζεται ότι τηρείται η προστασία της ιδιωτικότητας και του απορρήτου των υποκειμένων από τον σχεδιασμό και εξ ορισμού» ("privacy by design"). Είναι θεμελιώδους σημασίας για την έναρξη οποιασδήποτε διαδικασίας σχεδίασης ή κατασκευής συστήματος, που θέτει τον χρήστη στο επίκεντρο, να διασφαλίζεται εκ των προτέρων πως το σύστημα του ΔτΠ προστατεύει το απόρρητο του χρήστη[109].

Βέβαια, ένα ασφαλές σύστημα ΔτΠ πρέπει να δημιουργεί το αίσθημα ασφάλειας στους χρήστες του και να αποφευχθεί η «ασύμμετρη πληροφόρηση», η οποία αναλύθηκε σε προηγούμενο κεφάλαιο. Προς αυτή την κατεύθυνση κινείται η αιτιολογική σκέψη 100 του ΓΚΠΔ, η οποία ενθαρρύνει τους υπεύθυνους επεξεργασίας να λαμβάνουν πιστοποιήσεις, σφραγίδες και σήματα προστασίας των δεδομένων. Αυτό επιτρέπει στα υποκείμενα να αξιολογούν το επίπεδο προστασίας των δεδομένων τους και βοηθούν στη δημιουργία μιας σχέσης εμπιστοσύνης μεταξύ των παρόχων και των χρηστών υπηρεσιών/αγαθών του ΔτΠ[110]. Το αίσθημα ασφάλειας μπορεί να ενισχυθεί, αν οι χρήστες γνωρίζουν ότι ακόμα και στην περίπτωση που συμβεί ένα περιστατικό παραβίασης των δεδομένων τους, αυτοί θα ενημερωθούν γι' αυτό και θα είναι προετοιμασμένοι για τους κινδύνους που ενδέχεται να επιφέρει αυτό. Γι' αυτό, είναι σημαντικό οι πάροχοι να τηρούν πιστά την υποχρέωση τους ως υπεύθυνοι επεξεργασίας για ενημέρωση των υποκειμένων κατά την τέλεση των περιστατικών παραβίασης δεδομένων που ενδέχεται να επιφέρουν «υψηλό κίνδυνο» για τα υποκείμενα, όπως αυτό προκύπτει από το άρθρο 34 του ΓΚΠΔ. Παρόλο που είναι κατανοητό ότι δεν χρειάζεται να κοινοποιείται κάθε παραβίαση, παραμένει ασαφές ποιος θα αξιολογήσει αυτόν τον «υψηλό» κίνδυνο ή με ποια κριτήρια θα εξαχθούν οι αρνητικές συνέπειες για τους χρήστες. Γι' αυτόν τον λόγο οι πάροχοι συστημάτων του ΔτΠ μπορούν να αναπτύξουν εσωτερικούς κανονισμούς και κώδικες δεοντολογίας (άρθρο 40 του ΓΚΠΔ) για να προσδιορίσουν πότε προκύπτει «υψηλός κίνδυνος» και τι πρέπει να κοινοποιείται στα υποκείμενα

[108] βλ. Metallidou, Psannis, Alexandropoulou-Egyptiadou (2020), ο.π., σελ 81-82
[109] βλ. Nicola Fabiano (2017, Ιούλιος), Internet of Things and the Legal Issues related to the Data Protection Law according to the new European Genaral Data Protection Regulation,, *Athens Journal of Law*, σ.σ. 201-214, σελ. 210 επ. (Volume 3, Issue 3)
[110] βλ. Ziegler (2019), ο.π. σελ. 122-123

των δεδομένων σε αυτές τις περιπτώσεις[111].

Όσον αφορά τα τελικά στάδια του ελέγχου και της αναθεώρησης της συμμόρφωσης με το ΓΚΠΔ, βασικό ρόλο διαδραματίζει ο Υπεύθυνος Προστασίας Δεδομένων (DPO). Σύμφωνα με τα άρθρα 38 και 39 του ΓΚΠΔ, ο ορισμός ενός ΥΠΔ, στις περιπτώσεις που ορίζονται από το άρθρο 37, είναι καταλυτικής σημασίας για την παροχής της κατάλληλης υποστήριξης και τον έλεγχο και την αναθεώρηση της συμμόρφωσης του υπεύθυνου. Ο ρόλος του είναι καθαρά συμβουλευτικός και γνωμοδοτικός ως προς το καθήκον της εσωτερικής διασφάλισης της τήρησης των επιταγών του ΓΚΠΔ. Είναι, μάλιστα, το πρόσωπο που διασφάλισης την εύκολη επικοινωνία των υποκειμένων με τον υπεύθυνο επεξεργασίας, καθώς είναι αυτός που παραλαμβάνει, χειρίζεται και απαντά στα διάφορα παράπονα και καταγγελίες τους. Μπορεί, επίσης, να προτείνει, ακόμα και αν δεν του έχει ζητηθεί, συστάσεις για πρακτικές βελτιώσεις των συστημάτων και αναθεώρηση των μέτρων ασφαλείας[112].

4.5 Γνώμες της Ομάδας Εργασίας του Άρθρου 29 σχετικά με το ΔτΠ

Η Ομάδα Εργασίας του Άρθρου 29 (ΟΕ29) για την προστασία των προσωπικών δεδομένων ήταν μια ανεξάρτητη ευρωπαϊκή ομάδα εργασίας που χειριζόταν θέματα σχετικά με την προστασία της ιδιωτικής ζωής και των δεδομένων προσωπικού χαρακτήρα έως τις 25 Μαΐου 2018 οπότε και αντικαταστάθηκε από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ). Είχε συσταθεί δυνάμει του άρθρου 29 της Οδηγίας 95/46/ΕΚ για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.

Είχε συμβουλευτικό χαρακτήρα αλλά ήταν ανεξάρτητη ως προς την Ευρωπαϊκή Επιτροπή και απαρτιζόταν από έναν εκπρόσωπο των Αρχών Προστασίας Δεδομένων κάθε κράτους-μέλους. Εξέταζε θέματα ιδιαίτερης βαρύτητας ή θέματα που παρουσίαζαν ειδικότερο ενδιαφέρον σχετικά με την προστασία των προσωπικών δεδομένων και περιλαμβάνονταν στον πρώτο πυλώνα της ΕΕ.
Η Ομάδα έχει εκδόσει γνωμοδοτήσεις και κείμενα εργασίας, κάποια από τα οποία είναι σχετικά με την τεχνολογία του ΔτΠ. Οι βασικότερες γνωμοδοτήσεις της Ομάδας του Άρθρου 29 είναι οι κάτωθι:

[111] βλ.Sandra Wachter (2018), ο.π., σελ. 21 επ.
[112] βλ. Σωτηρόπουλος Α. Βασίλης (2017), Υπεύθυνος Προστασίας Δεδομένων,εκδόσεις Σάκκουλας, σελ. 29-33

4.5.1 Γνώμη 13/2011 σχετικά με τις υπηρεσίες εντοπισμού γεωγραφικής θέσης που παρέχονται μέσω έξυπνων κινητών συσκευών.

Στην υπό κρίση Γνώμη η Ομάδα Εργασίας του Άρθρου 29 προβαίνει σε διάκριση των υπεύθυνων επεξεργασίας με κριτήριο τη δυνατότητα εντοπισμού γεωγραφικής θέσεως της συσκευής του ΔτΠ. Προχωρά, λοιπόν, στη διάκριση τους σε υπεύθυνους των διαφόρων υποδομών εντοπισμού γεωγραφικής θέσεως,σε παρόχους εφαρμογών και υπηρεσιών αυτού του τύπου και στους σχεδιαστές των λειτουργικών συστημάτων «έξυπνων» κινητών συσκευών και υπογραμμίζει ότι κατά την αγορά μιας συσκευής με δυνατόττηα εντοπισμού θέσης, οι υπηρεσίες αυτές θα πρέπει να είναι εξ'ορισμού (by default) απενεργοποιημένες.

Γίνεται, ακόμα, αναφορά στις προϋποθέσεις λήψης νόμιμης συγκατάθεσης, η οποία πρέπει να δίδεται για τον εκάστοτε σκοπό επεξεργασίας. Η συγκατάθεση, δηλαδή, δεν θα πρέπει να είναι γενική αλλά να αφορά συγκεκριμένο σκοπό επεξεργασίας, ενώ σε περίπτωση που ο σκοπός της αρχικής επεξεργασίας αλλάξει ο υπεύθυνος επεξεργασίας οφείλει να λάβει εκ νέου συγκατάθεση για τον σκοπό αυτό.

4.5.2 Γνώμη 12/2011 σχετικά για την προστασία των δεδομένων σε ευφυή συστήματα μέτρησης.

Στη Γνώμη 12/2011 γίνεται εκτενής αναφοράστα στα ευφυή συστήματα μέτρησης, τα οποία προβαίνουν σε επεξεργασία δεδομένων με ποικίλους τρόπους. Γίνονται σχετικές συστάσεις στους υπεύθυνους επεξεργασίας των συστημάτων, οι οποίοι πρέπει να προσδιορίζονται πάντα με σαφήνεια, να τηρούν την Αρχή της προστασίας της ιδιωτικής ζωής «ήδη από τον σχεδιασμό» (“by design”), να ενημερώνουν τα υποκείμενα για τις πράξεις επεξεργασίας πριν την παροχή της συγκατάθεσής τους και να τους παρέχουν ανεμπόδιστα τη δυνατότητα να ασκούν τα δικαιώματα τους.

4.5.3 Γνώμη 02/2013 σχετικά για τις εφαρμογές των έξυπνων συσκευών.

Η συγκεκριμένη Γνώμη είναι η πρώτη χρονικά που εκδίδει η Ομάδα Εργασίας του Άρθρου 29 αποκλειστικά για το οικοσύστημα των εφαρμογών του ΔτΠ, του οποίου η ανάπτυξη υπήρξε ιλλιγιώδης τα χρόνια που προηγήθηκαν της έκδοσής της. Η Γνώμη αυτή αναφέρει το σημαντικό

ζήτημα της δυσκολίας που αντιμετωπίζουν οι χρήστες κατά την πρόσβασητους στα δεδομένα που αποθηκεύονται σε φορητές συσκευές και τους αφορούν. Επίσης, εντοπίζει την έλλειψη ευαισθητοποίησης των σχεδιαστών και των κατασκευαστών των εφαρμογών αυτών, που επιλέγουν να αγνοήσουν τους κίνδυνους που σχετίζονται με την προστασία των προσωπικών δεδομένων, και προχωρά σε συστάσεις προς αυτούς επισημαίνοντας τους τις υποχρεώσεις τους.

Οι σχεδιαστές των εφαρμογών του ΔτΠ οφείλουν να τηρούν όλες τις υποχρεώσεις του ως υπεύθυνοι επεξεργασίας και μεριμνούν για την τήρηση των υποχρεώσεων των εκτελούντων την επεξεργασία συνεργατών τους. Επίσης, τονίζεται η σημασία της ενημέρωσης του υποκειμένου των δεδομένων πριν τη χρήση της εφαρμογής και η λήψη της συγκατάθεσης του πριν η κάθε εφαρμογή αρχίσει να συλλέγει ή να διαμοιράζει δεδομένα στις συσκευές. Τους εφιστά, μάλιστα, την προσοχή ότι η συγκατάθεση δεν μπορεί να νομιμοποιεί την υπερβολική ή δυσανάλογη επεξεργασία προσωπικών δεδομένων.

Ακόμη, στην υπό κρίση Γνώμη, τονίζεται η σημασία εφαρμογής της «αρχής της ελαχιστοποιήσης», της τήρησης μιας εύκολα προσβάσιμης πολτικής απορρήτου και της λήψης κάθε πρόσφορου και αναγκαίου οργανωτικού και τεχνικού μέτρου για την προστασία των προσωπικών δεδομένων. Τέλος, τονίζει ότι οι σχεδιαστές των εφαρμογών του ΔτΠ οφείλουν να παρέχουν τη δυνατότητα στους χρήστες των εφαρμογών τους να ασκούν τα δικαιώματά τους.

4.5.4 Γνώμη 8/2014 σχετικά με τις εξελίξεις στο ΔτΠ

Τα χρόνια που προηγήθηκαν της έκδοσης της Γνώμης 8/2014 το ΔτΠ έκανε γιγαντιαία βήματα ανάπτυξης, γεγονός που οδήγησε την Ομάδα Εργασίας του Άρθρου 29 να εκδόσει τη σχετική Γνώμη σχετικά με τις εξελίγεις στο ΔτΠ. Στη Γνώμη αυτή γίνεται αναφορά στους βασικότερους κινδύνους στο ΔτΠ για τα προσωπικά δεδομένα. Βέβαια στην παρούσα Γνώμη δεν καλύπτονται όλες οι πτυχές του, μιας και το ΔτΠ δεν είχε ακόμα φτάσει στα σημερινά επίπεδα ανάπτυξης του,. Εστιάζει, λοιπόν, στους τρείς βασικότερους και πιο διαδεδομένους τότε τομείς ανάπτυξης του ΔτΠ, οι οποίοι ήταν οι κάτωθι:

- **Φορετές υπολογιστικές συσκευές (wearable devices)**

  Οι «φορετές υπολογιστικές συσκευές» σύμφωνα πάντα με τη Γνώμη περιλάμβαναν μια μεγάλη ποικιλία προϊόντων, όπως ρολόγια χειρός, γυαλιά και αθλητικά παπούτσια, τα οποία με τη χρήση αισθητήρων, καμερών και μικροφώνων πετύχαιναν τη συλλογή δεδομένων απο τους χρήστες των συσκευών και το περιβάλλον τους, τα οποία δεδομένα αποθήκεαν σε

απομακρυσμένα τερματικά. Επιπλέον, με την ύπαρξη διαθέσιμων διεπαφών προγραμματισμού εφαρμογών και τη δημιουργία εφαρμογών από τρίτους, πετυχαίνουν την έυκολη πρόσβαση στις πληροφορίες που εξάγονται από τα δεδομένα και τη δημιουργία προφίλ χρήστη.

- **Ποσοτικοποιημένος εαυτός (quantified self)**

  Με τις συσκευές του «ποσοτικοποιημένου εαυτού» γίνεται η καταγραφή των δραστηριοτήτων του χρήστη ("activity tracker"), όπως λχ οι ώρες ύπνου του, οι καρδιακοί παλμοί του, η απόσταση και η διαδρομή που έχουν διανύσει. Η εξαγωγή των πληροφοριών από τις ανωτέρω δεδομένα μπορεί να οδηγήσει τον χρήστη στη βελτίωση της καθημερινότητας και της υγεάς του, αλλά μπορεί παράλληλα να οδηγήσει στη συνεχή του παρακολούθηση. Υπάρχει, λοιπόν, ο κίνδυνος της κοινοποίησης των ανωτέρω δεδομένων σε μη εξουσιοδοτημένους τρίτους και η χρήση τους από εταιρίες και οργανισμούς για διαφορετικούς σκοπούς χωρίς τη συναίνεση των υποκειμένων.

- **Οικιακός αυτοματισμός (domotics)**

Αφορούν συσκευές που δίνουν τη δυνατότητα του απομακρυσμένου ελέγχου όλων των επιμέρους συσκευών του «έξυπνου» σπιτιού. Συλλέγουν δεδομένα κίνησης, περιβάλλοντος (θερμοκρασία, υγρασία κ.α.) και καταφέρνουν να βελτιώνουν την καθημερινότητα των χρηστών τους. Είναι φανερό ότι η οικιακή αυτοματοποίηση Δημιουργούν, όμως, και σημαντικά ζητήματα ιδιωτικότητας, καθώς το άτομο μπορεί να βρεθεί να παρακολουθείται μέσα στο ίδιο του το σπίτι.

Σύμφωνα πάντα με τη Γνώμη 8/2014, η συνεχόμενη εξέλιξη του ΔτΠ καθιστά επιτακτική ανάγκη την θέσπιση ενός νέο νομικού πλαισίου για την προστασία των προσωπικών δεδομένων και της ιδιωτικότητας των χρηστών στο ΔτΠ. Γίνεται αναφορά στα βασικότερα ζητήματα που προκύπτουν κατά τη χρήση των τεχνολογιών αυτών και εφιστά την προσοχή στους κατασκευαστές τους για τον κίνδυνο που ενέχει το ΔτΠ για τα προσωπικά δεδομένα.

Συγκεκριμένα, γίνεται αναφορά στην έλλειψη ενημέρωσης και ελέγχου των επιμέρους πράξεων επεξεργασίας δεδομένων, που ενδέχεται να έχουν οι χρήστες λόγω της τεράστιας ροής δεδομένων ανάμεσα στα αντικείμενα και τις συσκευές του ΔτΠ. Στις περισσότερες περιπτώσεις, η επικοινωνία και η ανταλλαγή δεδομένων μεταξύ των συσκευών γίνεται αυτοματοποιημένα και δεν καθίσταται δυνατός ο έλεγχος των πράξεων επεξεργασίας από τον χρήστη. Εγείρονται, λοιπόν, σημαντιά ζητήματα για το ποιος πραγματικά προβαίνει σε πράξεις επεξεργασίας δεδομένων των χρηστών, για ποιούς σκοπούς και με ποιά μέσα. Το γεγονός αυτό οδηγεί σε μια συνεχή και μη ελεγχόμενη παρακολούθηση του χρήστη με τρόπο αδιαφανή.

Η Ομάδα Εργασίας του Άρθρου 29 θεωρεί, επίσης, σημαντικό το θέμα της συγκατάθεσης των υποκειμένων των δεδομένων στο ΔτΠ. Ο μεγαλύτερος αριθμός των συσκευών του ΔτΠ δεν διαθέτουν κατάλληλους μηχανισμούς λήψης συγκατάθεσης για την επεξεργασία των προσωπικών δεδομένων των χρηστών τους. Αυτό έχει ως αποτέλεσμα να τελούνται πράξεις επεξεργασίας δεδομένων χωρίς τη συγκατάθεση του υποκειμένου. Βέβαια, ακόμα και στις περιπτώσεις που οι κατασκευαστές έχουν προβλέψει για την ύπαρξη μηχανισμού λήψης συγκατάθεσης, παρατηρείται ελλειπής, αλλά ακόμη και τελείως απούσα, ενημέρωση του χρήστη για τον τρόπο επεξεργασίας των δεδομένων από τα επιμέρους συστήματα του ΔτΠ, με αποτέλεσμα να μην υπάρχει νόμιμη συγκατάθεση. Η έλλειψη ενημέρωσης σε συνδυασμό με την επεξεργασία δεδομένων από τρίτα μέρη (third parties) χωρίς την λήψη ειδικής συγκατάθεσης αποτελούν σοβαρό πρόβλημα για την ιδιωτικότητα των χρηστών. Πολλώ δε μάλλον στις περιπτώσεις που η χρήση αυτών των δεδομένων μπορεί να εξάγει περαιτέρω πληροφορίες για το υποκείμενο και να δημιουργήσει ένα «προφίλ χρήστη».

Τέλος, γίνεται αναφορά στα «κενά ασφαλείας» που έχουν παρατηρηθεί στις συσκευές και τα συστήματα του ΔτΠ, τα οποία τα καθιστούν ευάλωτα σε κακόβουλες επιθέσεις. Αυτό συμβαίνει, συνήθως, από επιλογή των κατασκευαστών, καθώς όταν καλούνται να επιλέξουν ανάμεσα στην αποδοτικότητα και την ασφάλεια, πάντα επιλέγουν να θυσιάσουν την ασφάλεια στο βωμό της αποδοτικότητας και της βέλτιστης προσφερόμενης υπηρεσίας.

Στη συνέχεια η Ομάδα Εργασίας του άρθρου 29 στην υπό εξέταση Γνώμη προέβη σε συστάσεις προς τους κατασκευαστές των εφαρμογών του ΔτΠ σχετικά με την προστασία του δικαιώματος των υποκειμένων στην ιδιωτικότητα, οι οποίες αποτελούν κατευθυντήριες γραμμές ως προς τη χρήση, τη λειτουργία και την ανάπτυξη τους. Οι συστάσεις αυτές αφορούσαν όλα τα ενδιαφερόμενα μέρη και ήταν οι εξής:

• Διαγραφή των μη επεξεργασμένων δεδομένων και όσων δεδομένων έχουν υποστεί επεξεργασία και δεν είναι πια απαραίτητα για τους σκοπούς της επεξεργασίας που εκτελείται.

• Σχεδιασμός όλων των συσκευών και των συστημάτων του ΔτΠ με βάση την αρχή της Προστασίας εξ' ορισμού και ήδη από τον σχεδιασμό (“Privacy by default” και “Privacy by design”).

• Εφαρμογή των αρχών Προστασίας της ιδιωτικής ζωής, σεβασμός του ιδιωτικού απορρήτου των χρηστών και ενημέρωση τους για κάθε επιμέρους πράξη επεξεργασίας δεδομένων τους.

• Δημιουργία προσιτής διεπαφής (interface) χρήστη, ώστε οι πληροφορίες, η ενημέρωση και η λήψη της συγκατάθεσης να γίνεται με τρόπο απλό και εύκολο για τους χρήστες.

• Λήψη των κατάλληλων μέτρων ασφαλείας, σύμφωνα με τα ισχύοντα πρότυπα αντιμετώπισης

κακόβουλων επιθέσεων, όπως λ.χ. συστήματα κρυπτογράφησης κλειδιού.

• Τα δεδομένα να είναι σε κατάλληλη μορφή που να επιτρέπει την άσκηση των δικαιωμάτων της πρόσβασης και της φορητότητας των δεδομένων των υποκειμένων. Να παρέχεται, επίσης, η δυνατότητα επεξεργασίας των δεδομένων που κοινοποιούνται και να ασκείται χωρίς δυσανάλογη προσπάθεια το δικαίωμα διαγραφής των δεδομένων.

• Οι σχεδιαστές εφαρμογών πρέπει να δίνουν ιδιαίτερη προσοχή κατά την επεξεργασία ευαίσθητων δεδομένων .

• Εφαρμογή της αρχής της Ελαχιστοποίησης των Δεδομένων, όπως αυτή αναλύθηκε ανωτέρω.

• Η μη παροχή συγκατάθεσης εκ μέρους του χρήστη δεν θα πρέπει να συνεπάγεται τον αποκλεισμό του από τη χρήση της εφαρμογής.

• Οι μη χρήστες των συσκευών του ΔτΠ, των οποίων τα δεδομένα συλλέγονται θα πρέπει να ενημερώνονται με κάθε πρόσφορο μέσο.

• Οι οργανισμοί τυποποίησης θα πρέπει να αναπτύξουν ελαφριά πρωτόκολλα κρυπτογράφησης και επικοινωνίας, τα οποία θα διασφαλίζουν την εμπιστευτικότητα και την ακεραιότητα των δεδομένων, τον έλεγχο ταυτότητας και τον έλεγχο πρόσβασης των χρηστών.

Οι συστάσεις, όμως, αφορούσαν και ειδικότερες κατηγορίες σχεδιαστών και κατασκευαστών εφαρμογών των τεχνολογιών του ΔτΠ. Ειδικότερα, έγιναν συστάσεις για την κατασκευή και ανάπτυξη των πλατφόρμων κοινωνικής δικτύωσης (social media), που αφορούσαν την από προεπιλογή μη καταχώριση των πληροφοριών που δημοσιεύονται σ΄αυτά στα ευρετήρια μηχανών αναζήτησης και την παροχή της δυνατότητας στους χρήστες να διαμορφώνουν οι ίδιοι τις ρυθμίσεις της κάθε πλατφόρμας, που αφορούν την κοινοποίηση και επεξεργασία των δεδομένων τους.

4.6 Η Οδηγία 2002/58/ΕΚ

Η 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-”ePD”), είναι ευρέως γνωστή ως “e-Privacy” Οδηγία ή “Cookie Law”. Η εν λόγω Οδηγία ρυθμίζει ζητήματα σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα στον τομέα των ηλεκτρονικών επικοινωνιών, θέτοντας περιορισμούς στους παρόχους υπηρεσιών τηλεπικοινωνίας. Η ανωτέρω Οδηγία τροποποιήθηκε βάσει της Οδηγίας 2009/136/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 25ης Νοεμβρίου 2009 για την καθολική

υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών[113].

Η "e-Privacy" Οδηγία, λοιπόν, όπως τροποποιήθηκε και ισχύει σήμερα, ορίζει ότι οι πάροχοι υπηρεσιών τηλεπικοινωνίας οφείλουν να τηρούν τα κάτωθι:

- **Επεξεργασία δεδομένων cookies αποκλειστικά μετά την παροχή νόμιμης συγκατάθεσης**

Έχει γίνει αναφορά ανωτέρω ότι τα δεδομένα που περιέχονται στα μπισκότα ("cookies") που τοποθετούνται στους τερματικούς των χρηστών διαδικτυακών εφαρμογών αποτελούν δεδομένα προσωπικού χαρακτήρα. Με βάση την Οδηγία για την τοποθέτηση των "cookies" και την πρόσβαση στις πληροφορίες τους, απαιτείται πρώτα η λήψη της συγκατάθεσής των χρηστών. Σύμφωνα με το άρθρο 5 παρ. 3 της Οδηγίας 2002/58/ ΕΚ, τα κράτη μέλη θα πρέπει να 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 για το συγκεκριμένο σκοπό της επεξεργασίας. Βέβαια, υπάρχουν και δεδομένα και πληροφορίες, που θεωρούνται απολύτως αναγκαία για τη λειτουργία της εφαρμογής και χωρίς αυτές δεν δύναται να λειτουργήσει. Έτσι, κρίνεται αναγκαία η διάκριση στα "αναγκαία cookies", για τα οποία δεν απαιτείται η λήψη της συγκατάθεσης του χρήστη, και στις υπόλοιπες κατηγορίες τους, για την επεξεργασία των οποίων θα πρέπει να ζητείται πάντα η συγκατάθεση του χρήστη.

Εν προκειμένω και προχωρώντας σε ανάλυση της ανωτέρω πρόβλεψης της Οδηγίας σε σχέση με το ΔτΠ, εντοπίζουμε σοβαρό ζήτημα κατά τη λειτουργία μεγάλου μέρους των συσκευών του ΔτΠ, τα οποία ενδέχεται να συλλέγουν και δεδομένα που δεν αφορούν μόνο το χρήστη τους. Έτσι, λοιπόν, υπάρχει μεγάλος αριθμός δεδομένων στα οικοσυστήματα του ΔτΠ, που δεν αφορούν τον χρήστη που έχει δώσει τη συγκατάθεση του για την επεξεργασίας τους. Χαρακτηριστικό παράδειγμα αποτελούν τα δεδομένα που συλλέγονται μέσω των "google glasses", όπου μπορούμε να έχουμε βιντεοσκόπηση άλλων υποκειμένων δεδομένων εκτός από τον χρήστη τους χωρίς την προηγούμενη συγκατάθεσή τους[114].

- **Τήρηση αυστηρών μέτρων ασφαλείας της επεξεργασίας των δεδομένων**

Οι πάροχοι είναι υποχρεωμένοι να τηρούν κάθε πρόσφορο οργανωτικό και τεχνικό μέτρο για την προστασία των δεδομένων, επιτρέποντας πρόσβαση σ' αυτά μόνο στο εξουσιοδοτημένο

[113] βλ. Αλεξανδροπούλου-Αιγυπτιάδου (2016), ο.π., σελ. 213 επ.
[114] βλ. Φ. Παναγοπούλου-Κουτνατζή (2014), ο.π., σελ 352 επ.

προσωπικό του και προστατεύοντας τα δεδομένα αυτά από καταστροφή, τυχαία απώλεια, αλλοίωση και κάθε άλλη παράνομη πράξη επεξεργασίας.

- **Τήρηση του απορρήτου των επικοινωνιών**

Τα κράτη μέλη οφείλουν να εγγυώνται το απόρρητο των επικοινωνιών, που πραγματοποιούνται μέσω δημόσιου δικτύου. Απαγορεύεται, δηλαδή, η πρόσβαση, η αποθήκευση των επικοινωνιών και των δεδομένων κίνησης απο άλλα πρόσωπα χωρίς τη συγκατάθεση των χρηστών, εκτός εάν το εν λόγω πρόσωπο είναι νομίμως εγκεκριμένο.

- **Επεξεργασία δεδομένων κίνησης και θέσης και ανωνυμοποίησή τους**

Δεδομένα κίνησης χρηστών που υφίστανται επεξεργασία και αποθηκεύονται από πάροχο δημόσιου δικτύου, πρέπει να διαγράφονται οριστικά ή να ανωνυμοποιούνται όταν δεν είναι πλέον απαραίτητα. Τα δεδομένα θέσης υφίστανται επεξεργασία μόνο μετά από τη λήψη της συγκατάθεσης του χρήστη ή μετά από ανωνυμοποίησή τους.

4.7 Η Οδηγία 2006/24/ΕΚ

Αντικείμενο της Οδηγίας είναι η εναρμόνιση των κρατών μελών της ΕΕ όσον αφορά τα δεδομένα κίνησης και θέσης που οφείλουν οι πάροχοι υπηρεσιών ηλεκτρονικών επικοινωνιών να διατηρούν για σκοπούς διερεύνησης, διαπίστωσης και δίωξης σοβαρών ποινικών αδικημάτων. Η υποχρέωση διατήρησης, βέβαια, δεν περιλαμβάνει το περιεχόμενων των επικοινωνιών για το οποίο εξακολουθούν να ισχύουν οι κείμενες διατάξεις.

Σύμφωνα με την παρ. 2 εδ.α' του άρθρου 3 της Οδηγίας, η διατήρηση των δεδομένων θέσης και κίνησης δεν είναι υποχρεωτική, αλλά επιτρέπεται στις περιπτώσεις όπου τα δεδομένα παράγονται ή υποβάλλονται σε επεξεργασία και όταν αποθηκεύονται (για τα τηλεφωνικά δεδομένα) και όταν καταγράφονται (για τα διαδικτυακά) από παρόχους υπηρεσιών ή δικτύων επικοινωνιών κατά την παροχή των οικείων υπηρεσιών.

Οι ορισμοί του «δικτύου ηλεκτρονικών επικοινωνιών» και των αυτών υπηρεσιών είναι αρκετά ευρείς στην Οδηγία 2002/21 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 7ης Μαρτίου 2002 σχετικά με κοινό κανονιστικό πλαίσιο για δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών με αποτέλεσμα να δημιουργούνται ζητήματα ερμηνείας σε σχέση με τους παρόχους διαθέσιμων για το κοινό υπηρεσιών ή δημοσίων δικτύων επικοινωνίας. Κι αυτό γιατί σε χώρες όπως

η Γαλλία, η υποχρέωση διατήρησης καταλαμβάνει ακόμα και internet cafes, ξενοδοχεία και κάθε άλλο πρόσωπο που παρέχει υπηρεσίες πρόσβασης στο Διαδίκτυο.[115]

4.8 Γνωμοδότηση 2018/C 440/02 της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής

Η Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή (ΕΟΚΕ) εξέδωσε τη Γνωμοδότηση 2018/C 440/02 σχετικά με την εμπιστοσύνη, την ιδιωτικότητα και την ασφάλεια των καταναλωτών και των επιχειρήσεων στο ΔτΠ, η οποία υιοθετήθηκε από την Ολομέλεια στις 19 Σεπτεμβρίου το 2018[116].

Σύμφωνα με τη Γνωμοδότηση, προβλέπεται ότι εντός της επόμενης δεκαετίας η επανάσταση του ΔτΠ θα επηρεάσει διάφορους τομείς της καθημερινής ζωής, όπως της ενέργειας, της γεωργίας και των μεταφορών, όπως επίσης και τους πιο παραδοσιακούς τομείς της οικονομίας και της κοινωνίας.

Τα ειδικά χαρακτηριστικά της τεχνολογίας του ΔτΠ, όπως τα υψηλά επίπεδα πολυπλοκότητας, η ισχυρή αλληλεξάρτηση κ.α., αποτελούν τη βασική αιτία των προκλήσεων που αντιμετωπίζει η ΕΕ και τα κράτη μέλη της. Η πολυπλοκότητα του ΔτΠ, η οποία επιτρέπει τη διασύνδεση συσκευών διαφορετικών κατασκευαστών, διανομέων ή παραγωγών λογισμικού, δημιουργεί δυσκολίες στην απόδοση ευθυνών σε περιπτώσεις μη συμμόρφωσης με τη νομοθεσία. Παρατηρείται, επίσης, ότι πολλοί από τους επαγγελματίες του ΔτΠ δεν διαθέτουν επαρκείς γνώσεις και εμπειρία σε θέματα ασφάλειας ή προστασίας δεδομένων όσον αφορά τις δικτυωμένες συσκευές. Για τον λόγο αυτόν απαιτείται μια νέα προσέγγιση όσον αφορά τις ευθύνες, με στόχο να διασφαλιστεί ότι τόσο οι καταναλωτές όσο και οι επιχειρήσεις που υιοθετούν εφαρμογές του ΔτΠ προστατεύονται σε περιπτώσεις που προϊόντα με ενδεδειγμένες ρυθμίσεις μπορεί να αποδειχθούν ελαττωματικά ή μη ασφαλή λόγω συμβάντων ψηφιακής ασφάλειας ή λόγω μη εξουσιοδοτημένης αθέμιτης χρήσης (π.χ. από hackers)[117].

---

[115] βλ. Ιγγλεζάκης Ιωάννης (2021), Δίκαιο Πληροφορικής, εκδόσεις Σάκκουλα, σελ.392 επ. (4η έκδοση)

[116] βλ. Αναλυτικότερα βλ. το κείμενο της Γνωμοδότησης 2018/C 440/02 της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής(2018). Ανάκτηση στις 22 Ιανουαρίου 2022, διαθέσιμη στην επίσημη ιστοσελίδα της Ευρωπαϊκής Επιτροπής στο διαδικτυακό σύνδεσμο: https://www.eesc.europa.eu/el/node/59507?fbclid=IwAR28bSm9c9gZzskz_Q_F11CTKsXXhDsSeHOEWnBcZ_6wJNWHis6A8lnqdRM

[117] βλ. *Internet of Things: Ιδιωτικότητα και ασφάλεια καταναλωτών και επιχειρήσεων στο Διαδίκτυο των πραγμάτων* (2018, 01 Νοεμβρίου). Ανάκτηση από lawspot.gr στις 22 Ιανουαρίου 2022, στον διαδικτυακό σύνδεσμο*:*

Μετά την εφαρμογή του ΓΚΠΔ, έχει ενισχυθεί ο έλεγχος των καταναλωτών επί των προσωπικών τους δεδομένων και των ιδιωτικών τους προτιμήσεων. Βάσει του ΓΚΠΔ οι εταιρείες οφείλουν να εφαρμόζουν τα κατάλληλα τεχνικά και οργανωτικα μετρά και να επανεξετάζουν τακτικά αν τα δεδομένα που υφίστανται επεξεργασία είναι κατάλληλα και τα απολύτως αναγκαία για την παροχή της υπηρεσίας. Οι πτυχές και οι επιπτώσεις της ιδιωτικότητας πρέπει να αξιολογούνται σε όλη τη διάρκεια της σύλληψης, του κύκλου σχεδιασμού και της ανάπτυξης μιας συσκεύης ή ενός δικτύου του ΔτΠ.

Οι πολλές διασυνδεδεμένες συσκευές του ΔτΠ δημιουργούν γόνιμο έδαφος για παράνομες ή ανεπιθύμητες τεχνολογικές πρακτικές και μετατρέπει το ΔτΠ σε ένα περιβάλλον με δεδομένα εύκολα προσπελάσιμα και ταχύτατα διαδιδόμενα. Για την ασφάλεια, λοιπόν, της ιδιωτικότητας και των δεδομένων που διακινούνται ανάμεσα στις συσκευές αυτές θα πρέπει να τηρηθούν τα βέλτιστα τεχνολογικά πρότυπα ασφαλείας για καθένα από τα ξεχωριστά στοιχεία του συστήματος του ΔτΠ, ενώ ο μεγάλος αριθμός τους δεν πρέπει να οδηγεί σε έκπτωση των προτύπων ασφαλείας. Στο πλαίσιο αυτό, η ΕΟΚΕ στηρίζει τις αρμοδιότητες της πολυσυμμετοχικής ομάδας εμπειρογνωμόνων σχετικά με την ευθύνη και τις νέες τεχνολογίες[118].

Με γνώμονα τα ανωτέρω και με σκοπό την προστασία των καταναλωτών και των επιχειρήσεων που εμπλέκονται στο οικοσύστημα του ΔτΠ, η ΕΟΚΕ εξέδωσε τις κατωτέρω προτάσεις για ανάληψη δράσης στο πλαίσιο των δημόσιων πολιτικών:

1. Δημιουργία περιβαλλόντων δοκιμών (sand boxes) για τα πιλοτικά έργα και τις αποδείξεις αρχών, οι οποίες δεν θα στοχεύουν στην απλή δοκιμή τεχνολογιών, αλλά και στη δοκιμή κανονιστικών προτύπων.
2. Ορισμός ιδρυμάτων και ανεξάρτητων αρχών ως παράγοντες διευκόλυνσης και εποπτείας των έργων του ΔτΠ.
3. Να γίνει προώθηση συμπράξεων και πλατφόρμων συνεργασίας δημόσιου και ιδιωτικού τομέα και εκστρατειών ευαισθητοποίησης και εκπαιδευτικών προγραμμάτων για την ευκολότερη υιοθέτηση του ΔτΠ από τις επιχειρήσεις και τους καταναλωτές.
4. Να γίνει αξιολόγηση της ισχύουσας νομοθεσίας για το ΔτΠ από την Ευρωπαϊκή Επιτροπή και να προβεί στις απαιτούμενες αναθεωρήσεις της, όπου αυτό απαιτείται.

---

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

[118] ibid

4.9 Νομικό Πλαίσιο στην Ελλάδα

4.9.1 Ο Νόμος 4624/2019

Στις 29-08-2019 δημοσιεύθηκε στην Εφημερίδα της Κυβερνήσεως ο Ν. 4624/2019 (ΦΕΚ 137/Α/29-8-2019) σχετικά με την «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις.», η ισχύς του οποίου άρχισε από την δημοσίευση του. Ήρθε να καλύψει του κενό που άφησε στην ελληνική έννομη τάξη η παύση ισχύος του Ν. 2472/1997, η οποία ουσιαστικά ήρθε με την έναρξη ισχύος του ΓΚΠΔ, καθώς ο ελληνικός Νόμος είχε ισχύ μόνο ως προς τα ζητήματα, που δεν ρύθμιζε ο ΓΚΠΔ. Στην ουσία ο ΓΚΔΠ κάλυπτε ένα ευρύ φάσμα των ζητημάτων που άπτονται της προστασίας της ιδιωτικότητας και των δεδομένων προσωπικού χαρακτήρα και άφηνε ενα μικρό κομμάτι τους να ρυθμιστεί από τις εθνικές νομοθεσίες των κρατών μελών.

Ο Ν. 4624/2019 αφορά: α) στην αντικατάσταση του νομοθετικού πλαισίου που ρυθμίζει τη συγκρότηση και λειτουργία της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, β) τη λήψη μέτρων εφαρμογής του ΓΚΠΔ και (γ) την ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων.

Ο νέος Νόμος περιλαμβάνει ενδιαφέρουσες διατάξεις, οι σημαντικότερες εκ των οποίων αφορούν:

α) τη **λήψη συγκατάθεσης ανηλίκου**, όπου ορίζει ότι «όταν εφαρμόζεται το άρθρο 6 παράγραφος 1 στοιχείο α) του ΓΚΠΔ, η επεξεργασία δεδομένων προσωπικού χαρακτήρα ανηλίκου, κατά την προσφορά υπηρεσιών της κοινωνίας των πληροφοριών απευθείας σε αυτόν, είναι σύννομη, εφόσον ο ανήλικος έχει συμπληρώσει το 15ο έτος της ηλικίας του και παρέχει τη συγκατάθεσή του». Στις περιπτώσεις που ο ανήλικος δεν έχει συμπληρώσει το 15ο έτος της ηλικίας του, η συγκατάθεση είναι νόμιμη αν έχει δοθεί από τον νόμιμο αντιπρόσωπό του.

β) Κατ' εφαρμογή της παραγράφου 4 του άρθρου 9 του ΓΚΠΔ απαγορεύεται **η επεξεργασία γενετικών δεδομένων** για σκοπούς ασφάλισης υγείας και ζωής.

γ) Την επεξεργασία δεδομένων **στο πλαίσιο των σχέσεων απασχόλησης** και το **δικαίωμα στην**

ελευθερία έκφρασης και πληροφόρησης.

δ) Τη ρύθμιση διαφόρων ζητημάτων που αφορούν την αρμόδια Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

ε) Την επεξεργασία δεδομένων προσωπικών χαρακτήρα από **δημόσιους φορείς**.

4.9.2 Ο Νόμος 2472/1997

Η προισχύουσα Οδηγία 95/46/ΕΚ ενσωματώθηκε στην ελληνική έννομη τάξη με τον Ν. 2472/1997 (ΦΕΚ Α-50/10-4-1997) που αφορά την «προστασία του Ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα», ο οποίος τροποποιήθηκε αργότερα με τον Ν. 3471/2006. Η Οδηγία 95/46/ΕΚ, όπως αναφέρθηκε ανωτέρω, καταργήθηκε με τον ΓΚΠΔ και ο Ν. 2472/1997 καταργήθηκε οριστικά με τον Ν. 4624/2019.

Αντικείμενο του Ν.2472/1997 ήταν η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα, ενώ ήταν αυτός που οδήγησε στη συγκρότηση της εθνικής Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και της έδωσε αυξημένες αρμοδιότητες και δικαιώματα.

Στο **άρθρο 8 του Ν.2472/1997** υπήρχε ειδική αναφορά στη «διασύνδεση αρχείων», στο οποίο προσδιοριζόταν:

α) Ο σκοπός 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 όρους και τις προϋποθέσεις για την αποτελεσματικότερη προστασία των δικαιωμάτων και ελευθεριών και ιδίως του δικαιώματος ιδιωτικής ζωής των υποκειμένων ή τρίτων.

Στον μεταγενέστερο Ν. 4624/2019 δεν υπάρχει κάποια αναφορά στη διασύνδεση των αρχείων, καθώς θεωρήθηκε ότι ο ΓΚΠΔ έχει καλύψει επαρκώς τα ζητήματα που αφορούσαν την προστασία της ιδιωτικότητας στα συστήματα του ΔτΠ.

4.9.3 Ο Νόμος 4070/2012

Η Οδηγία 2002/58/ΕC (“e-Privacy Οδηγία”) ενσωματώθηκε στην ελληνική έννομη τάξη με τον Ν. 3471/2006 (ΦΕΚ 133/Α/28-6-2006), ο οποίος αφορούσε την προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίησε τον

Ν. 2472/1997. Όπως αναφέρθηκε στο οικείο υποκεφάλαιο η Οδηγία 2002/58/ΕC τροποποιήθηκε με την Οδηγία 2009/136/ΕΚ και συνακόλουθα ο Ν. 3471/2006 τροποποιήθηκε με τον Ν. 4070/2012.

Ο Νόμος αυτός έχει πεδίο εφαρμογής την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τη διασφάλιση του απορρήτου των ηλεκτρονικών επικοινωνιών σε δημόσια δίκτυα. Ενσωματώνοντας την Οδηγία απαγορεύει την ακρόαση, την υποκλοπή, την αποθήκευση ή παρακολούθηση των επικοινωνιών από τρίτα πρόσωπα χωρίς τη συγκατάθεσή των χρηστών, όπως και την εγκατάσταση κατασκοπευτικών λογισμικών και κρυφών αναγνωριστικών στοιχείων. Σχετικά με τα δεδομένα κίνησης/θέσης, ορίζει ότι οι πάροχοι υπηρεσιών οφείλουν να τα διαγράφουν ή να τα ανωνυμοποιούν όταν δεν είναι πια απαραίτητα για τον σκοπό συλλογής τους. Ακόμη, οι πάροχοι υπηρεσιών και οι φορείς δικτύων ηλεκτρονικών επικοινωνιών οφείλουν να λαμβάνουν τα κατάλληλα τεχνικά και οργανωτικά μέτρα ασφαλείας και να προβαίνουν σε έγκαιρη και λεπτομερή ενημέρωση των συνδρομητών τους.

Ορίζει, ακόμα, ότι οι πάροχοι οφείλουν να τηρούν αυστηρά τις αρχές τις επεξεργασίας, όπως αναλύθηκαν σε προηγούμενο κεφάλαιο. Προβλέπει, μάλιστα, την αυστηρή τήρηση της αρχής της καθορισμένης διάρκειας διατήρησης των δεδομένων, ορίζοντας ως έκφρασης της την υποχρέωση του παρόχου να καταστρέψει ή να ανωνυμοποιεί τα υπό επεξεργασία δεδομένα κίνησης μόλις λήξει η επικοινωνία, με εξαίρεση όσα οφείλουν βάσει της εθνικής νομοθεσίας να τηρούν για διάστημα 12 μηνών και αφορούν δεδομένων κίνησης και θέσης φυσικών προσώπων και όλα τα συναφή δεδομένα για την αναγνώριση του κάθε συνδρομητή ή εγγεγραμμένου χρήστη.[119]

Επιπλέον, με το άρθρο 170 του Ν. 4070/2012, που αντικατέστησε την παρ.5 του άρθρου 4 του Ν.3471/2006 ρυθμίζεται η χρήση των αυτοεγκαθιστώμενων αρχείων cookies. Συγκεκριμένα, με το ανωτέρω άρθρο καταργήθηκε το σύστημα “opt-out”, με το οποίο ο χρήστης ο χρήστης μπορούσε να δηλώσει τη μη συγκατάθεση του για την τοποθέτηση των cookies στον τερματικό του μόνο εκ των υστέρων. Έτσι, υιοθετείται πια το σύστημα «opt-in, όπου η αποθήκευση και επεξεργασία πληροφοριών μέσω των cookies επιτρέπεται μόνο αφού ο χρήστης/συνδρομητής δώσει τη συγκατάθεση του και αφού πρώτα ενημερωθεί σύμφωνα με το άρθρο 13 του ΓΚΠΔ. Σύμφωνα με την ίδια διάταξη η συγκατάθεση μπορεί να δίδεται μέσω κατάλληλων ρυθμίσεων στο φυλλομετρητή ιστού ή της εκάστοτε εφαρμογής[120].

[119] βλ. Αλεξανδροπούλου-Αιγυπτιάδου (2016), ο.π. , σελ. 176 επ.
[120] βλ. Ιγγλεζάκης (2021), ο.π., σελ. σελ.383-384

Κεφάλαιο 5ο

5. Συμπεράσματα

Την τελευταία δεκαετία το Διαδίκτυο των πραγμάτων (ΔτΠ) είναι από τις βασικότερες τεχνολογίες που έχει κάνει μεγάλα βήματα προόδου και έχει αναπτύξει εφαρμογές σε πολλούς τομείς. Το ΔτΠ αποτελεί μια τεχνολογία που σχετίζεται με ποικίλα αντικείμενα της καθημερινότητας μας,όπως λ.χ. οικιακές συσκεύες, φορετές συσκεύες και βιομηχανικά και γεωργικά μηχανήματα, που μέσω της χρήσης ενσωματωμένων αισθητήρων πετυχαίνουν τη συλλογή και επεξεργασία δεδομένων προσφέροντας τις βέλτιστες δυνατές υπηρεσίες στους χρήστες τους. Οι συσκευές αυτές μέσω της διασύνδεσης τους με άλλες συσκευές καταφέρνουν ανταλλάσσοντας δεδομένα να εξάγουν σημαντικές πληροφορίες, διαδικασία που τους επιτρέπει να μεγιστοποιούν τις προσφερόμενες υπηρεσίες με τη μικρότερη δυνατή κατανάλωση πόρων. Με άλλα λόγια, το ΔτΠ είναι μια «έξυπνη» τεχνολογία του μέλλοντος που σκοπό έχει να κάνει την καθημερινότητα μας καλύτερη.

Τα οφέλη λειτουργίας των εφαρμογών της τεχνολογίας του ΔτΠ στην καθημερινή μας ζωή γίνονται ακόμα περισσότερα, όταν εκμεταλλεύεται τα οφέλη και των άλλων ταχέως αναπτυσόμενων τεχνολογιών, όπως είναι τα «Μεγάλα Δεδομένα», η τεχνολογία του «Υπολογιστικού νέφους» και η «Τεχνητή Νοημοσύνη».

Βέβαια, η ανάπτυξη του ΔτΠ εκτός από τα σημαντικά πλεονεκτήματα έφερε στην επιφάνεια και σοβαρά ζητήματα ιδιωτικότητας και προστασίας των προσωπικών δεδομένων των χρηστών των εφαρμογών τους. Ο τεράστιος όγκος δεδομένων που υφίστανται επεξεργασία από τον συνεχώς αυξανόμενο αριθμό διασυνδεδεμένων συσκευών αποτελεί μία από τις βασικότερες ανησυχίες ως προς την ασφάλεια των χρηστών και την προστασία των δεδομένων τους. Ανησυχίες που εντάθηκαν λόγω των ευπαθειών που παρουσιάζουν οι «έξυπνες» συσκευές, οι οποίες από πλευράς ασφάλειας μόνο «έξυπνες» δεν μπορούν να χαρακτηριστούν. Αυτό συμβαίνει, διότι, οι σχεδιαστές και οι κατασκευαστές των εφαρμογών αυτών, άλλοτε με σκοπό τη μείωση του κόστους και άλλοτε παρασυρμένοι από την ανάγκη δημιουργίας ενός αποδοτικότερου συστήματος/συσκευής, παραβλέπουν τα διεθνή πρότυπα ασφαλείας δημιουργώντας συσκευές και συστήματα με σοβαρές ευπάθειες.

Τις ευπάθειες αυτές είναι πάντα έτοιμοι να εκμεταλλευτούν διάφοροι κακόβουλοι χρήστες, ώστε να διεισδύσουν και να υποκλέψουν προσωπικές πληροφορίες των χρηστών. Τα ζητήματα

ιδιωτικότητας, όμως, δεν σχετίζονται μόνο με κακόβουλους χρήστες αλλά ακόμα και με τους φορείς παροχής υπηρεσιών του ΔτΠ, οι οποίοι ενδέχεται να επεξεργάζονται δεδομένα των χρηστών για σκοπούς διαφορετικούς από αυτούς της παροχής της υπηρεσίας και της βελτιστοποίησης της απόδοσης των συστημάτων και των συσκευών.

Την ανάγκη για λήψη αποτελεσματικότερων μέτρων ασφαλείας καταδεικνύουν τα περιστατικά παραβίασης δεδομένων, που έχουν αυξητική τάση τα τελευταία χρόνια, αλλά και η ποικιλομορφία των τρόπων τέλεσης τους από τους διάφορους κακόβουλους χρήστες. Το απόρρητο, λοιπόν, σχετίζεται άμεσα με την ασφάλεια και απαιτεί τη λήψη μέτρο σε επίπεδο εφαρμογής, δικτύου και συσκευών. Θα πρέπει να διασφαλίζεται το σύστημα του ΔτΠ από μη εξουσιοδοτημένη παρέμβαση στα δεδομένα του και το δίκτυο να έχει δομηθεί με τέτοιο τρόπο ώστε, ακόμη και αν επιτευχθεί η μη εξουσιοδοτημένη πρόσβαση στα δεδομένα, να μην είναι εύκολο να τεθούν υπό επεξεργασία και να εξαχθούν πληροφορίες που αφορούν τους χρήστες τους.

Γίνεται εύκολα κατανοητό ότι όσο πιο εκτεταμένη είναι η συλλογή, η επεξεργασία και ο διαμοιρασμός των προσωπικών δεδομένων από τις συσκευές του ΔτΠ, τόσο μεγαλύτερος και ο κίνδυνος για την ιδιωτικότητα και το απόρρητο των χρηστών τους. Τα δεδομένα υφίστανται επεξεργασία ακόμη και αν είναι σε μορφή που δεν μπορεί να αναγνωστεί από τους απλούς χρήστες, μπορούν σε συνδυασμό με άλλα δεδομένα να ταυτοποιήσουν το χρήστη και να σκιαγραφήσουν ένα προφίλ για αυτόν. Αυτό μπορεί να έχει ως επακόλουθο τη λήψη αυτοματοποιημένων αποφάσεων εις βάρος του χρήστη με γνώμονα το προφίλ που έχει σκιαγραφηθεί. Υπάρχει, επίσης, ο κίνδυνος για τους χρήστες να τελείται εν αγνοία τους επεξεργασία των δεδομένων τους σε τέτοιο βαθμό, ώστε οι πληροφορίες, που εξάγονται από την επεξεργασία αυτή, να χρησιμοποιηθούν για δευτερεύοντες σκοπούς πέρα του αρχικού σκοπού της συλλογής και επεξεργασίας τους χωρίς αυτοί να έχουν δώσει τη συγκατάθεσή τους. Βέβαια, ακόμα και στις περιπτώσεις που τα δεδομένα υφίστανται νόμιμη επεξεργασία για τους σκοπούς που συλλέχθησαν, θα πρέπει ο χρήστης να έχει ενημερωθεί πριν τη χρήση της υπηρεσίας για κάθε επικείμενη πράξη επεξεργασίας των δεδομένων του.

Προκύπτει, λοιπόν, η ανάγκη λήψης των κατάλληλων τεχνικών και οργανωτικών μέτρων εκ μέρους των σχεδιαστών, των κατασκευαστών και των φορέων παροχής των υπηρεσιών του ΔτΠ με σκοπό την εύρυθμη λειτουργία των συσκευών και γνώμονα την προστασία της ιδιωτικότητας και του απορρήτου των χρηστών.

Σύμφωνα με την ισχύουσα ελληνική αλλά και Ευρωπαϊκή νομοθεσία ορίζεται το νομικό πλαίσιο σωστής χρήσης και λειτουργίας των συσκευών αυτών για την προστασία των δεδομένων

προσωπικού χαρακτήρα. Βέβαια, αυτό δεν απαλλάσσει του χρήστες των εφαρμογών του ΔτΠ από την ανάγκη να είναι προσεκτικοί με τα δεδομένα που διαθέτουν για επεξεργασία και να γνωρίζουν πολύ καλά τα δικαιώματά τους ως υποκείμενα των προσωπικών δεδομένων. Συνεπώς, είναι επιτακτική η ανάγκη λήψης σημαντικών αποφάσεων που αφορούν την ασφάλεια της ιδιωτικότητας και του απορρήτου στα συστήματα του ΔτΠ, καθώς και συνεχή επικαιροποίηση των διεθνών προτύπων ασφαλείας. Την εποπτεία για την προστασία τους έχουν αναλάβει οι Ευρωπαϊκές Αρχές Προστασίας Δεδομένων, οι οποίες οφείλουν να ελέγχουν τους κατασκευαστές και τους φορείς των υπηρεσιών του ΔτΠ ως προς τη συμμόρφωση τους με την ισχύουσα νομοθεσία και δη με τον ΓΚΠΔ. Η εφαρμογή του ΓΚΠΔ, αν και καλύπτει επαρκώς την ασφάλεια των δεδομένων από την παράνομη επεξεργασία τους, απαιτεί συνεχή επαγρύπνηση, καθώς οι τεχνολογικές εξελίξεις ενδέχεται να είναι τόσο αλματώδεις που να καθιστά την εκάστοτε ισχύουσα νομοθεσία απαρχαιωμένη. Απαιτείται, δηλαδή, συνεχή αναθεώρηση και επικαιροποίηση της ισχύουσας εγχώριας και ευρωπαϊκής νομοθεσίας, ώστε να συμβαδίζει με τις τεχνολογικές εξελίξεις, ακόμα και να τις προλαβαίνει (όταν αυτό καθίσταται δυνατό).

Συμπερασματικά, το ΔτΠ δεν αναφέρεται απλώς στη διασύνδεση συσκευών, αλλά εν τοις πράγμασι είναι κάτι πολύ περισσότερο από αυτό. Η ποσότητα και η φύση των δεδομένων και η πολυπλοκότητα των συστημάτων του ΔτΠ, εκτός από βέλτιστες υπηρεσίες και αποδοτικότητα συστημάτων, εγείρει και σημαντικά ζητήματα προστασίας του δικαιώματος της ιδιωτικότητας και των απορρήτου των χρηστών ους. Οι προκλήσεις που δημιουργούνται στο πλαίσιο της ανάπτυξης των τεχνολογιών ΔτΠ είναι αδιαμφισβήτητα πολλές και σύνθετες, αλλά το ζητούμενο κάθε φορά είναι η τήρηση επικαιροποιημένων προτύπων ασφαλείας και η συμμόρφωση με την ισχύουσα νομοθεσία για την προστασία των δεδομένων, που διασφαλίζουν τον σεβασμό των δικαιωμάτων των υποκειμένων των δεδομένων χωρίς να εμποδίζουν την ανάπτυξη της τεχνολογίας του ΔτΠ.

ΒΙΒΛΙΟΓΡΑΦΙΑ - ΑΡΘΡΟΓΡΑΦΙΑ

Ελληνόγλωσση

- Αλεξανδροπούλου-Αιγυπτιάδου Ευγενία (2016), Προσωπικά Δεδομένα, Νομική Βιβλιοθήκη
- Ιγγλεζάκης Ιωάννης (2021), Δίκαιο Πληροφορικής, εκδόσεις Σάκκουλας, σελ.392 επ. (4η έκδοση)
- Κανέλλος Λεωνίδας (2020), The GDPR Handbook, Για DPOs, Επιχειρήσεις & Οργανισμούς, Νομική Βιβλιοθήκη
- Κόμνιος Γ.Κομνηνός (2018), Από κοινού υπεύθυνοι επεξεργασίας δεδομένων – Η περίπτωση του διαχειριστή σελίδας fan page στο Facebook, Δίκαιο Τεχνολογίας & Επικοινωνίας**,** σ.σ. 298 επ.
- Κόμνιος Γ. Κομνηνός (2021), Ζητήματα από την εφαρμογή το κανονισμού για την προστασία δεδομένων στη διεθνή διαιτησία, εκδόσεις Σάκκουλα, 1η έκδοση
- Κόμνιος Γ. Κομνηνός (2020), Η αξιολόγηση το Γενικού Κανονισμού για την Προστασία Δεδομένων. Διαδικασία- Γνώμες – Προτάσεις, Περιοδικό Αρμενόπουλος, σ.σ. 1129-1140 (Τεύχος 7)
- Κοτσαλής -Κ. Μενουδάκος (2018), Γενικος Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (GDPR) Νομική διάσταση και πρακτική εφαρμογή
- Μαυρίδης Ιωάννης(2015), Ασφάλεια Πληροφοριών στο Διαδίκτυο, Ελληνικά Ακαδημαϊκά Ηλεκτρονικά Συγγράμματα και Βοηθήματα
- Μήτρου Λίλιαν(2017), ο γενικός κανονισμός προστασίας προσωπικών δεδομένων, εκδόσεις Σάκκουλας
- Παναγιωτοπούλου Μαρία, Αναστασία Στρατηγέα, Γιώργος Σωμαρακάκης (2014, Ιούνιος), Εξυπνες πόλεις και βιώσιμη αστική ανάπτυξη – παραδείγματα από τη μεσογειακή και την ελληνική εμπειρία, conference paper : conference: Ελληνικό Τμήμα της Ευρωπαϊκής και Διεθνούς Εταιρείας Περιφερειακής Επιστήμης, 12ο Επιστημονικό Συνέδριο «Αστική και Περιφερειακή ανάπτυξη: σύγχρονες προκλήσεις» στην Αθήνα
- Παναγοπούλου-Κουτνατζή Φ.(2014), Διαδίκτυο των πραγμάτων (Internet of Things-IoT): Αποικισμός της καθημερινής ζωής ή νέα τεχνολογική πρόκληση;, ΔιΜΕΕ 3/2014- έτος 11ο,σ.σ. 343-358
- Σωτηρόπουλος Βασίλης Α(2017), Υπεύθυνος Προστασίας Δεδομένων,εκδόσεις Σάκκουλας

• Charles P.A., Shari Lawrence Pfleeger και Jonathan Margulies (2018), Ασφάλεια Πληροφοριακών Συστημάτων, Εκδόσεις Τζιόλα, Έκδοση 5η

Ξενόγλωσση

• Aman Ullah (2018), IoT: Applications of RFID and Issues, International Journal of Internet of Things and Web Services,Volume 3, σελ 1-2

• Ashton Kevin (2009, Ιούνιος), In the real world, things matter more than ideas, *RFID Journal*, διαθέσιμο στον διαδικτυακό σύνδεσμο: https://www.rfidjournal.com/articles/view?4986

• Bizer C., Cyganiak R.(2007), *How to publish Linked Data on the Web*, *T. Heath*, Workshop at the 17th International World Wide Web Conference Beijing, China, April 22, 2008

• Boo, Y.L., Stirling, D., Chi, L., Liu, L., Ong, K.-L. & Williams, G. (2018), Data Mining, *Springer, Volume 845,* 15th Australasian Conference, AusDM 2017, Melbourne, VIC, Australia, August 19-20

• Brij B. Gupta, Gregorio Martinez Perez, Dharma P. Agrawal & Deepak Gupta (2020), Handbook of computer networks and cyber security, (chapter 21). Στο Christos Stergiou, Andreas P. Plageras, Konstantinos E. Psannis & Brij B. Gupta, *Secure Machine Learning scenario from Big Data in Cloud Computing via Internet of Things network* (σ.σ. 525-554)

• Chen M., & Chen S (2016), RFID Technologies for Internet of Things, Switzerland: Springer International Publishing AG, σελ. 11-13

• Dr. Ovidiu Vermesan & Dr. Peter Friess (2013), Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, Rivers Publishers Series in Communication

• Dr Lachlan Urquhart και Dr Lachlan Urq*uhart, Avoiding the Internet of Insecure Industrial Things,* Computer Law and Security Review, σ.σ. 450-466 (Volume 34, Issue 3)

• ENISA (2016, Νοέμβριος), *Smart Hospitals-Security and Resilience for Smart Health Service and Infrastructures*, European Union Agency For Network And Information Security, σελ.9, στο: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals/at_download/fullReport

• Evans Dave (2011, Απρίλιος), The Internet of Things: How the Next Evolution of the Internet Is Changing Everything, *Cisco Internet Business Solutions Group,*σελ. 2-4, διαθέσιμο στον διαδικτυακό

σύνδεσμο*:*
https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

- Fabiano Nicola (2017, Ιούλιος), *Internet of Things and the Legal Issues related to the Data Protection Law according to the new European Genaral Data Protection Regulation*, Athens Journal of Law, σ.σ. 201-214 (Volume 3, Issue 3)

- Gubbi J., Buyya R., Marusi S, Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions, Technical Report CLOUDS-TR-2012-2 (2012), Palaniswamia M.The University of Melbourne, διαθέσιμο στον διαδικτυακό σύνδεσμο: https://arxiv.org/ftp/arxiv/papers/1207/1207.0203.pdf

- Huawei and IDC (2017,27 Ιουλίου), *Huawei Smart City White Paper*

- *Internet of Things: Wireless Sensor Networks* (2014, 26 Νοεμβρίου), International Electrotechnical Commission, White Paper, σελ. 39-40, διαθέσιμο στο: https://www.ipwea.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=e0619c58-f639-080a-86c2-055ae9c8af4d

- International Telecomunication Union - Internet Reports 2005: The Internet of Things, 2005, 7η Έκδοση, διαθέσιμο στον διαδικτυακό σύνδεσμο: http://handle.itu.int/11.1002/pub/800eae6f-en

- Jatinder Singh Christopher Millard, Chris Reed, Jennifer Cobbe & Jon Crowcroft (2018), *Accountability in the Internet of Things (IoT): Systems, law & ways forward* (vol.51)

- Kitchin Rob (2016, Ιανουάριος), *Getting smarter about smart cities: Improving data privacy and data security*, Data Protection Unit, Department of Taoiseach, Dublin Ireland

- Macaulay Tyson & Morgan Kaufmann (2016), RIoT Control-Understanding and Managing Risks and the Internet of Things (Chapter 8). Στο Macaulay Tyson, *Availability and Reliability Requierements in the IoT*, σ.σ. 141-155, σελ 141 επ. (1st Edition)

- Metallidou Chrysi, Konstantinos E. Psannis & Eugenia Alexandropoulou-Egyptiadou (2020), *An Efficient IoT System Respecting the GDPR,* The *3rd World Symposium on Communication Engineering*

- Mohammad Abdur Razzaque, Marija Milojevic Andrei Palade, Siobhán Clarke (2015) *Middleware for Internet of Things: A Survey,IEEE Internet of Things Journal,*σ.σ. 70-95

- National Institute of Standards and Technology-NIST (2013), Foundations for Innovation in Cyber-Physical Systems, Workshop report

• Oreku, G., & Pazynyuk, T (2016), Security in Wireless Sensor Networks, Springer International Publishing

• Ouhbi Sofia, José Luis Fernández-Alemán, Juan Manuel Carrillo-de-Gea, Ambrosio Toval & Ali Idri (2017), E-health internationalization requirements for audit purposes, *Journal Elsevier North-Holland,* Inc. New York, NY, USA Computer Methods and Programs in Biomedicine archive, σ.σ. 49-60

• Psannis Konstantinos, Stergiou Christos (2016, Ιούνιος), Recent advances delivered by mobile cloud computing and Internet of Things for Big data applications: A Survey, Special Issue: Management of the Internet of things and big data, *International Journal of Network Management,* (Volume 27, Issue 3)

• Qin Y., Sheng Q.Z., Edward Curry (2015), Matching Over Linked Data Streams in the Internet of Things, *IEEE Internet Computing*

• Romkey John (2016), Toast of the IoT: The 1990 Interop Internet Toaste, *IEEE Consumer Eletronics Magazine* , σ.σ. 116-119

• Sakr S, Wylot M., Mutharaju, R.,Le Phuoc, D.,Fundulaki, I (2018), Linked Data, *Springer International Publishing*

• Shah J. Miah, Jahidul Hasan, John G. Gammack (2017) On-Cloud Healthcare Clinic: An e-health consultancy approach for remote communities in a developing country, *Telematics and Informatics*, σ.σ. 311-322 (volume 34, issue 1)

• Shivanjali Khare and Michael Totaro(2019, Ιούλιος), Big Data in IoT, *IEEE Internet of Things Journal*, Conference Paper- 10th ICCCNT 2019

• Teciher Jordan (2018), The little-known story of the first IoT device, IBM, διαθέσιμο στον διαδικτυακό σύνδεσμο: https://www.ibm.com/blogs/industries/little-known-story-first-iot-device

• Torppeta D. (2010), *The Smart City Vision: How Innovation and ICT Can Build Smart, Livable, Sustainable Cities,* Think! The Innovation Knowledge Foundation, Report 5/2010

• Wachter Sandra (2018, 28 Σεπτεμβρίου), *The GDPR and the IoT:a three-step transparecy model, Law, Innovation and Technology*, Taylor and Francis Group

• Weber Rolf H. και Studer Evelyne (2016), Cybersecurity in the Internet of Things: Legal aspects, *Elsevier, Computer law & Security*, σ.σ. 715-728 (volume 32, issue 5)

• Xi Lin Jun Wu, Haoran Liang & Wu Yang Jianhua Li (2019, Μάϊος), Making Knowledge Tradable in Edge-AI Enabled IOT: A Consortium Blockchain-based Efficient and Incentive Approach, *IEEE Internet of Things Journal*, Student Member

• Yinong Chen *(2020, Ιούλιος),* IoT, cloud, big data and AI in interdisciplinary domains, *Simulation Modeling Practice and Theory (*Article 102070)

• Zhang M., Yu T., Zhai G.F. (2011), Smart Transport System Based on -The Internet of Things, σελ. 1073–1076

• Ziegler Sebastien (2019), Internet of Things Security and Data Protection, Springer International Publishing

Νομοθεσία-Γνώμες/Κατευθυντήριες Γραμμές

• Γνωμοδότηση 2018/C 440/02 της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής(2018). Ανάκτηση στις 22 Ιανουαρίου 2022 από την επίσημη ιστοσελίδα της Ευρωπαϊκής Επιτροπής.

• Κατευθυντήριες γραμμές 5/2020 σχετικά με τη συγκατάθεση βάσει του κανονισμού 2016/679», Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2020, 4 Μαΐου), έκδοση 1.1. . Ανάκτηση από την επίσημη ιστοσελίδα της Ευρωπαϊκής Επιτροπής στις 20 Ιανουαρίου 2022

• Κατευθυντήριες γραμμές της Ομάδας του Άρθρου 29 για την αυτοματοποιημένη λήψη αποφάσεων και την κατάρτιση προφίλ για τους σκοπούς του Κανονισμού 2016/679 (2018,6 Φεβρουαρίου), Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, έκδοση 1.1., σελ. 14-15. Ανάκτηση στις 20 Ιανουαρίου 2022 από την επίσημη ιστοσελίδα της Ευρωπαϊκής Επιτροπής

• Κατευθυντήριες γραμμές της Ομάδας του Άρθρου 29 σχετικά με τη συγκατάθεση βάσει του Κανονισμού 2016/679 (2017, 28 Νοεμβρίου) , όπως τελικώς αναθεωρήθηκαν και εκδόθηκαν στις 10 Απριλίου 2018. Ανάκτηση στις 20 Ιανουαρίου 2022 από την επίσημη ιστοσελίδας της Ευρωπαϊκής Επιτροπής

Ιστοσελίδες-Ηλεκτρονική Αρθρογραφία

• *Έκθεση του Οργανισμού Ηνωμένων Εθνών για τις πόλεις Παγκοσμίως κατά το έτος 2018* (2019).Ανάκτηση από un.org 30 Φεβρουαρίου 2021,στον διαδικτυακό σύνδεσμο:https://www.un.org/en/events/citiesday/assets/pdf/the_worlds_cities_in_2018_data_booklet.pdf

• *Εκμετάλλευση των δυνατοτήτων του υπολογιστικού νέφους (Cloud Computing) στην Ευρώπη – τι είναι και τι σημαίνει αυτό για μένα;* (2012, 27 Σεπτεμβρίου). Ανάκτησησ τις 21 Φεβρουαρίου 2021 από την επίσημη ιστοσελίδα της Ευρωπαϊκής Επιτροπής:https://ec.europa.eu/commission/presscorner/detail/el/MEMO_12_713

• *Εξόρυξη Δεδομένων*. Ανάκτηση σπό el.wikipedia.org στις 25 Φεβρουαρίου 2021, στο:https://el.wikipedia.org/wiki/%CE%95%CE%BE%CF%8C%CF%81%CF%85%CE%BE%CE%B7_%CE%B4%CE%B5%CE%B4%CE%BF%CE%BC%CE%AD%CE%BD%CF%89%CE%BD

• *Πρόστιμο 5 δισ. δολάρια στο Facebook για το σκάνδαλο της Cambridge Analytica* (2019, 13 Ιουλίου). *Ανάκτηση από tovima.gr στις 20 Απριλίου 2021, στον διαδικτυακό σύνδεσμο:* https://www.tovima.gr/2019/07/13/science/prostimo-5-dis-dolaria-sto-facebook-gia-to-skandalo-tis-cambridge-analytica/

• *Σημασιολογικός Ιστός*. Ανάκτηση από el.wikipedia.org στις 25 Φεβρουαρίου 2021, στον διαδικτυακό σύνδεσμο: https://el.wikipedia.org/wiki/%CE%A3%CE%B7%CE%BC%CE%B1%CF%83%CE%B9%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CE%BA%CF%8C%CF%82_%CE%99%CF%83%CF%84%CF%8C%CF%82

• *Τι είναι η τεχνητή νοημοσύνη και πώς χρησιμοποιείται;* (2020, 9 Σεπτεμβρίου).Ανάκτηση στις 30 Φεβρουαρίου 2021 από την επίσημη ιστοσελίδα της Ευρωπαϊκής Επιτροπής:https://www.europarl.europa.eu/news/el/headlines/society/20200827STO85804/ti-einai-i-techniti-noimosuni-kai-pos-chrisimopoieitai

• Alison DeNisco Rayome (2020, 5 Φεβρουαρίου), *Beware Windows 7 users: Malware campaign targeting IoT devices.* Ανάκτηση από cnet.com στις 23 Απριλίου 2021,στον διαδικτυακό σύνδεσμο: https://www.cnet.com/news/beware-windows-7-users-malware-campaign-targeting-iot-devices/

• Andrews Evan (2013,18 Δεκεμβρίου), *Who invented Internet*?, Ανάκτηση από history.com στις 16 Φεβρουαρίου 2021, στον διαδικτυακό σύνδεσμο: https://www.history.com/news/who-invented-the-internet

• Catalin Cimpanu (2019, 20 Οκτωβρίου), *Alexa and Google Home devices leveraged to phish and eavesdrop on users, again.* Ανάκτηση από zdnet.com στις 23 Απριλίου 2021,στον διαδικτυακό σύνδεσμο: https://www.zdnet.com/article/alexa-and-google-home-devices-leveraged-to-phish-and-eavesdrop-on-users-again/

• Catalin Cimpanu (2020, 2 Φεβρουαρίου), *Hackers are hijacking smart building access systems to launch DDoS attacks.* Ανάκτηση από zdnet.com στις 23 Απριλίου 2021,στον διαδικτυακό σύνδεσμο: https://www.zdnet.com/article/hackers-are-hijacking-smart-building-access-systems-to-launch-ddos-attacks/

• Chenda Ngak (2013, 13 Αυγούστου), *Baby monitor hacked, spies on Texas child.* Ανάκτηση από cbsnews.com στις 21 Απριλίου 2021, στον διαδικτυακό σύνδεσμο: https://www.cbsnews.com/news/baby-monitor-hacked-spies-on-texas-child/

• Day Matthew (2019, 19 Φεβρουαρίου), *Your Smart Light Can Tell Amazon and Google When You Go to Bed.* Ανάκτηση από bloombergquint.com στις 15 Απριλίου 2021,στο :https://www.bloombergquint.com/pursuits/your-smart-light-can-tell-amazon-and-google-when-you-go-to-bed

• Darlene Storm (2015, 2 Φεβρουαρίου), *Hacker hijacks wireless Foscam baby monitor, talks and freaks out nanny.* Ανάκτηση από computerworld.com στις 20 Απριλίου 2021,στον διαδικτυακό σύνδεσμο: https://www.computerworld.com/article/2878741/hacker-hijacks-wireless-foscam-baby-monitor-talks-and-freaks-out-nanny.html

• Fergal Gallagher (2015, 09 Ιουνίου), *Hackers Could Remotely Send Fatal Doses To Patients Via Flawed Hospital Pumps.* Ανάκτηση από techtimes.com στις 20 Απριλίου 2021, στο: https://www.techtimes.com/articles/59180/20150609/hackers-remotely-send-fatal-doses-patients-via-flawed-hospital-pumps.htm

• *Final Version of NIST Cloud Computing Definition Published* (2011, 25 Οκτωβρίου). Ανάκτηση από nist.gov.com στις 20 Φεβρουαρίου 2021, στον διαδικτυακό τόπο: https://www.nist.gov/news-events/news/2011/10/final-version-nist-cloud-computing-definition-published

• *Information asymmetry* (2022). Ανάκτηση από en.wikipedia.org στις 20 Ιανουαρίου 2022, στον διαδικτυακό σύνδεσμο: https://en.wikipedia.org/wiki/Information_asymmetry

• *Internet of Things: Ιδιωτικότητα και ασφάλεια καταναλωτών και επιχειρήσεων στο Διαδίκτυο των πραγμάτων* (2018, 01 Νοεμβρίου). Ανάκτηση από lawspot.gr στις 22 Ιανουαρίου 2022, στον διαδικτυακό σύνδεσμο*:* https://www.lawspot.gr/nomika-nea/internet-things-idiotikotita-kai-asfaleia-katanaloton-kai-epiheiriseon-sto-diadiktyo-ton

• Ipsos Mori (2019, 1 Μαΐου), *The Trust Opportunity: Exploring Consumer Attitudes to the Internet of Things.* Ανάκτηση από internetsociety.org στις 23 Απριλίου 2021, στον διαδικτυακό σύνδεσμο: https://www.internetsociety.org/resources/doc/2019/trust-opportunity-exploring-consumer-attitudes-to-iot/

• O'Donnell Lindsey (2020, 27 Φεβρουαρίου), *IoT Insecurity: When Your Vacuum Turns on You.* Ανάκτηση από threatpost.com στις 23 Απριλίου 2021,στον διαδικτυακό σύνδεσμο: https://threatpost.com/vacuum-cleaners-baby-monitors-and-other-vulnerable-iot-devices/153294

• *Raw* Data (23 Ιανουαρίου 2022,. Ανάκτηση από en.wikipedia.org στις 25 Ιανουαρίου 2022, στο διαδικτυακό σύνδεσμο: https://en.wikipedia.org/wiki/Raw_data

• Roman Golubov (2020, 24 Μαρτίου), *There Are No Winter Breaks on the Darknet: Our Top 10 IoT Cyber Stories of Q1 2020.* Ανάκτηση από firedome.io στις 23 Απριλίου 2021,στον διαδικτυακό σύνδεσμο: https://firedome.io/blog/top-10-iot-cyber-stories-of-q1-2020/

• *The first electric telegraph in 1837 revolutionised communications* (2016,2 Φεβρουαρίου). Ανάκτηση από Telegram.co.uk στις 15 Φεβρουαρίου 2021 στο: https://www.telegraph.co.uk/technology/connecting-britain/first-electric-telegraph

• *The 15 biggest data breaches of the 21st century* (2021, 16 Ιουλίου). Ανάκτηση από csoonline.com στις 20 Απριλίου 2021,στον διαδικτυακό σύνδεσμο: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

• *US parents warned on hacked baby webcams* (2016, 28 Ιανουαρίου). Ανάκτηση από bbc.com στις 21 Απριλίου 2021,στον διαδικτυακό σύνδεσμο: https://www.bbc.com/news/technology-35427586

• *Yahoo triples likely scoope of 2013 hack to 3 billion users* (2017, 03 Μαρτίου). Ανάκτηση από bloomberg.com στις 20 Απριλίου 2021,στον διαδικτυακό σύνδεσμο: https://www.bloomberg.com/news/articles/2017-10-03/yahoo-says-all-3-billion-users-probably-affected-by-2013-breach

• Wakefield Jane (2018, 14 Απριλίου), *TED 2018: The smart home that spied on its owner.* Ανάκτηση από bbc.comστις 21 Απριλίου 2021, στον διαδικτυακό σύνδεσμο: https://www.bbc.com/news/technology-43747421