ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ

ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ

ΤΜΗΜΑ ΝΟΜΙΚΗΣ

ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ (Δ.Π.Μ.Σ)

«ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ»

ΜΕΛΕΤΗ ΥΠΗΡΕΣΙΩΝ ΚΑΙ ΖΗΤΗΜΑΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΕ ΠΕΡΙΒΑΛΛΟΝ ΕΞΥΠΝΗΣ ΠΑΝΕΠΙΣΤΗΜΙΟΥΠΟΛΗΣ (SMART CAMPUS)

Διπλωματική Εργασία

της

Γεωργιάδου Ευφροσύνης

Επιβλέπων Καθηγητής: κ. Παπαδημητρίου Παναγιώτης,

Αναπληρωτής Καθηγητής του Τμήματος Εφαρμοσμένης Πληροφορικής του Πανεπιστημίου Μακεδονίας

Θεσσαλονίκη, Φεβρουάριος 2024

ΜΕΛΕΤΗ ΥΠΗΡΕΣΙΩΝ ΚΑΙ ΖΗΤΗΜΑΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΕ ΠΕΡΙΒΑΛΛΟΝ ΕΞΥΠΝΗΣ ΠΑΝΕΠΙΣΤΗΜΙΟΥΠΟΛΗΣ (SMART CAMPUS)

Γεωργιάδου Ευφροσύνη

Πτυχίο Νομικής, Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης,2020

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ

ΣΤΟ Δ.Π.Μ.Σ «ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ»

Επιβλέπων Καθηγητής: κ. Παπαδημητρίου Παναγιώτης,

Αναπληρωτής Καθηγητής του Τμήματος Εφαρμοσμένης Πληροφορικής του Πανεπιστημίου Μακεδονίας

Εγκρίθηκε από την Τριμελή Εξεταστική Επιτροπή στις ……/2024

Παναγιώτης Παπαδημητρίου Ευγενία Αλεξανδροπούλου Κωνσταντίνος Ψάννης

…… …… ……

Γεωργιάδου Ευφροσύνη

ΠΕΡΙΛΗΨΗ

Με την παρούσα διπλωματική εργασία επιχειρείται η ανάδειξη της έννοιας της έξυπνης πανεπιστημιούπολης (smart campus) και των ζητημάτων που ανακύπτουν στο πλαίσιο αυτής τόσο από τεχνολογική σκοπιά όσο και από τη σκοπιά του δίκαιου προστασίας των προσωπικών δεδομένων. Στόχος της είναι η διερεύνηση του κατά πόσο η τεχνολογική ανάπτυξη της έξυπνης πανεπιστημιούπολης μπορεί να εναρμονιστεί με το ισχύον κανονιστικό πλαίσιο για την προστασία δεδομένων προσωπικού χαρακτήρα. Στο πρώτο μέρος αυτής (κεφάλαια 1-4), γίνεται εκτενής αναφορά στην τεχνολογική υποδομή και τις επιμέρους υπηρεσίες που παρέχονται στο πλαίσιο της έξυπνης πανεπιστημιούπολης. Στο δεύτερο μέρος (κεφάλαιο 5), παρουσιάζονται οι κίνδυνοι και οι προκλήσεις αναφορικά με τη προστασία των δεδομένων προσωπικού χαρακτήρα των συναλλασσόμενων με την έξυπνη πανεπιστημιούπολη προσώπων. Εν κατακλείδι, παρατίθενται τα προβλεπόμενα από το ισχύον κανονιστικό πλαίσιο μέτρα προστασίας των προσωπικών δεδομένων πηγάζοντα από τις υποχρεώσεις του υπευθύνου επεξεργασίας καθώς και τα συμπεράσματα της παρούσας εργασίας (κεφάλαια 6-7).

Λέξεις κλειδιά: Έξυπνη πανεπιστημιούπολη (Smart Campus), Τεχνολογίες αιχμής, Διαδίκτυο των Πραγμάτων, Προσωπικά Δεδομένα, Ιδιωτικότητα.

ABSTRACT

This Diploma Thesis aims to elucidate the concept of the smart campus as well as the issues that arise within this framework, both from a technological perspective and within the framework of personal data protection law. The objective is to investigate the extent to which the technological advancement of the smart campus can align with the current regulatory framework for the protection of personal data. In the first part (Chapters 1-4), there is an in-depth examination of the technological infrastructure and the individual services provided within the context of the smart campus. The second part (Chapter 5) addresses the risks and challenges related to the protection of personal data for individuals interacting with the smart campus. In conclusion, the anticipated measures for personal data protection arising from data controllers' requirements within the existing regulatory framework are outlined, accompanied by the conclusions drawn from this diploma thesis (Chapters 6-7).

Keywords: Smart Campus, Cutting-edge Technologies, Internet of Things, Personal Data, Privacy

ΕΥΧΑΡΙΣΤΙΕΣ

Στο «ταξίδι» της συγγραφής της παρούσας διπλωματικής εργασίας μου, η οποία αποτελεί και το επισφράγισμα των σπουδών μου στο πλαίσιο του μεταπτυχιακού προγράμματος «ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ», συνοιδοπόροι μου υπήρξαν πολλοί συμβάλλοντας ο καθένας με τον δικό του τρόπο.

Πρώτα από όλα θα ήθελα να ευχαριστήσω από καρδιάς τον επιβλέποντα Καθηγητή μου, κ. Παπαδημητρίου Παναγιώτη, ο οποίος από την πρώτη στιγμή της συνεργασίας μας ήταν ιδιαίτερα υποστηρικτικός, βοηθητικός, καθοδηγητικός και πρόθυμος να απαντήσει άμεσα κάθε ερώτηση και απορία που είχα.

Θα ήθελα επίσης να ευχαριστήσω τους συνεργάτες και συναδέλφους μου που με βοήθησαν μέσα από τις συζητήσεις μας και τα εποικοδομητικά τους σχόλια να αντιληφθώ καλύτερα ορισμένες συγκεχυμένες στο μυαλό μου έννοιες.

Τέλος, ένα ιδιαίτερο ευχαριστώ για τη στήριξη, κατανόηση, συμπαράσταση και εμψύχωση καθ’ όλη τη διάρκεια των μεταπτυχιακών μου σπουδών οφείλω στην οικογένεια μου, τους φίλους μου και ιδιαίτερα στον Αποστόλη.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΚΕΦΑΛΑΙΟ 1

1. ΕΙΣΑΓΩΓΗ

1.1 Συνεισφορά

Η ραγδαία εξέλιξη των νέων τεχνολογιών φέρνει κατά καιρούς στο προσκήνιο έννοιες και ιδέες που φιλοδοξούν να επιτύχουν τον εκσυγχρονισμό και τη βελτίωση των διαφόρων τομέων της καθημερινότητας μας. Μία από αυτές τις έννοιες που θα μας απασχολήσει στη παρούσα διπλωματική εργασία είναι αυτή της έξυπνης πανεπιστημιούπολης, η οποία έχει προκαλέσει έντονα το ενδιαφέρον των ερευνητών καθώς επιχειρεί να ανατρέψει ριζικά τα παραδοσιακά πρότυπα των εκπαιδευτικών ιδρυμάτων. Μια έξυπνη πανεπιστημιούπολη ενσωματώνει τεχνολογίες αιχμής για τη δημιουργία ενός διασυνδεδεμένου, ευφυούς και δυναμικού περιβάλλοντος που στοχεύει στη βελτιστοποίηση της αποδοτικότητας, της βιωσιμότητας και της καινοτομίας σε διάφορες πτυχές των ακαδημαϊκών, διοικητικών και οργανωτικών λειτουργιών της. Η ενσωμάτωση αυτών των νέων τεχνολογιών όχι μόνο εκσυγχρονίζει τη φυσική δομή των πανεπιστημιουπόλεων, αλλά και καλλιεργεί ένα περιβάλλον όπου η καινοτομία και η συνδεσιμότητα βρίσκονται στο επίκεντρο της εκπαιδευτικής εμπειρίας.

Συνιστώντας μία μικρογραφία της έξυπνης πόλης, η έξυπνη πανεπιστημιούπολη είναι πολυδιάστατη με αποτέλεσμα να παρέχεται μία πληθώρα υπηρεσιών ανά πυλώνα της. Η ασφάλεια αποτελεί πρωταρχικό πυλώνα, για αυτό και επιλέγεται η ένταξη εξελιγμένων συστημάτων παρακολούθησης και ελέγχου στο εσωτερικό της πανεπιστημιούπολης. Στον τομέα της εκπαίδευσης, έξυπνες αίθουσες διδασκαλίας με διαδραστικές οθόνες και εργαλεία συνεργασίας ενισχύουν την βιωματική μάθηση. Η χρήση της Επαυξημένης Πραγματικότητας και της Εικονικής Πραγματικότητας προσφέρει στους φοιτητές πλούσιες εκπαιδευτικές εμπειρίες.

Εκτός από την εκπαίδευση, η διαχείριση των διαθέσιμων πόρων αποτελεί επίσης ζωτικής σημασίας πυλώνα. Η χρήση συστημάτων και συσκευών που αξιοποιούν τη Τεχνολογία του Διαδικτύου των Πραγμάτων επιτρέπει σε πραγματικό χρόνο τη παρακολούθηση και επίβλεψη των πόρων, συμβάλλοντας έτσι στην αποδοτική χρήση τους, στη διαχείριση της ενέργειας καθώς και στη μείωση του περιβαλλοντικού αποτυπώματος.

Επιπρόσθετα, σύγχρονα εργαλεία ανάλυσης μπορούν να αποβούν χρήσιμα για τη πρόβλεψη και επεξήγηση συμπεριφορών και επιδόσεων των φοιτητών,

επιτρέποντας την εξατομίκευση της υποστήριξης και την υλοποίηση στρατηγικών βασισμένων σε δεδομένα για τη βελτίωση του πανεπιστημιακού ιδρύματος.

Στο πλαίσιο όμως των ως άνω διαδικασιών, πληθώρα δεδομένων και δη προσωπικών, συλλέγονται, διακινούνται και τίθενται υπό επεξεργασία συνεχώς με αποτέλεσμα η υλοποίηση της έξυπνης πανεπιστημιούπολης να μην είναι μία διαδικασία άμοιρη νομικών συνεπειών αλλά αντιθέτως να γεννά προβληματισμούς σχετικά με το κατά πόσο και σε ποιο βαθμό μπορεί η τεχνολογική υποδομή της να συμβαδίζει με τις νομοθετικές και κανονιστικές επιταγές της πολιτείας στον τομέα του δικαίου προστασίας προσωπικών δεδομένων.

Σκοπός της παρούσας είναι να αναδείξει τόσο τις τεχνολογικές εξελίξεις όσο και τις νομικές προεκτάσεις του ζητήματος της υλοποίησης μίας πολυδιάστατης και ολοκληρωμένης έξυπνης πανεπιστημιούπολης και εν συνεχεία να διερευνηθεί εάν υπάρχει τεχνολογική και νομική σύγκλιση που επιτρέπει η έννοια της έξυπνης πανεπιστημιούπολης να μετουσιωθεί από βιβλιογραφικό ιδεώδες σε πραγματικό δημιούργημα.

1.2 Διάρθρωση Μελέτης

Στο δεύτερο κεφάλαιο επιχειρείται η πληρέστερη παρουσίαση της έννοιας της έξυπνης πανεπιστημιούπολης και των χαρακτηριστικών αυτής μέσω ανάδειξης και των επιμέρους σταδίων εξέλιξης της. Στο τρίτο κεφάλαιο, επιχειρείται η ανάδειξη της τεχνολογικής υποδομής αυτής με αναφορές σε επιμέρους τεχνολογίες που τυγχάνουν εφαρμογής στα πλαίσια αυτής ενώ στο τέταρτο κεφάλαιο παρουσιάζονται οι επιμέρους υπηρεσίες που παρέχονται ανά πυλώνα και τομέα δράσης, όπως αυτές έχουν προταθεί από έγκριτους επιστήμονες ανά τον κόσμο. Σημειώνεται πως από το σύνολο των προαναφερόμενων έξυπνων υπηρεσιών και εφαρμογών που μελετήθηκαν κατά τη διάρκεια της έρευνας πάνω στο επίμαχο ζήτημα, επιλέχθηκαν εκείνες που ήταν πιο πρόσφατες και παρουσίαζαν ιδιαίτερο ενδιαφέρον.

Στο πέμπτο κεφάλαιο αναδεικνύονται τα κυριότερα ζητήματα που απειλούν την ιδιωτικότητα και την προστασία των δεδομένων προσωπικού χαρακτήρα των συναλλασσόμενων με την έξυπνη πανεπιστημιούπολη προσώπων με ιδιαίτερη έμφαση στα ζητήματα που ανακύπτουν ως προς την προστασία των προσωπικών δεδομένων από την εκτεταμένη χρήση των νέων τεχνολογιών στο πλαίσιο της έξυπνης πανεπιστημιούπολης ενώ στο έκτο κεφάλαιο γίνεται αναφορά στις

υποχρεώσεις που φέρει η έξυπνη πανεπιστημιούπολη ως υπεύθυνος επεξεργασίας προκειμένου να διασφαλίσει την ακεραιότητα των προσωπικών δεδομένων.

Στο έβδομο κεφάλαιο παρουσιάζονται τα συμπεράσματα της εν λόγω εργασίας και στο όγδοο κεφάλαιο εκτίθενται οι βιβλιογραφικές αναφορές επί των οποίων βασίστηκε η παρούσα.

ΚΕΦΑΛΑΙΟ 2 – ΕΙΣΑΓΩΓΙΚΕΣ ΕΝΝΟΙΕΣ ΚΑΙ ΠΑΡΑΤΗΡΗΣΕΙΣ

2.1 Έννοια έξυπνης πόλης και έξυπνης πανεπιστημιούπολης

Με την ραγδαία εξέλιξη της τεχνολογίας και την ταυτόχρονη ανάπτυξη του παγκόσμιου πληθυσμού ο οποίος υπολογίζεται ότι θα αυξηθεί κατά 66% το έτος 2050 [1], παρατηρείται σε παγκόσμιο επίπεδο ένας σταδιακός μετασχηματισμός των παραδοσιακών πόλεων σε «έξυπνες» πόλεις.

Αν και ο όρος «έξυπνη πόλη» χρησιμοποιείται πάνω από 20 περίπου χρόνια στη βιβλιογραφία [2], μόλις τα τελευταία χρόνια έχει απασχολήσει εννοιολογικά το ενδιαφέρον των ερευνητών. Ειδικότερα, οι Gil-Garcia, Pardo και Nam [3] διεξήγαγαν μια εκτενή ανασκόπηση των διαθέσιμων ορισμών της έξυπνης πόλης και εντόπισαν τα ακόλουθα κοινά χαρακτηριστικά μεταξύ πολλών από αυτούς: (α) τεχνολογία· (β) υποδομές ζωτικής σημασίας· (γ) καλύτερες υπηρεσίες για τον πληθυσμό· (δ) ενοποίηση συστημάτων και υποδομών· και, (ε) όραμα για ένα καλύτερο μέλλον. Οι πιο πρόσφατες ερμηνείες μιας «έξυπνης πόλης» δίνουν επίσης μεγάλη έμφαση στις ανάγκες των ανθρώπων και της κοινότητας, καθώς και στη βιώσιμη ανάπτυξη. [4] Αναμφίβολα πάντως το χαρακτηριστικό γνώρισμα των «έξυπνων πόλεων» είναι η ευρεία εφαρμογή Τεχνολογιών Πληροφορικής και Επικοινωνιών (ΤΠΕ) όπως είναι το Διαδίκτυο των Πραγμάτων (ΔτΠ) με στόχο την αποτελεσματική διαχείριση των πόρων και των περιουσιακών τους στοιχείων και τη συνακόλουθη βελτίωση της ποιότητας ζωής και της ευημερίας των πολιτών.

Μικρογραφία των έξυπνων πόλεων αποτελούν οι έξυπνες πανεπιστημιουπόλεις (smart campuses), καθότι επιδιώκουν κατά βάση να αντιμετωπίσουν τις ίδιες προκλήσεις και φέρουν παρόμοια χαρακτηριστικά γνωρίσματα με αυτά των έξυπνων πόλεων. Ο όρος έξυπνη πανεπιστημιούπολη ερμηνεύεται ποικιλοτρόπως στη βιβλιογραφία αλλά δεν υπάρχει ένας παγκόσμιος, κοινά αποδεκτός ορισμός. Οι Bandara et al. [5] αναφέρουν ότι συνιστά μία πρωτοβουλία περί εφαρμογής των τεχνολογιών πληροφορικής και επικοινωνιών εντός της Πανεπιστημιούπολης με στόχο τη βελτίωση της ποιότητας των υπηρεσιών,

τη μείωση του κόστους και της κατανάλωσης πόρων καθώς και της ενεργότερης και αποτελεσματικότερης συμμετοχής των μελών. Κατά τον Muhamad et al. [6], ο κυριότερος κύριος ρόλος της έξυπνης πανεπιστημιούπολης είναι να παρουσιάσει τις δυναμικές υπηρεσίες της σύμφωνα με τις ανάγκες των χρηστών με την αρωγή κάποιου πληροφοριακού συστήματος.

Γενικότερα, στη βιβλιογραφία υπάρχει μία τριπλή προσέγγιση της έννοιας της έξυπνης πανεπιστημιούπολης [6]: 1) τεχνολογική, 2) βασιζόμενη στο μοντέλο της έξυπνης πόλης, 3) βασιζόμενη στην ανάπτυξη ενός οργανισμού ή μίας επιχειρηματικής διεργασίας.

Με βάση την τεχνολογική προσέγγιση, η έξυπνη πανεπιστημιούπολη είναι το αποτέλεσμα της εξέλιξης του ψηφιακού πανεπιστημίου, με τη χρήση των κατάλληλων τεχνολογιών και την παροχή διαδικτυακών υπηρεσιών όπως αυτών που βασίζονται στο Διαδίκτυο των Πραγμάτων και στην υπολογιστική νέφους. Με την υπηρεσία του Διαδικτύου των Πραγμάτων επιδιώκεται η μετατροπή των κοινών αντικειμένων που συναντώνται στους πανεπιστημιακούς χώρους σε έξυπνα αντικείμενα με την προσθήκη αισθητήρων και συστημάτων ολοκληρωμένης πληροφόρησης ώστε να υποστηρίξουν τη διαδικασία της έξυπνης λήψης αποφάσεων στα πλαίσια της πανεπιστημιούπολης. Έτσι, η έξυπνη πανεπιστημιούπολη δημιουργεί ένα ψηφιακό κεντρικό νευρικό σύστημα (digital nervous system) που κατευθύνει έναν ολοκληρωμένο κύκλο μάθησης εντός του πανεπιστημιακού οικοσυστήματος, επιτρέπει την ανάπτυξη κατάλληλων εφαρμογών ή υπηρεσιών που βελτιώνουν τις αποδόσεις της πανεπιστημιούπολης και συνάμα διευκολύνει την ένταξη όλων των ενδιαφερόμενων μερών σε ένα προσαρμοστικό περιβάλλον που περιλαμβάνει τρεις παράγοντες: τη διδασκαλία, τη διοίκηση και τις υπηρεσίες.

Σύμφωνα με την προσέγγιση που βασίζεται στο μοντέλο της έξυπνης πόλης, υποστηρίζεται ότι η έξυπνη πανεπιστημιούπολη συνιστά μία μικρή αυτοδύναμη πόλη καθότι παρατηρείται λειτουργική ομοιότητα από τη σκοπιά του αριθμού των λειτουργιών, των χρηστών, των δραστηριοτήτων και των συνδέσεων μεταξύ των αναγκών και των προκλήσεων που μία έξυπνη πανεπιστημιούπολη φέρει με εκείνες μίας έξυπνης πόλης.

Σύμφωνα δε με την τρίτη προσέγγιση που βασίζεται στην ιδέα ανάπτυξης μίας έξυπνης πανεπιστημιούπολης σύμφωνα με τις διαδικασίες ανάπτυξης ενός οργανισμού ή μίας επιχειρηματικής διεργασίας, γίνεται δεκτό ότι πρόκειται για την δημιουργία μίας πανεπιστημιούπολης δια της χρήσης των διαθέσιμων πόρων και της

εφαρμογής ευφυών συστημάτων και υπηρεσιών με σκοπό την παροχή υψηλού επιπέδου υπηρεσιών στην πανεπιστημιακή κοινότητα και ταυτοχρόνως μειώνοντας τα λειτουργικά κόστη.

2.2 Εξέλιξη της δομής και υποδομής των Πανεπιστημίων

Προβαίνοντας σε μία επισκόπηση της εξέλιξης του πανεπιστημίου, παρατηρούμε ότι διαχρονικά πριν τη μετάβαση στη σημερινή έννοια της έξυπνης πανεπιστημιούπολης, προηγήθηκαν τρία στάδια: από το παραδοσιακό πανεπιστήμιο όπου η διδασκαλία πραγματοποιούνταν με τον κλασικό τρόπο ήτοι με την δια ζώσης παρουσία μαθητών και εκπαιδευτικών στις αίθουσες διδασκαλίας και την διανομή έντυπου υλικού περάσαμε στο στάδιο του e-campus και στη συνέχεια στο στάδιο του digital campus. Το χαρακτηριστικό γνώρισμα τόσο του e-campus όσο και του digital campus είναι η υιοθέτηση νέων τεχνολογιών και η προσαρμογή της εκπαιδευτικής διδασκαλίας στις ανάγκες και τις ιδιαιτερότητες της σύγχρονης εποχής. Σταδιακά ακολούθησε η μετάβαση από τα προαναφερόμενα στάδια σε αυτό της έξυπνης πανεπιστημιούπολης (smart campus), οι διαφορές του οποίου σε σχέση με το digital campus παρουσιάζονται συνοπτικά παρακάτω[7]:

TABLE V. DIFFERENCE BETWEEN DIGITAL CAMPUS AND SMART CAMPUS

	Digital campus	**Smart campus**
Technical Environemnt	Local area network internet	IoT, cloud computing, wireless network, mobile terminal, RFID
Application	Learning resource in digtal form, distance learning, digital library, network management	Intelligent system using sensor, interoperability, and control ability
System Management	Isolated	System sharing, intelligent, push

Εικόνα 1 Διαφορές ψηφιακής και έξυπνης πανεπιστημιούπολης [7]

Εν συντομία, η έξυπνη πανεπιστημιούπολη (smart campus) αποτελεί την αναβαθμισμένη έκδοση της ψηφιακής πανεπιστημιούπολης (digital campus) με κεντρική ιδέα την προσπάθεια ενσωμάτωσης σε αυτό προηγμένων τεχνολογιών προκειμένου να επιτευχθούν υψηλές εκπαιδευτικές επιδόσεις, να βελτιωθεί η καθημερινότητα της ακαδημαϊκής κοινότητας και με στόχο να είναι φιλικό προς το περιβάλλον [6].

2.3 Χαρακτηριστικά γνωρίσματα του smart campus

Σε σύγκριση με το digital campus, το smart campus φέρει τα ακόλουθα χαρακτηριστικά γνωρίσματα [8]:

1) Context – aware: Η έξυπνη πανεπιστημιούπολη είναι συχνά εξοπλισμένη με ένα σύνολο έξυπνων συσκευών ανίχνευσης που παρακολουθούν μια ευρεία φυσική περιοχή, η οποία παρέχει τα θεμέλια για την χωρική επίγνωση. Το χαρακτηριστικό της χωρικής επίγνωσης αναφέρεται κυρίως στην ικανότητα παρατήρησης και συνειδητοποίησης της κατάστασης του περιβάλλοντος και της συμπεριφοράς των χρηστών εντός της πανεπιστημιούπολης με σκοπό την παροχή προσαρμοσμένων υπηρεσιών για την ικανοποίηση των ατομικών αναγκών. Το εν λόγω χαρακτηριστικό υποστηρίζεται από την τεχνολογία του Διαδικτύου των Πραγμάτων και θεωρείται βασικό χαρακτηριστικό της έξυπνης πανεπιστημιούπολης.

2) Data – driven: Τα δεδομένα της έξυπνης πανεπιστημιούπολης συλλέγονται αυτόματα σε πραγματικό χρόνο από διάφορες πηγές, ήτοι από τις συσκευές ανίχνευσης, από τις διαδικασίες διδασκαλίας/μάθησης, από την αξιολόγηση επιδόσεων, από εξωσχολικές δραστηριότητες κ.λπ. Με τη βοήθεια της υπηρεσίας υπολογιστικού νέφους και του Διαδικτύου των Πραγμάτων, ένας μεγάλος όγκος δεδομένων συσσωρεύεται και υπόκειται σε κοινή χρήση. «Ο προσανατολισμός στα δεδομένα (data- driven)» είναι ένα σημαντικό χαρακτηριστικό για την επίτευξη της ευφυίας μιας πανεπιστημιούπολης υπό την έννοια ότι η πλειοψηφία των έξυπνων λειτουργιών που προσφέρονται από μία πανεπιστημιούπολη βασίζονται στην ανάλυση μεγάλων δεδομένων.

3) Προβλεψιμότητα (Forecasting): Τα τεράστια σύνολα δεδομένων που αντλούνται από τα πληροφοριακά συστήματα δίνουν τη δυνατότητα μάθησης μέσω της παρατήρησης και της πρόβλεψης μελλοντικών γεγονότων. Χάρη σε αυτό το χαρακτηριστικό που επιτρέπει την ανάλυση των δεδομένων καθίσταται εφικτός ο προγραμματισμός διαδικασιών, η πρόβλεψη των απαραίτητων κάθε φορά ενεργειών αλλά και η λήψη αποφάσεων ενόψει πρόβλεψης μελλοντικών γεγονότων.

4) Εμβυθιστικές τεχνολογίες (immersive): Οι εμβυθιστικές τεχνολογίες εντός της έξυπνης πανεπιστημιούπολης επιτρέπουν ένα μείγμα εικονικών και πραγματικών περιβαλλόντων για μάθηση, το οποίο εμπλουτίζει την μαθησιακή εμπειρία. Είναι γεγονός ότι η γνώση που μπορεί να αποκτηθεί από τον πραγματικό κόσμο είναι συνήθως περιορισμένη. Θα είναι πρόκληση για τους φοιτητές να παρατηρήσουν και να κατανοήσουν ορισμένα φαινόμενα που υπάρχουν αλλά σπάνια βιώνουν στον

πραγματικό κόσμο. Σε αυτές τις περιπτώσεις, οι φοιτητές θα μπορούσαν να ζητήσουν βοήθεια από ένα εικονικό περιβάλλον για να επιτύχουν μεγαλύτερα ποσοστά μαθησιακής κατανόησης. Η μάθηση με τη χρήση εμβυθιστικών τεχνολογιών όπως η επαυξημένη πραγματικότητα (AR), η εικονική πραγματικότητα (VR) και η μεικτή πραγματικότητα (MR), βελτιώνει επίσης τη συγκέντρωση των φοιτητών και τα κίνητρα στις μαθησιακές τους δραστηριότητες.

5) Συνεργατικότητα (collaborative): Η συνεργατική μάθηση μπορεί να ενθαρρύνει την ανταλλαγή γνώσεων μεταξύ των φοιτητών και μεταξύ εκπαιδευτών και φοιτητών. Σε ένα συνεργατικό περιβάλλον μάθησης, νέα γνώση μπορεί να δημιουργηθεί από την αλληλεπίδραση μεταξύ εφαρμογών και ανθρώπων, πράγμα που σημαίνει ότι οι φοιτητές μπορούν να δημιουργούν ενεργά τη γνώση με βάση την εμπειρία και όχι παθητικά λαμβάνοντας γνώση από τον καθηγητή. Με την βοήθεια τεχνολογιών που βασίζονται στο υπολογιστικό νέφος, η διαδικτυακή συνεργασία θα μπορούσε να επιτευχθεί αποτελεσματικά στην εκπαιδευτική κοινότητα, είτε εντός είτε εκτός της πανεπιστημιούπολης, μέσω μιας διαδικτυακής πλατφόρμας.

Παρακάτω θα αναλυθεί η τεχνολογική υποδομή καθώς και οι επιμέρους υπηρεσίες που παρέχονται στα πλαίσια μίας έξυπνης πανεπιστημιούπολης και τα οποία παρουσιάζονται συνοπτικά στην ακόλουθη εικόνα:

Εικόνα 2 Τεχνολογίες και υπηρεσίες μίας έξυπνης πανεπιστημιούπολης [60]

ΚΕΦΑΛΑΙΟ 3 – ΤΕΧΝΟΛΟΓΙΚΗ ΥΠΟΔΟΜΗ ΕΞΥΠΝΗΣ ΠΑΝΕΠΙΣΤΗΜΙΟΥΠΟΛΗΣ

Η εξέλιξη της έννοιας της έξυπνης πανεπιστημιούπολης όπως αυτή περιγράφηκε ανωτέρω, δεν θα ήταν δυνατή χωρίς τη παρουσία και τη χρήση νέων, προηγμένων τεχνολογιών. Παρακάτω αναφέρονται οι βασικότερες εξ αυτών που θα μπορούσαν να τύχουν εφαρμογής στο εσωτερικό της, επί τη βάσει των οποίων έχουν αναπτυχθεί και υποστηρίζονται πολλές υπηρεσίες και εφαρμογές που θα αναλυθούν στο επόμενο κεφάλαιο. Ειδικότερα:

3.1 Διαδίκτυο των Πραγμάτων (Internet of Things)

3.1.1 Ορισμός

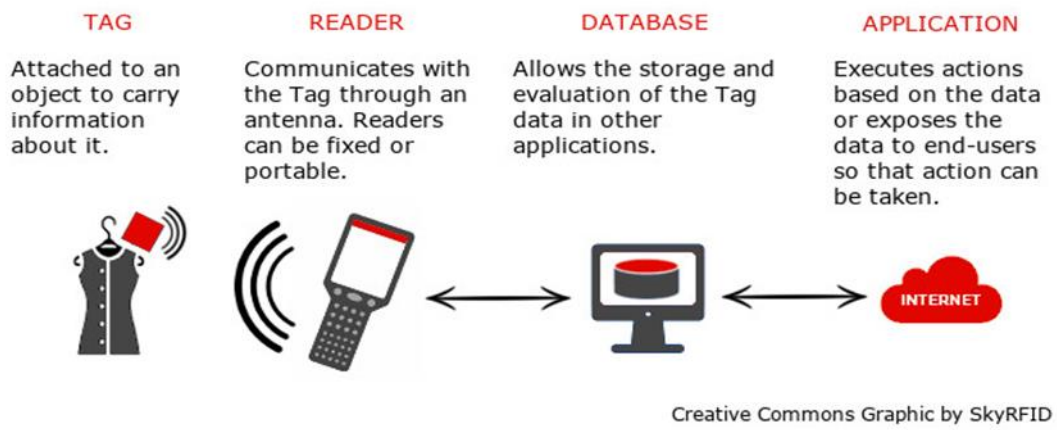
Με τον όρο «Διαδίκτυο των Πραγμάτων» νοείται ένα σύστημα από διασυνδεδεμένες μεταξύ τους συσκευές και εν γένει αντικείμενα τα οποία, με ελάχιστη έως μηδαμινή ανθρώπινη παρέμβαση, εντός του δικτύου στο οποίο βρίσκονται, ανταλλάσσουν και μοιράζονται δεδομένα που άλλοτε παράγουν μόνα τους και άλλοτε συλλέγουν από το εξωτερικό περιβάλλον με τη χρήση αισθητήρων. Μάλιστα χάρη στη μεταξύ τους διασύνδεση, τα «έξυπνα» αυτά αντικείμενα μπορούν να απομονώνουν δεδομένα, να τα επεξεργάζονται, να τα αναλύουν και συνεπώς να εξάγουν από αυτά χρήσιμες πληροφορίες τις οποίες και μεταφέρουν στους ανθρώπους. [85]

3.1.2 Η αρχιτεκτονική του Διαδικτύου των Πραγμάτων και οι τεχνολογίες - πυλώνες αυτής

Το Διαδίκτυο των Πραγμάτων απαρτίζεται από 3 βασικά επίπεδα, ήτοι το επίπεδο αντίληψης (perception layer), το επίπεδο δικτύου (network layer) καθώς και το επίπεδο εφαρμογής (application layer) [4].

Α) α. Το επίπεδο αντίληψης είναι το χαμηλότερο επίπεδο της αρχιτεκτονικής των 3 επιπέδων του διαδικτύου των πραγμάτων και ονομάζεται αλλιώς και επίπεδο αντίληψης και ελέγχου. Στο επίπεδο αυτό γίνεται η συλλογή δεδομένων από τις διάφορες συσκευές και τα αντικείμενα με τη χρήση συναφών εργαλείων όπως ενδεικτικά είναι διάφοροι τύποι αισθητήρων και πομπών (αισθητήρας συγκέντρωσης αερίου, αισθητήρας θερμοκρασίας, αισθητήρας υγρασίας, μετασχηματιστής ρεύματος, μετατροπέας τάσης, κ.λπ.), σαρωτής ετικέτας RFID/EPC code, κάμερα, μικρόφωνο και στη συνέχεια γίνεται η επεξεργασία και μεταφορά των συλλεχθέντων δεδομένων ως πληροφοριών πλέον στα επόμενα επίπεδα [90].

β. Προκειμένου να είναι εφικτή η συλλογή δεδομένων από τις διάφορες συσκευές και τα αντικείμενα προϋποτίθεται η ανίχνευση και ιχνηλάτηση αυτών. Μία από τις βασικές τεχνολογίες που χρησιμοποιούνται προς τον σκοπό τούτο είναι η RFID (Radio Frequency Identification) / Τεχνολογία Ταυτοποίησης μέσω Ραδιοσυχνοτήτων, η οποία υποστηρίζει την ανέπαφη ανταλλαγή δεδομένων μέσω ραδιοκυμάτων και φέρει πολλά πλεονεκτήματα όπως: γρήγορη σάρωση, ανθεκτικότητα, ανάγνωση χωρίς επαφή, μικρό μέγεθος, χαμηλό κόστος. Στην πράξη, ένα σύστημα RFID αποτελείται από μία ετικέτα (tag) δηλαδή ένα μικροτσίπ, έναν αναγνώστη (reader) και μία κεραία (antenna) [104]. Κάθε μία από τις ετικέτες RFID είναι ενσωματωμένη σε ένα αντικείμενο προσδίδοντας του έτσι ένα μοναδικό αναγνωριστικό αριθμό. Κάθε αναγνώστης δια της αλληλεπίδρασης με την ετικέτα με τη χρήση ραδιοκυμάτων, αναγνωρίζει ένα αντικείμενο και αντλεί από αυτό τις απαιτούμενες πληροφορίες. Η μετάδοση των σημάτων μεταξύ των ετικετών και των αναγνωστών πραγματοποιείται χάρη στις κεραίες [88].



Εικόνα 3 Λειτουργία Τεχνολογίας RFID [152]

Μία άλλη ασύρματη τεχνολογία που χρησιμοποιείται στο επίπεδο αυτό είναι η Επικοινωνία Κοντινού Πεδίου (NFC). Η τεχνολογία αυτή επιτρέπει την επικοινωνία συσκευών από πολύ μικρή απόσταση (4-10 εκατοστά) και ενδείκνυται για περιπτώσεις άμεσης και εύκολης ανταλλαγής δεδομένων. Υπάρχουν δύο τρόποι επικοινωνίας, ήτοι η αμφίδρομη επικοινωνία όπου οι συσκευές διαβάζουν και γράφουν η μία στην άλλη (μεταφορά φωτογραφιών, επαφών, συνδέσεων) καθώς και η μονόδρομη επικοινωνία όπου η ανάγνωση και η εγγραφή σε ένα τσιπ NFC γίνεται από μία τροφοδοτούμενη με ηλεκτρική ενέργεια συσκευή όπως τηλέφωνο ή συσκευή ανάγνωσης πιστωτικών καρτών [9]. Πρόκειται για μία τεχνολογία που

χρησιμοποιείται κατα κόρον στον τομέα των πληρωμών με τη χρήση πιστωτικών και χρεωστικών καρτών καθώς ο τρόπος λειτουργίας του NFC και η υποδομή του προσφέρουν ασφάλεια και αμεσότητα κατά την μεταφορά των δεδομένων των συναλλαγών [86].

Β) α. Το επίπεδο δικτύου είναι το ενδιάμεσο επίπεδο της αρχιτεκτονικής των 3 επιπέδων του διαδικτύου των πραγμάτων και ονομάζεται και αλλιώς και επίπεδο μετάδοσης. Στο επίπεδο αυτό γίνεται η παραλαβή της παραχθείσας, από τα δεδομένα του προηγούμενου επιπέδου, πληροφορίας και ο καθορισμός της πορείας που θα ακολουθήσει η πληροφορία αυτή εντός του δικτύου των διασυνδεδεμένων συσκευών και αντικειμένων. Με άλλα λόγια, το επίπεδο δικτύου επιτρέπει τη μετάδοση πληροφοριών από και προς τις διάφορες συσκευές μέσω πυλών χρησιμοποιώντας διάφορα πρωτόκολλα επικοινωνίας και διάφορες τεχνολογίες και στην ουσία αποτελεί τον δίαυλο επικοινωνίας μεταξύ του επιπέδου αντίληψης και του επιπέδου εφαρμογής. [92]

β. Ορισμένες από τις τεχνολογίες που χρησιμοποιούνται στο επίπεδο αυτό είναι ενδεικτικά η ZigBee και η Z-Wave. Η μεν πρώτη αποτελεί μία τεχνολογία ασύρματου δικτύου σχεδιασμένη για την επικοινωνία μικρής εμβέλειας καθότι προσφέρει πολλά πλεονεκτήματα όπως χαμηλή κατανάλωση ενέργειας, αξιοπιστία, χαμηλό ρυθμό δεδομένων, χαμηλό κόστος. Η μεν δεύτερη αποτελεί ομοίως τεχνολογία ασύρματου δικτύου μικρής εμβέλειας με τα ίδια ακριβώς πλεονεκτήματα με την πρώτη. Η κυριότερη διαφορά μεταξύ των δύο είναι η ζώνη συχνοτήτων του φυσικού στρώματος καθώς επίσης το πλήθος των τελικών συσκευών που μπορεί να υποστηρίξει η καθεμία [87].

ZigBee	Z-Wave
Data Rate: 250kb/s	Data Rate: 40kb/s
Power Consumption: ~40mA	Power Consumption: ~2.5mA
Range: 10-20 meters	Range: 30-65 meters
Operates at 2.4GHz	Operates at 908MHz
Chips and modules available from multiple manufacturers	Chips only sold by Silicon Labs
Variable certification process	Strict certification process
Supports over 65,000 end nodes	Supports over 232 end nodes
More difficult to configure and set up	More user-friendly and easier to set up
More cost-effective	More expensive than Zigbee

Εικόνα 4 Διαφορές ZigBee - Z-Wave [153]

Γ) Το επίπεδο εφαρμογής είναι το ανώτατο επίπεδο της αρχιτεκτονικής των 3 επιπέδων του διαδικτύου των πραγμάτων. Στο επίπεδο αυτό η πληροφορία που έχει μεταβιβαστεί από το επίπεδο δικτύου χρησιμοποιείται για την παροχή των υπηρεσιών και λειτουργιών όπως π.χ για την αποθήκευση των επίμαχων πληροφοριών σε βάσεις δεδομένων, για την ανάλυση και αξιολόγηση των πληροφοριών αυτών και την εξαγωγή συμπερασμάτων ή την πρόβλεψη μελλοντικών καταστάσεων [93].

3.1.3 Χρησιμότητα και προκλήσεις του Διαδικτύου των Πραγμάτων στα πλαίσια του Smart Campus

Το Διαδίκτυο των Πραγμάτων αποτελεί τη ραχοκοκαλιά της τεχνολογικής υποδομής του Smart Campus συνιστώντας τη βάση επί της οποίας στηρίζονται και οι υπόλοιπες τεχνολογίες που ενυπάρχουν και καθιστούν εφικτή τη λειτουργία αυτού. Ειδικότερα, το Διαδίκτυο των Πραγμάτων παρέχει μία ψηφιακή βάση που ευνοεί την ανάπτυξη και εφαρμογή νέων υπηρεσιών καθώς επίσης και τη διασύνδεση συσκευών και ανθρώπων, συμβάλλοντας στην βελτίωση εν γένει της καθημερινότητας των φοιτητών και του εκπαιδευτικού προσωπικού [95].

Η χρησιμότητα του δεν περιορίζεται μόνο σε έναν τομέα αλλά διαπνέει το σύνολο της υπόστασης του Smart Campus. Πιο συγκεκριμένα στον τομέα της εκπαίδευσης, με τη χρήση του Διαδικτύου των Πραγμάτων, μπορεί να δημιουργηθεί μία πλατφόρμα πληροφοριών για τους εκπαιδευτές ώστε παρακολουθούν την πρόοδο των φοιτητών και να προβαίνουν στη συνέχεια σε στοχευμένες και εξατομικευμένες για τον κάθε φοιτητή ενέργειες. Περαιτέρω, με τη βοήθεια του περιβάλλοντος εργαστηρίου που βασίζεται στο Διαδίκτυο των Πραγμάτων και των εργαστηριακών οργάνων που βασίζονται σε τεχνητή νοημοσύνη, αναμένεται ότι τα μελλοντικά εργαστήρια θα είναι εξοπλισμένα με έξυπνο λογισμικό που μπορεί να αλληλεπιδράσει σημαντικά με τους φοιτητές παρέχοντας τους σε πραγματικό χρόνο παραδείγματος χάρη, αυτόματα σχόλια σχετικά με το αποτέλεσμα της εργασίας τους και βοηθώντας τους έτσι να ολοκληρώσουν τις εργαστηριακές εργασίες τους [94]. Εν ολίγοις, το Διαδίκτυο των Πραγμάτων εγγυάται την αποτελεσματική αναβάθμιση των λειτουργιών της πανεπιστημιακής εκπαίδευσης όπως είναι η διδασκαλία, η μάθηση, η έρευνα και η καινοτομία.

Στον τομέα του περιβάλλοντος και της διαχείρισης των πόρων, το Διαδίκτυο των Πραγμάτων επιτρέπει την μείωση του λειτουργικού κόστους και του οικολογικού αποτυπώματος καθώς ένα μεγάλο μέρος των διαδικασιών διαχείρισης των εγκαταστάσεων μπορεί να αυτοματοποιηθεί με γνώμονα την υιοθέτηση πιο

φιλικών προς το περιβάλλον κατευθύνσεων και λύσεων[101]. Για παράδειγμα, με την εγκατάσταση αισθητήρων που θα είναι συνδεδεμένοι στο δίκτυο θα μπορεί να παρακολουθείται σε εικοσιτετράωρη βάση η χρήση και κατανάλωση ενέργειας τόσο σε επιμέρους αίθουσες όσο και στο σύνολο των κτηριακών υποδομών με αποτέλεσμα να ρυθμίζεται αυτόματα, ανάλογα με τις απαιτούμενες κάθε φορά ανάγκες, η κατανάλωση ηλεκτρικής ενέργειας, νερού και θέρμανσης [100].

Για την αποτελεσματική υλοποίηση όλων των προαναφερόμενων λειτουργιών του Διαδικτύου των Πραγμάτων βασική προϋπόθεση συνιστά η γρήγορη αποστολή των δεδομένων, η οποία επιτυγχάνεται μέσω της ασύρματης επικοινωνίας των επιμέρους συσκευών. Λόγω δε της μεγάλης ποσότητας των παραγόμενων δεδομένων απαιτείται σε πρώτο στάδιο η ασφαλής αποθήκευση τους και εν συνεχεία η επεξεργασία τους η οποία περιλαμβάνει τον έλεγχο για ύπαρξη τυχόν αλλοιωμένων ή ελλιπών δεδομένων και την μετατροπή των δεδομένων σε μία καθορισμένη μορφή. Σε δεύτερο στάδιο, λαμβάνει χώρα η ενοποίηση των δεδομένων και ο διαμοιρασμός τους προκειμένου να γίνει χρήση τους από τις επιμέρους εφαρμογές.[10]

3.2. Ασύρματο Δίκτυο Πέμπτης Γενιάς (5G)

Η ολοένα και αυξανόμενη προσθήκη έξυπνων και συνδεδεμένων στο ευρύτερο δίκτυο του Smart Campus συσκευών που βρίσκονται σε άμεση, γρήγορη και αδιάκοπη επικοινωνία μεταξύ τους, συνεπάγεται την ταυτόχρονη αύξηση του όγκου και της κυκλοφορίας των δεδομένων που παράγονται από τις συσκευές αυτές και χρήζουν επεξεργασίας. Οι τεράστιες απαιτήσεις κυκλοφορίας δεδομένων συνεπάγονται ομοίως αυξημένες απαιτήσεις για πλήρη κάλυψη, για ασύρματες επικοινωνίες εξαιρετικά υψηλής ταχύτητας με εξαιρετικά υψηλή αξιοπιστία και εξαιρετικά χαμηλή καθυστέρηση. Η επίτευξη όλων των προαναφερόμενων είναι εφικτή χάρη στην εφαρμογή του ασύρματου δικτύου πέμπτης γενιάς (5G) [102].

3.2.1 Χαρακτηριστικά γνωρίσματα ασύρματου δικτύου πέμπτης γενιάς

Το ασύρματο δίκτυο πέμπτης γενιάς (5G) αποτελεί πυλώνα του ψηφιακού μετασχηματισμού και φέρει τα ακόλουθα χαρακτηριστικά [96] :

- Προσφέρει συνδεσιμότητα υψηλής ταχύτητας στο διαδίκτυο, μεγάλο εύρος ζώνης, υψηλή κάλυψη, υψηλή απόδοση, υψηλή αξιοπιστία, χαμηλή καθυστέρηση και βελτιωμένη ποιότητα υπηρεσιών. Παρέχει μέγιστη απόδοση down-link έως και 20 Gbps. Επιπλέον υποστηρίζει το 4G WWWW

(4ης γενιάς World Wide Wireless Web) και βασίζεται στο πρωτόκολλο Internet protocol version 6 (IPv6). Χρησιμοποιεί χιλιοστομετρικά κύματα για τη μετάδοση δεδομένων, παρέχοντας μεγαλύτερο εύρος ζώνης και τεράστιο ρυθμό δεδομένων από τις χαμηλότερες ζώνες LTE.

- Δύναται να προσφέρει 120 καρέ ανά δευτερόλεπτο με υψηλή ανάλυση και ροή βίντεο υψηλότερου δυναμικού εύρους, ενώ τα τηλεοπτικά κανάλια HD μπορούν επίσης να είναι προσβάσιμα σε κινητές συσκευές χωρίς διακοπές. Το 5G παρέχει επικοινωνία υψηλής ευκρίνειας με χαμηλή καθυστέρηση, μικρότερη από ένα χιλιοστό του δευτερολέπτου, οπότε νέες τεχνολογίες όπως η επαυξημένη πραγματικότητα (AR) και η εικονική πραγματικότητα (VR) μπορούν να υλοποιηθούν βασιζόμενες σε αυτό.
- Διαδραματίζει σημαντικό ρόλο στην ανάπτυξη του Διαδικτύου των πραγμάτων (IoT) καθότι παρέχει πολύ γρήγορη συνδεσιμότητα στο διαδίκτυο για τη συλλογή, τη μετάδοση, τον έλεγχο και την επεξεργασία δεδομένων που συλλέγονται από τις διασυνδεδεμένες μεταξύ τους αλλά και με το διαδίκτυο συσκευές και αισθητήρες. Το 5G είναι ένα ευέλικτο δίκτυο με άφθονο εύρος ζώνης που προσφέρει πολύ χαμηλού κόστους ανάπτυξη, γι' αυτό και είναι η πιο αποτελεσματική τεχνολογία για το Διαδίκτυο των Πραγμάτων.

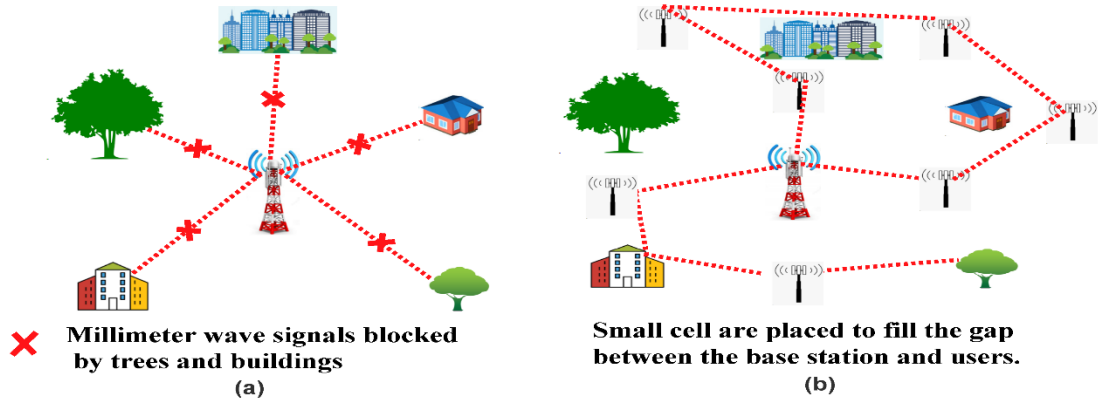
3.2.2 Συστατικά μέρη των ασύρματων δικτύων πέμπτης γενιάς (5G)

Ειδικότερα, τα χαρακτηριστικά γνωρίσματα των ασύρματων δικτύων 5G είναι τα ακόλουθα [96] :

Α) Μικρές κυψέλες (Small cells) : Οι μικρές κυψέλες είναι κυψελοειδείς κόμβοι ραδιοπρόσβασης χαμηλής ισχύος που λειτουργούν σε εύρος από 10 μέτρα έως μερικά χιλιόμετρα. Οι μικρές κυψέλες διαδραματίζουν πολύ σημαντικό ρόλο στην υλοποίηση του ασύρματου δικτύου 5G καθότι αποτελούν σταθμούς βάσης χαμηλής ισχύος που καλύπτουν μικρές περιοχές. Οι μικρές κυψέλες είναι παρόμοιες με όλες τις προηγούμενες κυψέλες που χρησιμοποιούνται σε διάφορα ασύρματα δίκτυα. Ωστόσο, αυτές οι κυψέλες έχουν ορισμένα πλεονεκτήματα, όπως ότι μπορούν να λειτουργούν με χαμηλή ισχύ και είναι επίσης ικανές να λειτουργούν με υψηλούς ρυθμούς δεδομένων. Οι μικρές κυψέλες βοηθούν στην ανάπτυξη του δικτύου 5G με επικοινωνία εξαιρετικά υψηλής ταχύτητας και χαμηλής καθυστέρησης [98]. Οι μικρές κυψέλες στο δίκτυο 5G χρησιμοποιούν ορισμένες νέες τεχνολογίες όπως η Τεχνολογία Πολλαπλής Εισόδου- Πολλαπλής Εξόδου (ΤΠΕΙΣΠΕΞ (MIMO), η

διαμόρφωση δέσμης και το mmWave για μετάδοση δεδομένων υψηλής ταχύτητας. Ο σχεδιασμός του υλικού των μικρών κυψελών είναι πολύ απλός, οπότε η υλοποίησή του είναι αρκετά πιο εύκολη και γρήγορη.

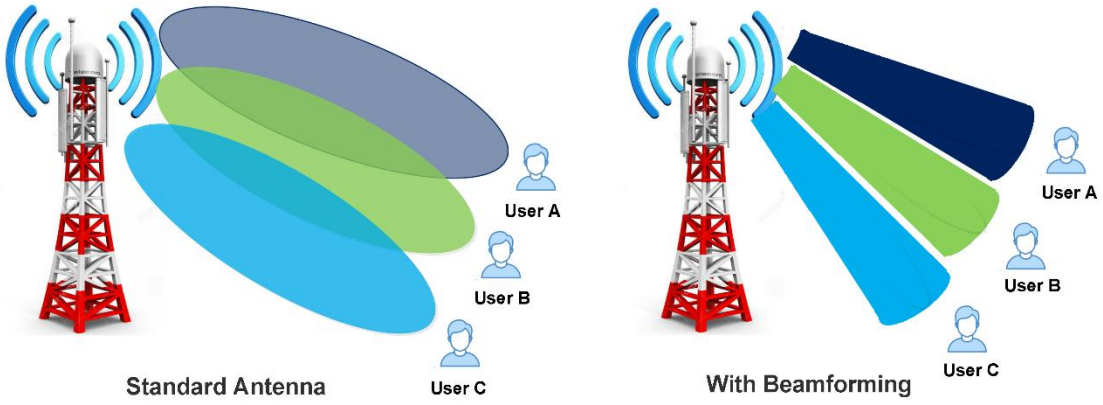
Το MmWave (χιλιοστομετρικό κύμα) είναι μία εξαιρετικά υψηλή ζώνη συχνοτήτων μεταξύ 30 και 300 GHz. Μέχρι τώρα τα συστήματα ραντάρ και οι δορυφόροι χρησιμοποιούν μόνο mmWave, καθώς πρόκειται για πολύ γρήγορες ζώνες συχνοτήτων που παρέχουν ασύρματη επικοινωνία πολύ υψηλής ταχύτητας ενώ παράλληλα ολοένα και περισσότεροι πάροχοι δικτύων κινητής τηλεφωνίας ξεκίνησαν να χρησιμοποιούν επίσης τα mmWave για τη μετάδοση δεδομένων μεταξύ σταθμών βάσης. Το MmWave προσφέρει εξαιρετικά μεγάλο εύρος ζώνης για κινητά δίκτυα επόμενης γενιάς. Το MmWave έχει πολλά πλεονεκτήματα, αλλά έχει και κάποια μειονεκτήματα, όπως ότι τα σήματα mmWave είναι σήματα πολύ υψηλής συχνότητας, οπότε συγκρούονται περισσότερο με εμπόδια στον αέρα, με αποτέλεσμα τα σήματα να χάνουν γρήγορα ενέργεια. Τα κτίρια και τα δέντρα εμποδίζουν επίσης τα σήματα MmWave, οπότε τα σήματα αυτά καλύπτουν μικρότερη απόσταση. Για την επίλυση αυτών των προβλημάτων, εγκαθίστανται πολλαπλοί σταθμοί μικρών κυψελών για να καλύψουν το κενό μεταξύ του τελικού χρήστη και του σταθμού βάσης. Η μικρή κυψέλη καλύπτει πολύ μικρότερη εμβέλεια, οπότε η εγκατάσταση μιας μικρής κυψέλης εξαρτάται από τον πληθυσμό μιας συγκεκριμένης περιοχής. Γενικά, σε ένα κατοικημένο μέρος, η απόσταση μεταξύ κάθε μικρής κυψέλης κυμαίνεται από 10 έως 90 μέτρα. Όπως φαίνεται στο ακόλουθο σχήμα (περίπτωση a), το mmWave έχει μεγαλύτερη εμβέλεια, οπότε μπορεί εύκολα να εμποδιστεί από διάφορα παρεμβαλλόμενα αντικείμενα. Αυτό είναι ένα από τα βασικά προβλήματα της μετάδοσης σήματος χιλιοστομετρικών κυμάτων. Για την επίλυση αυτού του ζητήματος, η μικρή κυψέλη μπορεί να τοποθετηθεί σε μικρή απόσταση για να μεταδίδει τα σήματα εύκολα, όπως φαίνεται στην περίπτωση b του ίδιου σχήματος [96,99].



Εικόνα 5 Παράδειγμα χιλιοστομετρικού κύματος με και χωρίς μικρή κυψέλη [96]

Β) Διαμόρφωση δέσμης (Beamforming): Η διαμόρφωση δέσμης είναι μια βασική τεχνολογία των ασύρματων δικτύων που κατευθύνει τα μεταδιδόμενα σήματα. Η διαμόρφωση δέσμης 5G δημιουργεί μια ισχυρή ασύρματη σύνδεση προς ένα άκρο λήψης. Στα συμβατικά συστήματα, όταν οι μικρές κυψέλες δεν χρησιμοποιούν διαμόρφωση δέσμης, η μετακίνηση των σημάτων σε συγκεκριμένες περιοχές είναι αρκετά δύσκολη. Η διαμόρφωση δέσμης αντιμετωπίζει αυτό το πρόβλημα δια της χρήσης των μικρών κυψελών οι οποίες είναι σε θέση να μεταδίδουν τα σήματα σε συγκεκριμένη κατεύθυνση προς μια συσκευή όπως κινητό τηλέφωνο, φορητούς υπολογιστές, αυτόνομα οχήματα και συσκευές του Διαδικτύου των Πραγμάτων. Η διαμόρφωση δέσμης βελτιώνει την αποδοτικότητα και εξοικονομεί ενέργεια στο δίκτυο 5G. [97]

Τα ασύρματα σήματα στο δίκτυο 5G εξαπλώνονται σε μεγάλες περιοχές και η φύση δεν είναι πανκατευθυντική. Έτσι, η ενέργεια εξαντλείται γρήγορα και οι χρήστες που έχουν πρόσβαση σε αυτά τα σήματα αντιμετωπίζουν επίσης προβλήματα παρεμβολών. Η τεχνική διαμόρφωσης δέσμης χρησιμοποιείται στο δίκτυο 5G για την επίλυση αυτού του προβλήματος. Στη διαμόρφωση δέσμης τα σήματα είναι πανκατευθυντικά. Κινούνται σαν ακτίνα λέιζερ από το σταθμό βάσης προς το χρήστη, οπότε τα σήματα φαίνεται να ταξιδεύουν σε ένα αόρατο καλώδιο. Η διαμόρφωση δέσμης βοηθά στην επίτευξη ταχύτερου ρυθμού μετάδοσης δεδομένων- καθώς τα σήματα είναι πανκατευθυντικά, οδηγεί σε μικρότερη κατανάλωση ενέργειας και λιγότερες παρεμβολές [96]. Στο παρακάτω σχήμα παρουσιάζεται η εικονογραφική αναπαράσταση της επικοινωνίας με και χωρίς τη χρήση διαμόρφωσης δέσμης.



Εικόνα 6 Επικοινωνία με και χωρίς τη χρήση διαμόρφωσης δέσμης [96]

3.2.3 Χρησιμότητα των ασύρματων δικτύων πέμπτης γενιάς στο πλαίσιο του Smart Campus

Εν αντιθέσει με τα ασύρματα δίκτυα των προηγούμενων γενιών που παρουσίαζαν υψηλή καθυστέρηση δικτύου, αργή ταχύτητα μετάδοσης και σχετικά χαμηλή ασφάλεια, τα ασύρματα δίκτυα πέμπτης γενιάς προσφέρουν υψηλότερες ταχύτητες και μεγαλύτερο εύρος ζώνης το οποίο συνεπάγεται ταχύτερες συνδέσεις στο διαδίκτυο και απρόσκοπτη μεταφορά δεδομένων εντός της πανεπιστημιούπολης. Αυτό με τη σειρά του επιτρέπει τη δημιουργία ενός τεχνολογικά προηγμένου εκπαιδευτικού περιβάλλοντος καθότι συνεπάγεται την ταχύτερη πρόσβαση σε εκπαιδευτικό υλικό, σε εφαρμογές εικονικής και επαυξημένης πραγματικότητας καθώς επίσης και σε διαδραστικές -εικονικές αίθουσες διδασκαλίας [11].

Επιπλέον, τα ασύρματα δίκτυα πέμπτης γενιάς διακρίνονται από την ικανότητα τους να διαχειρίζονται αποτελεσματικά τεράστιες ποσότητες δεδομένων που είναι ζωτικής σημασίας για τις ακαδημαϊκές αναζητήσεις και τις ερευνητικές δραστηριότητες. Με τον τρόπο αυτό, οι ερευνητές και οι φοιτητές μπορούν να επεξεργάζονται και να μοιράζονται μεγάλα σύνολα δεδομένων και να διεξάγουν αναλύσεις βάσει δεδομένων, προωθώντας ακαδημαϊκές και ερευνητικές πρωτοβουλίες χωρίς να δημιουργείται συμφόρηση του δικτύου [103].

Επιπρόσθετα, τα ασύρματα δίκτυα πέμπτης γενιάς συμβάλλουν στην μακροπρόθεσμη εξοικονόμηση κόστους και ενέργειας μέσω της ταχύτερης επεξεργασίας δεδομένων, του μειωμένου χρόνου διακοπής λειτουργίας, των βελτιστοποιημένων λειτουργιών και της πιθανής ενοποίησης διαφόρων συστημάτων επικοινωνιών. Η ευρεία χρήση τους μάλιστα αποδυναμώνει την ανάγκη επένδυσης σε επιτόπια υποδομή πληροφορικής (IT infrastructure), περιλαμβάνουσα το υλικό, το λογισμικό και τον εξοπλισμό δικτύωσης του Smart Campus, των οποίων η αγορά, η

συντήρηση και η αναβάθμιση είναι δαπανηρή [105]. Τα ασύρματα δίκτυα πέμπτης γενιάς λοιπόν μπορούν να υποστηρίξουν την μεταφορά όλων των εφαρμογών και των δεδομένων στο υπολογιστικό νέφος, παρέχοντας την απαιτούμενη για την εκτέλεση των εφαρμογών, συνδεσιμότητα υψηλής ταχύτητας και χαμηλής καθυστέρησης.

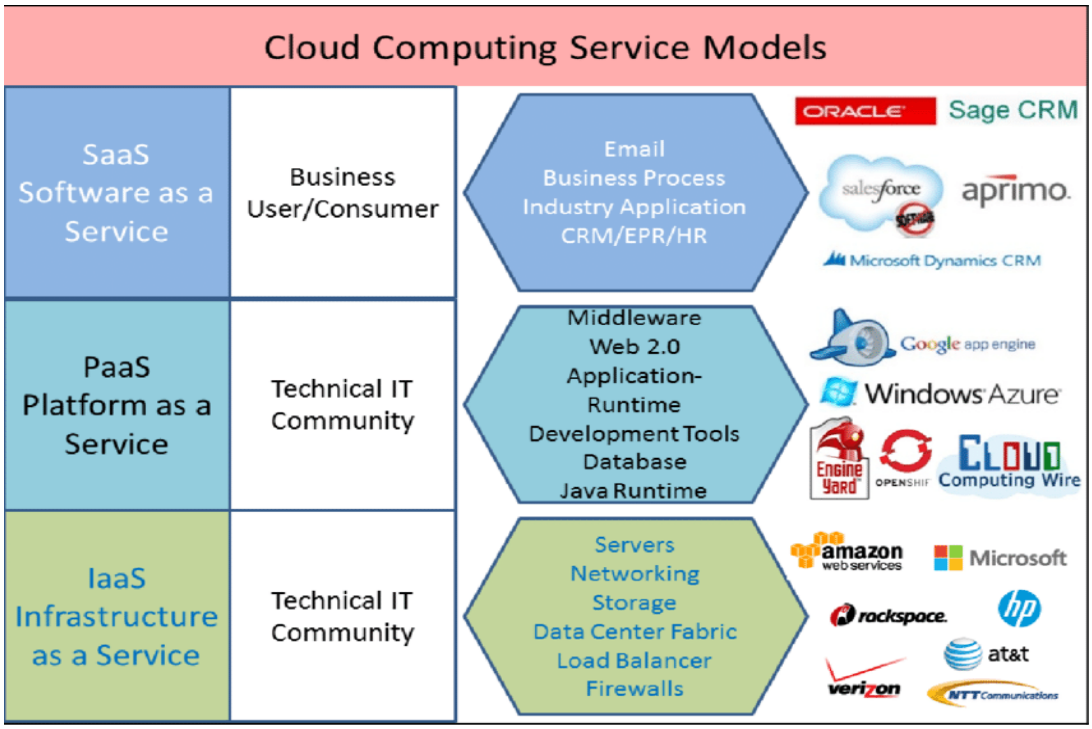
3.3. Υπολογιστικό Νέφος (Cloud Computing)

3.3.1 Ορισμός

Το υπολογιστικό νέφος είναι ένα μοντέλο που επιτρέπει την κατ' απαίτηση πρόσβαση μέσω του διαδικτύου σε ένα σύνολο υπολογιστικών πόρων (δικτύων, εφαρμογών, διακομιστών) που φιλοξενούνται σε ένα απομακρυσμένο κέντρο δεδομένων το οποίο κέντρο διαχειρίζεται ένας πάροχος υπηρεσιών υπολογιστικού νέφους (cloud services provider). Το υπολογιστικό νέφος παρέχει τη δυνατότητα της ανα πάσα στιγμής και πανταχού παρούσας πρόσβασης και αποθήκευσης πληροφοριών χωρίς να απαιτείται η προσφυγή στις φυσικές συσκευές ή στην παραδοσιακή υποδομή πληροφορικής (IT Infrastructure) ενώ παράλληλα προσφέρει πολλαπλά οφέλη όπως ενδεικτικά: επεκτασιμότητα και ευελιξία, εξοικονόμηση κόστους, πρόληψη απώλειας δεδομένων χάρη στη δυνατότητα δημιουργίας αντιγράφων ασφαλείας και αποκατάστασης καταστροφών [106].

3.2.1 Βασικά μοντέλα παροχής υπηρεσιών υπολογιστικού νέφους

Υπάρχουν τρία βασικά μοντέλα παροχής υπηρεσιών υπολογιστικού νέφους και ειδικότερα:[7]



Εικόνα 7 Διάκριση των μοντέλων παροχής υπηρεσιών του υπολογιστικού νέφους [154]

- Υποδομή ως Υπηρεσία (Infrastructure as a Service- IaaS)

Παρέχει την κατ΄ απαίτηση πρόσβαση σε θεμελιώδεις υπολογιστικούς πόρους (πχ εικονικούς απομακρυσμένους διακομιστές) και επιτρέπει στους τελικούς χρήστες να διαχειρίζονται κατάλληλα, ανάλογα με τις ανάγκες τους, την έκταση των πόρων των οποίων θα κάνουν χρήση, απαλλάσσοντας τους έτσι από υψηλές, προκαταβολικές δαπάνες καθώς και από κοστοβόρες και σε κάποιες περιπτώσεις, περιττές εγκαταστάσεις.

- Πλατφόρμα ως Υπηρεσία (Platform as a Service- PaaS)

Πρόκειται για ένα μοντέλο που δίνει τη δυνατότητα χρήσης μίας ολοκληρωμένης, κατα παραγγελία πλατφόρμας για την εκτέλεση, ανάπτυξη και διαχείριση εφαρμογών χωρίς την ανάγκη συντήρησης αυτής της πλατφόρμας σε τοπικές συσκευές. Στην πράξη, ο πάροχος του υπολογιστικού νέφους φιλοξενεί όλα τα συστατικά της πλατφόρμας ήτοι τους εξυπηρετητές, τον αποθηκευτικό χώρο, το λογισμικό, τις βάσεις δεδομένων στο δικό του κέντρο δεδομένων. Οι προγραμματιστές έτσι λαμβάνουν τα εργαλεία για να δημιουργήσουν, να κατασκευάσουν, να δοκιμάσουν, να συντηρήσουν, απομακρυσμένα, τις εφαρμογές τους σε ένα ήδη υπάρχον περιβάλλον back-end.

- Λογισμικό ως Υπηρεσία (Software as a Service- SaaS)

Πρόκειται για μοντέλο που παρέχει στους χρήστες τη δυνατότητα της διάθεσης και χρήσης διαφόρων υπηρεσιών εφαρμογών που φιλοξενούνται από τον πάροχο στο νέφος και είναι προσβάσιμες μέσω του Διαδικτύου και ειδικότερα μέσω προγραμμάτων περιήγησης ιστού. Οι χρήστες έτσι δε χρειάζεται να αγοράσουν κάποιο λογισμικό, αλλά στην πράξη καταβάλλουν ένα μηνιαίο ή ετήσιο αντίτιμο ή επιλέγουν την κοστολόγηση βάσει της πραγματικής χρήσης “pay-as-you-go”. Έτσι, επιδίωξή του παρόχου είναι οι υπηρεσίες αυτές να υποκαταστήσουν τις συμβατικές εφαρμογές που εγκαθιστούν οι χρήστες στα κατά τόπους συστήματά τους και, αντίστοιχα, να αναθέσουν τελικά οι χρήστες τα δεδομένα τους στον εξωτερικό πάροχο. Σε αυτήν την περίπτωση εντάσσονται, π.χ., συνήθεις διαδικτυακές

εφαρμογές γραφείου όπως λογιστικά φύλλα, εργαλεία επεξεργασίας κειμένου, ηλεκτρονικά μητρώα και ατζέντες, ημερολόγια κοινής χρήσης καθώς επίσης και εφαρμογές ηλεκτρονικού ταχυδρομείου μέσω υπολογιστικού νέφους [141]. Πέρα από τη δυνατότητα επιλογής περιορισμένων παραμέτρων των ρυθμίσεων των εφαρμογών που χρησιμοποιούν, οι χρήστες δεν μπορούν να ελέγξουν ούτε την ίδια την υποδομή του σύννεφου ούτε τις επιμέρους εφαρμογές, ενώ τα μέτρα ασφάλειας λαμβάνονται πρωτίστως από τον πάροχο [139].

3.2.2. Μοντέλα ανάπτυξης υπολογιστικού νέφους

Το υπολογιστικό νέφος επίσης διακρίνεται σε δημόσιο, ιδιωτικό και υβριδικό:

Στο δημόσιο, ο πάροχος υπηρεσιών νέφους καθιστά υπολογιστικούς πόρους διαθέσιμους στους χρήστες μέσω του δημόσιου δικτύου και οι πόροι αυτοί είναι προσβάσιμοι είτε δωρεάν είτε με ένα μοντέλο κοστολόγησης ανά συνδρομή ή χρήση. Ο πάροχος του δημόσιου νέφους κατέχει, διαχειρίζεται και αναλαμβάνει την ευθύνη για τα κέντρα δεδομένων, το υλικό και την υποδομή στα οποία εκτελούνται οι εντολές των χρηστών. Χαρακτηριστικά παραδείγματα δημόσιων νεφών είναι το Google Cloud και το Amazon Web Services (AWS).

Στο ιδιωτικό, όλες οι υποδομές και οι υπολογιστικοί πόροι είναι διαθέσιμοι και προσβάσιμοι από έναν μόνο πελάτη. Συνδυάζει τα οφέλη του δημοσίου νέφους ήτοι ελαστικότητα, ευκολία πρόσβασης σε συνδυασμό με τον έλεγχο πρόσβασης, την ασφάλεια και την προσαρμογή των υποδομών της εγκατάστασης. Το ιδιωτικό νέφος τις περισσότερες φορές φιλοξενείται στο κέντρο δεδομένων των εγκαταστάσεων του πελάτη, αλλά μπορεί επίσης να φιλοξενείται και στην υποδομή ενός ανεξάρτητου παρόχου ή κάποιου συνεργάτη αυτού.

Στο υβριδικό, συνδυάζονται στοιχεία τόσο από το δημόσιο όσο και από το ιδιωτικό νέφος με στόχο τη σύνδεση των ιδιωτικών υπηρεσιών νέφους ενός οργανισμού και των δημοσίων νεφών σε μια ενιαία, ευέλικτη υποδομή για την εκτέλεση των εφαρμογών και των εργασιών της εκάστοτε επιχείρησης.

3.3.3 Το υπολογιστικό νέφος στα πλαίσια του Smart Campus

Η ευρεία υιοθέτηση στα πλαίσια της έξυπνης πανεπιστημιούπολης, εφαρμογών που βασίζονται στη τεχνολογία του υπολογιστικού νέφους συμβάλει καταρχήν στην εξοικονόμηση κόστους και στην ορθότερη και αποτελεσματικότερη διαχείριση των διαθέσιμων χρημάτων καθώς επιτρέπει την κατ’ απαίτηση και

ανάλογη με τις εκάστοτε ανάγκες της πανεπιστημιακής κοινότητας πρόσβαση σε πόρους αντί της ανάγκης αγοράς και συντήρησης υλικού και λογισμικού [89].

Επιπλέον, το υπολογιστικό νέφος μπορεί να συμβάλει στην επίτευξη καλύτερης συνεργασίας μεταξύ φοιτητών και εκπαιδευτικού προσωπικού και τούτο διότι οι εφαρμογές που βασίζονται στο νέφος επιτρέπουν στους χρήστες να έχουν πρόσβαση και να μοιράζονται δεδομένα από οπουδήποτε, ανά πάσα στιγμή. Με τον τρόπο αυτό ακόμη και φοιτητές που βρίσκονται σε απομακρυσμένα σημεία της ευρύτερης πανεπιστημιούπολης έχουν πρόσβαση στο εκπαιδευτικό υλικό το οποίο βρίσκεται στη διάθεση τους ανά πάσα ώρα και στιγμή και αντίστοιχα οι καθηγητές μπορούν να κάνουν χρήση αυτού προκειμένου να αναρτούν σημειώσεις ή διαλέξεις τους χωρίς την ανάγκη συνεχούς φυσικής παρουσίας σε αίθουσες διδασκαλίας. [14]

Περαιτέρω, ενόψει της αρχιτεκτονικής της υποδομής του υπολογιστικού νέφους, παρέχονται αυξημένα επίπεδα διαχείρισης και ασφάλειας των πληροφοριών. Ειδικότερα, η τεχνολογία αυτή παρέχει τη δυνατότητα κρυπτογράφησης, αντιγραφής και ανάκτησης δεδομένων σε περίπτωση απώλειας ή καταστροφής τους με αποτέλεσμα να διαφυλάσσεται αποτελεσματικά η ακεραιότητα των δεδομένων και μάλιστα καλύτερα από ότι αν τα δεδομένα υπήρχαν αποθηκευμένα μόνο τοπικά σε κάποια μόνιμη εγκατάσταση [107].

Εν ολίγοις, η τεχνολογία του υπολογιστικού νέφους σε συνδυασμό και με ένα ευρύ φάσμα έτερων σύγχρονων τεχνολογιών που αναλύονται αμέσως κατωτέρω όπως η τεχνητή νοημοσύνη, η μηχανική μάθηση και η ανάλυση μεγάλων δεδομένων μπορούν να μεταμορφώσουν και να αναβαθμίσουν σημαντικά το επίπεδο των παρεχόμενων εκπαιδευτικών και εν γένει πανεπιστημιακών υπηρεσιών εντός της έξυπνης πανεπιστημιούπολης.

3.4.Τεχνητή Νοημοσύνη/Μηχανική Μάθηση/Ανάλυση Μεγάλων Δεδομένων

3.4.1 Έννοια Τεχνητής Νοημοσύνης

Ο όρος Τεχνητή Νοημοσύνη αναφέρεται στο πεδίο ανάπτυξης υπολογιστών και εν γένει μηχανών που είναι ικανές να αναπαράγουν τις γνωστικές λειτουργίες ενός ανθρώπου όπως η μάθηση, η κατανόηση, ο σχεδιασμός με αποτέλεσμα οι μηχανές αυτές να μπορούν να αναλύουν και να προσαρμόζουν τα δεδομένα για να αυτοματοποιούν εργασίες και να λαμβάνουν αποφάσεις [108].

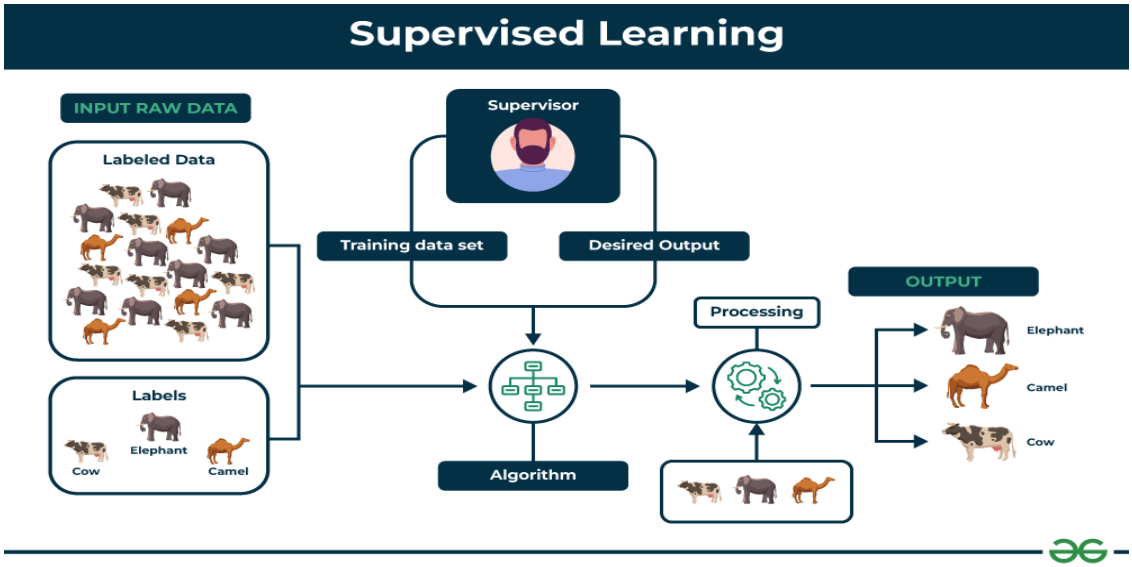
3.4.2 Έννοια Μηχανικής Μάθησης

Υποκατηγορία της τεχνητής νοημοσύνης αποτελεί η Μηχανική Μάθηση που πρόκειται στην ουσία για μία διαδικασία μετατροπής δεδομένων σε νέα γνώση συνήθως με τη μορφή ενός μαθηματικού μοντέλου (αλγορίθμου). Ετσι, στη Μηχανική Μάθηση χρησιμοποιούνται αλγόριθμοι που μπορούν να αναγνωρίζουν μοτίβα από δεδομένα, να μαθαίνουν από αυτά και να προβαίνουν σε ακριβέστερες προβλέψεις που ελαχιστοποιούν τον κίνδυνο σφάλματος με απώτερο σκοπό την λήψη ολοένα και καλύτερων αποφάσεων [108].

3.4.3 Τύποι Τεχνικών Μηχανικής Μάθησης

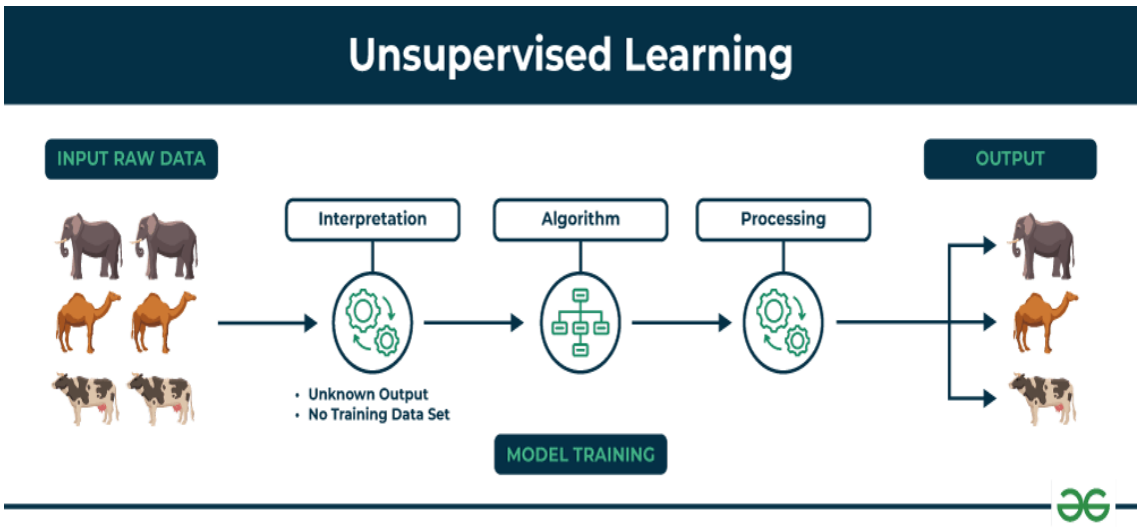
Η μηχανική μάθηση χρησιμοποιεί δύο τύπους τεχνικών με τις οποίες λειτουργεί [12,109]: την μάθηση με επίβλεψη και την μάθηση χωρίς επίβλεψη.

Στην μηχανική μάθηση με επίβλεψη ο αλγόριθμος λαμβάνει ένα γνωστό σύνολο δεδομένων εισόδου που συσχετίζονται με ένα γνωστό σύνολο δεδομένων εξόδου- αποκρίσεων που επιτρέπουν στο μοντέλο να μαθαίνει με την πάροδο του χρόνου. Για την εκμάθηση εννοιών, το σύστημα τροφοδοτείται με παραδείγματα που ανήκουν (θετικά παραδείγματα) ή δεν ανήκουν (αρνητικά παραδείγματα) στη συγκεκριμένη έννοια. Στη συνέχεια πρέπει να παραχθεί μία γενικευμένη περιγραφή της έννοιας δηλαδή να δημιουργηθεί ένα μοντέλο ώστε να είναι δυνατό στη συνέχεια να μπορεί να αποφασιστεί αν μία άγνωστη περίπτωση θα ανήκει ή όχι σε αυτή την έννοια. Η μηχανική μάθηση με επίβλεψη χρησιμοποιεί τεχνικές ταξινόμησης (classification) και τεχνικές παρεμβολής (regression). Οι τεχνικές ταξινόμησης ταξινομούν τα δεδομένα εισόδου σε κατηγορίες και είναι αποδοτικές στις περιπτώσεις που τα δεδομένα είναι τέτοιας φύσης που μπορούν να επισημανθούν, να κατηγοριοποιηθούν ή να διαχωριστούν σε συγκεκριμένες ομάδες ή κλάσεις (πχ γράμματα, αριθμοί). Οι τεχνικές παρεμβολής καθιστούν δυνατή την πρόβλεψη ενός αποτελέσματος (y) με βάση την τιμή μίας ή περισσοτέρων μεταβλητών πρόβλεψης (x) και είναι χρήσιμες και αποδοτικές για δεδομένα αριθμητικών τιμών όπως η θερμοκρασία, πρόβλεψη τιμής μετοχής.



Εικόνα 8 Παράδειγμα Μηχανικής Μάθησης με Επίβλεψη [32]

Στην μηχανική μάθηση χωρίς επίβλεψη ο αλγόριθμος εξάγει συμπεράσματα από σύνολα δεδομένων που εισάγονται σε αυτό και τα οποία όμως δεν αντιστοιχούν σε μία συγκεκριμένη έξοδο ήτοι πρόκειται για σύνολα δεδομένων χωρίς ετικέτα. Στην περίπτωση αυτή ο αλγόριθμος πρέπει να εντοπίσει από τα σύνολα δεδομένων χωρίς ετικέτα, τα κρυφά μοτίβα ή τις εγγενείς δομές αυτών και να τα ταξινομήσει. Σαν αποτέλεσμα του εντοπισμού προκύπτουν πρότυπα καθένα από τα οποία περιγράφει ένα μέρος από τα δεδομένα. Κατά τη διαδικασία αυτή ο αλγόριθμος χρησιμοποιεί κάποιους κανόνες συσχέτισης και στη συνέχεια προβαίνει στη διαδικασία της ομαδοποίησης (clustering) και την δημιουργία ομάδων δεδομένων ανάλογα με το βαθμό ομοιότητας αυτών.



Εικόνα 9 Παράδειγμα Μηχανικής Μάθησης χωρίς Επίβλεψη [32]

3.4.4 Έννοια και χαρακτηριστικά Μεγάλων Δεδομένων

Αξίζει στο σημείο αυτό να τονιστεί ότι η αποτελεσματική αξιοποίηση των δυνατότητων της μηχανικής μάθησης εξαρτάται άμεσα από την ύπαρξη των παραχθέντων με τη χρήση του Διαδικτύου των Πραγμάτων, Μεγάλων Δεδομένων. Ο όρος «Μεγάλα Δεδομένα» (Big Data) χρησιμοποιείται για να περιγράψει μεγάλα ή σύνθετα σύνολα δεδομένων προερχόμενα από διαφορετικές πηγές, τα οποία δεν είναι δεκτικά καταγραφής, αποθήκευσης και επεξεργασίας με τις παραδοσιακές τεχνικές επεξεργασίας [91]. Σύμφωνα δε με τον ορισμό της ανεξάρτητης ευρωπαϊκής ομάδας εργασίας για θέματα προστασίας της ιδιωτικής ζωής (Ομάδα εργασίας του άρθρου 29), τα μεγάλα δεδομένα αναφέρονται στον γιγαντιαίο όγκο ψηφιακών δεδομένων που τίθενται σε επεξεργασία από επιχειρήσεις, κρατικές αρχές και οργανισμούς, μέσω της χρήσης αλγόριθμων, με σκοπό την εξαγωγή νέων συμπερασμάτων και την αξιοποίηση πληροφοριών στο ύψιστο. Πρόκειται δηλαδή για μία κατηγορία δεδομένων που υφίσταται χάρη στην εξελισσόμενη ικανότητα της τεχνολογίας να υποστηρίζει όχι μόνο τη συλλογή και αποθήκευση μεγάλου όγκου δεδομένων, αλλά και την ανάλυση, κατανόηση και εκμετάλλευση της πλήρους αξίας των δεδομένων ιδίως με τη χρήση εφαρμογών ανάλυσης [122].

Τα Μεγάλα Δεδομένα φέρουν κατά βάση τα ακόλουθα χαρακτηριστικά γνωρίσματα [13]: όγκος, ποικιλία, ταχύτητα, ακρίβεια. Ειδικότερα: 1) Το χαρακτηριστικό του όγκου αναφέρεται στη μεγάλη ποσότητα δεδομένων που παράγονται και αποθηκεύονται, 2) Το χαρακτηριστικό της ποικιλίας αναφέρεται στο γεγονός ότι τα δεδομένα μπορεί να είναι πολλών διαφορετικών ειδών (δομημένα ή μη) και προερχόμενα από διάφορες πηγές (αισθητήρες, συσκευές), 3) Το χαρακτηριστικό της ταχύτητας αναφέρεται στην υψηλή ταχύτητα με την οποία παράγονται (ακόμη και σε πραγματικό χρόνο) και γίνεται επεξεργασία των δεδομένων, 4) Το χαρακτηριστικό της ακρίβειας αναφέρεται στην υψηλή ποιότητα και αξία των δεδομένων που συλλέγονται και αναλύονται.

3.4.5 Τεχνητή Νοημοσύνη και Μηχανική Μάθηση στο πλαίσιο του Smart Campus

Σε μία έξυπνη πανεπιστημιούπολη, στην οποία εξαίρετη θέση κατέχει η τεχνολογία του διαδικτύου των πραγμάτων, παράγονται εκατομμύρια δεδομένα το λεπτό από ποικίλης φύσεως πηγές (συσκευές IoT, αισθητήρες) τα οποία χρήζουν άμεσης αποθήκευσης και επεξεργασίας. Η ταχεία και αποτελεσματική διαχείριση

αυτών γίνεται με την βοήθεια των αλγορίθμων της τεχνητής νοημοσύνης και της μηχανικής μάθησης.

Ειδικότερα, ο αλγόριθμος της τεχνητής νοημοσύνης μπορεί να χρησιμοποιηθεί σε συστήματα βιντεοεπιτήρησης για την ανίχνευση προσώπων και αντικειμένων αλλά και για την ανίχνευση πιθανών απειλών με σκοπό την ενίσχυση και της ασφάλειας της πανεπιστημιούπολης [20]. Επίσης, μπορεί να χρησιμοποιηθεί και στον τομέα της εκπαίδευσης με την υιοθέτηση εκπαιδευτικών πλατφορμών και συστημάτων διδασκαλίας ικανών να παράσχουν εξατομικευμένο και προσωποποιημένο περιεχόμενο, να παρακολουθούν την πρόοδο και να προτείνουν συμπληρωματικό υλικό με βάση τις επιδόσεις κάθε φοιτητή [111].

Αντίστοιχα, με τα μοντέλα της Μηχανικής Μάθησης μπορεί να επιτευχθεί η ανάλυση και πρόβλεψη μελλοντικών καταστάσεων όπως πχ η πρόβλεψη της εγγραφής των φοιτητών, των επιδόσεων ενός φοιτητή, της χρήσης και κατανομής των φυσικών πόρων [110]. Τα μοντέλα μηχανικής μάθησης μπορούν επίσης να βελτιστοποιήσουν τη χρήση ενέργειας εντός των κτιρίων της πανεπιστημιούπολης, προσαρμόζοντας τα συστήματα φωτισμού, θέρμανσης και ψύξης με βάση τα πρότυπα χρήσης και τις καιρικές συνθήκες ενώ παράλληλα με τη συνεχή παρατήρηση και ομαδοποίηση των δεδομένων μπορούν να εντοπίσουν περιοχές και σημεία που χρήζουν βελτιστοποίησης.

Συμπερασματικά, σε μια έξυπνη πανεπιστημιούπολη, η Τεχνητή Νοημοσύνη σε συνδυασμό με την Μηχανική Μάθηση και την ανάλυση μεγάλων δεδομένων συνδράμουν στην αξιοποίηση της δύναμης των δεδομένων προς το σκοπό βελτίωσης του τρόπου λήψης αποφάσεων, της λειτουργικής αποδοτικότητας, της μάθησης και προώθησης ενός ασφαλέστερου και φιλικότερου περιβάλλοντος. Αυτή η σύγκλιση των τεχνολογιών συμβάλλει στην προώθηση της έννοιας της έξυπνης πανεπιστημιούπολης, καθιστώντας την ένα καινοτόμο και καθοδηγούμενο από τα δεδομένα εκπαιδευτικό οικοσύστημα.

ΚΕΦΑΛΑΙΟ 4– ΠΥΛΩΝΕΣ ΓΙΑ ΤΗΝ ΑΝΑΠΤΥΞΗ ΤΗΣ ΕΞΥΠΝΗΣ ΠΑΝΕΠΙΣΤΗΜΙΟΥΠΟΛΗΣ ΚΑΙ ΕΠΙΜΕΡΟΥΣ ΥΠΗΡΕΣΙΕΣ ΑΥΤΗΣ

Η έξυπνη πανεπιστημιούπολη, με αρωγούς της τις τεχνολογίες που αναλύθηκαν ανωτέρω, στοχεύει στο να παράσχει στην ευρύτερη ακαδημαϊκή κοινότητα, υψηλής ποιότητας υπηρεσίες που θα αναδείξουν την κοινωνική, περιβαλλοντολογική, οικονομική αλλά και ακαδημαϊκή της διάσταση.[15] Οι

υπηρεσίες αυτές μάλιστα, συμβαδίζοντας με την έννοια της έξυπνης πανεπιστημιούπολης, δεν μπορεί παρά να είναι ομοίως «έξυπνες». Με τον όρο «έξυπνες υπηρεσίες» νοούνται οι υπηρεσίες που έχουν ως βασικό τους στόχο την ελαχιστοποίηση της ανθρώπινης παρέμβασης και εν γένει την αυτοματοποίηση των διαδικασιών με σκοπό να βοηθήσουν τεχνολογικά τις καθημερινές ανθρώπινες λειτουργίες, αποτελώντας τη βελτιστοποιημένη εκδοχή των υπαρχόντων υπηρεσιών [16]. Βασικά χαρακτηριστικά γνωρίσματα των έξυπνων υπηρεσιών είναι η δυνατότητα αλληλεπίδρασης τους με δεδομένα από διαφορετικές πηγές (πχ. βάσεις δεδομένων, αισθητήρες) και η ενσωμάτωση τους σε ένα κοινό πλαίσιο, η προσαρμογή των λειτουργιών ανάλογα με τις ανάγκες και τις ειδικές συνθήκες παρέχοντας έτσι εξατομικευμένη εμπειρία στους χρήστες και τέλος η υιοθέτηση μίας προληπτικής προσέγγισης προβλέποντας τις ανάγκες των χρηστών και παρέχοντας τους αναγκαίες πληροφορίες εκ των προτέρων. [17]. Οι Akrif et al υποστηρίζουν ότι μεταξύ των χαρακτηριστικών των έξυπνων υπηρεσιών είναι και το ότι είναι επικεντρωμένες στο χρήστη, ανοικτές, πανταχού παρούσες, ολοκληρωμένες και προσαρμοστικές.[18]

Η έξυπνη πανεπιστημιούπολη, αποτελώντας μικρογραφία μίας έξυπνης πόλης κι όντας ένας ζωντανός και σύνθετος οργανισμός, αποτελείται από επιμέρους συστατικά/ κατηγορίες, στο πλαίσιο καθενός εκ των οποίων, παρέχονται και οι έξυπνες υπηρεσίες, όπως θα αναλυθούν και κατωτέρω. Οι κατηγορίες αυτές σύμφωνα με τους Noemie Chagnon – Lessard et al [19] είναι οι ακόλουθες: 1) Έξυπνο Περιβάλλον (Smart Environment), 2) Έξυπνη Κινητικότητα (Smart Mobility), 3) Έξυπνη Διαβίωση (Smart Living), 4) Έξυπνα Άτομα (Smart People), 5) Έξυπνη Διακυβέρνηση (Smart Governance) και 6) Έξυπνα Δεδομένα (Smart Data).

4.1 ΕΞΥΠΝΟ ΠΕΡΙΒΑΛΛΟΝ (SMART ENVIRONMENT)

4.1.1 Έξυπνο Δίκτυο (Smart Grid)

Σύμφωνα με τον B. Lamia et al [22] ένα έξυπνο δίκτυο αποτελείται από τα ακόλουθα στοιχεία: α) έξυπνους μετρητές οι οποίοι μετρούν την κατανάλωση ηλεκτρικής ενέργειας σε πραγματικό χρόνο και επικοινωνούν με το δίκτυο ηλεκτρικής ενέργειας, β) αισθητήρες που μετρούν στο δίκτυο παραμέτρους του ηλεκτρικού ρεύματος, όπως η τάση, η συχνότητα και η ισχύς, γ) Δίκτυα επικοινωνίας που επιτρέπουν την αμφίδρομη επικοινωνία μεταξύ των διαφόρων στοιχείων του δικτύου, δ) Συστήματα ελέγχου και διαχείρισης τα οποία παρακολουθούν και

ελέγχουν το ηλεκτρικό δίκτυο σε πραγματικό χρόνο, ε) Συστήματα αποθήκευσης ενέργειας όπως πχ μπαταρίες που χρησιμοποιούνται για την αποθήκευση της ενέργειας που παράγεται από ανανεώσιμες πηγές και να την απελευθερώνουν όταν είναι απαραίτητο, στ) Συστήματα διαχείρισης της ζήτησης που μειώνουν την κατανάλωση ηλεκτρικής ενέργειας σε περιόδους αιχμής ρυθμίζοντας έξυπνα τη ζήτηση, η) Έξυπνα δίκτυα διανομής που έχουν σχεδιαστεί για να επιτρέπουν την αποτελεσματικότερη και ακριβέστερη διανομή της ηλεκτρικής ενέργειας με τη χρήση ελέγχου και ρύθμισης συσκευών όπως έξυπνοι μετασχηματιστές, διακόπτες και ρυθμιστές τάσης. Το έξυπνο δίκτυο συνιστά ένα πολύπλοκο και διασυνδεδεμένο σύστημα που συνδυάζει διαφορετικές τεχνολογίες για να επιτρέψει την αποτελεσματική και ευέλικτη διαχείριση της ηλεκτρικής ενέργειας.

Το έξυπνο δίκτυο έχει το ρόλο του εξισορροπητή των ενεργειακών αποθεμάτων με σκοπό να διασφαλίσει την βέλτιστη χρήση της αποθηκευμένης ενέργειας σε συνάρτηση με τις ανάγκες της πανεπιστημιούπολης. Πιο συγκεκριμένα, οι έξυπνες πανεπιστημιουπόλεις συνήθως χρησιμοποιούν ένα κατανεμημένο σύστημα χαμηλής τάσης για την παροχή υπηρεσιών, παρέχοντας παράλληλα ευκαιρίες για ενεργειακή εξοικονόμηση και αποθήκευση ενέργειας. Οι συσκευές του Διαδικτύου των Πραγμάτων στην πανεπιστημιούπολη είναι σε θέση να λειτουργούν σε διάφορα επίπεδα ταχύτητας ανάλογα με το φορτίο με αποτέλεσμα το έξυπνο δίκτυο να υιοθετεί το κατάλληλο φορτίο και τη χαμηλότερη ταχύτητα των επεξεργαστών σε περιπτώσεις που ο φόρτος εργασίας είναι χαμηλός. Περαιτέρω, η χρήση ηλιακής ενέργειας επιτρέπει την προσαρμογή στις κλιματικές αλλαγές, ενώ η ενέργεια που παράγεται από ηλιακές κυψέλες (φωτοβολταϊκά) σε έξυπνους χώρους στάθμευσης χρησιμοποιείται για την τροφοδότηση φωτών και αισθητήρων που βρίσκονται στους χώρους αυτούς. Γενικότερα χάρη στις ηλιακές κυψέλες, είναι εφικτή η συλλογή ενέργειας καθ όλη τη διάρκεια μίας ηλιόλουστης ημέρας και η αποθήκευση της συλλεγόμενης ενέργειας για περαιτέρω χρήση σε διάφορες περιοχές της πανεπιστημιούπολης που χρήζουν ενέργειας και ιδίως τις βραδινές ώρες. [20]

Σύμφωνα με τους H. Talei et al [21], η βασικότερη λειτουργία ενός έξυπνου δικτύου είναι η παρακολούθηση και βελτιστοποίηση της ενέργειας σε πραγματικό χρόνο με τη χρήση προηγμένης υποδομής. Η τελευταία αποτελείται από διάφορα ετερογενή στοιχεία που παράγουν ποικίλους τύπους δεδομένων τα οποία καθίστανται υπό επεξεργασία από ένα σύστημα ενδιάμεσου λογισμικού έτσι ώστε να προκύψουν οι κατάλληλες πληροφορίες που προορίζονται για τις εφαρμογές του έξυπνου

δικτύου. Το σύστημα του ενδιάμεσου λογιστικού έχει ως ρόλο το φιλτράρισμα των περιττών δεδομένων που λαμβάνονται από αισθητήρες και άλλες συσκευές, την αποθήκευση των επεξεργασμένων δεδομένων ώστε να μπορούν να χρησιμοποιηθούν από οποιοδήποτε εφαρμογή καθώς και την παραγωγή κατάλληλων αποτελεσμάτων μετά τη συνάθροιση διαφορετικών δεδομένων από διαφορετικούς αισθητήρες. Στη συνέχεια, οι παραχθείσες πληροφορίες χρησιμοποιούνται από το σύστημα διαχείρισης ενέργειας το οποίο και ενορχηστρώνει το δίκτυο ώστε η ενέργεια να αξιοποιηθεί αποτελεσματικά.

4.1.2 Έξυπνη Διαχείριση Αποβλήτων (Smart Waste)

Ο τομέας των αποβλήτων αποτελεί έναν σημαντικό παράγοντα εκπομπής διοξειδίου του άνθρακα εντός μίας έξυπνης πανεπιστημιούπολης. Η χρήση προηγμένων τεχνολογιών, όπως το Διαδίκτυο των Πραγμάτων (IoT) και η τεχνητή νοημοσύνη (ΤΝ), μπορεί να συνδυαστεί με στόχο την υλοποίηση της έξυπνης διαχείρισης των αποβλήτων. Τα δεδομένα που συλλέγονται σε πραγματικό χρόνο από αισθητήρες, ανιχνευτές και ενεργοποιητές αναλύονται προκειμένου να επιτευχθεί αποτελεσματική και βέλτιστη συλλογή, ανακύκλωση και διάθεση των αποβλήτων.

Επί παραδείγματι, οι κάδοι στην έξυπνη πανεπιστημιούπολη είναι εξοπλισμένοι με ένα δίκτυο αισθητήρων που μετρά το βάρος και το επίπεδο απορριμμάτων μέσα σε αυτούς. Τα δεδομένα αυτά κοινοποιούνται σε πραγματικό χρόνο στα σχετικά τμήματα και στους αρμόδιους υπαλλήλους με στόχο τη λήψη κατάλληλων μέτρων που στοχεύουν στη μείωση του αποτυπώματος διοξειδίου του άνθρακα και στη μεγιστοποίηση των οικονομικών οφελών. Επιπλέον, αυτά τα δεδομένα μπορούν να κοινοποιούνται σε πραγματικό χρόνο και σε εταιρείες που δραστηριοποιούνται στον τομέα της ανακύκλωσης και της διαχείρισης αποβλήτων, προκειμένου να οργανώνουν λογικούς χρόνους συλλογής απορριμμάτων ή να υποστηρίξουν τους υπαλλήλους καθαρισμού στον σχεδιασμό καθαρισμού κατά παραγγελία. [23]

4.1.3 Έξυπνη Διαχείριση της Ενέργειας και Πανεπιστημιακή Περιβαλλοντική Παρακολούθηση (Smart Energy and Campus Environmental Monitoring)

Η ενεργειακή σπατάλη και η μη βιώσιμη παραγωγή και κατανάλωση ενέργειας έχουν σημαντικές επιπτώσεις στο περιβάλλον και αυξάνουν το λειτουργικό κόστος των πανεπιστημιουπόλεων. Προτείνεται λοιπόν η συλλογή ενέργειας από ανανεώσιμες πηγές καθώς και η παρακολούθηση και ο έλεγχος της χρήσης της

ενέργειας σε πραγματικό χρόνο. Αυτό επιτρέπει την έξυπνη διαχείριση, παρέχοντας καλύτερη κατανόηση της κατανάλωσης ενέργειας, προβλέποντας μελλοντικές αλλαγές και εξετάζοντας τρόπους εξοικονόμησης ενέργειας. Ένα ολοκληρωμένο σύστημα μπορεί να συνδράμει στη μέγιστη χρήση των ανανεώσιμων πηγών ενέργειας και στην ελαχιστοποίηση του ενεργειακού αποτυπώματος. Υπάρχουν επίσης μέθοδοι ανίχνευσης προβλημάτων και συστήματα παρακολούθησης ενέργειας σε πραγματικό χρόνο, χρησιμοποιώντας τεχνολογίες όπως το υπολογιστικό νέφος και οι τεχνικές επεξεργασίας μεγάλων δεδομένων. [23]

Ειδικότερα, οι Ren Hao Liu et al [24] ανέπτυξαν ένα έξυπνο σύστημα παρακολούθησης ενέργειας το οποίο παρακολουθεί σε πραγματικό χρόνο την ποσότητα της ηλεκτρικής ενέργειας που χρησιμοποιείται, προειδοποιεί εγκαίρως τους διαχειριστές των ηλεκτρικών συστημάτων σε περίπτωση ανίχνευσης κάποιας ανωμαλίας, αναλύει τα δεδομένα και παρέχει χρήσιμες πληροφορίες με σκοπό την εξοικονόμηση ενέργειας. Αντίστοιχα, οι Yu Weng et al [25] πρότειναν έναν αλγόριθμο ανίχνευσης ανωμαλιών δεδομένων ήτοι μοτίβων δεδομένων που δε συμμορφώνονται με την αναμενόμενη συμπεριφορά (μη φυσιολογικά), με τη βοήθεια της τεχνικής της βαθιάς μάθησης και με απώτερο σκοπό τον έλεγχο και τη μείωση της καταναλισκόμενης ενέργειας.

Αρωγοί στην προσπάθεια αποδοτικότερης διαχείρισης της ενέργειας είναι και οι επιμέρους εφαρμογές που έχουν υλοποιήσει ερευνητές, οι οποίες αντλώντας μέσω των αισθητήρων διάφορα περιβαλλοντολογικά δεδομένα ενημερώνουν σε πραγματικό χρόνο τους υπεύθυνους για την τρέχουσα κατάσταση που επικρατεί στους χώρους της πανεπιστημιούπολης ώστε να ληφθούν τα απαιτούμενα μέτρα εξοικονόμησης ενέργειας. Πιο συγκεκριμένα, η εφαρμογή AlmaMap συλλέγει από αισθητήρες που είναι τοποθετημένοι στο εσωτερικό της πανεπιστημιούπολης διάφορα περιβαλλοντικά δεδομένα όπως η θερμοκρασία, η υγρασία, η πίεση και τα αιωρούμενα σωματίδια και τα αναπαριστά σε ψηφιακούς χάρτες που είναι τοποθετημένοι σε διάφορα σημεία της πανεπιστημιούπολης ώστε οι χρήστες να ενημερώνονται σε πραγματικό χρόνο για τις επικρατούσες περιβαλλοντικές συνθήκες [65]. Η δε εφαρμογή USC AiR είναι μία εφαρμογή για κινητά τηλέφωνα η οποία εμφανίζει δεδομένα σχετικά με την ποιότητα του αέρα εντός της πανεπιστημιούπολης και η οποία αξιοποιεί την τεχνολογία της επαυξημένης πραγματικότητας για να εμπνεύσει τους χρήστες να συμβάλουν και οι ίδιοι στην μείωση της ατμοσφαιρικής ρύπανσης [67].

Οι Tarabieh et al. [66] σχεδίασαν και εγκατέστησαν στο εσωτερικό των κτηρίων της πανεπιστημιούπολης ψηφιακούς πίνακες απεικόνισης και ελέγχου των δεδομένων που σχετίζονται με την κατανάλωση ενέργειας οι οποίοι έχουν ως στόχο την καλλιέργεια της περιβαλλοντικής συνείδησης των μελών της πανεπιστημιακής κοινότητας. Η υποδομή των πινάκων απαρτίζεται από τρία επίπεδα: Στο πρώτο επίπεδο λαμβάνει χώρα η συλλογή των δεδομένων από το κεντρικό σύστημα παρακολούθησης της ηλεκτρικής ενέργειας της πανεπιστημιούπολης, στο δεύτερο επίπεδο τα δεδομένα φιλτράρονται, ταξινομούνται και δημιουργούνται επιμέρους θεματικές αναφορές και στο τρίτο επίπεδο τα επίμαχα δεδομένα μεταφορτώνονται μέσω ενός εισαγωγέα δεδομένων και αναπαρίστανται στους πίνακες σε μορφή γραφημάτων και κυκλικών διαγραμμάτων.

4.2 ΕΞΥΠΝΗ ΚΙΝΗΤΙΚΟΤΗΤΑ (SMART MOBILITY)

4.2.1 Έξυπνη Παρακολούθηση και Πλοήγηση εντός της πανεπιστημιούπολης

Η ενίσχυση των δυνατοτήτων κατανόησης και παρακολούθησης της κινητικότητας των ατόμων σε μια πανεπιστημιούπολη διευκολύνει τη βελτίωση των υφιστάμενων υποδομών, τον προγραμματισμό καθώς και τις προσφερόμενες υπηρεσίες.

Οι Toutouh j. et al [28] επικεντρώθηκαν στην ανάπτυξη ενός φυσικού - κυβερνητικού συστήματος παρακολούθησης των δρόμων της πανεπιστημιούπολης του Πανεπιστημίου της Μάλαγα το οποίο με τη βοήθεια του διαδικτύου των πραγμάτων λαμβάνει πληροφορίες από ασύρματες συσκευές και από το θόρυβο της πανεπιστημιούπολης και εν συνεχεία αξιοποιεί τις αντληθείσες πληροφορίες. Ειδικότερα με τη βοήθεια της τεχνολογίας της μηχανικής μάθησης και του προτεινόμενου εξελικτικού αλγορίθμου, από τις καταγραφείσες από το σύστημα πληροφορίες, κατέστη εφικτή η εξαγωγή μοτίβων κινητικότητας καθώς και η πρόβλεψη της ροής της οδικής κυκλοφορίας, μειώνοντας παράλληλα τον όγκο των δεδομένων που απαιτούνται για τη δημιουργία της πρόβλεψης.

Οι Torres Sospedra J. et al [29] με γνώμονα ότι η γνώση της πραγματικής θέσης του χρήστη είναι ιδιαίτερα σημαντική για την κατανόηση της κινητικότητας στο πλαίσιο μίας πανεπιστημιούπολης, ανέπτυξαν ένα σύστημα εντοπισμού θέσης σε εσωτερικούς χώρους που συνδυάζεται και ενσωματώνεται σε ένα σύστημα εντοπισμού θέσης σε εξωτερικούς χώρους για την υποστήριξη απρόσκοπτης

πλοήγησης σε εσωτερικούς και εξωτερικούς χώρους και εύρεσης της ζητούμενης διαδρομής.

Ενόψει δε της πανδημίας του κορωνοϊού COVID-19 και της συνακόλουθης υποχρέωσης των πολιτών να φορούν την μάσκα τους, οι G.Y Shien at al [46] πρότειναν μία μέθοδο ανίχνευσης μάσκας προσώπου μέσω του κλειστού κυκλώματος καμερών παρακολούθησης μίας πανεπιστημιούπολης προκειμένου να εντοπίζονται αυτόματα οι φοιτητές που δε φορούν τη μάσκα προστασίας τους. Για να επιτευχθεί αυτό χρησιμοποιήθηκε ένα Συνελικτικό Νευρωνικό Δίκτυο (CNN) το οποίο μπορούσε να αναγνωρίσει προηγμένα χαρακτηριστικά προσώπου αλλά και χαρακτηριστικά διαφόρων τύπων μάσκας, καθότι είχε εκπαιδευτεί προς τούτο με τη τεχνολογία της μηχανικής μάθησης και ειδικότερα μέσα από σύνολα δεδομένων με αποτέλεσμα να δίνει ακριβή αποτελέσματα. Οι ερευνητές επισημαίνουν μάλιστα ότι χρησιμοποίησαν αντί των απλών καμερών, ένα κλειστό σύστημα καμερών παρακολούθησης (CCTV) καθότι οι κάμερες αυτές είναι ικανές να εντοπίζουν το Σημείο Ενδιαφέροντος υπερνικώντας τα πιθανά εμπόδια που προκύπτουν κατά την ανίχνευση (πχ δέντρα, αντικείμενα, κλπ.). ενώ παράλληλα τα συστήματα αυτά διαθέτουν υψηλότερη ανάλυση και μπορούν να μεταφέρουν γρηγορότερα και αποτελεσματικότερα το υλικό μέσω του διαδικτύου.

4.2.2 Έξυπνη Διαχείριση των θέσεων στάθμευσης (Car Parking)

Ένα από τα προβλήματα που αντιμετωπίζουν τα μέλη της ευρύτερης ακαδημαϊκής κοινότητας είναι η εύρεση διαθέσιμου χώρου στάθμευσης εντός της πανεπιστημιούπολης με αποτέλεσμα τη σπατάλη χρόνου και καυσίμου ειδικά σε ώρες αιχμής. Με την βοήθεια ενός συστήματος έξυπνης διαχείρισης των θέσεων στάθμευσης το οποίο παρέχει πληροφορίες στους χρήστες σε πραγματικό χρόνο σχετικά με τις ελεύθερες θέσεις στάθμευσης επιδιώκεται τόσο η διευκόλυνση των χρηστών όσο και η μέγιστη κατάληψη των κενών θέσεων στάθμευσης.

Ειδικότερα, οι Pandey D. και Hanchate S. [26] πρότειναν τη δημιουργία ενός συστήματος έξυπνης στάθμευσης χρησιμοποιώντας την θεωρία των «ουρών αναμονής» (queuing theory) και του διαδικτύου των πραγμάτων το οποίο παρέχει σε πραγματικό χρόνο πληροφορίες περί της διαθεσιμότητας των κενών θέσεων στάθμευσης. Το σύστημα αυτό λειτουργεί ως εξής: Κάθε διαπιστευμένος χρήστης συνδέεται μέσω του κινητού τηλεφώνου του στην διαδικτυακή εφαρμογή. Η εφαρμογή αυτή παρέχει στους χρήστες πληροφορίες σχετικά με τη διαθεσιμότητα

των κενών θέσεων στάθμευσης, τις οποίες έχει αντλήσει από τα δεδομένα των αισθητήρων τα οποία αποθηκεύονται και αποστέλλονται στη κεντρική βάση δεδομένων. Επίσης μέσω της εφαρμογής ο χρήστης μπορεί να προβεί σε κράτηση θέσης στάθμευσης η οποία του προτείνεται με κριτήριο την εγγύτητα αυτής σε σχέση με το που βρίσκεται ο ίδιος. Προκειμένου δε να επιτευχθεί ο μέγιστος βαθμός απόδοσης του συστήματος αυτού και για την καλύτερη εμπειρία των χρηστών προτείνεται και η αξιοποίηση της θεωρίας των ουρών αναμονής. Η θεωρία προτείνει λύσεις για τη βελτιστοποίηση της κατανομής των θέσεων στάθμευσης, την ελαχιστοποίηση των χρόνων αναμονής και τη βελτίωση της συνολικής αποδοτικότητας. Έτσι, κατά τη διάρκεια των ωρών αιχμής, εφαρμόζεται ένα σύστημα κατανομής βάσει προτεραιότητας. Αυτό σημαίνει ότι οι χρήστες κατηγοριοποιούνται βάσει ορισμένων κριτηρίων και σε όσους έχουν προτεραιότητα παρέχεται προνομιακή μεταχείριση όσον αφορά την κατανομή των θέσεων στάθμευσης. Επιπρόσθετα, μέσω της ανάλυσης των ιστορικών δεδομένων προσδιορίζονται στατιστικές παράμετροι όπως ο ρυθμός μεταξύ των αφίξεων (ο μέσος χρόνος μεταξύ των αφίξεων των οχημάτων) και ο ρυθμός εξυπηρέτησης (ο μέσος χρόνος που απαιτείται για την εξυπηρέτηση ενός οχήματος). Το σύστημα στάθμευσης μοντελοποιείται στη συνέχεια ως σύστημα πολλαπλών διακομιστών με πολλαπλές ουρές αναμονής, βάσει στατιστικών παραμέτρων όπως ο χρόνος που χρειάζεται κάθε όχημα για να σταθμεύσει, ο μέσος χρόνος αναμονής σε μια ουρά, η μέση χωρητικότητα κάθε διακομιστή κ.λπ. Σε αυτό το πλαίσιο, κάθε χώρος στάθμευσης μπορεί να θεωρηθεί διακομιστής. Τα οχήματα που περιμένουν να σταθμεύσουν θεωρούνται ότι βρίσκονται σε «ουρές αναμονής». Κάθε χώρος στάθμευσης (διακομιστής) έχει τη δική του ουρά, όπου τα οχήματα περιμένουν τη σειρά τους για στάθμευση.

Αντίστοιχα, οι Yoanes Bandung et al [27] σχεδίασαν και ανέπτυξαν ένα βασισμένο στη τεχνολογία του διαδικτύου των πραγμάτων, έξυπνο σύστημα στάθμευσης για τη βελτιστοποίηση της διαχείρισης των χώρων στάθμευσης στην πανεπιστημιούπολη. Το σύστημα αυτό αντιμετωπίζει διάφορα ζητήματα στάθμευσης στην πανεπιστημιούπολη παρέχοντας πληροφορίες σε πραγματικό χρόνο και προβλέψεις για το ποσοστό κατάληψης των θέσεων στάθμευσης. Επιπλέον, προσφέρει συστάσεις για τις διαθέσιμες θέσεις στάθμευσης, τις συντομότερες διαδρομές προς αυτές, καθώς και τις θέσεις εξόδου. Επιπλέον, παρακολουθεί την καθαριότητα των χώρων στάθμευσης και τιμολογεί αυτόματα το κόστος – αντίτιμο

μέσω ανίχνευσης των πινακίδων των οχημάτων. Οι ερευνητές επισημαίνουν ότι οι εξαχθείσες πληροφορίες από τους αισθητήρες και τους ενεργοποιητές θα είναι περαιτέρω επεξεργάσιμες με τη χρήση της μηχανικής μάθησης, έτσι ώστε οι χρήστες να είναι σε θέση με τη βοήθεια μίας εφαρμογής για κινητά τηλέφωνα να σταθμεύουν το όχημα τους γρηγορότερα και αποτελεσματικότερα.

4.3 ΕΞΥΠΝΗ ΔΙΑΒΙΩΣΗ (SMART LIVING)

4.3.1 Εξατομικευμένες υπηρεσίες για τη βελτίωση της καθημερινότητας

Βασικό χαρακτηριστικό γνώρισμα μίας έξυπνης πανεπιστημιούπολης είναι και η παροχή εξατομικευμένων υπηρεσιών, με προσαρμοσμένες στις εκάστοτε ανάγκες, προτιμήσεις και συμπεριφορές των μελών της πανεπιστημιακής κοινότητας, παροχές και εμπειρίες. Για την παροχή εξατομικευμένων και κατάλληλων ανά άτομο υπηρεσιών λαμβάνονται υπόψη διάφορα προσωπικά δεδομένα του όπως πχ η τοποθεσία, η IP της συσκευής του, τα οποία συλλέγονται και μέσα από τα οποία επιχειρείται η δημιουργία μοτίβων για την καλύτερη κατανόηση των καθημερινών συνηθειών και αναγκών του κάθε χρήστη και κατ' επέκταση για την βελτίωση της καθημερινότητας του.

Οι De Paola et al [30] πρότειναν τη δημιουργία ενός συστήματος ανίχνευσης των σημείων ενδιαφέροντος των χρηστών δια της παρακολούθησης των ιχνών τους από τα κινητά τους τηλέφωνα με στόχο την παροχή εξατομικευμένων υπηρεσιών και ψηφιακής προσωποποιημένης βοήθειας. Το σύστημα αυτό αξιοποιεί τις τεχνικές της εποπτευόμενης και μη εποπτευόμενης μηχανικής μάθησης με αποτέλεσμα να μπορεί να χειρίζεται διάφορα δεδομένα και να αντλεί πληροφορίες από αυτά και από την παλιότερη συμπεριφορά του χρήστη ώστε να εξάγει «γνώση» για αυτόν και συνεπώς να του προτείνει πιο στοχευμένες υπηρεσίες.

Αντίστοιχα, οι Manquele et al [31] πρότειναν τη χρήση ενός αλγορίθμου βασισμένου στο περιεχόμενο ο οποίος λαμβάνοντας υπόψη τις προτιμήσεις και τις ανάγκες των χρηστών, τους προτείνει τις κατάλληλες υπηρεσίες έχοντας προηγουμένως κάνει αντιστοίχιση του προφίλ της υπηρεσίας και του προφίλ του χρήστη. Έτσι και οι Zhang S. et al [61] χρησιμοποίησαν την τεχνολογία του WiFi για να δημιουργήσουν προφίλ χρηστών με βάση την παρακολούθηση των κινήσεων των φοιτητών. Στόχος τους ήταν να αναλύσουν τα μοτίβα κινητικότητας των φοιτητών, όπως οι καθημερινοί περίπατοι, οι δραστηριότητες και οι κοινωνικές

αλληλεπιδράσεις, με σκοπό τη βελτιστοποίηση των παρεχόμενων υπηρεσιών και την προσαρμογή τους στις ανάγκες και προτιμήσεις των φοιτητών.

4.3.2 Γεωεντοπισμός και ενίσχυση της ασφάλειας των χρηστών εντός της πανεπιστημιούπολης

Ο προσδιορισμός της θέσης των χρηστών για υπηρεσίες που λαμβάνουν υπόψη το περιβάλλον προϋποθέτει την εφαρμογή μεθόδων εντοπισμού τόσο σε εσωτερικούς όσο και σε εξωτερικούς χώρους, όπως οι ραδιοφάροι και το GPS. Αυτή η διαδικασία είναι ουσιώδης όχι μόνο για την παροχή υπηρεσιών πλοήγησης, αλλά και για την ενίσχυση της ασφάλειας εντός της πανεπιστημιούπολης.

Ο Θεόδωρος Αναγνωστόπουλος [20] πρότεινε την υλοποίηση ενός έξυπνου συστήματος χωροχρονικής αυθεντικοποίησης. Το εν λόγω σύστημα λειτουργεί με τη μέθοδο ταυτοποίησης των χρηστών (φοιτητών, καθηγητών, λοιπού ακαδημαϊκού προσωπικού) μέσω ενός αναγνωριστικού το οποίο παράγεται με βάση ένα χωροχρονικό ιστορικό που σχετίζεται με έναν ορισμένο έξυπνο μεμονωμένο χρήστη πανεπιστημιούπολης και το οποίο ταυτοποιεί μοναδικά αυτόν. Υπάρχουν πολλές περιπτώσεις στις οποίες απαιτείται έλεγχος ταυτότητας των χρηστών όπως πχ. για την παροχή πρόσβασης σε μία τοποθεσία, για την παροχή πρόσβασης σε ευαίσθητα προσωπικά δεδομένα που είναι αποθηκευμένα σε ένα υπολογιστικό σύστημα. Συνήθως ο έλεγχος ταυτότητας γίνεται με την αποστολή κωδικών γρήγορης απόκρισης (QR codes) σε μία έξυπνη συσκευή του χρήστη. Οι κωδικοί χρησιμοποιούνται μία φορά για την εκτέλεση μίας συγκεκριμένης ενέργειας, πλην όμως οι κωδικοί αυτοί δεν παρέχουν υψηλής κλίμακας επίγνωση του πλαισίου ασφαλείας της ταυτότητας του χρήστη διότι δεν είναι δυνατό να διακριθεί εάν το άτομο που χρησιμοποιεί τον κωδικό γρήγορης απόκρισης είναι πράγματι ο εξουσιοδοτημένος χρήστης ή κάποιος άλλος που πιθανώς να έχει υποκλέψει τον κωδικό. Για το λόγο αυτό, ο Θ. Αναγνωστόπουλος προτείνει η ταυτοποίηση των χρηστών γίνεται μέσω των χωροχρονικών δεδομένων τους όπως αυτά αντλούνται από πολλαπλά συστήματα με τα οποία αλληλεπιδρά ο κάθε χρήστης (δίκτυα κλειστού κυκλώματος τηλεόρασης, δίκτυα μικροφώνων, δίκτυα ρομποτικών συστημάτων ασφαλείας). Αυτά τα δεδομένα χρησιμοποιούνται για την δημιουργία ενός χωροχρονικού δακτυλικού αποτυπώματος με το οποίο γίνεται η επαλήθευση της ταυτότητας κάθε χρήστη και η ανίχνευση μη φυσιολογικής και απροσδόκητης συμπεριφορά. Συγκεκριμένα, ο χρήστης παρακολουθείται διαδικτυακά σε πραγματικό

χρόνο από μια συσκευή εντοπισμού που διαθέτει παγκόσμιο σύστημα εντοπισμού θέσης (GPS), έτσι ώστε να του χορηγείται πρόσβαση εντός της πανεπιστημιούπολης μόνο εάν οι κινήσεις του είναι σύμφωνες με το χωροχρονικό αποτύπωμα του. Αντίθετα, οποιαδήποτε απόκλιση από το χωροχρονικό αποτύπωμα μπορεί να υποδηλώνει εισβολή στην περιοχή της έξυπνης πανεπιστημιούπολης.

Οι Kwon D. et al [33] πρότειναν ένα σύστημα ασφαλείας των πυλών μίας έξυπνης πανεπιστημιούπολης στο οποίο εφαρμόζεται ο έλεγχος ταυτοποίησης δύο παραγόντων, τόσο μέσω της ταυτότητας των χρηστών (ID card) όσο και μέσω της αναγνώρισης προσώπου. Η ταυτοποίηση με βάση την ταυτότητα έχει πολύ υψηλή ακρίβεια και χαμηλή πολυπλοκότητα, αλλά ενέχει τον κίνδυνο κλοπής της ταυτότητας και αντιγραφής της. Αντίθετα, η αναγνώριση προσώπου, δηλαδή ο έλεγχος ταυτότητας με βάση βιομετρικά δεδομένα, έχει χαμηλότερη ακρίβεια και πολύ υψηλή πολυπλοκότητα. Συνδυάζοντας αυτές τις μεθόδους ελέγχου ταυτότητας, η προτεινόμενη στο σύστημα μέθοδος μειώνει τον κίνδυνο κλοπής της ταυτότητας και διατηρεί υψηλή την ακρίβεια της ταυτοποίησης. Στην πράξη για την αναγνώριση προσώπων, μία κάμερα που έχει τοποθετηθεί στην πύλη ανιχνεύει καταρχάς τα πρόσωπα των επισκεπτών. Οι καταγραφόμενες εικόνες αποθηκεύονται σε ένα διακομιστή πρωτοκόλλου μεταφοράς αρχείων και εν συνεχεία προωθούνται στις πλατφόρμες υπηρεσιών αναγνώρισης προσώπου μέσω του διαδικτύου των πραγμάτων.

Σε αντίστοιχη περίπτωση, οι Baswaraj Gadgay et al [34] σχεδίασαν ένα αυτοματοποιημένο ρομπότ παρακολούθησης της κινητικότητας και των συναφών διαδρομών εντός της πανεπιστημιούπολης το οποίο βρίσκεται σε απομακρυσμένη τοποθεσία αλλά μπορεί να επιβλέπει και να παρακολουθεί σε πραγματικό χρόνο τις εγκαταστάσεις της πανεπιστημιούπολης για την ανίχνευση τυχόν ύποπτων δραστηριοτήτων. Ένα σημαντικό χαρακτηριστικό που διαθέτει το σύστημα αυτό είναι η δυνατότητα ανίχνευσης ανθρώπου μαζί με τη λήψη εικόνας, με αποτέλεσμα όχι μόνο να ανιχνεύει και να καταγράφει την εικόνα ενός αγνώστου προσώπου αλλά και να προειδοποιεί τον υπεύθυνο ασφαλείας για μία πιθανή, μη εξουσιοδοτημένη προσπάθεια εισόδου στην πανεπιστημιούπολη.

4.4 ΕΞΥΠΝΗ ΕΚΠΑΙΔΕΥΣΗ (SMART EDUCATION) ΚΑΙ ΕΞΥΠΝΑ ΑΤΟΜΑ (SMART PEOPLE)

Η θεμελιωδέστερη υπηρεσία κάθε πανεπιστημιακού ιδρύματος τυγχάνει η εκπαίδευση η οποία με την συνεχή εξέλιξη της τεχνολογίας αποκτά μία νέα διάσταση,

πλήρως εναρμονισμένη με τα καινούρια δεδομένα. Η ενσωμάτωση της τεχνολογίας στη διαδικασία της εκπαίδευσης έχει δημιουργήσει μια εκπαιδευτική εμπειρία που υπερβαίνει τα παραδοσιακά πλαίσια. Οι φοιτητές έχουν πρόσβαση σε πλούσιο ψηφιακό εκπαιδευτικό υλικό, διαδραστικά μαθήματα και εκπαιδευτικά παιχνίδια που ενισχύουν την κατανόηση. Από την άλλη πλευρά, το εκπαιδευτικό προσωπικό προκειμένου να βελτιώσει όπως μαθησιακές εμπειρίες των φοιτητών στοχεύει στην σταδιακή μεταμόρφωση των φοιτητών σε «έξυπνους ανθρώπους». Το χαρακτηριστικό γνώρισμα των έξυπνων ανθρώπων δεν αφορά μόνο στην ικανότητά τους να αποκτούν γνώση μέσω της τεχνολογίας, αλλά και στη δυνατότητά να τη χρησιμοποιούν εποικοδομητικά για την επίλυση προβλημάτων και την εφεύρεση καινοτόμων λύσεων. Οι έξυπνοι άνθρωποι σε μια έξυπνη πανεπιστημιούπολη αξιοποιούν τις τεχνολογίες αιχμής για τη δημιουργία ενεργών κοινοτήτων και την ανταλλαγή ιδεών, δίνοντας ιδιαίτερη έμφαση στην ανάπτυξη δεξιοτήτων όπως η κριτική σκέψη και η δημιουργικότητα.

4.4.1 Καινοτόμες μέθοδοι διδασκαλίας

Στο πλαίσιο μίας έξυπνης πανεπιστημιούπολης, εφαρμόζονται καινοτόμες μέθοδοι διδασκαλίας οι οποίες αξιοποιούν προηγμένες τεχνολογίες και παιδαγωγικές προσεγγίσεις για τη δημιουργία δυναμικών και ελκυστικών μαθησιακών εμπειριών.

4.4.1.2 Gamification και Διδασκαλία σε περιβάλλον Εικονικής/Επαυξημένης Πραγματικότητας

Οι Chandra et al [35] με σκοπό να εγείρουν το ενδιαφέρον συμμετοχής ολοένα και περισσότερων φοιτητών σε δραστηριότητες που προωθούν την ανάπτυξη και βελτίωση της καθημερινότητας των μελών της πανεπιστημιούπολης τους, πρότειναν την δημιουργία ενός παιχνιδιού όπου οι χρήστες κάθε φορά που επιτυγχάνουν ένα επιθυμητό επίπεδο σε μία συγκεκριμένη δεξιότητα (soft skill) κερδίζουν ένα ηλεκτρονικό σήμα επιβράβευσης, ανεβαίνοντας επίπεδα.

Αντίστοιχα, οι Ms.N.Deepika et al [36] πρότειναν τη δημιουργία μίας εφαρμογής που δίνει κίνητρο στους φοιτητές να προβαίνουν σε δραστηριότητες που εκφεύγουν των καθημερινών τους ασχολιών. Τέτοιες είναι ενδεικτικά η εθελοντική εργασία, οι εκδηλώσεις κοινωνικής υπηρεσίας, η συμμετοχή σε πολιτιστικά ή αθλητικά γεγονότα, και άλλες εκπαιδευτικές εκτός της συνηθισμένης ακαδημαϊκής δραστηριότητας εμπειρίες. Η εφαρμογή αυτή αναμένεται να ενθαρρύνει τους φοιτητές να συμμετέχουν σε δραστηριότητες που ενισχύουν τις γενικές τους

δεξιότητες, προωθούν τη συνεργασία, και προσφέρουν ευκαιρίες για προσωπική ανάπτυξη. Στην πραγματικότητα, υπάρχει ένας πίνακας κατάταξης ανάλογα με την απόδοση των φοιτητών. Η εφαρμογή αποτελείται από πολλά επίπεδα και φέρει σταδιακό ξεκλείδωμα αυτών καθώς επίσης και ανταμοιβή ανά επίπεδο (κονκάρδες, νομίσματα).

Οι Chamba-Eras, L. et al [37] μελέτησαν τα αποτελέσματα της χρήσης της επαυξημένης πραγματικότητας στο πλαίσιο της εκπαιδευτικής διδασκαλίας η οποία περιελάμβανε πχ εικονικά μοντέλα ορισμένων πολύπλοκων δομών, εικονικά μοντέλα που αναπαράγουν ήχους, «μαγικούς» καθρέφτες, «μαγικά» παράθυρα και πόρτες, «μαγικά» γυαλιά. Παρατηρήθηκε ότι οι φοιτητές παρουσίαζαν υψηλότερη συγκέντρωση, προσοχή, ενδιαφέρον και κίνητρα συμμετοχής στο μάθημα. Ακόμη, παρατηρήθηκε βελτίωση της συνεργατικής διαδικασίας μάθησης, υψηλότερη κατανόηση του περιεχομένου και υψηλότερη διαδραστικότητα φοιτητών και καθηγητών.

Οι S. AlAwadhi et al [38] ανέπτυξαν μία εφαρμογή που λειτουργεί με τη τεχνολογία της εικονικής πραγματικότητας με στόχο να καταστήσουν την εκπαιδευτική διαδικασία πιο διαδραστική και πιο αποτελεσματική. Χάρη στην εφαρμογή αυτή οι φοιτητές είχαν τη δυνατότητα να πραγματοποιούν εικονικά πειράματα αλλά και να παρακολουθούν παγκοσμίως άλλα πειράματα με τη χρήση ειδικού εξοπλισμού, να παρακολουθούν τα μαθήματα με τη χρήση κάμερας αλλά και να έχουν πρόσβαση ανά πάσα ώρα και στιγμή στα ηχογραφημένα και βιντεοσκοπημένα μαθήματα.

4.4.1.3 Πανταχού παρούσα και Εξατομικευμένη Μάθηση

Ένα από τα βασικά χαρακτηριστικά μοντέλα μάθησης που συναντώνται στις έξυπνες πανεπιστημιουπόλεις είναι αυτό της πανταχού παρούσας μάθησης (U-Learning) το οποίο επιτρέπει στους εκπαιδευόμενους να αποκαλύπτουν ποικίλα περιβάλλοντα και να χρησιμοποιούν τις διάφορες αλληλεπιδράσεις μεταξύ αυτών και των έξυπνων συσκευών για τη διαμόρφωση του περιβάλλοντος εκπαίδευσης, μέσα από το οποίο μπορούν να αποκτήσουν το σωστό εκπαιδευτικό περιεχόμενο και να επιτύχουν την αυτομάθηση την στιγμή που επιθυμούν. Βασικά πλεονεκτήματα του μοντέλου αυτού είναι ότι: 1) Το σύστημα ανιχνεύει συνεχώς την τοποθεσία και το περιβάλλον του φοιτητή και αποθηκεύει τις πληροφορίες στη βάση δεδομένων, 2) Βάσει της κατάστασης του περιβάλλοντος, παρέχει επαρκείς πληροφορίες

οποτεδήποτε και από οποιαδήποτε τοποθεσία, 3) Το σύστημα είναι ανεξάρτητο από αλλαγές σε ένα δίκτυο ενώ ο χρήστης κινείται, 4) Το σύστημα προσαρμόζεται στις απαιτήσεις της πλατφόρμας που χρησιμοποιεί ο φοιτητής, 5) Ο φοιτητής δεν χάνει ποτέ την εργασία και την πρόοδο του· αυτή αποθηκεύεται μόνιμα στη βάση δεδομένων. [45].

Παρατίθεται μάλιστα ένας συγκριτικός πίνακας [47] των χαρακτηριστικών των 3 μεθόδων εκπαίδευσης ήτοι του Ubiquitous Learning (U-Learning), του Mobile Learning (M-Learning) καθώς και του Electronic Learning (E-Learning) από τον οποίο προκύπτουν τα συντριπτικά πλεονεκτήματα του U-Learning έναντι των υπολοίπων μεθόδων τα οποία δικαιολογούν και την ευρεία εφαρμογή του στο πλαίσιο της έξυπνης πανεπιστημιούπολης:

Κριτήρια	u-learning	m-learning	e-learning
Έννοια	Μαθαίνεις το σωστό πράγμα την σωστή στιγμή και με τον σωστό τρόπο.	Μαθαίνεις στο σωστό χρόνο και στη σωστή στιγμή.	Μαθαίνεις στη σωστή στιγμή.
Μονιμότητα	Οι εκπαιδευόμενοι δε χάνουν ποτέ τις εργασίες τους.	Οι εκπαιδευόμενοι πιθανώς να χάσουν τις εργασίες τους.	Οι εκπαιδευόμενοι πιθανώς να χάσουν τις εργασίες τους.
Πρόσβαση	Πρόσβαση στο σύστημα μέσω των πανταχού παρουσών τεχνολογιών.	Πρόσβαση στο σύστημα μέσω ασύρματων δικτύων.	Πρόσβαση στο σύστημα μέσω του δικτύου των υπολογιστών.
Αμεσότητα	Οι εκπαιδευόμενοι λαμβάνουν αμέσως πληροφορίες.	Οι εκπαιδευόμενοι λαμβάνουν αμέσως πληροφορίες αλλά μόνο σε συγκεκριμένα περιβάλλοντα μέσω κινητών συσκευών.	Οι εκπαιδευόμενοι δε λαμβάνουν αμέσως πληροφορίες.
Διαδραστικότητα	Οι εκπαιδευόμενοι	Οι εκπαιδευόμενοι	Η αλληλεπίδραση

	αλληλεπιδρούν αποτελεσματικά με τους καθηγητές και τους συμφοιτητές τους μέσα από επιφάνειες των συστημάτων u-learning.	μπορούν να αλληλεπιδράσουν με τους καθηγητές και τους συμφοιτητές τους σε συγκεκριμένα περιβάλλοντα.	Εκπαιδευόμενων και καθηγητών είναι περιορισμένη.
Επίγνωση του πλαισίου (context awareness)	Το σύστημα μπορεί να καταλάβει το περιβάλλον του εκπαιδευόμενου μέσα από βάσεις δεδομένων και από μέσα από αισθητήρες που εντοπίζουν τη τοποθεσία του εκπαιδευόμενου καθώς και τη προσωπική και περιβαλλοντική κατάσταση.	Το σύστημα καταλαβαίνει και εντοπίζει το περιβάλλον του εκπαιδευόμενου μέσω πρόσβασης στη βάση δεδομένων.	Το σύστημα δε καταλαβαίνει το περιβάλλον του εκπαιδευόμενου.

Οι W.Jia et al [39] μελέτησαν την επίδραση των καινούριων τεχνολογιών κατά την εκπαιδευτική διαδικασία καταλήγοντας στα εξής συμπεράσματα: Χάρη στις δυνατότητες της Τεχνητής Νοημοσύνης καθίσταται εφικτή η εξατομικευμένη μάθηση, καθώς μπορούν να συλλεχθούν και να αναλυθούν τα δεδομένα των φοιτητών και από αυτά να προκύψουν κάποια χαρακτηριστικά ανά φοιτητή με αποτέλεσμα στη συνέχεια οι εκπαιδευτικοί να προσαρμόζουν τη διδασκαλία και το εκπαιδευτικό μοντέλο που ακολουθούν επι τη βάσει των στοιχείων που έχουν συλλέξει. Με άλλα λόγια, η εκπαιδευτική πλατφόρμα στην οποία συνδέονται τόσο οι

φοιτητές όσο και οι καθηγητές, παρακολουθώντας τις κινήσεις των φοιτητών (πχ τι δεδομένα κατεβάζουν, απαντήσεις σε ερωτηματολόγια) μπορεί να προτείνει τη καταλληλότερη ανά φοιτητή εκπαιδευτική προσέγγιση και αντίστροφα οι καθηγητές μπορούν μέσα από την πλατφόρμα αυτή να αντιληφθούν τις μαθησιακές ανάγκες κάθε φοιτητή και να προσαρμόσουν καλύτερα την εκπαιδευτική τους διδασκαλία. Περαιτέρω, με τη συμβολή της τεχνολογίας του υπολογιστικού νέφους, οι φοιτητές έχοντας ο καθένας έναν λογαριασμό στο cloud, έχουν ανά πάσα ώρα και στιγμή πρόσβαση στους εκπαιδευτικούς πόρους (σεμινάρια, διαλέξεις, σημειώσεις) που αναρτούν οι εκπαιδευτικοί.

Οι T.Zobel et al [42] σχεδίασαν μία ψηφιακή πλατφόρμα μάθησης ονόματι AI-Campus. Αυτή έχει ως στόχο την παροχή εξατομικευμένων μαθησιακών εμπειριών στους χρήστες οι οποίες επιτυγχάνονται μέσω λειτουργιών που βασίζονται στην Τεχνητή Νοημοσύνη όπως πχ chatbot. Το chatbot στο συγκεκριμένο εγχείρημα λειτουργεί ως έξυπνος βοηθός μάθησης χρησιμοποιώντας αλγόριθμους επεξεργασίας γλώσσας για να κατανοήσει τις ερωτήσεις και να απαντά με ακριβείς, σχετικές πληροφορίες σε πραγματικό χρόνο. Η χρησιμότητα του επίμαχου έξυπνου βοηθού μάθησης εντοπίζεται στα ακόλουθα πεδία: 1) Παροχή εξατομικευμένων και στοχευμένων εκπαιδευτικών υπηρεσιών βασισμένων στις ανάγκες των φοιτητών, 2) Διατήρηση της εγρήγορσης και του κινήτρου συμμετοχής των φοιτητών, 3) Άνεση και χρήση αυτού κάθε ώρα της ημέρας με αποτέλεσμα οι φοιτητές να λαμβάνουν βοήθεια κατ' απαίτηση αλλά και να συμμετέχουν στην εκπαιδευτική διαδικασία από όπου και αν βρίσκονται και 4) μείωση του φόρτου εργασίας των διδασκόντων επιτρέποντας τους να εστιάσουν στα πιο σύνθετα καθήκοντα τους και μειώνοντας έτσι τα λειτουργικά κόστη του πανεπιστημίου.

4.4.2 Επιμέρους υπηρεσίες προς το σκοπό δημιουργίας έξυπνου μαθησιακού περιβάλλοντος

Πριν εξετάσουμε τις κατ' ιδίαν υπηρεσίες που υποστηρίζουν την δημιουργία ενός έξυπνου μαθησιακού περιβάλλοντος, κρίνεται σκόπιμο να οριστεί η έννοια αυτού. Σύμφωνα λοιπόν με τους Hwang et al [40] ένα έξυπνο μαθησιακό περιβάλλον/σύστημα φέρει τρία βασικά χαρακτηριστικά: 1. Το σύστημα πρέπει να είναι σε θέση να παρέχει μαθησιακή υποστήριξη με βάση την κατάσταση των φοιτητών, 2. Το σύστημα πρέπει να προσφέρει άμεση και προσαρμοστική υποστήριξη στους εκπαιδευόμενους με βάση τις ατομικές τους ανάγκες (μαθησιακή επίδοση, μαθησιακές συμπεριφορές, προφίλ, προσωπικοί παράγοντες, κ.λπ.), καθώς

και το διαδικτυακό και πραγματικό πλαίσιο στο οποίο βρίσκονται, 3. Το σύστημα πρέπει να είναι σε θέση να προσαρμόζει τη διεπαφή του χρήστη δηλαδή τους τρόπους παρουσίασης πληροφοριών και τα περιεχόμενα του θέματος με τέτοιο τρόπο ώστε να ανταποκρίνονται στους προσωπικούς παράγοντες (π.χ. μαθησιακά στυλ και προτιμήσεις) και στην κατάσταση μάθησης (π.χ. μαθησιακή επίδοση) των μεμονωμένων εκπαιδευομένων. Η διεπαφή χρήστη δεν περιορίζεται σε συμβατικούς υπολογιστές, αλλά οι εκπαιδευόμενοι μπορούν να αλληλεπιδρούν με το μαθησιακό περιβάλλον μέσω κινητών συσκευών (π.χ. smartphones, υπολογιστών, tablet), φορητών συσκευών (π.χ. Google Glass ή ψηφιακών ρολογιών χειρός), ή ακόμη και μέσω πανταχού παρόντων υπολογιστικών συστημάτων εννσωματωμένων σε καθημερινά αντικείμενα.

Κατά τον Spector [41], για την ανάπτυξη έξυπνων περιβαλλόντων μάθησης, είναι σημαντικό να προσφέρονται κίνητρα που να συμβαδίζουν με τις ανάγκες της πλειοψηφίας των φοιτητών, αναγνωρίζοντας τις ικανότητές τους, τα μαθησιακά τους στυλ και τα ενδιαφέροντά τους. Το εκπαιδευτικό περιβάλλον θα πρέπει να παρέχει προσαρμοσμένες υπηρεσίες, ενσωματώνοντας εκπαιδευτικές προσεγγίσεις που προωθούν: **α.** Τον Διάλογο: Το περιβάλλον πρέπει να παροτρύνει τον φοιτητή σε διάλογο και να διευκολύνει ομαδικές συζητήσεις σχετικά με σημαντικά ζητήματα**, β.** Τον Αναστοχασμό: Το περιβάλλον μπορεί να ενθαρρύνει την αυτοαξιολόγηση βασιζόμενο στην πρόοδο και την απόδοση του φοιτητή, **γ.** Την Καινοτομία: Το εκπαιδευτικό περιβάλλον ενσωματώνει αναδυόμενες τεχνολογίες για την υποστήριξη της διαδικασίας μάθησης και διδασκαλίας, **δ.** Την Αυτοοργάνωση: Το εκπαιδευτικό περιβάλλον έχει τη δυνατότητα να ανακατανείμει πόρους και να θεσπίζει μηχανισμούς για τη βελτίωση της απόδοσής του με την πάροδο του χρόνου, βασιζόμενο σε δεδομένα που συλλέγονται αυτόματα και χρησιμοποιούνται για τη βελτίωση της αλληλεπίδρασής του με τους εκπαιδευόμενους σε διάφορες περιστάσεις.

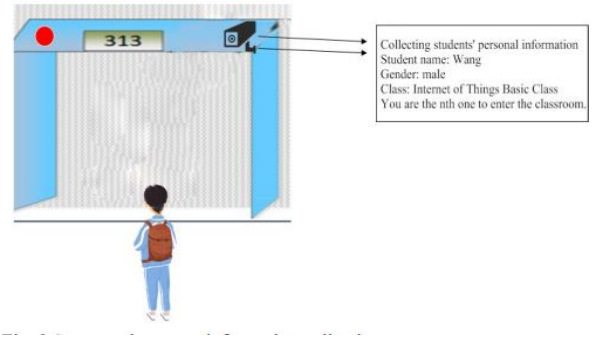
4.4.2.1 Έξυπνες Αίθουσες Διδασκαλίας

Οι Shen at al [48] ανέπτυξαν ένα έξυπνο σύστημα σχολικής αίθουσας που ενσωματώνει τις τεχνολογίες του NFC, της οθόνης LED και αφής και το οποίο έχει ως βασικές λειτουργίες την αυτοματοποιημένη διαχείριση του παρουσιολογίου των φοιτητών, τον εντοπισμό αυτών σε πραγματικό χρόνο και την εξαγωγή πληροφοριών αναφορικά με τους αυτούς. Ειδικότερα, το σύστημα αυτό μπορεί να εντοπίσει που

κάθονται οι φοιτητές και να εμφανίσει τα ονόματά τους σε μια οθόνη LED. Επιπλέον, το σύστημα επιτρέπει στους φοιτητές να καταγράψουν την παρουσία τους, να εκφράσουν αμέσως το βαθμό κατανόησής τους για το περιεχόμενο του μαθήματος και να παρακολουθούν τα αποτελέσματα της επίδοσής τους από άλλα σημεία.

Οι Huang et al [49] σχεδίασαν και υλοποίησαν μία έξυπνη αίθουσα διδασκαλίας η οποία περιλαμβάνει ασύρματους πίνακες, σύστημα ελέγχου εισόδου με την τεχνολογία του RFID ή με βιομετρικά δεδομένα, αισθητήρες για την συλλογή περιβαλλοντικών δεδομένων, αυτόματο φωτισμό, απομακρυσμένο έλεγχο όλων των συσκευών από τους καθηγητές, ένα chatbot που λειτουργεί με Τεχνητή Νοημοσύνη για την παροχή πληροφοριών στους φοιτητές όπως πχ για το πρόγραμμα τους, το οργανόγραμμα κτλ καθώς και κάμερες παρακολούθησης που καταγράφουν σε πραγματικό χρόνο και οι οποίες μπορούν να δώσουν χρήσιμες πληροφορίες αναφορικά με τη διαχείριση του παρουσιολογίου και την αξιολόγηση της ποιότητας της διάλεξης. Μάλιστα, πολλές από τις λειτουργίες της αίθουσας διδασκαλίας μπορούν να ενεργοποιηθούν με φωνητικές εντολές ενώ ταυτόχρονα έχουν εφαρμοστεί και έξυπνες στρατηγικές εξοικονόμησης ενέργειας, όπως η ενεργοποίηση ή απενεργοποίηση εξοπλισμού ανάλογα με την δραστηριότητα και την κίνηση των παρόντων προσώπων στην αίθουσα.

Οι X.Hu [50] δημιούργησαν μία έξυπνη αίθουσα διδασκαλίας που βασίζεται στις τεχνολογίες του Διαδικτύου των Πραγμάτων και της Τεχνητής Νοημοσύνης. Ειδικότερα, όταν ένας φοιτητής πλησιάζει προς την αίθουσα και φθάνει κοντά στον τοποθετημένο αισθητήρα, ο αισθητήρας αυτός αναγνωρίζει την κίνηση του ατόμου. Έτσι, δίνει σήμα στην κάμερα να ενεργοποιηθεί προκειμένου να ξεκινήσει τη διαδικασία της αναγνώρισης προσώπου και στη συνέχεια να τον συσχετίσει με τα δεδομένα που είναι ήδη αποθηκευμένα στη βάση δεδομένων. Στη συνέχεια το όνομα του ατόμου και το φύλο του εμφανίζεται στην οθόνη που βρίσκεται μέσα στην αίθουσα και από την οποία προκύπτουν και τα λοιπά στοιχεία των έτερων παρόντων προσώπων.



Εικόνα 10 Αναπαράσταση της έξυπνης αίθουσας διδασκαλίας [50]

Όταν δε το σύστημα εντοπίζει ότι η τοποθεσία των αργοπορημένων προσώπων βρίσκεται κοντά στην αίθουσα διδασκαλίας, αποστέλλει σε αυτούς έναν QR-code τον οποίο σκανάρουν οι φοιτητές στον ανιχνευτή που βρίσκεται έξω από την τάξη και επομένως το σύστημα αυτό εμφανίζει στην οθόνη της αίθουσας, τον αριθμό και τα στοιχεία των αργοπορημένων προσώπων.

Οι T. Sutjarittham et al [110] χρησιμοποιώντας τις τεχνολογίες του Διαδικτύου των Πραγμάτων και της Τεχνητής Νοημοσύνης, σχεδίασαν ένα έξυπνο σύστημα εντοπισμού της πληρότητας των αιθουσών της πανεπιστημιούπολης. Το προτεινόμενο σύστημα μέσω των τοποθετημένων σε εννέα αίθουσες αισθητήρων συλλέγει δεδομένα και τα ενσωματώνει στο ωρολόγιο πρόγραμμα του πανεπιστημίου για την παροχή πολύτιμων πληροφοριών, όπως ο αριθμός ακυρωμένων διαλέξεων, το ποσοστό παρακολούθησης των φοιτητών και οι ημερομηνίες εξετάσεων. Επίσης, οι τεχνολογίες τεχνητής νοημοσύνης και ένα μοντέλο μηχανικής μάθησης αξιοποιήθηκε για την πρόβλεψη της παρουσίας των φοιτητών στα μαθήματα. Τα αποτελέσματα της μελέτης έδειξαν ότι το εν λόγω σύστημα ήταν πολλά υποσχόμενο, βοηθώντας τη διοίκηση να ελαχιστοποιήσει τον ανεκμετάλλευτο χώρο και να εξοικονομήσει περίπου 10% του κόστους που επωμίζονταν κάθε χρόνο για την αξιοποίηση και συντήρηση των αιθουσών.

4.4.2.2 Έξυπνα Εργαστήρια

Οι Chi-Un Lei et al [51] ορίζοντας αρχικά την έννοια του έξυπνου εργαστηρίου ως εκείνου που φέρει τα ακόλουθα χαρακτηριστικά: 1) ικανότητα να εντοπίζει κινδύνους, όπως πυρκαγιές και πιθανή διαρροή χημικών και βακτηρίων, 2) ικανότητα να παρακολουθεί μακροπρόθεσμα την υγεία του προσωπικού και των φοιτητών, καθώς και των κατάλληλων συνθηκών συντήρησης του, 3) ικανότητα να παρακολουθεί την κατάσταση του εξοπλισμού για τη διατήρηση της ασφάλειας, 4)

ικανότητα να ρυθμίζει τη θερμοκρασία και άλλες περιβαλλοντικές συνθήκες για τη μείωση της κατανάλωσης ενέργειας και άλλων πόρων χωρίς να υποβαθμίζεται η αποτελεσματικότητα των ερευνητικών δραστηριοτήτων, εν συνεχεία πρότειναν την ανάπτυξη ενός έξυπνου εργαστηρίου κατασκευασμένου μέσω ενός κυβερνο-φυσικού συστήματος. Τα κυβερνο-φυσικά συστήματα είναι συστήματα που περιέχουν πολυάριθμους κατανεμημένους, συνδεδεμένους και αυτόνομους κόμβους αισθητήρων και κόμβους ενεργοποίησης και τα οποία χρησιμοποιούνται για τη συλλογή πληροφοριών από το περιβάλλον μέσω αισθητήρων. Στην προκειμένη περίπτωση, το κυβερνο-φυσικό σύστημα χρησιμοποιείται για την συλλογή πληροφοριών και την διαχείριση των περιβαλλοντικών και συγκεκριμένα των θερμικών συνθηκών του εργαστηρίου με σκοπό να διασφαλίζεται η σωστή λειτουργία και συντήρηση του εργαστηριακού εξοπλισμού.

Οι Φωτάρης Π. et al [43] σχεδίασαν ένα σύστημα ηλεκτρονικής μάθησης, το VRLAB, το οποίο συνδυάζει αποτελεσματικά τις τεχνολογίες διαδικτύου, πολυμέσων και τρισδιάστατων γραφικών και το οποίο δημιουργήθηκε προκειμένου να δώσει τη δυνατότητα στους εκπαιδευόμενους να συμμετέχουν εικονικά στη μελέτη του εκπαιδευτικού υλικού και να εκτελούν διάφορες εργαστηριακές ασκήσεις και πειράματα.

Οι Akçayır M. et al [44] εφάρμοσαν την τεχνολογία της επαυξημένης πραγματικότητας σε ένα εργαστήριο φυσικών επιστημών προκειμένου να μελετήσουν το κατά πόσο αυτή μπορεί να επηρεάσει τις εργαστηριακές δεξιότητες των φοιτητών. Οι ερευνητές διαπίστωσαν ότι η παροχή στοιχείων επαυξημένης πραγματικότητας (βίντεο, κινούμενα σχέδια, εικόνες, κ.λπ.) βοήθησε τους εκπαιδευόμενους να αποκτήσουν καλύτερες εργαστηριακές δεξιότητες, καθότι μπορούσαν να παρακολουθήσουν γεγονότα που δεν είναι ορατά σε ένα πραγματικό εργαστήριο, όπως πχ η παρακολούθηση της κίνησης μορίων. Περαιτέρω, προέκυψε ότι οι φοιτητές ολοκλήρωσαν σε συντομότερο χρόνο τις πειραματικές δοκιμές σε σχέση με το χρόνο που θα τους έπαιρνε αν τις πραγματοποιούσαν σε πραγματικό εργαστήριο ενώ ταυτόχρονα παρατηρήθηκε και αυξημένο ενδιαφέρον των φοιτητών να συμμετάσχουν ενεργά σε αυτές.

4.4.2.3 Έξυπνες Βιβλιοθήκες

Ο J.Yu [52] ανέπτυξε με την βοήθεια της τεχνολογίας της υπολογιστικής νέφους, της κατανεμημένης επεξεργασίας, της αποθήκευσης και της εξόρυξης των

μεγάλων δεδομένων, ένα σύστημα παροχής υπηρεσιών εξατομικευμένης βιβλιοθήκης το οποίο λειτουργεί ως εξής: Το σύστημα αξιοποιώντας τους διαθέσιμους πόρους του και λαμβάνοντας υπόψη τις απαιτήσεις των αναγνωστών, προσαρμόζει το περιεχόμενο του έτσι ώστε να παρέχει εξατομικευμένες υπηρεσίες ανάγνωσης στον εκάστοτε αναγνώστη. Τα χαρακτηριστικά δε των αναγνωστών αλλά και των βιβλίων εξάγονται και αναλύονται μέσω εργαλείων και μεθόδων εξόρυξης δεδομένων. Στη συνέχεια, αφού προκύψουν τα χαρακτηριστικά των αναγνωστών και συσχετιστούν με το περιεχόμενο των βιβλίων, γίνονται και οι σχετικές συστάσεις στους αναγνώστες από το σύστημα βάσει των ενδιαφερόντων τους.

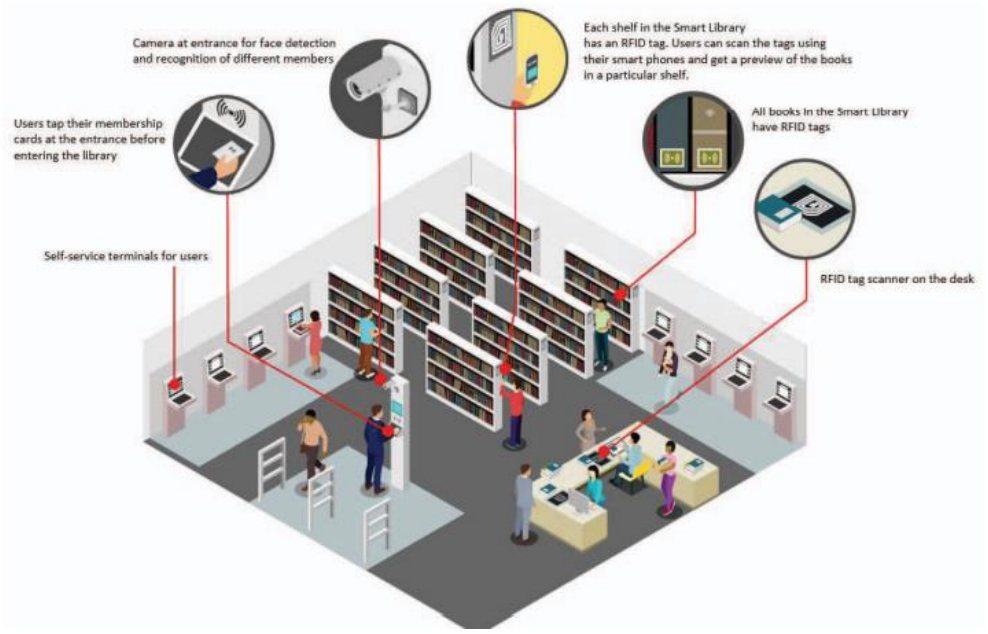
Οι A.Ozeer et al [53] επιχείρησαν να μετατρέψουν μία παραδοσιακή βιβλιοθήκη που επικεντρωνόταν περισσότερο στον έλεγχο της πρόσβασης στη βιβλιοθήκη χρησιμοποιώντας μαγνητικές κάρτες ή τη χειροκίνητη αποθήκευση των στοιχείων σε ένα ηλεκτρονικό αρχείο, σε έξυπνη βιβλιοθήκη που λειτουργεί ως εξής: Η έξυπνη βιβλιοθήκη χρησιμοποιεί τη τεχνολογία του NFC που ενσωματώνεται σε βιβλία και κάρτες χρηστών οι οποίες είναι αναγνώσιμες με αναγνώστες NFC ή με τη χρήση του smartphone του χρήστη. Ο σκοπός της είναι η απλοποίηση της αναζήτησης βιβλίων και η αποτελεσματική και απαλλαγμένη από κλοπές λειτουργία των βιβλιοθηκών. Η διαδικασία ξεκινά με τον χρήστη που αναζητά ένα βιβλίο στο ράφι. Ο τελευταίος θα σαρώσει το βιβλίο που περιέχει το τσιπ NFC για να αποκτήσει την περίληψη αυτού. Ο χρήστης πρέπει στη συνέχεια να σαρώσει την ταυτότητά του και θα έχει τη δυνατότητα να δανειστεί το βιβλίο.

Η έξυπνη βιβλιοθήκη περιέχει επίσης και ένα σύστημα καταγραφής όλων των υπαρχόντων βιβλίων επί των οποίων υπάρχουν ετικέτες RFID για τον εντοπισμό της ακριβούς θέσης τους και την συνακόλουθη αποτύπωση αυτής σε μια μικρή οθόνη που θα εμφανίζει τα αποτελέσματα και τη συντομότερη διαδρομή προς τα βιβλία αυτά. Αυτό το σύστημα έχει ως στόχο την επίλυση του προβλήματος της αταξίας των βιβλίων στα ράφια. Ο χρήστης λοιπόν πρέπει να έχει ήδη εντοπίσει την τοποθεσία του ραφιού του βιβλίου που θα εισάγει σε μια φορητή συσκευή εξοπλισμένη με οθόνη και πληκτρολόγιο. Η συσκευή θα διαβάσει την τοποθεσία του χρήστη και θα εντοπίσει την ετικέτα RFID που αντιστοιχεί στην τοποθεσία του ραφιού και θα εμφανίσει τη συντομότερη διαδρομή στον χρήστη.

Επιπλέον, ο χρήστης πιστοποιείται μέσω ενός αναγνώστη δακτυλικών αποτυπωμάτων για να αποκτήσει πρόσβαση στη βιβλιοθήκη. Κάθε φορά που ο χρήστης αναζητά ένα βιβλίο μέσω του συστήματος της βιβλιοθήκης, ο διακομιστής

ανακτά τη θέση του βιβλίου στο ράφι. Η πληροφορία αυτή αποστέλλεται στο Σύστημα Τοπικής Θέσης (LPS), το οποίο εντοπίζει το βιβλίο με το smartphone του χρήστη. Έπειτα, το βιβλίο δίδεται στον χρήστη. Για τη διαδικασία επιστροφής, ο χρήστης εναποθέτει το βιβλίο σε ένα έξυπνο καρότσι επιστροφής με αναγνώστη NFC, το οποίο το αφαιρεί από τη λίστα των δανεισμένων βιβλίων και το καθιστά εκ νέου διαθέσιμο για δανεισμό.

Οι S. D. Nagowah et al [54] πρότειναν τη δημιουργία μίας έξυπνης βιβλιοθήκης βασισμένης στο Διαδίκτυο των Πραγμάτων και στην προγνωστική ανάλυση, ονόματι SmartLibOnto. Ο στόχος αυτής είναι να αυτοματοποιήσει διαδικασίες όπως ο εντοπισμός και η αναζήτηση βιβλίων, ο έλεγχος ταυτότητας, ο έλεγχος πρόσβασης, ο δανεισμός και η επιστροφή των βιβλίων καθώς επίσης να μειώσει και το κόστος του ανθρώπινου δυναμικού.



Εικόνα 11 Έξυπνη βιβλιοθήκη σχεδιασμένη από τους τους S.D. Nagowah et al [54]

4.5 ΕΞΥΠΝΗ ΔΙΑΚΥΒΕΡΝΗΣΗ (SMART GOVERNANCE)

Με τον όρο έξυπνη διακυβέρνηση νοείται η ικανότητα ή δυνατότητα διεξαγωγής έξυπνων δραστηριοτήτων, κατά βάση με τη χρήση τεχνολογίας με σκοπό τη διευκόλυνση της λήψης αποτελεσματικότερων αποφάσεων, τη βελτίωση της παροχής υπηρεσιών και την αύξηση της διαφάνειας και της λογοδοσίας. Τα κύρια χαρακτηριστικά αυτής είναι η αποτελεσματική διαχείριση της γραφειοκρατίας καθώς και η αποτελεσματική διαχείριση της ευρύτερης δημόσιας διοίκησης και των επιμέρους υπηρεσιών αυτής. [55]

4.5.1 Έξυπνα Συστήματα Λήψης Αποφάσεων και Διαχείρισης Καταστάσεων

Οι Zhan Xin et al [56] σχεδίασαν ένα έξυπνο σύστημα λήψης αποφάσεων που ανταποκρίνεται στις ανάγκες μίας σύγχρονης, έξυπνης πανεπιστημιούπολης. Εκκινώντας από το στάδιο της ανάλυσης των απαιτήσεων της πανεπιστημιούπολης που είχαν ως σημείο αναφοράς, ερεύνησαν την πραγματική κατάσταση κάθε τμήματος του πανεπιστημίου, των καθηγητών και των φοιτητών με σκοπό το σύστημα αυτό να διασφαλίσει ένα πιο βολικό περιβάλλον μάθησης και εργασίας. Κατά το σχεδιασμό του συστήματος επεσήμαναν ότι ο βασικός του στόχος είναι να διασφαλιστεί ότι η πλατφόρμα του συστήματος θα μπορεί να παρέχει την αντίστοιχη βοήθεια στον χρήστη της εκάστοτε επιμέρους υπηρεσίας μέσω των αντίστοιχων δεδομένων και πληροφοριών που έχει συλλέξει. Για την υλοποίηση του επίμαχου συστήματος, οι ερευνητές επισήμαναν τα ακόλουθα: 1) Το σύστημα θα πρέπει να διαθέτει λειτουργία εισαγωγής δεδομένων και πρόσβασης στις παραχθείσες πληροφορίες προκειμένου να τροφοδοτείται από αυτές, 2) Είναι απαραίτητο τα δεδομένα που συλλέγονται, να οργανωθούν σε μια βάση δεδομένων, ώστε να διασφαλιστεί ότι η εξόρυξη και η επεξεργασία τους πραγματοποιείται με συστηματοποιημένο τρόπο, 3) Με την ενσωμάτωση των δεδομένων των φοιτητών και την ανάλυση τους, το σύστημα θα μπορεί να υποστηρίζει τη λήψη καλύτερων αποφάσεων αναφορικά με την χορήγηση των υποτροφιών καθώς από την επεξεργασία των δεδομένων των φοιτητών θα έχει προκύψει ποιοι είναι οι λιγότερο ευκατάστατοι φοιτητές που έχουν περισσότερη ανάγκη έναντι των υπολοίπων τη λήψη υποτροφίας.

Έτσι και οι Wu et al [57] σχεδίασαν ένα έξυπνο σύστημα το οποίο κάνει χρήση των μεγάλων δεδομένων της πανεπιστημιούπολης για τον εντοπισμό των φοιτητών που αντιμετωπίζουν οικονομικές δυσκολίες και υποστηρίζει τη λήψη αποφάσεων σχετικά με το ύψος της επιδότησης τους. Το εν λόγω σύστημα μπορεί παράλληλα να ειδοποιεί τους εκπαιδευτικούς συμβούλους ώστε να παρέχουν ψυχολογική υποστήριξη στους εν λόγω φοιτητές. Ο εντοπισμός των φοιτητών γίνεται με βάση πληροφορίες όπως η ποσότητα, η ποικιλία, η τιμή και το σημείο αγοράς των αγαθών που αυτοί καταναλώνουν καθώς επίσης και από τα χαρακτηριστικά των δραστηριοτήτων που αυτοί συμμετέχουν. Σημειώνεται ότι λόγω του μεγάλου όγκου και της ανομοιομορφίας των συλλεχθέντων δεδομένων, τέσσερις μέθοδοι επεξεργασίας δεδομένων (υποδειγματοληψία, επαναδειγματοληψία, μάθηση με ευαισθησία στο κόστος και SMOTE) εφαρμόστηκαν για την παραγωγή τεσσάρων

διαφορετικών πειραματικών συνόλων δεδομένων και πέντε αλγόριθμοι ταξινόμησης(Random Forest, J48, Naïve Bayes, SMO, Logistic regression) χρησιμοποιήθηκαν για την εκπαίδευση του μοντέλου ταξινόμησης σε κάθε σύνολο δεδομένων.

Οι Opranescu V. et al [58] σχεδίασαν μία εφαρμογή υποστήριξης λήψης αποφάσεων των φοιτητών σε σχέση με την εκπαιδευτική τους πορεία η οποία περιλαμβάνει τις ακόλουθες δυνατότητες: 1) Δημιουργία εξατομικευμένου προγράμματος του φοιτητή με πληροφορίες που εισάγει ο τελευταίος στη βάση δεδομένων της εφαρμογής και κατ' επέκταση 2) δημιουργία ενός έξυπνου, εξατομικευμένου ημερολογίου το οποίο θα ενημερώνει τον φοιτητή για γεγονότα που σχετίζονται με εκπαιδευτικές του δραστηριότητες, 3) Υπηρεσία έξυπνου εικονικού βοηθού (chatbot) ο οποίος μιμούμενος την ανθρώπινη αλληλεπίδραση και επεξεργαζόμενος τις πληροφορίες που του εισάγει ο χρήστης αναφορικά με τις προθέσεις του, τα ενδιαφέροντα του, την αναφορά του σχετικά με ένα θέμα, θα μπορεί να συστήσει στον φοιτητή την εκπαιδευτική κατεύθυνση που του ταιριάζει περισσότερο, 4) Υπηρεσία Αυτοματοποιημένης Διαδικασίας Αλλαγής Μαθημάτων που στόχο έχει να αυτοματοποιήσει τη διαδικασία εγγραφής και έγκρισης αιτημάτων αλλαγής μαθημάτων, εξοικονομώντας χρόνο για φοιτητές και διοικητικό προσωπικό. Ο φοιτητής μπορεί να δει όλες τις επιλογές του όταν επιθυμεί να αλλάξει ένα μάθημα το οποίο έχει περάσει με ένα άλλο, λαμβάνοντας υπόψη συγκεκριμένες προϋποθέσεις όπως τα δύο αυτά μαθήματα πρέπει να ανήκουν στο ίδιο είδος (να είναι προαιρετικά), στο ίδιο εξάμηνο και στην ίδια κατηγορία. Επίσης, κάθε φοιτητής έχει μια συγκεκριμένη ποσότητα μονάδων μεταφερόμενων πιστώσεων (ECTS) που μπορεί να χρησιμοποιήσει κατά την αλλαγή μαθημάτων.

Οι Zhangbin Chen et al [59] δημιούργησαν ένα σύστημα διακυβέρνησης των δεδομένων μίας έξυπνης πανεπιστημιούπολης με το οποίο επιχειρείται η πραγματοποίηση υψηλής ποιότητας διαλογής, αποθήκευσης, ταξινόμησης, εξόρυξης και ανάλυσης των συνεχώς παραγόμενων δεδομένων με σκοπό τη βελτίωση της ποιότητας των εκπαιδευτικών υπηρεσιών και την εν γένει της διδασκαλίας και της επιστημονικής έρευνας. Ειδικότερα, οι κύριες λειτουργίες του εν λόγω συστήματος είναι οι ακόλουθες: 1) Διαχείριση των δεδομένων της πανεπιστημιούπολης, ήτοι καθορισμός όλων των επιμέρους χαρακτηριστικών των δεδομένων της πανεπιστημιούπολης και ταξινόμηση αυτών σε θεματικούς καταλόγους, 2) Διαχείριση των μεταδεδομένων ήτοι των δεδομένων που περιλαμβάνουν πληροφορίες

για άλλα δεδομένα όπως η σημασία, η προέλευση, η μορφή ή άλλες χαρακτηριστικές περιγραφές των κύριων δεδομένων και τα οποία επιτελούν σημαντικό ρόλο στην αναζήτηση και την οργάνωση των κύριων δεδομένων, 3) Διαχείριση της ποιότητας των δεδομένων δια της κατασκευής ενός συστήματος παρακολούθησης της ποιότητας των δεδομένων με το οποίο επιτυγχάνεται η αυτοματοποίηση των διαδικασιών αναφορικά με όλους τους τύπους δεδομένων, εντοπίζονται εγκαίρως προβλήματα όπως λανθασμένα ή ελλιπή δεδομένα και παράγονται στη συνέχεια κάποιες αναφορές ποιότητας δεδομένων, 4) Διαχείριση των οικονομικών δεδομένων της πανεπιστημιούπολης με σκοπό την διευκόλυνση της παροχής των σχετικών υπηρεσιών και την εν γένει βελτιστοποίηση των επιχειρηματικών διαδικασιών και 5) Διαχείριση της ασφάλειας δεδομένων η οποία έχει τέσσερις πτυχές και ειδικότερα: α)ασφάλεια των δεδομένων ήτοι προστασία της ακεραιότητας και εμπιστευτικότητας των δεδομένων από τρίτα μη εξουσιοδοτημένα άτομα, β) ασφάλεια διαβίβασης των δεδομένων δια της αξιοποίησης της τεχνικής της κρυπτογράφησης και άλλων μέσων για την αποτροπή της ανεπιθύμητης παρακολούθησης ή αλλοίωσης των πληροφοριών κατά τη διαδικασία μεταφοράς, γ) ασφαλής προστασία των δεδομένων ήτοι λήψη μέτρων έναντι της απώλειας ή καταστροφής όπως δημιουργία αντιγράφων ασφαλείας, μέσων ανάκτησης δεδομένων και δ) ασφάλεια κατά την επεξεργασία των δεδομένων δυνάμει ελέγχου των δικαιωμάτων πρόσβασης.

4.5.2 Ειδικότερα: Συστήματα συμμετοχικής διακυβέρνησης εντός της πανεπιστημιούπολης

Είναι αναντίρρητο ότι η υλοποίηση του στόχου της έξυπνης διακυβέρνησης δε θα μπορούσε να επιτευχθεί χωρίς την ενεργή συμμετοχή των φοιτητών και της εν γένει ακαδημαϊκής κοινότητας στο κοινωνικό γίγνεσθαι.

Σύμφωνα με τους Lizzio και Wilson [69], η συμμετοχή των φοιτητών στην διακυβέρνηση του πανεπιστημίου είναι χαμηλότερη από το αναμενόμενο και αυτό οφείλεται στην έλλειψη δεσμευτικών κανόνων και κανονισμών, στην εξαφάνιση των φοιτητικών συλλόγων και στην καθιέρωση της αντίληψης ότι τα πανεπιστήμια έχουν άκαμπτη ιεραρχική δομή, με τις αποφάσεις να λαμβάνονται μόνο από τους ιεραρχικά ανώτερους.

Εντούτοις, στο πλαίσιο της έξυπνης πανεπιστημιούπολης, ενθαρρύνεται σημαντικά και έμπρακτα η συμμετοχή των φοιτητών σε όλα τα επίπεδα της διαμόρφωσης των κανόνων του πανεπιστημίου, επιτυγχάνοντας το μέγιστο βαθμό συναίνεσης κατά τη λήψη αποφάσεων που αφορούν την καθημερινότητα της

πανεπιστημιούπολης και μειώνοντας έτσι το υφιστάμενο «δημοκρατικό έλλειμμα» [70]. Ιδιαίτερο ρόλο σε αυτό διαδραματίζουν και οι νέες τεχνολογίες με τις τεράστιες δυνατότητες που προσφέρουν, συμβάλλοντας στην ενίσχυση της συμμετοχικής αλληλεπίδρασης, στην αύξηση της διαφάνειας και της νομιμότητας κατά τη λήψη αποφάσεων, στην εδραίωση της πολιτικής κουλτούρας και στην αύξηση του αριθμού των χρηστών που συμμετέχουν σε αυτού του είδους τις διαδικασίες [71].

Οι V. Peñafiel et al [72] έθεσαν σε λειτουργία μία πειραματική πλατφόρμα ονόματι MyUniversity η οποία υποστήριζε τις ακόλουθες λειτουργίες: 1) Διάλογο μεταξύ όλων των εμπλεκόμενων μερών κατά τη διαδικασία της λήψης αποφάσεων (φοιτητές, καθηγητές, εργαζόμενοι, διευθυντικά στελέχη) σχετικά με ζητήματα όπως η έγκριση του ετήσιου προϋπολογισμού, οι προεκλογικές εκστρατείες για την εκλογή των πανεπιστημιακών αρχών ή των φοιτητικών οργάνων, συμμετοχή σε φόρουμ και συνέδρια ή διαδικτυακές ομιλίες, 2) Καθολική Συμμετοχή σε διαδικασία ψηφοφορίας για την επιλογή Πρύτανη, αντιπροσώπων των εργαζομένων, των καθηγητών, του διδακτικού προσωπικού και των φοιτητικών οργανώσεων, 3) Χρήση ηλεκτρονικών ερωτηματολογίων με στόχο την ακαδημαϊκή ανατροφοδότηση και την κατάρτιση σχεδίων και στρατηγικών, 4) Ενημέρωση και Διάδοση σε πραγματικό χρόνο των αποφάσεων που λαμβάνονται αναφορικά με την πανεπιστημιούπολη, των συμφωνιών που υπογράφονται, των ψηφισμάτων, των αποφάσεων συνταξιοδότησης του ακαδημαϊκού προσωπικού. Οι ερευνητές κατέληξαν στο συμπέρασμα πως η πλατφόρμα αυτή συνέβαλε στην εξοικονόμηση χρόνου καθώς και στην αύξηση της αποτελεσματικότητας των διαδικασιών ενώ περαιτέρω ενδυνάμωσε την ενότητα της πανεπιστημιακής κοινότητας.

Οι Saad et al [76] σχεδίασαν ένα έξυπνο ηλεκτρονικό σύστημα ψηφοφορίας για εκλογές στις πανεπιστημιουπόλεις το οποίο βασίζεται σε ένα σύστημα πελάτη-εξυπηρετητή (client-server). Στο σύστημα υπάρχει ενσωματωμένο ένα σύστημα RFID για τον έλεγχο ταυτότητας των ψηφοφόρων. Πιο συγκεκριμένα, οι φοιτητές εγγράφονται σε αυτό δημιουργώντας ένα προφίλ και αποδίδεται στον καθένα μία ετικέτα RFID. Με αυτήν την ετικέτα οι φοιτητές συνδέονται στο σύστημα και αφού ολοκληρωθεί η διαδικασία αυθεντικοποίησης, οι φοιτητές μεταφέρονται στο πρόγραμμα του τερματικού της ψηφοφορίας και ψηφίζουν τον υποψήφιο που επιθυμούν. Στο τέλος της διαδικασίας οι ψήφοι καταμετρώνται γρήγορα και αυτόματα από το σύστημα χωρίς την ανάγκη ανθρώπινης παρέμβασης. Το προτεινόμενο αυτό σύστημα, αν ληφθεί υπόψη ότι προτάθηκε το 2014, αποτελεί μία

καινοτομία για την εποχή του, πλην όμως γεννά πολλά ζητήματα ασφαλείας και προστασίας της ιδιωτικότητας των ψηφισάντων καθότι δεν εξασφαλίζει την μυστικότητα της ψήφου, την ανωνυμία των χρηστών καθώς επίσης δεν φέρει τα απαιτούμενα μέτρα ασφάλειας τόσο του δικτύου που είναι απομακρυσμένο και συνεπώς πιο ευάλωτο σε επιθέσεις και κακόβουλες ενέργειες από ότι ένα τοπικό δίκτυο υπολογιστών όσο και της ίδιας της υποδομής του συστήματος.

Από την επισκόπηση της νεότερης βιβλιογραφίας αναφορικά με το ζήτημα της υλοποίησης ενός απομακρυσμένου και ηλεκτρονικού πλην όμως αξιόπιστου και διαφανούς συστήματος ψηφοφορίας, παρατηρείται ότι προτείνεται ολοένα και περισσότερο η ενσωμάτωση της τεχνολογίας του blockchain, με τις περισσότερες βιβλιογραφικές αναφορές να το μελετούν υπό το πρίσμα της έξυπνης πόλης και λιγότερο υπό το πρίσμα της έξυπνης πανεπιστημιούπολης. Στην πραγματικότητα, το blockchain είναι μια αποκεντρωμένη, κατανεμημένη βάση δεδομένων αμετάβλητων εγγραφών οι οποίες αποθηκεύονται με τη μορφή μπλοκ. Τα δεδομένα αποθηκεύονται σε ένα δίκτυο υπολογιστών που ονομάζονται και κόμβοι και τα οποία ομαδοποιούνται σε μπλοκ. Αυτά τα μπλοκ συνδέονται μεταξύ τους για να σχηματίσουν μια αλυσίδα γνωστή ως αλυσίδα μπλοκ (blockchain). Κάθε μπλοκ στην αλυσίδα αυτή περιέχει έναν μοναδικό κωδικό που ονομάζεται αλγόριθμος κρυπτογράφησης hash. Αυτός ο κωδικός δημιουργείται χρησιμοποιώντας τις πληροφορίες του μπλοκ και το hash του προηγούμενου μπλοκ. Αυτή η σύνδεση των μπλοκ με χρήση hash δημιουργεί ένα αλυσιδωτό δίκτυο. Για να προστεθεί ένα νέο μπλοκ στην αλυσίδα, η πλειοψηφία των κόμβων στο δίκτυο πρέπει να συμφωνήσει ότι οι συναλλαγές είναι έγκυρες. Αυτή η συμφωνία επιτυγχάνεται συνήθως μέσω ενός μηχανισμού συναίνεσης ο οποίος προσφέρει αξιοπιστία και εμπιστοσύνη μεταξύ αγνώστων σε ένα κατανεμημένο υπολογιστικό περιβάλλον. Χαρακτηριστικό γνώρισμα του blockchain είναι ότι τα δεδομένα και κατ' επέκταση οι πληροφορίες που προστίθενται σε ένα μπλοκ παραμένουν αμετάβλητες χάρη στην ύπαρξη ενός ισχυρού κρυπτογραφημένου αλγορίθμου ο οποίος τα διασφαλίζει έναντι αλλαγών. Πέραν τούτου, η αλλαγή των πληροφοριών σε ένα μπλοκ θα απαιτούσε την αλλαγή όλων των επόμενων μπλοκ και τη συναίνεση της πλειοψηφίας του δικτύου [74].

Υπάρχουν τρεις κυρίως τύποι Blockchain [75]: το δημόσιο, το ιδιωτικό και το κοινοπρακτικό. Στο δημόσιο blockchain οποιοσδήποτε μπορεί να συμμετέχει, να επικυρώνει συναλλαγές και να εντάσσεται στο δίκτυο. Είναι ανοιχτό στο κοινό και καμία κεντρική αρχή δεν ελέγχει την πρόσβαση ή την επικύρωση. Στο ιδιωτικό

blockchain μόνο επιλεγμένα μέλη εξουσιοδοτούνται να επαληθεύουν συναλλαγές στο μπλοκ. Συνήθως, μια κεντρική αρχή ή ένα σύνολο προκαθορισμένων κόμβων ελέγχουν το δίκτυο και οι συμμετέχοντες χρειάζονται άδεια για να ενταχθούν και να επικυρώσουν συναλλαγές. Θεωρείται ταχύτερο και πιο αποτελεσματικό από το δημόσιο blockchain λόγω της ύπαρξης λιγότερων κόμβων και λιγότερης πολυπλοκότητας κατά τη διαδικασία της συναίνεσης. Τέλος, το κοινοπρακτικό blockchain είναι ένα υβριδικό μοντέλο συνδυάζοντας στοιχεία τόσο από το δημόσιο όσο και από το ιδιωτικό. Σε αυτό συμμετέχουν πολλοί οργανισμοί που σχηματίζουν έναν σύνδεσμο και καθιστούν κοινόχρηστο τον έλεγχο του blockchain. Η διαδικασία συναίνεσης ελέγχεται από έναν προκαθορισμένο σύνολο κόμβων. Παρέχει μια ισορροπία μεταξύ αποκέντρωσης και ελέγχου, καθιστώντας το κατάλληλο για συνεργατικές προσπάθειες μεταξύ πολλαπλών οντοτήτων.

Οι M.Bhamare et al [73] εστιάζοντας στο κομμάτι της ενεργούς συμμετοχής των πανεπιστημιακών χρηστών στη λήψη αποφάσεων δια της ψηφοφορίας πρότειναν την αναβάθμιση του κλασικού συστήματος ψηφοφορίας με τη χρήση ενός μοντέλου που βασίζεται στην τεχνολογία του Blockchain το οποίο θα εξασφαλίζει ότι η διαδικασία της ψηφοφορίας θα είναι ανοιχτή, διαφανής και αξιόπιστη. Το σύστημα αυτό χρησιμοποιεί έξυπνα συμβόλαια και εγγυάται ότι η καταμέτρηση των ψήφων γίνεται με αποκεντρωμένο τρόπο ώστε να επιτυγχάνεται η ανωνυμία των ψηφοφόρων. Έτσι οι ψηφοφόροι θα μπορούν να ψηφίζουν από την άνεση του σπιτιού τους χωρίς να είναι απαραίτητη η φυσική παρουσία τους. Κάθε κόμβος στο δίκτυο διαθέτει ένα αναγνωριστικό ψηφοφόρου και το όνομα του προσώπου στο οποίο ρίχνει την ψήφο του ο ψηφοφόρος. Οι πληροφορίες στο μπλοκ κρυπτογραφούνται με ασφάλεια και διατηρούνται ως κόμβος στην αλυσίδα. Έτσι επιτυγχάνεται η ασφάλεια και το αδιάβλητο της εκλογικής διαδικασίας καθώς καθίσταται ιδιαίτερα δυσχερής η πρόσβαση στις κρυπτογραφημένες πληροφορίες σε τρίτους-μη εξουσιοδοτημένα πρόσωπα που έχουν σκοπό να αλλοιώσουν το εκλογικό αποτέλεσμα.

Οι G. Rathee et al [77] σχεδίασαν ένα σύστημα ηλεκτρονικής ψηφοφορίας στο οποίο η διαφάνεια των ψήφων, ο συντονισμός της εκλογικής διαδικασίας, η εγγραφή και η επαλήθευση της ταυτότητας των ψηφοφόρων λαμβάνει χώρα σε ένα αποκεντρωμένο περιβάλλον μέσω ενός μηχανισμού Blockchain. Το προτεινόμενο σύστημα είναι δύο άκρων δηλαδή τόσο οι υποψήφιοι όσο και κάθε επιμέρους χρήστης – ψηφοφόρος μπορούν να ελέγξουν το αδιάβλητο της διαδικασίας ενώ η ασφάλεια των συσκευών του Διαδικτύου των Πραγμάτων μέσω των οποίων

ψηφίζουν οι τελευταίοι είναι εγγυημένη δια της ανάλυσης και εξέτασης του τρόπου επικοινωνίας τους από έναν αλγόριθμο (κοινωνικού βελτιστοποιητή). Μάλιστα δε το σύστημα αυτό ειδοποιεί τους ψηφοφόρους σε περίπτωση οποιασδήποτε παρέμβασης επί της ψήφου τους πριν την προγραμματισμένη καταμέτρηση, εμπεδώνοντας έτσι το αίσθημα εμπιστοσύνης τους στους δημοκρατικούς θεσμούς. Από την εφαρμογή του μηχανισμού αυτού παρατηρήθηκε ότι φαινόμενα όπως αλλοιώσεις κατά τη μετάδοση μηνυμάτων λόγω κακόβουλων ενεργειών και απειλών, επιθέσεις άρνησης υπηρεσιών (DDos Attack), αναποτελεσματικοί μηχανισμοί επαλήθευσης της νομιμότητας των κόμβων μειώθηκαν σημαντικά ενώ επίσης αντιμετωπίστηκαν και περιπτώσεις όπως διπλή ψήφος του ίδιου προσώπου λόγω διπλοεγγραφής του.

Οι Singh A. et al [78] επικεντρώθηκαν στην ανάπτυξη ενός ισχυρού και φιλικού προς τον χρήστη συστήματος ψηφοφορίας αξιοποιώντας τα πλεονεκτήματα της τεχνολογίας του Blockchain. Το προτεινόμενο σύστημα χρησιμοποιεί το Ethereum ως την υποκείμενη πλατφόρμα blockchain καθώς επίσης έξυπνα συμβόλαια για την καταγραφή και την επικύρωση ψήφων αλλά και για την αναγνώριση των προσώπων η οποία καθίσταται εφικτή χάρη και στην τεχνολογία της Τεχνητής Νοημοσύνης. Πιο συγκεκριμένα, τα έξυπνα συμβόλαια είναι σε θέση να καταγράφουν και να αποθηκεύουν τα βιομετρικά δεδομένα του κάθε εγγεγραμμένου προσώπου με ασφαλή και κρυπτογραφημένο τρόπο. Όταν ένας ψηφοφόρος συνδέεται στο σύστημα ψηφοφορίας, το έξυπνο συμβόλαιο χρησιμοποιεί το μοντέλο αναγνώρισης προσώπου για να επαληθεύσει την ταυτότητά του. Για να διασφαλιστεί το απόρρητο και η ασφάλεια των ψηφοφόρων, τα βιομετρικά δεδομένα προσώπου αποθηκεύονται σε μια ξεχωριστή υπηρεσία που βασίζεται σε cloud, ενσωματωμένη στο σύστημα ψηφοφορίας που βασίζεται σε blockchain. Αυτό επιτρέπει την ασφαλή και αποτελεσματική πρόσβαση στα απαραίτητα δεδομένα κατά τη διάρκεια της ψηφοφορίας. Κατά τη διαδικασία της ψηφοφορίας, ο ψηφοφόρος υποβάλλει την ψήφο του μέσω μιας διεπαφής που συνδέεται με το δίκτυο blockchain. Στη συνέχεια, η ψήφος επαληθεύεται μέσω των έξυπνων συμβολαίων και αποθηκεύεται στο blockchain με ασφαλή και αμετάβλητο τρόπο. Στη συνέχεια ακολουθεί η καταμέτρηση των ψήφων που καταγράφηκαν στο blockchain για τον προσδιορισμό των εκλογικών αποτελεσμάτων. Τα ψηφοδέλτια μπορούν να μετρηθούν χειροκίνητα ή χρησιμοποιώντας ένα αυτοματοποιημένο σύστημα, ανάλογα με το μέγεθος των εκλογών και τους διαθέσιμους πόρους. Ανάλογα με την εξέλιξη του προηγούμενου

σταδίου, ανακηρύσσεται ο νικητής ή το σύστημα προκηρύσσει εκλογές δεύτερου γύρου.

4.5.3 Υιοθέτηση Πρακτικών Ανοιχτών Δεδομένων (Open Data)

Μία σημαντική πτυχή της έξυπνης διακυβέρνησης συνιστά και η υιοθέτηση πρακτικών «ανοιχτών δεδομένων» δηλαδή η υιοθέτηση και εφαρμογή αρχών και στρατηγικών ώστε τα δεδομένα που συλλέγονται και παράγονται από τις υπηρεσίες και τα συστήματα της πανεπιστημιούπολης να είναι ανοικτά, ελεύθερα και εύκολα προσβάσιμα στο κοινό. Οι πρακτικές ανοικτών δεδομένων αποσκοπούν στην ενίσχυση της διαφάνειας καθώς και στην προώθηση της συνεργασίας, της συμμετοχής, της λογοδοσίας και της καινοτομίας. [62]

Οι R.Vasileva et al [63] πραγματοποιώντας μία ερευνητική μελέτη σε φοιτητές και ακαδημαϊκό προσωπικό σχετικά με τις θέσεις τους για την έννοια των ανοιχτών δεδομένων διαπίστωσαν τα ακόλουθα: Η πλειοψηφία των συνεντευξιαζόμενων συμφώνησε ότι τα οφέλη από τη χρήση των ανοιχτών δεδομένων είναι: 1) η αύξηση της φήμης του πανεπιστημίου και της εμπιστοσύνης του κοινού στα πανεπιστημιακά επιτεύγματα, 2) η χρήση των δεδομένων ως εκπαιδευτικού υλικού και η ανάλυση τους με σκοπό την ενοποίηση τους με την πύλη δεδομένων ανοιχτής διακυβέρνησης της πόλης, 3) η καλύτερη αξιοποίηση των πόρων και παροχή έγκαιρης πληροφόρησης αναφορικά με την διαθεσιμότητα των υπηρεσιών και 4) η αύξηση της δέσμευσης και της συμμετοχής των φοιτητών του κοινού στις δραστηριότητες του πανεπιστημίου. Εντούτοις, η έρευνα έδειξε ότι πέρα από τα οφέλη, οι συνεντευξιαζόμενοι επεσήμαναν και τους κινδύνους από τη χρήση των ανοιχτών δεδομένων και ειδικότερα διατύπωσαν τις επιφυλάξεις τους σχετικά το απόρρητο και την ασφάλεια των δεδομένων στον κυβερνοχώρο.

Αντίστοιχα, οι N.Verstaevel et al [64] παρουσιάζοντας το εγχείρημα της μετατροπής του Πανεπιστημίου της Τουλούζης III Paul Sabatier σε έξυπνο (NeOCampus) επισήμαναν ως ένα από τα βασικά χαρακτηριστικά του νέου αυτού πανεπιστημίου την ύπαρξη της πλατφόρμας των Ανοιχτών Δεδομένων προκειμένου να γίνεται εύκολα και γρήγορα ο διαμοιρασμός των συλλεχθέντων δεδομένων μεταξύ των φοιτητών, των ερευνητών, των καθηγητών και της διοίκησης. Επισημαίνουν μάλιστα ότι λόγω της συνεχούς προσθήκης νέων πηγών δεδομένων στο πλαίσιο της πανεπιστημιούπολης, η πρόκληση του όλου εγχειρήματος έγκειται στον σχεδιασμό της υποδομής της ως άνω πλατφόρμας με τέτοιο τρόπο ώστε η πρόσβαση στα

δεδομένα που προέρχονται από πολλαπλές πηγές (αισθητήρες που διαχειρίζονται οι υπεύθυνοι της διοίκησης του πανεπιστημίου, δεδομένα που συλλέγονται χειροκίνητα από τα εργαστήρια) να είναι εύκολη για όλους τους χρήστες χωρίς ταυτόχρονα να παραβιάζεται η ασφάλεια και το απόρρητο των δεδομένων.

Στην ίδια κατεύθυνση και ο Tomás Langebaek Carrizosa [68] πρότεινε στο πλαίσιο του ψηφιακού μετασχηματισμού του Πανεπιστημίου του Los Andes την υιοθέτηση μίας πλατφόρμας ανοιχτών δεδομένων αποσκοπώσα στην ενσωμάτωση σε αυτή δεδομένων που συλλέγονται από συσκευές του διαδικτύου των πραγμάτων εντός της πανεπιστημιούπολης, αξιοποιήσιμων στους τομείς της διδασκαλίας, της έρευνας και της εν γένει βελτιστοποίησης των πόρων και των διεργασιών της πανεπιστημιούπολης. Επισημαίνει ως βασικές προκλήσεις που πρέπει η εν λόγω πλατφόρμα να υπερκεράσει τη συνεχή μεταβολή του αριθμού και του τύπου των προστιθέμενων συσκευών, την ετερογένεια των δεδομένων, τη χρηστικότητα αυτής από τους τελικούς χρήστες καθώς επίσης και τη διαφύλαξη της ασφάλειας του συστήματος και του απορρήτου των δεδομένων.

4.6. ΕΞΥΠΝΑ ΔΕΔΟΜΕΝΑ (SMART DATA)

Είναι αναντίρρητο ότι την πεμπτουσία του οικοδομήματος της έξυπνης πανεπιστημιούπολης αποτελούν τα ποικίλης φύσεως και είδους δεδομένα, τα οποία συλλέγονται, επεξεργάζονται, αναλύονται και μετουσιώνονται σε χρήσιμες πληροφορίες, από τις ως άνω περιγραφόμενες υπηρεσίες με τη χρήση των προηγμένων τεχνολογιών. Μάλιστα ο όγκος των δεδομένων που παράγονται σε καθημερινή βάση στο πλαίσιο της πανεπιστημιούπολης είναι τόσο μεγάλος που καθιστούν επιτακτική την ανάγκη της ορθής διαχείρισης τους με απώτερο σκοπό την αποτελεσματικότερη εξαγωγή γνώσης μέσα από αυτά. Οι Wilkison et al [79] περιγράφουν μία σειρά από θεμελιώδεις αρχές (Ευρεσιμότητα, Προσβασιμότητα, Διαλειτουργικότητα και Επαναχρησιμοποίηση) που χρησιμεύουν ως κατευθυντήρια γραμμή προς το σκοπό του μέγιστου βαθμού αξιοποίησης της αξίας των δεδομένων.

Η εφαρμογή των ανωτέρω κατευθυντήριων αρχών μπορεί αναμφίβολα να μετατρέψει τα μεγάλα δεδομένα σε έξυπνα δεδομένα, ήτοι σε δεδομένα που αν και προέρχονται από διαφορετικές πηγές, εισάγονται, συσχετίζονται, φιλτράρονται, αναλύονται κ.λπ. για να τροφοδοτήσουν συστήματα τα οποία είναι σε θέση να λαμβάνουν αποφάσεις και να προτείνουν ενέργειες που οδηγούν σε ορθές επιχειρηματικές αποφάσεις [80]. Μάλιστα, τα έξυπνα δεδομένα προσφέρουν

εξατομικευμένες και αξιοποιήσιμες γνώσεις, οι οποίες απαιτούν τη χρήση μεταδεδομένων, την εφαρμογή γνώσεων ειδικού τομέα, την προσφυγή στον επιστήμη της σημασιολογίας και την εφαρμογή διαδικασιών ευφυούς επεξεργασίας [81].

Κατ' άλλους ερευνητές [19] τα έξυπνα δεδομένα συνίστανται σε οργανωμένα δεδομένα που προστατεύονται από κακόβουλες προθέσεις τρίτων και είναι προσβάσιμα μόνο από εξουσιοδοτημένα πρόσωπα και συσκευές. Η δε προστασία αυτών επιτυγχάνεται με την υιοθέτηση μηχανισμών ψηφιακής αυθεντικοποίησης και αναγνώρισης των συνδεδεμένων στο δίκτυο συσκευών, με τη συνδρομή των οποίων μπορούν να ανιχνευθούν ύποπτες και ασυνήθιστες συμπεριφορές αυτών και κατ' επέκταση να ανιχνευθούν και οι κακόβουλοι κόμβοι που συνιστούν απειλή για την ασφάλεια και την ακεραιότητα των δεδομένων [82].

Στο πλαίσιο της έξυπνης πανεπιστημιούπολης, οι Yousefnezhad et al. [83] ανέπτυξαν έναν μηχανισμό Αναγνώρισης Συσκευών βάσει μετρήσεων (Measurementbased Device Identification – MeDI) που βασίζεται στην παρακολούθηση της συμπεριφοράς της συσκευής ή του προφίλ της συσκευής τον οποίο δοκίμασαν πειραματικά μέσω τριών μεθόδων αναγνώρισης. Πιο συγκεκριμένα, ο μηχανισμός αυτός παρακολουθεί τα πακέτα δεδομένων που προέρχονται από τις έξυπνες συσκευές με σκοπό τη προστασία του διακομιστή από τη λήψη και τη διάδοση εσφαλμένων δεδομένων. Αντίστοιχα, οι L.Zheng et al [84] με γνώμονα να αντιμετωπίσουν τις προκλήσεις που σχετίζονται με τον έλεγχο ταυτότητας και την προστασία της ιδιωτικής ζωής σε εφαρμογές RFID εντός έξυπνων πανεπιστημιουπόλεων, πρότειναν ένα νέο και βελτιωμένο πρωτόκολλο αμοιβαίου ελέγχου ταυτότητας RFID. Το πρωτόκολλο αυτό αναπτύσσεται μέσω ανάλυσης των υφιστάμενων πρωτοκόλλων ελέγχου ταυτότητας σε έξυπνες πανεπιστημιουπόλεις που βασίζονται σε αλγόριθμους κατακερματισμού. Ενσωματώνει τη χρήση τεχνολογιών τυχαίου αριθμού (S) και χρονοσήμανσης (T). Το προτεινόμενο πρωτόκολλο διευκολύνει τον αμοιβαίο έλεγχο ταυτότητας μεταξύ της ετικέτας RFID, του αναγνώστη και της βάσης δεδομένων backend, χωρίς να προϋποθέτει ότι η διαδρομή σήματος μεταξύ της βάσης δεδομένων και της επικοινωνίας του αναγνώστη είναι εγγενώς ασφαλής. Προστατεύει αποτελεσματικά από διάφορους τύπους επιθέσεων, συμπεριλαμβανομένων των επιθέσεων πλαστογράφησης, των επιθέσεων εντοπισμού θέσης, των επιθέσεων υποκλοπής, καθώς και των επιθέσεων άρνησης παροχής υπηρεσιών. Σε σύγκριση με τα υπάρχοντα πρωτόκολλα ελέγχου ταυτότητας, το προτεινόμενο υπερέχει όσον αφορά το κόστος πολυπλοκότητας του υπολογισμού και

των επιδόσεων ασφαλείας ενώ παράλληλα είναι σε θέση να ικανοποιήσει τις εξελισσόμενες απαιτήσεις ασφαλείας των κινητών εφαρμογών RFID σε έξυπνες πανεπιστημιουπόλεις.

ΚΕΦΑΛΑΙΟ 5 – ΖΗΤΗΜΑΤΑ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΚΑΙ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

5.1 Εγγενείς Ευπάθειες και Είδη (Κυβερνο)Επιθέσεων στο πλαίσιο της έξυπνης πανεπιστημιούπολης

Η ευρεία χρήση των προηγμένων και σύγχρονων τεχνολογιών που αναλύθηκαν ως άνω και επί τη βάση των οποίων στηρίζεται η οικοδόμηση και συνεχής εξέλιξη της έξυπνης πανεπιστημιούπολης με τις επιμέρους υπηρεσίες της, εκτός από τα πολυάριθμα οφέλη που προσφέρει, εγκυμονεί και ορισμένους κινδύνους για την κυβερνοασφάλεια καθώς και για τη διαφύλαξη της ιδιωτικότητας και του απορρήτου. Όλες αυτές οι διασυνδεδεμένες μεταξύ τους έξυπνες συσκευές και εφαρμογές μέσω των οποίων πραγματοποιείται η μεταφορά πληροφοριών πολλές φορές μάλιστα μέσω αδύναμων πρωτοκόλλων ή μη ασφαλών μέσων, αποτελούν εν δυνάμει απειλές για την ασφάλεια της πανεπιστημιούπολης, επειδή μπορούν να λειτουργήσουν ως σημεία εισόδου για επιθέσεις στο δίκτυο [113]. Με άλλα λόγια, υφίστανται εγγενώς ορισμένες ευπάθειες του τεχνολογικού εξοπλισμού της έξυπνης πανεπιστημιούπολης, ήτοι κάποια από τα συστήματα, τις εφαρμογές ή τις υπηρεσίες της φέρουν κάποια ελαττώματα που επιτρέπουν σε έναν εισβολέα να έχει πρόσβαση, να παραβιάζει τους ελέγχους ασφαλείας, να εκμεταλλεύεται το σύστημα και να το χειραγωγεί με τρόπους που δεν είχαν ποτέ προβλεφθεί από τον προγραμματιστή [112].

Οι ευπάθειες αυτές γίνονται καλύτερα αντιληπτές αν συσχετιστούν με το είδος των επιθέσεων που συναντώνται συνήθως στα πλαίσια των έξυπνων πανεπιστημιουπόλεων και οι οποίες επιθέσεις διακρίνονται στις ακόλουθες κατηγορίες:

5.1.1 Φυσικές Επιθέσεις (Physical Attacks)

Στην κατηγορία αυτή εμπίπτουν οι επιθέσεις που στοχεύουν κατά της ακεραιότητας του υλικού εξοπλισμού της πανεπιστημιούπολης ήτοι κατά των συσκευών, των αισθητήρων, των ελεγκτών, των αναγνωστών RFID με σκοπό να βλαφθεί η διάρκεια ζωής ή η λειτουργικότητα αυτών [114]. Πιο συγκεκριμένα, εδώ εμπίπτει: 1) η κλοπή των ως άνω φυσικών αντικειμένων που επιτρέπει στον

επιτιθέμενο να αποκτήσει την φυσική πρόσβαση στις συσκευές και στη συνέχεια να εκτελεί επιθέσεις που παραβιάζουν την ιδιωτική ζωή των φοιτητών και διαταράσσουν την διαθεσιμότητα και εμπιστευτικότητα των συστημάτων [115], 2) η κοινωνική μηχανική (Social Engineering) όπου ο επιτιθέμενος χειραγωγεί τους χρήστες με μηνύματα ηλεκτρονικού ταχυδρομείου ή τηλεφωνικές κλήσεις προκειμένου να αποσπάσει εμπιστευτικές πληροφορίες για την εκτέλεση ορισμένων ενεργειών[113], 3) η επίθεση στέρησης ύπνου (Sleep Deprivation Attack), η οποία πραγματοποιείται με τη διατήρηση των κόμβων σε εγρήγορση προκειμένου να επιτευχθεί μεγαλύτερη κατανάλωση ενέργειας των μπαταριών που τροφοδοτούν τους κόμβους και συνεπώς να οδηγήσουν σε απενεργοποίηση των κόμβων [114] και 4) Τοποθέτηση κακόβουλων κόμβων (Malicious Nodes Injection) όπου ο επιτιθέμενος εισάγει με φυσικό τρόπο έναν νέο κακόβουλο κόμβο μεταξύ δύο ή περισσότερων κόμβων για να χρησιμοποιηθεί ως κανονικός κόμβος με σκοπό να τροποποιήσει, να ανακτήσει, να επεξεργαστεί και να ανακατευθύνει τις εσφαλμένες πληροφορίες στους άλλους κόμβους. Αυτή η επίθεση αποσκοπεί στη δημιουργία μη φυσιολογικών συμπεριφορών που επιδρούν στη λειτουργικότητα και τις υπηρεσίες της πανεπιστημιούπολης ώστε να δώσει στον επιτιθέμενο τον πλήρη έλεγχο του συστήματος-στόχου [116].

5.1.2 Επιθέσεις κατά του Λογισμικού (Software Attacks)

Στην κατηγορία αυτή εμπίπτουν επιθέσεις κατά τις οποίες ο επιτιθέμενος εκμεταλλεύεται το σύστημα με τη χρήση προγραμμάτων δούρειου ίππου, σκουληκιών, ιών, spyware και κακόβουλων σεναρίων που μπορούν να αποσπάσουν πληροφορίες, να αλλοιώσουν δεδομένα, να αρνηθούν την παροχή υπηρεσιών και ακόμη και να βλάψουν τις συσκευές ενός συστήματος [114]. Πιο συγκεκριμένα, εδώ εμπίπτουν οι επιθέσεις phishing όπου ο επιτιθέμενος αποκτά πρόσβαση σε εμπιστευτικά δεδομένα παραποιώντας τα διαπιστευτήρια ελέγχου ταυτότητας ενός χρήστη, συνήθως μέσω μολυσμένων μηνυμάτων ηλεκτρονικού ταχυδρομείου ή ψεύτικων ιστοσελίδων καθώς και οι ιοί (virus), τα σκουλήκια (worms), ο δούρειος ίππος (trojan horse), το λογισμικό κατασκοπείας (spyware), άπαντα τα οποία συνιστούν κακόβουλα λογισμικά που χρησιμοποιούνται από έναν επιτιθέμενο για να μολύνει το σύστημα της έξυπνης πανεπιστημιούπολης. Αυτό το κακόβουλο λογισμικό μπορεί να εξαπλωθεί μέσω της λήψης αρχείων από το Διαδίκτυο, συνημμένων μηνυμάτων ηλεκτρονικού ταχυδρομείου κ.λπ. ενώ ορισμένα από αυτά μπορεί να

αναπαράγονται μόνα τους χωρίς να υπάρχει ανθρώπινη ενέργεια ή να αλλοιώνουν τα δεδομένα του χρήστη χωρίς καν ο χρήστης να το γνωρίζει [116].

5.1.3 Επιθέσεις Κρυπτογράφησης (Encryption Attacks)

Αυτός ο τύπος επιθέσεων αποτελεί επικίνδυνη απειλή για την ασφάλεια και την απόρρητο των κρυπτογραφικών μονάδων. Ο επιτιθέμενος έχει ως στόχο να ανακαλύψει και να καταστρέψει το κλειδί κρυπτογράφησης που χρησιμοποιείται στην κρυπτογράφηση και αποκρυπτογράφηση των πρωτοκόλλων, των ενοτήτων, των δεδομένων και των συσκευών με τη χρήση ειδικών τεχνικών [113], όπως: α) Επιθέσεις κρυπτανάλυσης (cryptanalysis attack): αυτός ο τύπος επιθέσεων χρησιμοποιείται για να σπάσει το σύστημα κρυπτογραφικής ασφάλειας με την ανίχνευση του κλειδιού κρυπτογράφησης που χρησιμοποιείται και στη συνέχεια αποκτήσει πρόσβαση σε κρυπτογραφημένα μηνύματα [113], β) Επιθέσεις πλευρικού καναλιού (Side channel attack): ο επιτιθέμενος συλλέγει πληροφορίες σχετικά με τις ενέργειες των συσκευών κατά την εκτέλεση κρυπτογραφικών πράξεων, όπως ο χρόνος που απαιτείται για την ολοκλήρωση της λειτουργίας, η κατανάλωση ενέργειας, η ηλεκτρομαγνητική ακτινοβολία, η συχνότητα σφαλμάτων και στη συνέχεια χρησιμοποιεί αυτές τις πληροφορίες για να ανιχνεύσει το κλειδί κρυπτογράφησης[116], γ) Επίθεση Ενδιαμέσου Ατόμου (Man in the Middle Attack): Στη περίπτωση αυτή, όταν δύο χρήστες ενός έξυπνου συστήματος, ανταλλάσσουν κλειδιά κατά τη διάρκεια ενός σεναρίου πρόσκλησης-απάντησης, ώστε να δημιουργηθεί ένα ασφαλές κανάλι επικοινωνίας μεταξύ τους, ένας κακόβουλος τρίτος τοποθετείται στη μεταξύ τους γραμμή επικοινωνίας. Στη συνέχεια, αυτός υποκλέπτει τα σήματα που στέλνουν ο ένας στον άλλον και επιχειρεί να παρέμβει πραγματοποιώντας ανταλλαγή κλειδιών με τους δύο χρήστες ξεχωριστά. Ο κακόβουλος τρίτος θα είναι τότε σε θέση να κρυπτογραφήσει/ αποκρυπτογραφήσει οποιαδήποτε δεδομένα προέρχονται από τους χρήστες με τα κλειδιά που μοιράζεται και με τους δύο ενώ οι χρήστες θα νομίζουν ότι μιλούν μεταξύ τους [114].

5.1.4 Επιθέσεις κατά του Δικτύου (Network Attacks)

Σε αυτή τη κατηγορία ανήκουν οι επιθέσεις που βάλλουν κατά του δικτύου της έξυπνης πανεπιστημιούπολης και μάλιστα ο επιτιθέμενος δε χρειάζεται να βρίσκεται κοντά στο δίκτυο για να λειτουργήσει η επίθεση αλλά μπορεί και

απομακρυσμένα. Τα κυριότερη είδη επιθέσεων αυτής της κατηγορίας είναι τα ακόλουθα: 1) Επιθέσεις ανάλυσης της κυκλοφορίας (Traffic Analysis Attack): βασίζεται στην υποκλοπή και εξέταση της κίνησης του δικτύου για την εξαγωγή συμπερασμάτων και την απόκτηση σημαντικών πληροφοριών από τα μοτίβα επικοινωνίας τις οποίες και θα χρησιμοποιήσει ο κακόβουλος τρίτος στις επιθέσεις του όπως η θέση των βασικών κόμβων, η δομή δρομολόγησης, ακόμη και τα πρότυπα συμπεριφοράς των εφαρμογών [113], 2) Υποκλοπή (Eavesdropping): Αυτή η επίθεση στρέφεται κατά της εμπιστευτικότητας του περιβάλλοντος της έξυπνης πανεπιστημιούπολης και είναι η πιο κοινώς αναγνωρισμένη απειλή που βάλλεο κατά της ασφάλειας στα ανοικτά συστήματα. Σε αυτή τη περίπτωση, ένας επιτιθέμενος μπορεί να παρακολουθεί όλη την κυκλοφορία δεδομένων στα δίκτυα έξυπνων πανεπιστημιουπόλεων χωρίς να το γνωρίζουν οι εξουσιοδοτημένοι χρήστες. Παραδείγματος χάρη, σε ένα σύστημα RFID, οι αναγνώστες και οι ετικέτες συνδέονται ασύρματα και επικοινωνούν χωρίς καμία ανθρώπινη παρέμβαση ή τεχνική κρυπτογράφησης. Επομένως, υπάρχει πιθανότητα το μέσο επικοινωνίας τους να υποκλαπεί για να αποκτηθούν ευαίσθητες πληροφορίες και δεδομένα από τις RFID ετικέτες χωρίς αυτό να γίνει εύκολα αντιληπτό [118,119], 3) Άρνηση παροχής υπηρεσιών (Denial of Service): Σε μια επίθεση άρνησης υπηρεσίας, ο στόχος είναι να καταστεί μια υπηρεσία δικτύου μη προσβάσιμη στους χρήστες ή απλώς να δυσχερανθεί η προσβασιμότητα των χρηστών σε υπηρεσίες. Ο επιτιθέμενος το επιτυγχάνει αυτό κατακλύζοντας τους διακομιστές και τις συσκευές που είναι συνδεδεμένες στο Διαδίκτυο με συντριπτικό όγκο μηνυμάτων ή κίνησης, υπερφορτώνοντας τη χωρητικότητά τους και καθιστώντας τους μη διαθέσιμους στους χρήστες. Η τακτική αυτή επεκτείνεται και με την παρεμπόδιση της μετάδοσης της κυκλοφορίας τόσο με ενσύρματα όσο και με ασύρματα μέσα εντός των ορίων της έξυπνης πανεπιστημιούπολης, διαταράσσοντας έτσι τις κανονικές λειτουργίες του δικτύου [118].

5.1.5 Επιθέσεις κατά της Προστασίας των Δεδομένων (Data Privacy Attacks)

Πρόκειται για μία κατηγορία επιθέσεων όπου οι επιτιθέμενοι εξαπολύουν απειλές και επιθέσεις που στοχεύουν στη χρήση, τη συλλογή, τη διαγραφή και την αποθήκευση δεδομένων. Ως εκ τούτου, η προστασία των ποικίλης φύσεως δεδομένων έχει καταστεί σημαντική απαίτηση λόγω του μεγάλου όγκου πληροφοριών στις

οποίες μπορεί να υπάρξει εύκολη πρόσβαση μέσω μηχανισμών απομακρυσμένης πρόσβασης [120]. Οι κυριότερες μορφές επιθέσεων αυτής της κατηγορίας είναι οι ακόλουθες: 1) Παραβιάσεις Δεδομένων (Data Breaches): Ως παραβίαση δεδομένων νοείται η διαρροή ευαίσθητων προσωπικών δεδομένων χρηστών της πανεπιστημιούπολης από μη εξουσιοδοτημένα άτομα. Αυτό συμβαίνει όταν κακόβουλοι χρήστες επιτίθενται με μη εξουσιοδοτημένο τρόπο στην πηγή δεδομένων της έξυπνης πανεπιστημιούπολης, χρησιμοποιώντας διάφορες τεχνικές για να διεισδύσουν στα δεδομένα και να αποσπάσουν ευαίσθητες πληροφορίες [113], 2) Απώλεια Δεδομένων (Data Loss): Υφίσταται στις περιπτώσεις που τα δεδομένα δεν είναι οχυρωμένα με ασφαλή τρόπο και έτσι μπορούν εύκολα να εκτεθούν σε κίνδυνο. Οι συνηθέστεροι λόγοι απώλειας δεδομένων είναι η διαγραφή ή αλλοίωση των δεδομένων, οι διακοπές ρεύματος [121], 3) Πειρατεία λογαριασμού ή υπηρεσίας (Account or Service Hijacking): Η πειρατεία υπηρεσιών ή λογαριασμών αναφέρεται στη μη εξουσιοδοτημένη πρόσβαση και τον έλεγχο της διαδικτυακής υπηρεσίας ή του λογαριασμού χρήστη ενός ατόμου ή οργανισμού από κακόβουλους φορείς. Αυτός ο τύπος κυβερνοεπίθεσης περιλαμβάνει συνήθως την παραβίαση των διαπιστευτηρίων σύνδεσης, όπως ονόματα χρήστη και κωδικούς πρόσβασης, επιτρέποντας στον επιτιθέμενο να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στον στοχευόμενο λογαριασμό ή υπηρεσία [113].

5.2 Εισαγωγικές Παρατηρήσεις για τα Ζητήματα Ιδιωτικότητας εντός της έξυπνης πανεπιστημιούπολης

Όπως προαναφέρθηκε, η ενσωμάτωση προηγμένων τεχνολογιών εντός της έξυπνης πανεπιστημιούπολης εγείρει σημαντικές ανησυχίες σχετικά με την προστασία της ιδιωτικής ζωής, με τα δεδομένα να βρίσκονται στο επίκεντρο αυτών των προβληματισμών. Ο διασυνδεδεμένος χαρακτήρας των έξυπνων συστημάτων, από κάμερες παρακολούθησης και βιομετρικούς σαρωτές έως συσκευές Διαδικτύου των Πραγμάτων και αισθητήρες εντοπισμού θέσης, παράγει έναν εκτεταμένο όγκο δεδομένων προσωπικού χαρακτήρα. Και ενώ οι νέες τεχνολογίες συμβάλλουν στην αποτελεσματικότητα και την ευκολία της καθημερινότητας στην πανεπιστημιούπολη, δεν παύουν να ενέχουν και εγγενείς κινδύνους για την ιδιωτική ζωή του ατόμου. Η συλλογή, η αποθήκευση και η ανάλυση δεδομένων, όπως οι κινήσεις των φοιτητών και του διδακτικού προσωπικού, τα πρότυπα συμπεριφοράς και οι βιομετρικές πληροφορίες, απαιτούν αυστηρά μέτρα για την προστασία από μη εξουσιοδοτημένη

πρόσβαση και πιθανή κατάχρηση. Η επίτευξη μιας λεπτής ισορροπίας μεταξύ των πλεονεκτημάτων των έξυπνων τεχνολογιών και της προστασίας των προσωπικών πληροφοριών είναι υψίστης σημασίας και απαιτεί ισχυρές πολιτικές προστασίας της ιδιωτικής ζωής, διαφανείς πρακτικές διαχείρισης των δεδομένων και προληπτικά μέτρα ασφαλείας, ώστε να διασφαλιστεί ότι η έξυπνη πανεπιστημιούπολη προωθεί την καινοτομία χωρίς να διακυβεύεται η ιδιωτικότητα των ατόμων.

Η προστασία των δεδομένων που παράγονται, συλλέγονται, αποθηκεύονται και καθίστανται αντικείμενο επεξεργασίας εντός της έξυπνης πανεπιστημιούπολης και ιδίως των προσωπικών δεδομένων των ατόμων της ευρύτερης ακαδημαϊκής κοινότητας θα μας απασχολήσει κατωτέρω υπό τη νομική σκοπιά.

5.3 Ευρωπαϊκό Νομοθετικό Πλαίσιο για την προστασία των προσωπικών δεδομένων

5.3.1 Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων

Το βασικότερο νομοθέτημα το οποίο εφαρμόζεται για την προστασία των προσωπικών δεδομένων των ατόμων στο πλαίσιο της ευρωπαϊκής ολοκλήρωσης γενικά και της έξυπνης πανεπιστημιούπολης ειδικά είναι ο Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου ή αλλιώς ο «Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (ΓΚΠΔ)/ General Data Protection Regulation (GDPR)» (εφεξής: ΓΚΠΔ), που τέθηκε σε εφαρμογή στις 25/5/2018.

Πρόκειται για ένα ενωσιακό νομοθέτημα που θεσπίζει κανόνες που αφορούν την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και κανόνες που αφορούν την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα, προστατεύοντας παράλληλα θεμελιώδη δικαιώματα και ελευθερίες των προσώπων αυτών [123]. Άξια αναφοράς στο παρόν σημείο είναι απόσπασμα της Σκέψης (4) του Προοιμίου του ΓΚΠΔ, σύμφωνα με το οποίο *«Το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα δεν είναι απόλυτο δικαίωμα· πρέπει να εκτιμάται σε σχέση με τη λειτουργία του στην κοινωνία και να σταθμίζεται με άλλα θεμελιώδη δικαιώματα, σύμφωνα με την αρχή της αναλογικότητας».*

Εκτός από τον ΓΚΠΔ, σε ευρωπαϊκό πλαίσιο εφαρμόζεται και το άρθρο 8 του Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ, το οποίο ορίζει ότι κάθε πρόσωπο έχει δικαίωμα στην προστασία των προσωπικών του δεδομένων, το άρθρο 8 της

Ευρωπαϊκής Σύμβασης των Δικαιωμάτων του Ανθρώπου, το άρθρο ΣΤ' της Συνθήκης για την Ευρωπαϊκή Ένωση, η Σύμβαση 108 του Συμβουλίου της Ευρώπης και η επικαιροποίηση αυτής [126]. Στην Ελλάδα, ο εφαρμοστικός εθνικός νόμος ως προς τα μέτρα εφαρμογής του ΓΚΠΔ είναι ο Ν. 4624/2019 (ΦΕΚ Α' 137/29-8-2019) ο οποίος εξειδικεύει τον ΓΚΠΔ και λειτουργεί συμπληρωματικά προς αυτόν.

5.3.2 Τα επιμέρους προσωπικά δεδομένα που συλλέγονται εντός της έξυπνης πανεπιστημιούπολης

Ο ΓΚΠΔ στο άρθρο 4 περ. 1 [123] περιέχει σαφή ορισμό της έννοιας των προσωπικών δεδομένων που καταλαμβάνονται από το ρυθμιστικό του πεδίο και ειδικότερα **απλά δεδομένα προσωπικού χαρακτήρα** είναι *«κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου».*

Ειδική κατηγορία των ως άνω δεδομένων προσωπικού χαρακτήρα τα οποία τυγχάνουν αυστηρότερης μεταχείρισης και αυξημένης προστασίας, συνιστούν τα **Ειδικά ή αλλιώς Ευαίσθητα** Δεδομένα Προσωπικού Χαρακτήρα ήτοι αυτά που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, τα γενετικά δεδομένα, τα βιομετρικά δεδομένα με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένα που αφορούν την υγεία καθώς επίσης και δεδομένα που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό του (άρθρο 9 παρ.1 του ΓΚΠΔ) [123].

Στο πλαίσιο της έξυπνης πανεπιστημιούπολης, συλλέγεται μία πληθώρα δεδομένων ανηκόντων είτε στην κατηγορία των απλών [δεδομένα ταυτότητας (Κωδικός χρήστη, Ονοματεπώνυμο, Όνομα Πατέρα και Μητέρας, Φωτογραφία, Αριθμός Ταυτότητας ή Διαβατηρίου, εκδούσα Αρχή, Ημ. Έκδοσης), δεδομένα επικοινωνίας (ταχυδρομική διεύθυνση, σταθερά και κινητά τηλέφωνα, διεύθυνση ηλεκτρονικού ταχυδρομείου), δεδομένα θέσης, εκπαιδευτικά δεδομένα σχετικά με τις επιδόσεις ή τις παρουσίες των φοιτητών] είτε στην κατηγορία των ευαίσθητων προσωπικών δεδομένων [δεδομένα που αφορούν δημογραφικά δεδομένα

(εθνικότητα, υπηκοότητα, θρήσκευμα), δεδομένα που αφορούν την υγεία (πχ ιατρικά πιστοποιητικά ή γνωματεύσεις) ή βιομετρικά δεδομένα (εικόνες προσώπου ή δακτυλοσκοπικά δεδομένα]. Προσωπικά δεδομένα μάλιστα συνιστούν και αυτά που έχουν προκύψει ως αποτέλεσμα ψευδωνυμοποίησης, ήτοι συνιστούν δεδομένα που δε μπορούν να αποδοθούν σε συγκεκριμένο υποκείμενο δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, οι οποίες πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα. Χαρακτηριστικό παράδειγμα αποτελούν τα επιγραμμικά αναγνωριστικά στοιχεία ταυτότητας όπως πχ η διεύθυνση IP, που σύμφωνα με την υπ' αριθμ. 2/2002 Γνώμη της Ομάδας Εργασίας του άρθρου 29 συνιστά προσωπικό δεδομένο, καθώς μπορεί έμμεσα και σε συνδυασμό με άλλες πληροφορίες να φανερώσει την ταυτότητα του φυσικού προσώπου που προβαίνει σε χρήση μιας συσκευής [125].

Σημειωτέον ότι δεν τυγχάνουν προστασίας από τον ΓΚΠΔ: α) τα δεδομένα προσωπικού χαρακτήρα θανόντων (Σκέψη 27 του Προοιμίου [123]), β) τα δεδομένα προσωπικού χαρακτήρα που έχουν καταστεί ανώνυμα κατά τρόπο ώστε η ταυτότητα του υποκειμένου των δεδομένων να μη μπορεί ή να μη μπορεί πλέον να εξακριβωθεί (Σκέψη 26 του Προοιμίου [123]) και γ) τα δεδομένα που δε σχετίζονται με φυσικά πρόσωπα όπως πχ. τα περιβαλλοντολογικά δεδομένα που συλλέγονται από τις διάφορες συσκευές του Διαδικτύου των Πραγμάτων.

5.3.3 Κατηγορίες υποκειμένων, Πράξεις επεξεργασίας προσωπικών δεδομένων και Αρχές που διέπουν αυτή

Τα δεδομένα προσωπικού χαρακτήρα που συλλέγονται εντός της έξυπνης πανεπιστημιούπολης προέρχονται κυρίως από τις ακόλουθες κατηγορίες υποκειμένων: α) εργαζόμενους του έξυπνου Πανεπιστημίου από τους οποίους συλλέγονται προσωπικά δεδομένα σχετιζόμενα με τη σύμβαση εργασίας τους, β) συνεργάτες ή προμηθευτές του έξυπνου πανεπιστημίου από τους οποίους συλλέγονται προσωπικά δεδομένα σχετιζόμενα με τη συμβατική σχέση που αναπτύσσουν με το τελευταίο όπως ενδεικτικά οικονομικά στοιχεία και φυσικά γ) όλους τους συναλλασσόμενους με την έξυπνη πανεπιστημιούπολη (Φοιτητές, καθηγητές, πολίτες) από τους οποίους συλλέγονται προσωπικά δεδομένα που προκύπτουν από έννομες υποχρεώσεις ή δραστηριότητες του πανεπιστημίου.

Τα προσωπικά δεδομένα όλων των ως άνω υποκειμένων υπόκεινται σε διάφορες πράξεις επεξεργασίας στις οποίες σύμφωνα με το άρθρο 4 περ. 2 του ΓΚΠΔ

εντάσσονται η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η συσχέτιση, ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή. Η νόμιμη βάση της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα ποικίλλει ανάλογα με την εκάστοτε επιτελούμενη λειτουργία και τον σκοπό για τον οποίο γίνεται η επεξεργασία [124].

Ο υπεύθυνος επεξεργασίας ήτοι εκείνος που καθορίζει τους σκοπούς και τον τρόπο επεξεργασίας των δεδομένων προσωπικού χαρακτήρα είναι το ίδιο το εκπαιδευτικό ίδρυμα μέσω της διοίκησης του, όντας υπεύθυνο για τη διαχείριση και τη λειτουργία της πανεπιστημιούπολης. Αντίθετα, οι εκτελούντες την επεξεργασία ήτοι τα φυσικά ή νομικά πρόσωπα, υπηρεσίες ή άλλοι φορείς που επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου επεξεργασίας είναι συνήθως οι πάροχοι υπηρεσιών νέφους, οι πάροχοι συσκευών διαδικτύου των πραγμάτων, οι πάροχοι συστημάτων πληροφοριών φοιτητών που διαχειρίζονται τα δεδομένα των φοιτητών, τα αρχεία παρουσίας, τους βαθμούς τους καθώς και οι πάροχοι συστημάτων ασφαλείας, συμπεριλαμβανομένων των καμερών παρακολούθησης, των συστημάτων ελέγχου πρόσβασης και άλλων μέτρων ασφαλείας.

Οι αρχές που διέπουν την επεξεργασία των προσωπικών δεδομένων είναι οι ακόλουθες (άρθρο 5 παρ. 1 και 2 του ΓΚΠΔ):

- Αρχή της νομιμότητας, αντικειμενικότητας και διαφάνειας. Πιο συγκεκριμένα, η αρχή αυτή επιτάσσει η επεξεργασία των δεδομένων να γίνεται με σύννομο τρόπο ήτοι να βασίζεται σε έναν από τους νόμιμους λόγους επεξεργασίας του άρθρου 6 του ΓΚΠΔ *[α) συγκατάθεση του υποκειμένου των δεδομένων, β) αναγκαιότητα για τη σύναψη σύμβασης, γ) συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας, δ) αναγκαιότητα για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου προσώπου, ε) αναγκαιότητα για την εκπλήρωση καθήκοντος δημόσιου συμφέροντος, στ) αναγκαιότητα για τα έννομα συμφέροντα του υπευθύνου επεξεργασίας ή τρίτου, εκτός εάν υπερισχύουν έναντι αυτών τα συμφέροντα και τα δικαιώματα του υποκειμένου των δεδομένων]* αν πρόκειται για απλά δεδομένα ή του άρθρου 9 παρ. 2 του ΓΚΠΔ αν πρόκειται για ευαίσθητα δεδομένα. Περαιτέρω, η επεξεργασία των προσωπικών δεδομένων πρέπει να γίνεται με αντικειμενικό τρόπο που σημαίνει πρακτικά ότι οι υπεύθυνοι επεξεργασίας θα πρέπει να ενημερώνουν τα υποκείμενα των δεδομένων και το ευρύ κοινό ότι θα επεξεργάζονται τα δεδομένα με

σύννομο και διαφανή τρόπο. Οι πράξεις επεξεργασίας πρέπει να διενεργούνται φανερά και τα υποκείμενα των δεδομένων θα πρέπει να έχουν επίγνωση των δυνητικών κινδύνων. Επιπλέον, στο μέτρο που είναι εφικτό, οι υπεύθυνοι επεξεργασίας πρέπει να ενεργούν κατά τρόπο που συμμορφώνεται άμεσα με τις επιθυμίες του υποκειμένου των δεδομένων, ιδίως όταν η συγκατάθεση αυτού αποτελεί τη νομική βάση για την επεξεργασία τους [127]. Ακόμη, η επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να πραγματοποιείται με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων που σημαίνει πρακτικά ότι ο υπεύθυνος επεξεργασίας οφείλει να λαμβάνει κατάλληλα μέτρα ώστε να τηρεί ενήμερα τα υποκείμενα των δεδομένων σχετικά με τον τρόπο χρήσης των δεδομένων τους. Η διαφάνεια μπορεί να αφορά τις πληροφορίες που παρέχονται στο φυσικό πρόσωπο προτού ξεκινήσει η επεξεργασία, τις πληροφορίες στις οποίες τα υποκείμενα των δεδομένων πρέπει να έχουν άμεση πρόσβαση κατά τη διάρκεια της επεξεργασίας, αλλά και τις πληροφορίες που παρέχονται στα υποκείμενα των δεδομένων κατόπιν αιτήματός τους για πρόσβαση στα δεδομένα που τα αφορούν [127].

- Αρχή του περιορισμού του σκοπού ήτοι η επεξεργασία πρέπει να πραγματοποιείται για καθορισμένους, νόμιμους και ρητούς σκοπούς. Οποιοσδήποτε νέος σκοπός επεξεργασίας δεδομένων που είναι ασύμβατος με τον αρχικό πρέπει να έχει τη δική του νομική βάση και δεν μπορεί να δικαιολογείται από το γεγονός ότι τα δεδομένα αποκτήθηκαν αρχικά ή υποβλήθηκαν σε επεξεργασία για άλλο νόμιμο σκοπό.
- Αρχή της αναλογικότητας άλλως ελαχιστοποίησης των δεδομένων ήτοι τα υπό επεξεργασία δεδομένα πρέπει να είναι κατάλληλα και συναφή και να περιορίζονται στο αναγκαίο μέτρο σε σχέση με τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία.
- Αρχή της ακρίβειας ήτοι τα υπό επεξεργασία δεδομένα πρέπει να είναι ακριβή και να επικαιροποιούνται κατά το αναγκαίο μέτρο ενώ ταυτόχρονα πρέπει να επιδιώκεται άμεση διαγραφή ή διόρθωση των δεδομένων που είναι ανακριβή σε σχέση με τους σκοπούς της επεξεργασίας.
- Αρχή του περιορισμού της περιόδου αποθήκευσης ήτοι 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. Επομένως, νόμιμη αποθήκευση δεδομένων τα οποία δεν είναι πλέον αναγκαία θα μπορούσε να επιτευχθεί μέσω της ανωνυμοποίησής τους [127].

- Αρχή της ακεραιότητας και της εμπιστευτικότητας ήτοι η επεξεργασία των δεδομένων πρέπει να γίνεται με τη χρήση κατάλληλων τεχνικών ή οργανωτικών μέτρων ώστε να διαφυλάσσεται η ασφάλεια των δεδομένων από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά.
- Αρχή της λογοδοσίας που ισχύει για τον υπεύθυνο επεξεργασίας ήτοι ο τελευταίος έχει την ευθύνη και την υποχρέωση να αποδείξει ανά πάσα στιγμή τη συμμόρφωση του με τις ως άνω αναλυτικά αναφερόμενες αρχές. Σύμφωνα με την υπ' αριθμ. 3/2010 γνώμη της Ομάδας εργασίας του άρθρου 29 [128], η λογοδοσία συνίσταται ουσιαστικά στην υποχρέωση του υπευθύνου επεξεργασίας να θεσπίζει και να εφαρμόζει μέτρα τα οποία να διασφαλίζουν την τήρηση των κανόνων προστασίας δεδομένων στο πλαίσιο των πράξεων επεξεργασίας καθώς επίσης να διαθέτει τεκμηρίωση που να αποδεικνύει στα υποκείμενα των δεδομένων και στις εποπτικές αρχές τη λήψη μέτρων για την επίτευξη συμμόρφωσης προς τους κανόνες περί προστασίας δεδομένων. Οι ειδικότερες εκφάνσεις της αρχής αυτής θα αναλυθούν περισσότερο στο επόμενο κεφάλαιο.

5.4 Ειδικότερα ζητήματα προσωπικών δεδομένων που ανακύπτουν στο πλαίσιο της έξυπνης πανεπιστημιούπολης σε σχέση και με τις νέες τεχνολογίες

Παρακάτω θα επιχειρήσουμε να παρουσιάσουμε ορισμένα ειδικά ζητήματα προστασίας προσωπικών δεδομένων και κινδύνους που ανακύπτουν και επιδρούν σε αυτά από την ευρεία και συνεχώς αυξανόμενη χρήση των νέων τεχνολογιών εντός της έξυπνης πανεπιστημιούπολης με ταυτόχρονη επισκόπηση γνωμοδοτικών ή άλλων πονημάτων με τα οποία έχει επιχειρηθεί η επίλυση αυτών και τα οποία λειτουργούν συμπληρωματικά προς τον ΓΚΠΔ.

5.4.1 Συλλογή δεδομένων από έξυπνες συσκευές και Διαδίκτυο των Πραγμάτων

Την επανάσταση στην παραδοσιακή υποδομή της πανεπιστημιούπολης έφερε η τεχνολογία του Διαδικτύου των Πραγμάτων μετατρέποντας την σε ένα τεχνολογικά προηγμένο και διασυνδεδεμένο περιβάλλον που προάγει την καινοτομία, τη βιωσιμότητα και μια εμπλουτισμένη συνολική εμπειρία για όλο το ακαδημαϊκό προσωπικό. Άμεσα συνυφασμένη με το Διαδίκτυο των πραγμάτων είναι και η έννοια της διάχυτης ή της πανταχού παρούσας υπολογιστικής με την ενσωμάτωση αισθητήρων σε αντικείμενα καθημερινής χρήσης. Έτσι τα αντικείμενα μετατρέπονται σε έξυπνα το οποίο πρακτικά σημαίνει ότι οι συσκευές είναι συνδεδεμένες συνεχώς

και διαρκώς διαθέσιμες στους άλλους με σκοπό να συμβάλλουν στην μετάδοση των δεδομένων με έναν εύκολο και αποτελεσματικό τρόπο [130]. Πληθώρα τέτοιων συσκευών βρίσκεται εντός της έξυπνης πανεπιστημιούπολης και ειδικότερα σε κτίρια, σε αίθουσες διδασκαλίας ή στον εξωτερικό χώρο, επιτρέποντας μεταξύ άλλων την παρακολούθηση και τον έλεγχο σε πραγματικό χρόνο διαφόρων συστημάτων, όπως ο φωτισμός, η θέρμανση, η ασφάλεια και η χρήση των πόρων.

Οι έξυπνες αυτές συσκευές συλλέγουν και επεξεργάζονται πολλά δεδομένα προσωπικού χαρακτήρα όπως δεδομένα ταυτοποίησης, δεδομένα θέσης εγείροντας έτσι προβληματισμούς σχετικά με το κατά πόσο διαφυλάσσεται ουσιαστικά η έννοια της ιδιωτικότητας των φυσικών προσώπων καθότι στην πλειοψηφία των περιπτώσεων δεν υπάρχει επαρκής ενημέρωση των χρηστών για την καταγραφή των δεδομένων τους από τις συσκευές και τις εφαρμογές του Διαδικτύου των Πραγμάτων ούτε είναι εφικτός ο έλεγχος των επιμέρους πράξεων επεξεργασίας καθότι η επικοινωνία και η ανταλλαγή δεδομένων μεταξύ των συσκευών γίνεται αυτοματοποιημένα.

Οι πολυάριθμες προκλήσεις στους τομείς της προστασίας της ιδιωτικής ζωής και της ασφάλειας που συνδέονται συχνά με το Διαδίκτυο των Πραγμάτων είχαν απασχολήσει την Ομάδα Εργασίας του άρθρου 29, η οποία εξέδωσε στις 16/9/2014 την υπ' αριθμ. 8/2014 Γνώμη της αναφορικά με τις έως τότε πρόσφατες εξελίξεις στο διαδίκτυο των πραγμάτων [134]. Σύμφωνα με την γνώμη αυτή, οι κυριότερες προκλήσεις του ΔτΠ είναι οι ακόλουθες: α) Έλλειψη ελέγχου των χρηστών ως προς την επεξεργασία των δεδομένων τους και ασυμμετρία πληροφόρησης λόγω της δημιουργίας μιας ροής δεδομένων από τις διασυνδεδεμένες συσκευές η οποία δεν είναι δυνατό να ελεγχθεί επαρκώς, β) Ζητήματα αναποτελεσματικής λήψης της συγκατάθεσης των χρηστών λόγω της ανυπαρξίας κατάλληλων μηχανισμών μέσω των οποίων ο τελικός χρήστης να μπορεί να δίνει τη συγκατάθεση του, για τα δεδομένα που επεξεργάζονται, αποθηκεύονται και διαμοιράζονται και πρόταση ενσωμάτωσης νέων μηχανισμών συγκατάθεσης στις ίδιες τις συσκευές όπως οι διακομιστές μεσολάβησης για την προστασία της ιδιωτικής ζωής («privacy proxies») και οι πολιτικές «συγκόλλησης» δεδομένων («sticky policies»), γ) Αλλαγή του αρχικού σκοπού επεξεργασίας των δεδομένων χωρίς ο μεταγενέστερος σκοπός να είναι συμβατός με τον αρχικό και χωρίς να έχει ενημερωθεί επαρκώς το υποκείμενο των δεδομένων, δ) Αποκάλυψη τυποποιημένων συμπεριφορών με επεμβατικά μέσα και κατάρτιση προφίλ, ε) Μη πλήρωση του απαιτούμενου επιπέδου ασφαλείας των

έξυπνων συσκευών με αποτέλεσμα τα δεδομένα να είναι ευάλωτα σε επιθέσεις και κινδύνους όπως μη εξουσιοδοτημένη πρόσβαση, παραβίαση τοπικών δικτύων με σκοπό την υποκλοπή ευαίσθητων πληροφοριών, αποστολή ιών.

Ειδικότερα, η ευρεία χρήση των δεδομένων γεωγραφικής θέσεως από τις έξυπνες συσκευές, που παρατηρείται κατά κόρον εντός της έξυπνης πανεπιστημιούπολης για την παροχή εξατομικευμένων υπηρεσιών όπως πχ υπόδειξη θέσης πάρκινγκ βάσει της υφιστάμενης τοποθεσίας του χρήστη, έχει απασχολήσει την Ομάδα Εργασίας του άρθρου 29, για αυτό και εξέδωσε την υπ' αριθμ. 13/2011 Γνώμη σχετικά με τις υπηρεσίες εντοπισμού γεωγραφικής θέσης που παρέχονται μέσω έξυπνων κινητών συσκευών [131]. Στη Γνώμη αυτή επισημαίνεται ότι οι έξυπνες συσκευές μπορούν να συλλέγουν μόνιμα σήματα από σταθμούς βάσης και σημεία πρόσβασης wifi. Τεχνικά, η παρακολούθηση μπορεί να γίνει μυστικά, χωρίς ενημέρωση του χρήστη ή ημι-μυστικά, στην περίπτωση που δεν προηγήθηκε σωστή ενημέρωση του χρήστη περί ενεργοποίηση των υπηρεσιών εντοπισμού θέσης ή όταν οι ρυθμίσεις προσβασιμότητας των δεδομένων θέσης αλλάζουν από "ιδιωτικές" σε "δημόσιες". Προκειμένου η επεξεργασία των δεδομένων θέσης να είναι σύννομη, απαιτείται να υπάρχει έγκυρη συγκατάθεση των υποκειμένων των δεδομένων, η οποία δε μπορεί να αποσπάται βάσει γενικών όρων και προϋποθέσεων. Η συγκατάθεση πρέπει να αφορά τον εκάστοτε συγκεκριμένο σκοπό επεξεργασίας των δεδομένων από τον υπεύθυνο της επεξεργασίας, όπως για παράδειγμα την κατάρτιση προφίλ και/ή την εξειδικευμένη αντιμετώπιση με βάση τη συμπεριφορά. Σε περίπτωση που οι σκοποί της επεξεργασίας τροποποιηθούν κατά τρόπο ουσιώδη, ο υπεύθυνος της επεξεργασίας πρέπει να ζητήσει την εκ νέου συγκατάθεση. Τέλος, επισημαίνεται ότι στα υποκείμενα των δεδομένων πρέπει να παρέχεται η δυνατότητα εύκολης ανάκλησης της συγκατάθεσής τους, χωρίς αυτό να επιφέρει αρνητικές συνέπειες στη χρήση της συσκευής τους.

Στις νεότερες Κατευθυντήριες γραμμές υπ' αριθμ. 04/2020 του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων σχετικά με τη χρήση δεδομένων θέσης και εργαλείων ιχνηλάτησης επαφών στο πλαίσιο της έξαρσης της νόσου COVID-19, τονίζεται ότι όταν πρόκειται για τη χρήση δεδομένων θέσης, θα πρέπει πάντα να προτιμάται η επεξεργασία ανωνυμοποιημένων δεδομένων και όχι δεδομένων προσωπικού χαρακτήρα. Η ανωνυμοποίηση αναφέρεται στη χρήση ενός συνόλου τεχνικών με σκοπό να καταστεί αδύνατη η σύνδεση των δεδομένων με φυσικό πρόσωπο που έχει ταυτοποιηθεί ή μπορεί να ταυτοποιηθεί με «εύλογες» προσπάθειες.

Αυτός ο έλεγχος «εύλογου χαρακτήρα» πρέπει να λαμβάνει υπόψη τόσο αντικειμενικές πτυχές (χρόνος, τεχνικά μέσα κ.λπ.) όσο και συγκυριακά στοιχεία που μπορεί να διαφέρουν ανάλογα με την περίπτωση (σπανιότητα φαινομένου με συνεκτίμηση π.χ. της πυκνότητας του πληθυσμού, φύση και όγκος των δεδομένων, κ.λπ.). Με αυτήν την έννοια, η επεξεργασία αυτού του τύπου δεδομένων περιλαμβάνει τον χειρισμό ολόκληρων των συνόλων δεδομένων θέσης, καθώς και την επεξεργασία δεδομένων από ένα ευλόγως μεγάλο σύνολο ατόμων με τη χρήση άρτιων τεχνικών ανωνυμοποίησης, υπό την προϋπόθεση ότι αυτές εφαρμόζονται επαρκώς και αποτελεσματικά. [138]

Επιπρόσθετα, πολλές από τις έξυπνες συσκευές κάνουν χρήση της τεχνολογίας ταυτοποίησης μέσω ραδιοσυχνοτήτων (Radio Frequency Identification) η οποία χρησιμοποιεί ραδιοκύματα για την αυτόματη αναγνώριση μεμονωμένων αντικειμένων και, ως εκ τούτου, επιτρέπει την επεξεργασία δεδομένων σε μικρές αποστάσεις [132]. Χαρακτηριστικά παραδείγματα εφαρμογών που βασίζονται σε αυτή τη τεχνολογία είναι οι κάρτες ταυτοποίησης των φοιτητών ως μηχανισμός ελέγχου πρόσβασης τους στις αίθουσες διδασκαλίας ή στα εργαστήρια καθώς επίσης η τοποθέτηση των ετικετών RFID σε αντικείμενα όπως βιβλία προκειμένου να παρακολουθείται η διακίνηση αυτών και να γίνεται καλύτερη διαχείριση των διαθέσιμων αντιτύπων. Στο μέτρο που η τεχνολογία αυτή σχετίζεται με πράξεις επεξεργασίας προσωπικών δεδομένων των χρηστών εγείρονται προβληματισμοί σχετικά με πιθανούς κινδύνους παραβίασης της ιδιωτικότητας των χρηστών λόγω της κεκαλυμμένης και αέναης παρακολούθησης της συμπεριφοράς τους από τις έξυπνες συσκευές. Η Ομάδα Εργασίας του άρθρου 29 εξέδωσε την υπ’ αριθμ. 5/2010 και την αναθεωρημένη αυτής, υπ’ αριθμ. 9/2011 Γνώμη σχετικά με την πρόταση του κλάδου για ένα πλαίσιο εκπόνησης εκτιμήσεων των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων για τις εφαρμογές RFID [133] οι οποίες τονίζουν την ανάγκη αναδείξεως και αξιολογήσεως των κινδύνων για την ιδιωτική ζωή του ατόμου που συνδέονται με μία εφαρμογή RFID από τον ίδιο τον φορέα εκμεταλλεύσεως RFID. Αξίζει να σημειωθεί ότι η συνεχής παρακολούθηση και επιτήρηση των συμπεριφορών των χρηστών και η συνακόλουθη αποκάλυψη προτύπων συμπεριφοράς μέσω των συσκευών του Διαδικτύου των Πραγμάτων είναι ικανή να οδηγήσει σε εσωτερική πίεση αποφυγής μη συνηθισμένων συμπεριφορών, καταπιέζοντας την ελεύθερη ανάπτυξη της προσωπικότητας τους, με χαρακτηριστικό παράδειγμα παραβίασης αυτής, σύμφωνα με την Φ. Παναγοπούλου – Κουτνατζή, την

χρήση RFID σε μαθητικές ταυτότητες με σκοπό τη παρακολούθηση των κινήσεων των μαθητών εντός του σχολείου [130].

5.4.2 Κατάρτιση προφίλ των χρηστών και λήψη αυτοματοποιημένων αποφάσεων

Όπως αναλύθηκε στο πρώτο μέρος της παρούσας μελέτης, στο πλαίσιο της έξυπνης πανεπιστημιούπολης, με τη βοήθεια της τεχνητής νοημοσύνης και της μηχανικής μάθησης, υποστηρίζεται η παροχή πληθώρας προσωποποιημένων υπηρεσιών προς τους χρήστες δεδομένων με σκοπό τη βελτίωση της αποτελεσματικότητας της μαθησιακής διαδικασίας ή τη βελτίωση της συνολικής εμπειρίας των χρηστών κατόπιν συστηματικής ανάλυσης των διαφόρων τύπων δεδομένων αυτών όπως πχ συστάσεις παρακολούθησης συγκεκριμένων μαθημάτων βάσει ανάλυσης των προτιμήσεων, του μαθησιακού υποβάθρου και των παλαιότερων επιδόσεων των χρηστών. Για την παροχή των συγκεκριμένων υπηρεσιών προϋποτίθεται η «κατάρτιση προφίλ» των χρηστών που σύμφωνα με τον ορισμό που δίνει ο ΓΚΠΔ στο άρθρο 4 περ. 4 συνίσταται σε «*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*». Η κατάρτιση προφίλ είναι μια διαδικασία που μπορεί να περιλαμβάνει σειρά στατιστικών αναγωγών. Χρησιμοποιείται συχνά για την πραγματοποίηση προβλέψεων σχετικά με φυσικά πρόσωπα, με χρήση δεδομένων από διάφορες πηγές και με σκοπό την εξαγωγή ενός συμπεράσματος σχετικά με ένα άτομο, με βάση τα παρόμοια από στατιστική άποψη χαρακτηριστικά άλλων προσώπων [129].

Με άλλα λόγια, ο φοιτητής σε μία έξυπνη πανεπιστημιούπολη παρακολουθείται σε συνεχή βάση με αξιολόγηση της συμπεριφοράς του ή των μαθησιακών του επιδόσεων, ταξινομείται σε συγκεκριμένη κατηγορία και από όλα τα διασυνδεόμενα μεταξύ τους δεδομένα δημιουργείται ένα ψυχογράφημα αυτού. Ακόμη και αν έχει συναινέσει ρητά το υποκείμενο των δεδομένων σε αυτό, δε πρέπει να λησμονείται ότι συντρέχει ο κίνδυνος τόσο του περιορισμού της «διανοητικής ιδιωτικότητας» υπό την έννοια ότι η αέναη παρακολούθηση του ατόμου μπορεί να αποτελέσει ανασταλτικό παράγοντα στην ελεύθερη ανάπτυξη των ιδεών και των σκέψεων του και κατ΄επέκταση της προσωπικότητας του [130] όσο και ο κίνδυνος

χρήσης των δεδομένων του για σκοπούς διαφορετικούς από τους αρχικούς και για τους οποίους είχε συγκατατεθεί με αποτέλεσμα αυτό να οδηγήσει σε καταστάσεις λήψης απαγορευμένων αυτοματοποιημένων αποφάσεων. Για παράδειγμα, από την αξιολόγηση των μαθησιακών επιδόσεων ενός φοιτητή που συνήθως λαμβάνει χαμηλούς βαθμούς σε ένα μάθημα, να αποφασίσει ο υπεύθυνος επεξεργασίας να του αποκλείσει την συμμετοχή στις τελικές εξετάσεις του εν λόγω μαθήματος επειδή είναι «πολύ πιθανό» ότι θα αποτύχει σε αυτές.

Για τους λόγους αυτούς, συμπεραίνεται ότι ο υπεύθυνος επεξεργασίας μπορεί μεν να καταρτίζει προφίλ των χρηστών και να λαμβάνει αυτοματοποιημένες αποφάσεις μόνο εφόσον είναι σε θέση να τηρήσει όλες τις αρχές της επεξεργασίας και προβαίνει σε αυτήν επί νόμιμης βάσης. Στην περίπτωση μάλιστα της αποκλειστικά αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, πρέπει να εφαρμόζονται οι πρόσθετες εγγυήσεις και περιορισμοί, που καθορίζονται στο άρθρο 22 του ΓΚΠΔ [129].

5.4.3 Νομικά Ζητήματα από τη Βιντεοεπιτήρηση και την αναγνώριση προσώπου στο πλαίσιο της έξυπνης πανεπιστημιούπολης

Ακρογωνιαίο λίθο στην ολοκληρωμένη υποδομή ασφάλειας μιας έξυπνης πανεπιστημιούπολης αποτελεί η εγκατάσταση συστημάτων βιντεοεπιτήρησης, παρέχοντας μια τεχνολογικά προηγμένη και προληπτική προσέγγιση για τη διασφάλιση της ευημερίας των χρηστών της. Τα προηγμένα συστήματα καμερών που αναπτύσσονται στρατηγικά σε καίριες περιοχές της, όπως σε εισόδους, εξόδους, χώρους στάθμευσης και κοινόχρηστους χώρους, ενισχύουν τη συνολική ασφάλεια παρακολουθώντας τις δραστηριότητες σε πραγματικό χρόνο. Η ενσωμάτωση έξυπνων αναλυτικών συστημάτων βίντεο επιτρέπει στο σύστημα να ανιχνεύει ανωμαλίες, μη εξουσιοδοτημένη πρόσβαση ή ασυνήθιστη συμπεριφορά, ενεργοποιώντας έγκαιρες ειδοποιήσεις για άμεση παρέμβαση. Εκτός από την ασφάλεια, η βιντεοεπιτήρηση σε μια έξυπνη πανεπιστημιούπολη συμβάλλει στη βελτιστοποίηση των διοικητικών λειτουργιών, προσφέροντας πολύτιμες πληροφορίες σχετικά με τη διαχείριση του πλήθους, την κατανομή των πόρων και τη χρήση των εγκαταστάσεων. Η βιντεοεπιτήρηση έχει ενισχυθεί μάλιστα, μέσω της εφαρμογής της ευφυούς ανάλυσης βιντεολήψεων, με τη χρήση βιομετρικών τεχνολογιών αναγνώρισης προσώπου και αλγορίθμων τεχνητής νοημοσύνης.

Παρά τα σημαντικά οφέλη που προσφέρει αυτή, δε πρέπει να παραγνωρίζεται ότι εγκυμονεί και πολλούς κινδύνους σχετικά με την διαφύλαξη της ιδιωτικότητας των προσώπων. Άλλωστε όπως επισημαίνει και η Ανεξάρτητη Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) στην υπ' αριθμ. 1/2011 Οδηγία της περί της χρήσης συστημάτων βιντεοεπιτήρησης για την προστασία προσώπων και αγαθών [135], η βιντεοεπιτήρηση επιδρά στην συμπεριφορά των προσώπων που βρίσκονται σε συγκεκριμένους χώρους και, κατ' επέκταση, την κατευθύνει, γεγονός που μπορεί να δημιουργεί ψυχολογική πίεση, καθώς ένα πρόσωπο που γνωρίζει ότι παρακολουθείται προσπαθεί να προσαρμόζει την συμπεριφορά του στις προσδοκίες εκείνου που κάθε φορά το παρακολουθεί.

Ειδικότερα και από τη σκοπιά του δικαίου προστασίας προσωπικών δεδομένων, η λειτουργία συστήματος βιντεοεπιτήρησης, συνιστά επεξεργασία δεδομένων προσωπικού χαρακτήρα, στο μέτρο που περιλαμβάνει λήψη και διατήρηση δεδομένων εικόνας ή ήχου φυσικών προσώπων, που είναι δυνατόν να ταυτοποιηθούν επί τη βάσει της εξωτερικής τους εμφάνισης ή άλλων συγκεκριμένων στοιχείων [136]. Κατ' ακριβολογία, σύμφωνα με το άρθρο 4 της Οδηγίας 1/2011 της ΑΠΔΠΧ [135] ως συστήματα βιντεοεπιτήρησης, στα οποία περιλαμβάνονται ιδίως τα κλειστά κυκλώματα τηλεόρασης, ορίζονται τα συστήματα που είναι μόνιμα εγκατεστημένα σε ένα χώρο, λειτουργούν συνεχώς ή σε τακτά χρονικά διαστήματα και έχουν τη δυνατότητα λήψης ή/και μετάδοσης σήματος εικόνας ή/και ήχου από τον χώρο αυτό προς έναν περιορισμένο αριθμό οθονών προβολής ή/και μηχανημάτων καταγραφής (πρβλ. και υπ' αρ. 2/2010 Γνωμοδότηση της Αρχής, σκέψη 8). Η μετάδοση της εικόνας μπορεί να γίνεται με απευθείας σύνδεση της κάμερας στην οθόνη προβολής ή/και στο μηχάνημα καταγραφής ή μέσω εσωτερικού δικτύου ή μέσω διαδικτύου για περιορισμένο όμως αριθμό νομιμοποιούμενων προς τούτο αποδεκτών.

Εν σχέσει με τη νομιμότητα επεξεργασίας, η ως άνω Οδηγία 1/2011 της ΑΠΔΠΧ [135] τονίζει στο άρθρο 5, ότι αυτή πρέπει να εξετάζεται στα πλαίσια του σκοπού επιδιώκει ο υπεύθυνος επεξεργασίας και σύμφωνα με την αρχή της αναλογικότητας, η οποία επιβάλλει τα συστήματα βιντεοεπιτήρησης να είναι πρόσφορα και αναγκαία σε σχέση με τον επιδιωκόμενο σκοπό, ο οποίος θα πρέπει να μη δύναται να επιτευχθεί με ηπιότερα μέσα. Ως ηπιότερα νοούνται τα μέσα που είναι εξίσου αποτελεσματικά, αλλά λιγότερο επαχθή για το άτομο, π.χ. τακτικότεροι έλεγχοι από υπάρχον προσωπικό ασφαλείας, σύστημα συναγερμού στην είσοδο και

την έξοδο κλειστών χώρων, καλύτερος φωτισμός κλπ. Περαιτέρω, τα σημεία εγκατάστασης των καμερών και ο τρόπος λήψης των δεδομένων πρέπει να προσδιορίζονται με τέτοιο τρόπο, ώστε τα δεδομένα που συλλέγονται να μην είναι περισσότερα από όσα είναι απολύτως αναγκαία για την εκπλήρωση του σκοπού της επεξεργασίας και να μη θίγονται τα θεμελιώδη δικαιώματα των προσώπων που ευρίσκονται στο χώρο που επιτηρείται και ιδίως να μην παραβιάζεται αυτό το οποίο μπορεί να θεωρηθεί ως «νόμιμη προσδοκία κάποιου βαθμού προστασίας της ιδιωτικής ζωής» σε κάποιον χώρο (πρβλ. Έγγραφο εργασίας για την επιτήρηση των ηλεκτρονικών επικοινωνιών στον τόπο εργασίας WP55 της 29 Μαΐου 2002 της 'Ομάδας εργασίας για την προστασία των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα' σελ. 4). Στο άρθρο 6 μάλιστα της εν λόγω Οδηγίας γίνεται ρητός προσδιορισμός ειδικών περιπτώσεων εφαρμογής της αρχής της αναλογικότητας.

Αξίζει βέβαια να επισημανθεί ότι η Οδηγία αυτή της ΑΠΔΠΧ εκδόθηκε μόλις το 2011 χωρίς φυσικά να έχει ισχύ νόμου, παρά αποτελεί κατευθυντήριες γραμμές και εξειδικεύει ζητήματα που σχετίζονται με τη νομιμότητα της χρήσης συστημάτων βιντεοεπιτήρησης για την προστασία προσώπων και αγαθών. Στην ίδια λογική, εκδόθηκαν μεταγενέστερα και οι Κατευθυντήριες γραμμές υπ' αριθμ. 3/2019 του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω βιντεοσυσκευών [137] στις οποίες αντιμετωπίζεται και θίγεται περισσότερο και το ζήτημα της επεξεργασίας ειδικών κατηγοριών δεδομένων δεδομένου ότι τα συστήματα βιντεοεπιτήρησης συλλέγουν συνήθως τεράστιο όγκο προσωπικών δεδομένων τα οποία ενδέχεται να αποκαλύψουν δεδομένα προσωπικής φύσης, ακόμη και ειδικών κατηγοριών. Ενδέχεται δηλαδή μη σημαντικά δεδομένα, που συλλέγονται αρχικά μέσω βίντεο, να χρησιμοποιηθούν για την εξαγωγή άλλων πληροφοριών για την επίτευξη διαφορετικού σκοπού (π.χ. για την χαρτογράφηση των συνηθειών ενός ατόμου). Κατά κανόνα, όταν εγκαθίσταται σύστημα βιντεοεπιτήρησης θα πρέπει να επιδιώκεται η εφαρμογή της αρχής της ελαχιστοποίησης των δεδομένων. Για αυτό είναι σημαντικό να λαμβάνονται τα απαιτούμενα μέτρα ελαχιστοποίησης του κινδύνου λήψης υλικού που αποκαλύπτει άλλα ευαίσθητα δεδομένα (πέραν του άρθρου 9), ανεξαρτήτως του σκοπού. Αν το σύστημα βιντεοεπιτήρησης χρησιμοποιείται για να γίνει επεξεργασία ειδικών κατηγοριών δεδομένων, ο υπεύθυνος επεξεργασίας πρέπει να προσδιορίσει τόσο την εξαίρεση που αφορά την επεξεργασία ειδικών κατηγοριών δεδομένων σύμφωνα με το

άρθρο 9 (π.χ. εξαίρεση από τον γενικό κανόνα ότι δεν θα πρέπει κανένας να επεξεργάζεται ειδικές κατηγορίες δεδομένων), όσο και τη νομική βάση.

Οι ως άνω Κατευθυντήριες γραμμές περιέχουν μάλιστα και ειδική αναφορά στην ευρεία χρήση βιομετρικών δεδομένων μέσω της οποίας γίνεται και η αναγνώριση προσώπου τονίζοντας ότι τα νέα τεχνολογικά μέσα τα οποία υποστηρίζονται από νέες τεχνολογίες όπως η Τεχνητή Νοημοσύνη και η Μηχανική Μάθηση, πρέπει οπωσδήποτε να χρησιμοποιούνται με γνώμονα τις αρχές της νομιμότητας, της αναγκαιότητας, της αναλογικότητας και της ελαχιστοποίησης δεδομένων όπως προβλέπονται στον ΓΚΠΔ. Μολονότι η χρήση αυτών των τεχνολογιών μπορεί να θεωρείται ιδιαίτερα αποτελεσματική, οι υπεύθυνοι επεξεργασίας θα πρέπει πρώτα από όλα να αξιολογούν τον αντίκτυπο που έχουν τα τεχνολογικά αυτά μέσα στα θεμελιώδη δικαιώματα και τις ελευθερίες και να εξετάζουν τη χρήση λιγότερο παρεμβατικών μέσων για να επιτυγχάνουν τον νόμιμο σκοπό της επεξεργασίας [137].

Σε κάθε περίπτωση, ο υπεύθυνος επεξεργασίας οφείλει να λαμβάνει όλα τα απαραίτητα προληπτικά μέτρα ώστε να διαφυλάξει τη διαθεσιμότητα, την ακεραιότητα και την εμπιστευτικότητα των υπό επεξεργασία δεδομένων. Για τον σκοπό αυτό, ο υπεύθυνος επεξεργασίας λαμβάνει κυρίως τα ακόλουθα μέτρα: διαχωρίζει τα δεδομένα κατά τη διάρκεια της διαβίβασης και της αποθήκευσής τους, αποθηκεύει τα βιομετρικά πρότυπα και τα ανεπεξέργαστα δεδομένα ή τα δεδομένα ταυτότητας σε χωριστές βάσεις δεδομένων, κρυπτογραφεί τα βιομετρικά δεδομένα, και κυρίως τα βιομετρικά πρότυπα, και καθορίζει πολιτική για την κρυπτογράφηση και τη διαχείριση των κλειδιών κρυπτογράφησης, ενσωματώνει οργανωτικά και τεχνικά μέτρα για τον εντοπισμό περιστατικών απάτης, συσχετίζει τον κωδικό ακεραιότητας με τα δεδομένα (για παράδειγμα, υπογραφή ή ετικέτα) και απαγορεύει κάθε εξωτερική πρόσβαση στα βιομετρικά δεδομένα. Τα μέτρα αυτά θα πρέπει να συμβαδίζουν με την πρόοδο της τεχνολογίας [137].

Στο σημείο αυτό αξίζει να επισημανθεί και το εξής: Τα συστήματα αναγνώρισης προσώπου ή αλλιώς συστήματα εξ αποστάσεως βιομετρικής ταυτοποίησης είναι στη πραγματικότητα συστήματα τεχνητής νοημοσύνης για την εξ αποστάσεως ταυτοποίηση φυσικών προσώπων που μπορεί να γίνεται είτε μέσω της αντιπαραβολής των βιομετρικών δεδομένων ενός προσώπου με τα βιομετρικά δεδομένα που περιέχονται σε αποθετήριο δεδομένων αναφοράς είτε σε πραγματικό χρόνο όπου η αντιπαραβολή και η ταυτοποίηση πραγματοποιούνται αυτοστιγμεί ή

σχεδόν αυτοστιγμεί. Αναφορικά με τη νομιμότητα εγκατάστασης και θέσης σε εφαρμογή των συστημάτων αυτών σε ευρωπαϊκό πλαίσιο, ενδιαφέρον παρουσιάζει η από 9/12/2023 προσωρινή συμφωνία του Ευρωπαϊκού Κοινοβουλίου και του Ευρωπαϊκού Συμβουλίου σχετικά με την πράξη της Τεχνητής Νοημοσύνης (AI ACT). Η εν λόγω πράξη αναμένεται να μετουσιωθεί σε Κανονισμό της ΕΕ που θα περιέχει δεσμευτικούς κανόνες αναφορικά με τη ρύθμιση της Τεχνητής Νοημοσύνης υψηλού κινδύνου και τη διασφάλιση της προστασίας των θεμελιωδών δικαιωμάτων, της δημοκρατίας, του κράτους δικαίου και της περιβαλλοντικής βιωσιμότητας. Σύμφωνα με τις επίσημες ανακοινώσεις του Ευρωπαϊκού Κοινοβουλίου [142] αναφορικά με το περιεχόμενο της προσωρινής αυτής συμφωνίας, με δεδομένο ότι ορισμένες εφαρμογές της Τεχνητής Νοημοσύνης αποτελούν πιθανή απειλή για τα δικαιώματα των πολιτών και τη δημοκρατία, συμφωνήθηκε να απαγορευτεί η χρήση βιομετρικών συστημάτων κατηγοριοποίησης που χρησιμοποιούν ευαίσθητα χαρακτηριστικά (π.χ. πολιτικές, θρησκευτικές, φιλοσοφικές πεποιθήσεις, σεξουαλικός προσανατολισμός, φυλή) ή έχουν στόχο τη μη στοχευμένη απόξεση εικόνων προσώπων από το διαδίκτυο ή πλάνα CCTV για τη δημιουργία βάσεων δεδομένων αναγνώρισης προσώπου ενώ ειδικά για τη χρήση βιομετρικών συστημάτων ταυτοποίησης σε χώρους προσβάσιμους στο κοινό συμφωνήθηκε να είναι επιτρεπτή μόνο για σκοπούς επιβολής του νόμου, υπό την προϋπόθεση προηγούμενης δικαστικής άδειας και για αυστηρά καθορισμένους καταλόγους εγκλημάτων. Εν σχέσει δε με τη χρήση βιομετρικών συστημάτων ταυτοποίησης σε πραγματικό χρόνο, συμφωνήθηκε ότι η εγκατάσταση κα η χρήση αυτών θα πρέπει να συμμορφώνεται με αυστηρούς όρους και η χρήση της θα είναι περιορισμένη σε χρόνο και τοποθεσία, για τους ειδικούς και μόνο σκοπούς όπως: στοχευμένες έρευνες θυμάτων (απαγωγή, εμπορία ανθρώπων, σεξουαλική εκμετάλλευση), πρόληψη συγκεκριμένης και παρούσας τρομοκρατικής απειλής, ή εντοπισμός ή ταυτοποίηση ατόμου που είναι ύποπτο ότι έχει διαπράξει ένα από τα συγκεκριμένα εγκλήματα που αναφέρονται στον κανονισμό (π.χ. τρομοκρατία, σωματεμπορία, σεξουαλική εκμετάλλευση, δολοφονία, απαγωγή, βιασμός, ένοπλη ληστεία, συμμετοχή σε εγκληματική οργάνωση, περιβαλλοντικό έγκλημα). Επισημαίνεται ότι αυτά δεν αποτελούν ακόμη ισχύον κανονιστικό πλαίσιο αλλά σε κάθε περίπτωση απηχούν την στάση της ΕΕ απέναντι στην ευρεία χρήση των συστημάτων τεχνητής νοημοσύνης για αυτό και γίνεται αναφορά τους στην παρούσα εργασία. Ενδιαφέρον θα έχει η παρακολούθηση των εξελίξεων διότι η ρύθμιση που τελικώς θα ακολουθήσει η Ευρωπαϊκή Ένωση στο ζήτημα αυτό θα καθορίσει εάν το

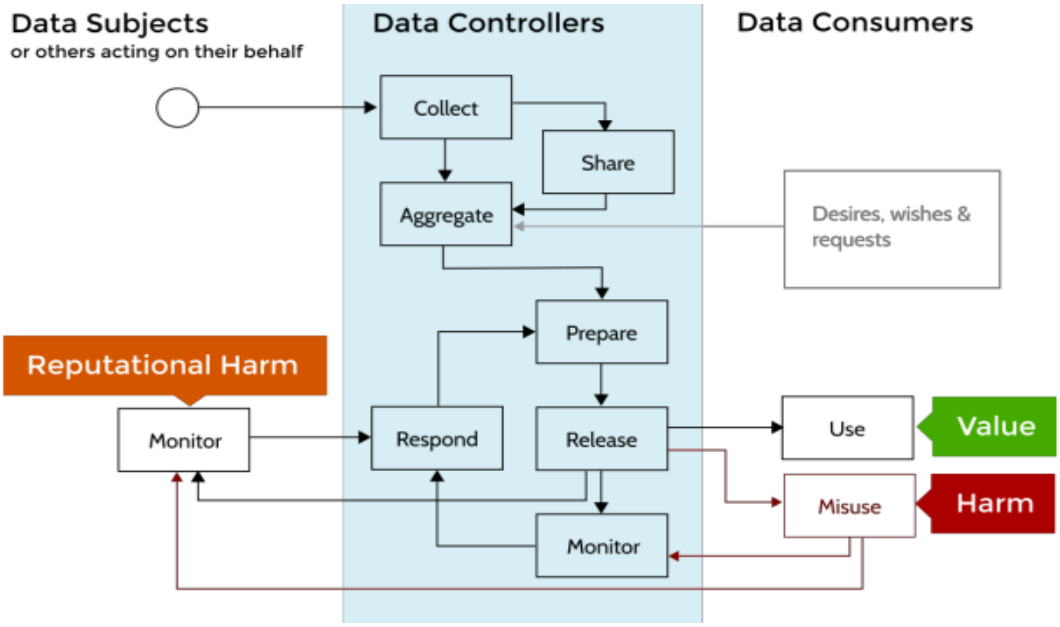
ρυθμιστικό και κανονιστικό πλαίσιο που θα αποφασισθεί, θα αποτελέσει τροχοπέδη στην υιοθέτηση και χρήση των προαναφερόμενων συστημάτων και στο πλαίσιο της έξυπνης -ευρωπαϊκής - πανεπιστημιούπολης. Επισημαίνεται πάντως ότι τέτοιοι προβληματισμοί και εμπόδια δε τίθενται σε χώρες όπως η Κίνα, στην οποία η γενικευμένη κρατική παρακολούθηση, μέσω ενός τεράστιου δικτύου βιντεοεπιτήρησης, με ενσωματωμένη εξαιρετικά προηγμένη τεχνολογία αναγνώρισης προσώπου, χρησιμοποιείται από το καθεστώς, για την κατάταξη των πολιτών σε κατηγορίες με βάση τις «επιδόσεις» τους και τη στέρηση, στις χαμηλότερες εξ αυτών, ακόμη και θεμελιωδών ανθρώπινων δικαιωμάτων, όπως του δικαιώματος στην εργασία και την παιδεία [136].

5.4.4 Εγειρόμενα ζητήματα σχετικά με τα Ανοιχτά Δεδομένα

Όπως προαναφέρθηκε στο κεφάλαιο 4, στα πλαίσια της έξυπνης πανεπιστημιούπολης επικροτείται η εφαρμογή πρακτικών ανοιχτών δεδομένων σε μία προσπάθεια ενίσχυσης της διαφάνειας και της συνεργατικότητας, πλην όμως τούτο πρέπει να γίνεται υπό την προϋπόθεση της προστασίας και διαφύλαξης των προσωπικών δεδομένων των υποκειμένων.

Φαινομενικά η ανοιχτή διάθεση δεδομένων είναι ασύμβατη με τη προστασία των προσωπικών δεδομένων και τούτο διότι εξ ορισμού η έννοια των ανοιχτών δεδομένων σημαίνει δεδομένα που είναι ανοιχτά για ελεύθερη πρόσβαση, χρήση και τροποποίηση για κοινή χρήση για οποιονδήποτε σκοπό [143]. Τα ανοιχτά δεδομένα δεν είναι εξ ορισμού προσωπικά δεδομένα ήτοι δεδομένα που αφορούν ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο, υπό την έννοια ότι η ταυτότητα του μπορεί να εξακριβωθεί άμεσα ή έμμεσα (άρθρο 4 περ.1 του ΓΚΠΔ). Ενδέχεται όμως ένα ανοιχτό μη προσωπικό δεδομένο να καταστεί προσωπικό δεδομένο όταν αναλυθεί με συγκεκριμένους τρόπους ή όταν συνδυαστεί με άλλες πληροφορίες. Για παράδειγμα, ένα ανοιχτό σύνολο δεδομένων αναφορικά με τη χρήση των δημόσιων συγκοινωνιών με λεπτομέρειες όπως ο αριθμός των επιβατών που επιβιβάζονται και αποβιβάζονται σε διάφορες στάσεις λεωφορείων, η συχνότητα των αφίξεων των λεωφορείων και οι διαδρομές που ακολουθούνται δεν είναι δεδομένο προσωπικού χαρακτήρα. Όμως, εάν το σύνολο δεδομένων περιλαμβάνει συγκεκριμένες πληροφορίες για μεμονωμένες στάσεις λεωφορείων και μπορούν να εντοπιστούν τα συνήθη πρότυπα επιβίβασης και αποβίβασης ενός ατόμου, μπορεί να οδηγήσει στην ταυτοποίηση αυτού και συνεπώς μετατρέπεται σε προσωπικό.

Επειδή λοιπόν η ισορροπία μεταξύ προσωπικού και μη προσωπικού δεδομένου είναι λεπτή, προτείνεται από τους ερευνητές του Πανεπιστημίου του Σαουθάμπτον που εκπόνησαν μία μελέτη αναφορικά με τα ανοιχτά δεδομένα και την ιδιωτικότητα στα πλαίσια του ευρωπαϊκού προγράμματος Data Portal, ο κάθε φορέας -συνεπώς και η έξυπνη πανεπιστημιούπολη- να ακολουθεί τα παρακάτω βήματα πριν, κατά τη διάρκεια και μετά τη δημοσιοποίηση δεδομένων:



Εικόνα 12 Βήματα πριν, κατά και μετά τη δημοσιοποίηση των δεδομένων [144]

1) Συλλογή των δεδομένων από το υποκείμενο, ιδανικά λαμβάνοντας τη συγκατάθεση του και αφού έχει προηγηθεί ενδελεχής ενημέρωση του σχετικά με τους σκοπούς συλλογής αυτών, 2) Ανταλλαγή δεδομένων με κατάλληλες τεχνικές ασφαλείας όπως ανωνυμοποίηση ή ψευδωνυμοποίηση μεταξύ των επιμέρους υπευθύνων ή εκτελούντων την επεξεργασία, 3) Συγκέντρωση των δεδομένων: Τα δεδομένα μπορούν να συνδυαστούν, πριν από την δημοσίευση, με άλλα σύνολα δεδομένων, είτε από τον αρχικό υπεύθυνο επεξεργασίας είτε από τρίτο μέρος. Το προκύπτον σύνολο δεδομένων μπορεί εντέλει να είναι ετερογενές σε σχέση με την αρχική πηγή των δεδομένων, 4) Προετοιμασία των δεδομένων για δημοσίευση: Κατά τη διαδικασία αυτή γίνεται ο «καθαρισμός» των δεδομένων που περιλαμβάνει τις περισσότερες φορές αφαίρεση των πιο ευαίσθητων πτυχών των δεδομένων ή εφαρμογή της τεχνικής της ανωνυμοποίησης έτσι ώστε να μειωθεί ο αριθμός των προσωπικών δεδομένων, 5) Θέση σε δημοσιότητα των δεδομένων, 6) Χρήση και εν

γένει επεξεργασία των δεδομένων από τρίτα μέρη. Στο μέτρο που η επεξεργασία των δεδομένων γίνεται με ορθό τρόπο επιτυγχάνεται ο σκοπός θέσπισης των πολιτικών ανοιχτών δεδομένων. Επειδή όμως είναι πιθανό να ανακύψουν και ζητήματα κατάχρησης των δεδομένων είναι σημαντικό να τηρούνται και τα επόμενα μέτρα από τους αρμόδιους φορείς, 7) Επίβλεψη των δεδομένων: Μετά τη δημοσίευση, ο υπεύθυνος φορέας είναι καλό να παρακολουθεί τα πλαίσια χρήσης των δεδομένων που διατίθενται ελεύθερα και τους πιθανούς κινδύνους που σχετίζονται με αυτά όπως πχ ο κίνδυνος αποανωνυμοποίησης, 8) Άμεση δράση σε περίπτωση κακής χρήσης των δεδομένων: Σε περίπτωση που προκύψουν θέματα μετά τη δημοσίευση ενός Ανοικτού Συνόλου Δεδομένων, ο αρμόδιος φορέας θα πρέπει να είναι σε θέση να αντιδράσει για να τα αντιμετωπίσει. Αυτό θα μπορούσε να περιλαμβάνει την τροποποίηση ή ακόμη και την ανάκληση του δημοσιευμένου συνόλου δεδομένων, την ειδοποίηση τρίτων που χρησιμοποιούν αυτά τα δεδομένα (όπου είναι δυνατόν) και την άμεση ειδοποίηση των υποκείμενων δεδομένων και άλλων εμπλεκόμενων μερών.

5.4.5 Νομικά Ζητήματα από την υπολογιστική νέφους (cloud)

Στην ανάπτυξη και λειτουργία της έξυπνης πανεπιστημιούπολης, σημαντικό ρόλο διαδραματίζει και η τεχνολογία της υπολογιστικής νέφους. Οι υπηρεσίες υπολογιστικού νέφους χρησιμοποιούνται εκτενώς για την αποθήκευση δεδομένων, επιτρέποντας την αποτελεσματική διαχείριση του τεράστιου όγκου των δεδομένων που παράγονται καθημερινά από τις διάφορες έξυπνες συσκευές. Οι έξυπνες πανεπιστημιουπόλεις αξιοποιούν το μοντέλο της Υποδομής ως Υπηρεσίας (IaaS) για τη φιλοξενία και τη συντήρηση υπολογιστικών πόρων (servers, data centers) αντί της κοστοβόρας τοποθέτησης συστημάτων στις εγκαταστάσεις αυτών. Με το μοντέλο της Πλατφόρμας ως Υπηρεσίας(PaaS), η ανάπτυξη και η εγκατάσταση προσαρμοσμένων διαδικτυακών εφαρμογών εκσυγχρονίζεται, διευκολύνοντας τη δημιουργία εξατομικευμένων λύσεων για την κάλυψη συγκεκριμένων ακαδημαϊκών και διοικητικών αναγκών. Με το μοντέλο του λογισμικού ως υπηρεσία (SaaS), η έξυπνη πανεπιστημιούπολη αντί να αγοράζει και να εγκαθιστά στο πληροφοριακό της σύστημα διάφορα λογισμικά όπως συστήματα διαχείρισης μάθησης, πλατφόρμες συνεργασίας κτλ, τα μισθώνει ως υπηρεσία και κάνει αποτελεσματικότερη χρήση αυτών.

Στο υπολογιστικό νέφος, τα πληροφοριακά δεδομένα -στην κατηγορία των οποίων υπάγονται και τα δεδομένα προσωπικού χαρακτήρα- αποθηκεύονται σε κάποιον εξυπηρετητή (server) ή data center και τις περισσότερες φορές το υποκείμενο των δεδομένων δε γνωρίζει ούτε που βρίσκονται αυτοί οι servers ούτε τι μηχανισμοί προστασίας έχουν ληφθεί από τον πάροχο σχετικά με την ασφάλεια των δεδομένων του. Οι κυριότεροι κίνδυνοι που σχετίζονται με τα δεδομένα προσωπικού χαρακτήρα τα οποία υφίστανται επεξεργασία «εντός του υπολογιστικού νέφους», σύμφωνα με τη γνώμη 05/2012 της Ομάδας Εργασίας του άρθρου 29 για την προστασία των δεδομένων [141] διακρίνονται σε δύο κυρίως κατηγορίες: στην έλλειψη ελέγχου επί των δεδομένων και στην ανεπάρκεια πληροφόρησης σχετικά με την ίδια την επεξεργασία (έλλειψη διαφάνειας).

Ειδικότερα, η έλλειψη ελέγχου δύναται να εκδηλωθεί με τους ακόλουθους τρόπους [141]: **1)** Έλλειψη διαλειτουργικότητας: Εάν ο πάροχος υπηρεσιών νεφοϋπολογιστικής χρησιμοποιεί ιδιόκτητη τεχνολογία, ο πελάτης υπηρεσιών νεφοϋπολογιστικής ενδέχεται να δυσκολευτεί να μεταφέρει τα δεδομένα και τα έγγραφά του από ένα σύστημα που έχει ως βάση τη νεφοϋπολογιστική σε άλλο (φορητότητα δεδομένων) ή να ανταλλάξει πληροφορίες με οντότητες που χρησιμοποιούν υπηρεσίες νεφοϋπολογιστικής οι οποίες τελούν υπό τη διαχείριση διαφορετικών παρόχων (διαλειτουργικότητα), **2)** Έλλειψη ακεραιότητας λόγω επιμερισμού των πόρων: Κάθε νέφος αποτελείται από επιμερισμένα συστήματα και υποδομές. Οι πάροχοι υπηρεσιών νεφοϋπολογιστικής επεξεργάζονται δεδομένα προσωπικού χαρακτήρα τα οποία προέρχονται από ευρύ φάσμα πηγών, τόσο από πρόσωπα στα οποία αναφέρονται τα δεδομένα όσο και από οργανισμούς, με επακόλουθο την πιθανότητα ύπαρξης αντικρουόμενων συμφερόντων ή/και διαφορετικών στόχων, **3)** Μη τήρηση του απορρήτου σε περίπτωση υποβολής αιτημάτων για σκοπούς επιβολής του νόμου απευθείας σε παρόχους υπηρεσιών νεφοϋπολογιστικής: Οι αρχές επιβολής του νόμου των κρατών μελών της ΕΕ και τρίτων χωρών δύνανται να υποβάλλουν αιτήματα επιβολής του νόμου ζητώντας την κοινοποίηση δεδομένων προσωπικού χαρακτήρα που υφίστανται επεξεργασία εντός του υπολογιστικού νέφους. Ελλοχεύει έτσι ο κίνδυνος κοινοποίησης δεδομένων προσωπικού χαρακτήρα σε (ξένες) αρχές επιβολής του νόμου χωρίς έγκυρη ενωσιακή νομική βάση, με αποτέλεσμα να παραβιάζεται η νομοθεσία της ΕΕ περί προστασίας των δεδομένων**, 4)** Αδυναμία παρέμβασης λόγω της πολυπλοκότητας και της δυναμικής της αλυσίδας εξωτερικής ανάθεσης: Κάθε υπηρεσία νεφοϋπολογιστικής

που παρέχεται μπορεί να είναι αποτέλεσμα συνδυασμού υπηρεσιών οι οποίες παρέχονται από διάφορους άλλους παρόχους, ο αριθμός των οποίων μπορεί να αυξομειώνεται δυναμικά κατά τη διάρκεια ισχύος της σύμβασης του πελάτη, **5)** Αδυναμία παρέμβασης (δικαιώματα των προσώπων στα οποία αναφέρονται τα δεδομένα): Οι πάροχοι υπηρεσιών νεφοϋπολογιστικής είναι πιθανό να μην παρέχουν στον υπεύθυνο της επεξεργασίας τα μέτρα και τα εργαλεία που χρειάζεται για να διαχειρίζεται ευκολότερα τα δεδομένα (π.χ. πρόσβαση σε αυτά και διόρθωση ή διαγραφή τους), **6)** Έλλειψη απομόνωσης των δεδομένων: Οι πάροχοι υπηρεσιών νεφοϋπολογιστικής είναι πιθανό να εκμεταλλεύονται τον φυσικό έλεγχο που ασκούν επί των δεδομένων που προέρχονται από διαφορετικούς πελάτες με σκοπό τη σύνδεση των δεδομένων προσωπικού χαρακτήρα μεταξύ τους.

Αντίστοιχα, από την έλλειψη κατάλληλης πληροφόρησης ελλοχεύουν οι κατωτέρω κίνδυνοι [141]: **1)** Έλλειψη κατάλληλης πληροφόρησης για την ταυτότητα του υπευθύνου επεξεργασίας όταν τα δεδομένα υφίστανται αλυσιδωτή επεξεργασία στην οποία συμμετέχουν πολυάριθμοι εκτελούντες την επεξεργασία και υπεργολάβοι, **2)** Ανεπαρκής πληροφόρηση όταν τα δεδομένα προσωπικού χαρακτήρα υφίστανται επεξεργασία σε διαφορετικές γεωγραφικές τοποθεσίες, γεγονός που έχει άμεσο αντίκτυπο στη νομοθεσία η οποία διέπει τις διαφορές που ενδέχεται να προκύψουν μεταξύ χρήστη και παρόχου όσον αφορά την προστασία των δεδομένων, **3)** Έλλειψη κατάλληλης πληροφόρησης για τα δεδομένα προσωπικού χαρακτήρα που διαβιβάζονται σε τρίτες χώρες εκτός του ΕΟΧ. Είναι πιθανόν οι τρίτες χώρες να μην εξασφαλίζουν επαρκές επίπεδο προστασίας των δεδομένων και η διαβίβαση των τελευταίων να μην προστατεύεται από κατάλληλα μέτρα (π.χ. τυποποιημένες συμβατικές ρήτρες ή δεσμευτικούς εταιρικούς κανόνες),και, ως εκ τούτου, ενδέχεται να είναι παράνομη.

Ο πάροχος υπηρεσιών νέφους ενόψει του ότι παρέχει τα μέσα και την πλατφόρμα, ενεργώντας εξ ονόματος του πελάτη υπηρεσιών νεφοϋπολογιστικής, λειτουργεί κατά βάση ως εκτελών την επεξεργασία. Τούτο σημαίνει σύμφωνα με το άρθρο 28 του ΓΚΠΔ ότι έχει καθήκον να παρέχει στον υπεύθυνο επεξεργασίας για λογαριασμό του οποίου και διενεργεί την επεξεργασία των δεδομένων, επαρκείς διαβεβαιώσεις για την εφαρμογή των κατάλληλων τεχνικών και οργανωτικών μέτρων κατά τρόπο ώστε η επεξεργασία να γίνεται με τρόπο τέτοιο που να διασφαλίζεται η προστασία των δικαιωμάτων του υποκειμένου των δεδομένων. Μάλιστα μεταξύ του παρόχου υπολογιστικής νέφους και του υπευθύνου επεξεργασίας, ήτοι εν προκειμένω

του οργανισμού της έξυπνης πανεπιστημιούπολης, συνάπτεται σύμφωνα με το άρθρο 28 παρ. 3 του ΓΚΠΔ, υποχρεωτικώς γραπτή δεσμευτική σύμβαση με σαφή καθορισμό του αντικειμένου και της διάρκειας της επεξεργασίας, της φύσης και του σκοπού της επεξεργασίας, του είδους των δεδομένων προσωπικού χαρακτήρα, των κατηγοριών των υποκειμένων των δεδομένων καθώς επίσης και των δικαιωμάτων και υποχρεώσεων του υπευθύνου επεξεργασίας. Ο εκτελών την επεξεργασία υπογράφοντας την ως άνω σύμβαση δεσμεύεται μεταξύ άλλων να επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα μόνο βάσει καταγεγραμμένων εντολών του υπευθύνου επεξεργασίας, να διασφαλίζει ότι τα πρόσωπα που είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα έχουν αναλάβει δέσμευση τήρησης εμπιστευτικότητας, να λαμβάνει υπόψη τη φύση της επεξεργασίας και να επικουρεί τον υπεύθυνο επεξεργασίας με τα κατάλληλα τεχνικά και οργανωτικά μέτρα, να διαγράφει ή να επιστρέφει κατ' απαίτηση του υπευθύνου επεξεργασίας όλα τα δεδομένα προσωπικού χαρακτήρα σε αυτόν μετά το πέρας της παροχής υπηρεσιών επεξεργασίας διαγράφοντας μάλιστα και όλα τα υφιστάμενα αντίγραφα εκτός αν το δίκαιο της Ένωσης ή του Κράτους μέλους απαιτεί την αποθήκευση των δεδομένων προσωπικού χαρακτήρα καθώς επίσης και να συνδράμει τον υπεύθυνο επεξεργασίας στη διασφάλιση της συμμόρφωσης προς τις υποχρεώσεις που απορρέουν από τα άρθρα 24 επόμενα του ΓΚΠΔ κι οποίες αναλύονται αμέσως παρακάτω, λαμβάνοντας υπόψη τη φύση της επεξεργασίας και τις πληροφορίες που διαθέτει ο ίδιος ο εκτελών την επεξεργασία.

ΚΕΦΑΛΑΙΟ 6 – ΥΠΟΧΡΕΩΣΕΙΣ ΤΟΥ ΥΠΕΥΘΥΝΟΥ ΕΠΕΞΕΡΓΑΣΙΑΣ ΣΥΜΦΩΝΑ ΜΕ ΤΟΝ ΓΚΠΔ

Ο ΓΚΠΔ έχοντας ως γνώμονα την ουσιαστική προστασία των δεδομένων προσωπικού χαρακτήρα δεν αρκείται σε διακηρύξεις και θεωρητικές έννοιες αλλά θεσπίζει και ειδικές υποχρεώσεις των υπευθύνων επεξεργασίας στους οποίους μετατοπίζει το βάρος λήψης κατάλληλων και αποτελεσματικών μέτρων προστασίας των δεδομένων αυτών. Οι περισσότερες από αυτές τις υποχρεώσεις είναι απόρροια της θεσπισμένης στο άρθρο 5 παρ. 2 του ΓΚΠΔ αρχής της λογοδοσίας η οποία επιβάλλει σε υπευθύνους επεξεργασίας να εφαρμόζουν, ενεργώς και αδιάλειπτα, μέτρα και πολιτικές για την προώθηση και τη διασφάλιση της προστασίας των δεδομένων στις δραστηριότητες επεξεργασίας, όντας υπεύθυνοι για τη συμμόρφωση των πράξεων επεξεργασίας προς το δίκαιο για την προστασία των δεδομένων και τις

αντίστοιχες υποχρεώσεις τους. Η λογοδοσία δεν θα πρέπει να ενεργοποιείται μόνο μετά την παράβαση. Αντιθέτως, οι υπεύθυνοι επεξεργασίας έχουν την υποχρέωση να εφαρμόζουν προληπτικά κατάλληλες πολιτικές διαχείρισης δεδομένων σε όλα τα στάδια της επεξεργασίας.

6.1 Εφαρμογή τεχνικών και οργανωτικών μέτρων προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού (privacy by design and by default)

Ο ΓΚΠΔ επιβάλλει στους υπευθύνους επεξεργασίας να εφαρμόζουν τεχνικά και οργανωτικά μέτρα ώστε να διασφαλίζουν και να είναι σε θέση να αποδείξουν ότι η επεξεργασία πραγματοποιείται σύννομα. Παρακάτω θα εκτεθούν ορισμένα από αυτά τα μέτρα που προτείνονται προς υιοθέτηση και από τον εν προκειμένω υπεύθυνο επεξεργασίας, ήτοι τον οργανισμό της έξυπνης πανεπιστημιούπολης.

Στο άρθρο 32 του ΓΚΠΔ γίνεται μία ενδεικτική απαρίθμηση των μέτρων που μπορούν να εφαρμόσουν οι υπεύθυνοι επεξεργασίας προκειμένου να διασφαλίσουν το κατάλληλο επίπεδο ασφαλείας των προσωπικών δεδομένων έναντι των κινδύνων, λαμβανομένων υπόψη των τελευταίων εξελίξεων, του κόστους εφαρμογής, της φύσης, του πεδίου εφαρμογής, του πλαισίου και των σκοπών επεξεργασίας καθώς και των κινδύνων διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Πιο συγκεκριμένα τα προτεινόμενα από τον ΓΚΠΔ με στόχο την ασφαλή επεξεργασία των προσωπικών δεδομένων και την αποτροπή τυχαίας απώλειας ή καταστροφής και μη εξουσιοδοτημένης ή/και παράνομης πρόσβασης σε αυτά, χρήσης, τροποποίησης ή αποκάλυψής τους, μέτρα του είναι μεταξύ άλλων:

- Εφαρμογή της τεχνικής της ψευδωνυμοποίησης και κρυπτογράφησης των δεδομένων. Ο ΓΚΠΔ ορίζει στο άρθρο 4 περ. 5 αυτού την «ψευδωνυμοποίηση» ως «*την επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα προσωπικού χαρακτήρα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι τα δεδομένα προσωπικού χαρακτήρα δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο».* Ένας τρόπος ψευδωνυμοποίησης είναι η κρυπτογράφηση των δεδομένων. Άπαξ και τα δεδομένα ψευδωνυμοποιηθούν, ο σύνδεσμος με την ταυτότητα υφίσταται με τη μορφή ψευδωνύμου σε συνδυασμό με κλειδί

αποκρυπτογράφησης. Ελλείψει τέτοιου κλειδιού, η εξακρίβωση της ταυτότητας των ψευδωνυμοποιημένων δεδομένων είναι δυσχερής [127]. Τα ψευδωνυμοποιημένα παραμένουν δεδομένα προσωπικού χαρακτήρα και, επομένως, υπόκεινται στη νομοθεσία για την προστασία των δεδομένων.

- Μέτρα διασφάλισης του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας.
- Μέτρα αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε περίπτωση απώλειας δεδομένων.
- Εφαρμογή διαδικασίας για τη δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των μέτρων.

Η Ελληνική Ανεξάρτητη Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα εξειδίκευσε έτι περαιτέρω τα τεχνικά μέτρα ως ακολούθως [145]: 1) Μέτρα ελέγχου πρόσβασης σε λογαριασμούς των χρηστών με ανάπτυξη μηχανισμών όπως πχ η ταυτοποίηση πολλών παραγόντων που να μην επιτρέπουν πρόσβαση σε πόρους/εφαρμογές/αρχεία από μη εξουσιοδοτημένους χρήστες καθώς επίσης και υιοθέτηση συγκεκριμένης πολιτικής διαχείρισης των συνθηματικών των χρηστών, η οποία να περιλαμβάνει τουλάχιστον κανόνες αποδοχής για το ελάχιστο μήκος και επιτρεπτούς χαρακτήρες των συνθηματικών (πολυπλοκότητα συνθηματικού), την ιστορικότητα του συνθηματικού και τη συχνότητα αλλαγής του,

2) Υιοθέτηση πολιτικής για τη λήψη και διαχείριση αντιγράφων ασφαλείας που να περιλαμβάνει κανόνες/διαδικασίες που αφορούν την επιλογή των κρίσιμων πόρων (εφαρμογές, λειτουργικά συστήματα, αρχεία, δεδομένα αρχείων χρηστών, κ.λπ.) που χρήζουν δημιουργίας αντιγράφων ασφαλείας, τη συχνότητα της δημιουργίας/λήψης των αντιγράφων ασφαλείας (ανά τακτά διαστήματα, σε ημερήσια ή εβδομαδιαία βάση, ανάλογα με το μέγεθος και το είδος των δεδομένων, καθώς και με το πότε αυτά μεταβάλλονται), την κατάλληλη επισήμανση αυτών, την ασφαλή αποθήκευσή τους και την ορθή ανάκτηση των δεδομένων από τα αντίγραφα ασφαλείας (συμπεριλαμβανομένου του περιοδικού ελέγχου ακεραιότητας/αξιοπιστίας των αντιγράφων που λαμβάνονται). Τα αντίγραφα ασφαλείας πρέπει να τηρούνται σε διαφορετική φυσική τοποθεσία από εκεί που τηρούνται τα πρωτογενή δεδομένα,

3) Μέτρα Προστασίας του υλικού εξοπλισμού όπως εφαρμογή μέτρων προστασίας από κακόβουλο λογισμικό (προγράμματα antivirus και τείχων προστασίας (firewall) ή με περιοδικό έλεγχο του εγκατεστημένου λογισμικού για τον τυχόν εντοπισμό προγραμμάτων που έχουν εγκατασταθεί εκτός των εγκεκριμένων διαδικασιών,

4) Μέτρα τήρησης και ελέγχου των αρχείων καταγραφής όλων των ενεργειών (log files) των χρηστών, συμπεριλαμβανομένων και των ενεργειών των διαχειριστών των συστημάτων, καθώς και των συμβάντων ασφαλείας,

5) Μέτρα ασφαλείας επικοινωνιών όπως έλεγχος των δικτυακών συσκευών, υιοθέτηση συγκεκριμένης διαδικασίας για την απομακρυσμένη πρόσβαση σε συστήματα μέσω ασφαλών καναλιών με δυνατή ταυτοποίηση/αυθεντικοποίηση και κρυπτογράφηση και πάντοτε υπό την εποπτεία και τον έλεγχο του υπευθύνου επεξεργασίας, αποφυγή ευπαθών ως προς την ασφάλεια πρωτοκόλλων όπως FTP, telnet (όπου δεν γίνεται κρυπτογράφηση) και, όταν υπηρεσίες τέτοιων πρωτοκόλλων είναι αναγκαίες, να γίνεται χρήση των αντίστοιχων ασφαλών (όπως, για παράδειγμα, SFTP, SSH), τήρηση επικαιροποιημένου καταλόγου με τις εγκεκριμένες συνδέσεις από και προς το δίκτυο του υπευθύνου επεξεργασίας και τις υπηρεσίες που εξυπηρετούν,

6) Υιοθέτηση μεθόδων για την αποτελεσματική κρυπτογράφηση (επιλογή σύγχρονων και ισχυρών αλγορίθμων κρυπτογράφησης, κατάλληλο μέγεθος κλειδιών και τεχνικές διαχείρισης αυτών, κ.λπ.) αρχείων με προσωπικά δεδομένα που τηρούνται σε φορητά αποθηκευτικά μέσα,

7) Υιοθέτηση σαφούς πολιτικής διαχείρισης όλων των αλλαγών που πραγματοποιούνται στα πληροφοριακά συστήματα, η οποία να περιέχει κατ' ελάχιστον: καταγραφή των αιτημάτων αλλαγής, καθορισμό των ρόλων που έχουν δικαίωμα έγκρισης των αλλαγών, καθορισμό των κριτηρίων αποδοχής της αλλαγής και χρονοδιάγραμμα υλοποίησης ενώ επίσης θα πρέπει να γίνεται δοκιμή των ενημερώσεων λογισμικού, τόσο σε επίπεδο επιμέρους εφαρμογών όσο και σε επίπεδο λειτουργικού συστήματος, σε δοκιμαστικό περιβάλλον και μάλιστα η χρήση πραγματικών δεδομένων στο δοκιμαστικό περιβάλλον θα πρέπει να αποφεύγεται καταρχήν εκτός εάν κάτι τέτοιο είναι απολύτως απαραίτητο και δεν υπάρχει εναλλακτική λύση. Αν είναι αναγκαίο μπορούν να χρησιμοποιηθούν πραγματικά δεδομένα σε ανωνυμοποιημένη μορφή ή διαφορετικά πρέπει να περιορίζονται στα απολύτως απαραίτητα για τους σκοπούς του ελέγχου.

Μεταξύ των οργανωτικών μέτρων που στοχεύουν στην ενίσχυση της ασφάλειας των δεδομένων συγκαταλέγονται μεταξύ άλλων [127, 146]:

1) Τακτική παροχή πληροφοριών σε όλους τους υπαλλήλους σχετικά με τους κανόνες ασφάλειας δεδομένων και τις υποχρεώσεις τους βάσει του δικαίου για την προστασία δεδομένων, ιδίως όσον αφορά τις υποχρεώσεις εμπιστευτικότητας,

2) Δημιουργία οργανωτικών ρόλων για συγκεκριμένες εργασίες εντός του οργανισμού και σύνδεση των ρόλων με συγκεκριμένα άτομα,

3) Υιοθέτηση πολιτικών διαχείρισης υλικού και λογισμικού, διαχείρισης του φυσικού αρχείου με θέσπιση συγκεκριμένων διαδικασιών για την ορθή οργάνωση/αρχειοθέτηση/ταξινόμηση αυτού,

4) Θέσπιση διαδικασίας ασφαλούς καταστροφής των προσωπικών δεδομένων μετά το πέρας της περιόδου που απαιτείται για την πραγματοποίηση του σκοπού της επεξεργασίας,

5) Λήψη κατάλληλων μέτρων για την προστασία των κτιρίων, των κρίσιμων χώρων, του εξοπλισμού πληροφορικής και του χώρου τήρησης φυσικού αρχείου από ζημιές που μπορούν να προκληθούν από φυσικές καταστροφές ή κακόβουλες ενέργειες, όπως πλημμύρα, υπερθέρμανση, πυρκαγιά, σεισμός, έκρηξη, διαρροή νερού, διακοπή ρεύματος, διάρρηξη/κλοπή, βανδαλισμός, κ.λπ. Ενδεικτικά μέτρα προς αυτή την κατεύθυνση είναι τα εξής: εγκατάσταση συναγερμού, πορτών και παραθύρων ασφαλείας, πυροπροστασίας, απομάκρυνση εξοπλισμού από υδροσωληνώσεις και πηγές σκόνης, τοποθέτηση ανιχνευτών υγρασίας και πλημμύρας, αδιάλειπτη παροχή ρεύματος μέσω σταθεροποιητών/γεννητριών, κ.λπ.

Τα ως άνω τεχνικά και οργανωτικά μέτρα λαμβάνονται τόσο κατά το σχεδιασμό των μέσων επεξεργασίας (πχ κρυπτογράφηση των δεδομένων του server και των υπολογιστών κλπ.), όσο και εξ ορισμού, ώστε να υφίστανται επεξεργασία μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για τον εκάστοτε σκοπό της επεξεργασίας (αρχή της ελαχιστοποίησης των δεδομένων προσωπικού χαρακτήρα).

6.2 Υποχρέωση κοινοποίησης παραβιάσεων δεδομένων

Στο πλέγμα των υποχρεώσεων που συναρτώνται στενά με την ασφάλεια των δεδομένων εντάσσεται και η κοινοποίηση παραβιάσεων ασφαλείας δεδομένων. Ως παραβίαση δεδομένων προσωπικού χαρακτήρα, ο ΓΚΠΔ ορίζει στο άρθρο 4 περ. 12 ως την παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ αδείας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.

Η γνωστοποίηση της παραβίασης πρέπει να γίνεται, σύμφωνα με τον ΓΚΠΔ, τόσο στην εποπτική αρχή όσο και στα ίδια τα υποκείμενα των δεδομένων.

Ειδικότερα, σύμφωνα με το άρθρο 33 του ΓΚΠΔ ο υπεύθυνος επεξεργασίας πρέπει αμελλητί και αν τούτο δεν είναι δυνατό, εντός 72 ωρών από τότε που έλαβε γνώση του γεγονότος της παραβίασης δεδομένων, να ειδοποιήσει την Εποπτική αρχή. Ο ΓΚΠΔ αναγνωρίζοντας ότι μπορεί να συντρέχουν περιστάσεις που να καθιστούν αδύνατη την ειδοποίηση της εποπτικής αρχής εντός των ως άνω τασσόμενων προθεσμιών επειδή πιθανόν ο υπεύθυνος επεξεργασίας χρειάζεται περισσότερο χρόνο να διαπιστώσει τον αριθμό και την έκταση των παραβιάσεων [148], δίνει τη δυνατότητα στον υπεύθυνο επεξεργασίας να πραγματοποιήσει αυτή και μετά την πάροδο των 72 ωρών αλλά με ταυτόχρονη έγγραφη αιτιολόγηση για την καθυστέρηση.

Παρακάτω παρατίθεται ένα υπόδειγμα φόρμας υποβολής γνωστοποίησης περιστατικού παραβίασης προσωπικών δεδομένων από το οποίο προκύπτει το ελάχιστο περιεχόμενο που πρέπει να έχει η γνωστοποίηση [149]:

Φόρμα υποβολής γνωστοποίησης περιστατικού παραβίασης προσωπικών δεδομένων **Σύμφωνα με το άρ. 33 του Γενικού Κανονισμού (ΕΕ) 2016/679**

0. Γενικές Πληροφορίες	**Επεξηγηματικά Σχόλια**
Είδος γνωστοποίησης **(Αρχική/Συμπληρωματική/Πλήρης)**	1) **Αρχική,** αν πρόκειται για υποβολή κάποιων πρώτων διαθέσιμων στοιχείων, ενώ εκκρεμούν κάποια γιατί ακόμη δεν είναι διαθέσιμα 2) **Συμπληρωματική**, αν παρέχονται συμπληρωματικά στοιχεία επί προηγούμενης υποβληθείσας ως αρχικής 3) **Πλήρης,** αν

						παρέχονται όλες οι πληροφορίες επί του περιστατικού
Ημερομηνία υποβολής προηγούμενης γνωστοποίησης για το ίδιο περιστατικό						Συμπληρώνεται εφόσον η παρούσα γνωστοποίηση είναι συμπληρωματική
1. Ποιος υποβάλλει την παρούσα γνωστοποίηση περιστατικού (υπεύθυνος επεξεργασίας)						
1.1 Επωνυμία υπευθύνου επεξεργασίας						
Όνομα οργανισμού/φορέα						
Αριθμός ΓΕΜΗ (αν υπάρχει)						
ΑΦΜ						
Διεύθυνση οργανισμού/φορέα **για επικοινωνία**						
Αρμόδιο πρόσωπο **για επικοινωνία με την Αρχή** **(ονοματεπώνυμο - θέση στον οργανισμό/φορέα)**						
Ηλεκτρονική Διεύθυνση						
Τηλέφωνο						
Ταχυδρομική Διεύθυνση						
1.2 Πληροφορίες τυχόν τρίτων εμπλεκομένων μελών						
Για την εν λόγω επεξεργασία προσωπικών δεδομένων συμμετέχει και τρίτος, πέραν του οργανισμού σας; (ΝΑΙ/ΟΧΙ)						
2. Πληροφορίες για το χρονοδιάγραμμα του περιστατικού						
Το περιστατικό είναι σε εξέλιξη; **(ΝΑΙ/ΟΧΙ)**						
Χρόνος έναρξης του περιστατικού **(μέρα/μήνας/έτος ώρα)**						Σε περίπτωση που δεν γνωρίζετε τον ακριβή χρόνο, συμπληρώνετε κατά

(π.χ. 14/3/2018 15:00)		προσέγγιση
Χρόνος που λάβατε γνώση του περιστατικού (μέρα/μήνας/έτος ώρα) **(π.χ. 14/3/2018 15:00)**		Σε περίπτωση που δεν γνωρίζετε τον ακριβή χρόνο, συμπληρώνετε κατά προσέγγιση
Τρόπος με τον οποίο λάβατε γνώση του περιστατικού		
Χρόνος που ενημερωθήκατε από τον εκτελούντα την επεξεργασία για το περιστατικό **(έτος/μήνας/μέρα/ώρα)**		Προαιρετικό πεδίο. Συμπληρώνεται μόνο εάν υπήρξε ενημέρωση από τον εκτελούντα. Σε περίπτωση που δεν γνωρίζετε τον ακριβή χρόνο, συμπληρώνετε κατά προσέγγιση
Λοιπές επεξηγηματικές πληροφορίες επί του χρονοδιαγράμματος		Προαιρετικό πεδίο. Συμπληρώνεται αν ο υπεύθυνος επεξεργασίας κρίνει ότι χρειάζονται επεξηγηματικές πληροφορίες - π.χ. προσδιορισμός για το ότι οι ανωτέρω χρόνοι είναι κατά προσέγγιση
3. Πληροφορίες για τη φύση του περιστατικού		
Παραβίαση της εμπιστευτικότητας των προσωπικών δεδομένων;	**ΟΧΙ**	Συμπληρώνετε ΝΑΙ εφόσον αποκτήθηκε μη εξουσιοδοτημένη πρόσβαση σε προσωπικά δεδομένα ή μη εξουσιοδοτημένη αποκάλυψη αυτών
Παραβίαση της ακεραιότητας των προσωπικών δεδομένων;		Συμπληρώνετε ΝΑΙ εφόσον πραγματοποιήθηκε μη εξουσιοδοτημένη

		τροποποίηση/αλλοίωση σε προσωπικά δεδομένα
Παραβίαση της διαθεσιμότητας των προσωπικών δεδομένων;		Συμπληρώνετε NAI εφόσον τα προσωπικά δεδομένα κατέστησαν μη διαθέσιμα ή καταστράφηκαν
Φύση του περιστατικού		**<u>Ενδεικτικά</u>** <u>παραδείγματα:</u> 1) Απώλεια ή κλοπή συσκευής/εξοπλισμού 2) Απώλεια ή κλοπή φυσικού αρχείου, ή τοποθέτησή του σε μη ασφαλές μέρος 3) Απώλεια αλληλογραφίας ή ανάγνωση αυτής από όχι εξουσιοδοτημένο παραλήπτη 4) Επίθεση ασφαλείας (Hacking) 5) Κακόβουλο λογισμικό (π.χ. ιός, ransomware) 6) E-mail εξαπάτησης (phishing) 7) Όχι σωστή καταστροφή εγγράφων/αρχείων (είτε έντυπα είτε ηλεκτρονικά)

		8) Δημοσίευση/κοινοποίηση δεδομένων εκ παραδρομής 9) Επίδειξη/χορήγηση/διαβίβαση δεδομένων λάθος προσώπου 10) Προφορική διάδοση δεδομένων εκ παραδρομής και άλλα (μπορεί να είναι και συνδυασμός πολλών)
Αιτία/ες του περιστατικού		**<u>Ενδεικτικά</u>** <u>παραδείγματα:</u> 1) Ανθρώπινο λάθος 2) Κακόβουλη εσωτερική ενέργεια 3) Κακόβουλη εξωτερική ενέργεια 4) φυσικό φαινόμενο 5) Παρωχημένο υλικό 6) Παρωχημένο λογισμικό 7) Άγνωστη αιτία και άλλα (μπορεί να είναι και συνδυασμός πολλών)
4. Είδος προσωπικών δεδομένων που αφορά το περιστατικό		

4.1 "Απλά" (όχι ευαίσθητα) δεδομένα						
Στοιχεία ταυτοποίησης (ονοματεπώνυμο, όνομα λογαριασμού σε ηλεκτρονική υπηρεσία, συνθηματικό κτλ.)						
Αριθμός ταυτότητας/διαβατηρίου						
Αριθμός Φορολογικού Μητρώου						
Αριθμός Μητρώου Κοινωνικής Ασφάλισης						
Άλλο μοναδικό αναγνωριστικό						
Ημερομηνία γέννησης (ΝΑΙ/ΟΧΙ)						
Στοιχεία επικοινωνίας (π.χ. ταχυδρομική ή ηλεκτρονική διεύθυνση, τηλέφωνο κτλ.) (ΝΑΙ/ΟΧΙ)						
Οικονομικά στοιχεία (ΝΑΙ/ΟΧΙ)						
Δεδομένα θέσης (ΝΑΙ/ΟΧΙ)						
Επίσημα έγγραφα (ΝΑΙ/ΟΧΙ)						
Δεδομένα που αφορούν ποινικές καταδίκες και αδικήματα (ΝΑΙ/ΟΧΙ)						
Άλλο (ΝΑΙ/ΟΧΙ)						
Άγνωστο (ΝΑΙ/ΟΧΙ)						
4.2 Δεδομένα ειδικών κατηγοριών						
Φυλετική ή εθνοτική καταγωγή (ΝΑΙ/ΟΧΙ)						
Πολιτικά φρονήματα (ΝΑΙ/ΟΧΙ)						
Θρησκευτικές ή φιλοσοφικές πεποιθήσεις (ΝΑΙ/ΟΧΙ)						
Συμμετοχή σε συνδικαλιστική οργάνωση (ΝΑΙ/ΟΧΙ)						
Γενετικά δεδομένα (ΝΑΙ/ΟΧΙ)						
Βιομετρικά δεδομένα (ΝΑΙ/ΟΧΙ)						
Δεδομένα υγείας (ΝΑΙ/ΟΧΙ)						
Δεδομένα που αφορούν σεξουαλική ζωή ή γενετήσιο προσανατολισμό (ΝΑΙ/ΟΧΙ)						
Άλλο (ΝΑΙ/ΟΧΙ)						
5. Πρόσωπα που αφορά το περιστατικό						

Πλήθος αρχείων (κατά προσέγγιση) που αφορά το περιστατικό		
Πλήθος προσώπων (κατά προσέγγιση) που αφορά το περιστατικό		
Δεδομένα εργαζομένων		
Δεδομένα χρηστών υπηρεσίας		
Δεδομένα συνδρομητών		
Δεδομένα μαθητών		
Δεδομένα στελεχών Σωμάτων Ασφαλείας		
Δεδομένα πελατών (νυν ή/και τέως)		
Δεδομένα ασθενών		
Δεδομένα ανηλίκων		
Άλλο (ΝΑΙ/ΟΧΙ)		
Άγνωστο (ΝΑΙ/ΟΧΙ)		
Αναλυτική περιγραφή των κατηγοριών των προσώπων που αφορά το περιστατικό		Παράθεση επεξηγηματικών πληροφοριών επί των όσων απαντήσατε ανωτέρω
6. Μέτρα που είχαν ληφθεί ΠΡΙΝ το περιστατικό		
Αναλυτική περιγραφή των μέτρων που είχαν ληφθεί πριν το περιστατικό		
7. Συνέπειες από το περιστατικό		
7.1 Παραβίαση εμπιστευτικότητας		
7.2 Παραβίαση ακεραιότητας		
7.3 Παραβίαση διαθεσιμότητας		
7.4 Σωματική, υλική ή μη υλική βλάβη ή σημαντικές συνέπειες για τα πρόσωπα		

Φύση των πιθανών συνεπειών που θα έχουν τα πρόσωπα που επηρεάζονται από το περιστατικό	**<u>Ενδεικτικά</u>** <u>παραδείγματα</u>: 1) Εμπόδια στην άσκηση ελέγχου επί των δεδομένων τους 2) Περιορισμός/στέρηση δικαιωμάτων και ελευθεριών 3) Διακρίσεις 4) Κατάχρηση ή υποκλοπή ταυτότητας, 5) Οικονομική απώλεια 6) Δυσφήμηση 7) Απώλεια εμπιστευτικότητας δεδομένων που προστατεύονται από επαγγελματικό απόρρητο 8) Παράνομη άρση της ψευδωνυμοποίησης 9) Αξιολόγηση προσωπικών πτυχών και άλλα (μπορεί να είναι και συνδυασμός πολλών). Εξηγήστε αναλυτικά.
Σοβαρότητα των πιθανών συνεπειών (Αμελητέα - Μικρή - Μεγάλη - Πολύ μεγάλη)	Απαντήστε βάσει της εκτίμησης που κάνατε

8. Ενέργειες ΜΕΤΑ το περιστατικό	
8.1 Ενημέρωση των προσώπων	
Ενημερώσατε τα πρόσωπα που επηρεάστηκαν από το περιστατικό;	Εάν απαντήσετε "ΔΕΝ ΑΠΟΦΑΣΙΣΤΗΚΕ ΑΚΟΜΗ ΑΝ ΠΡΕΠΕΙ ΝΑ ΕΝΗΜΕΡΩΘΟΥΝ", θα πρέπει να υποβληθεί στο εγγύς μέλλον και συμπληρωματική γνωστοποίηση για το εν λόγω περιστατικό
8.2 Μέτρα για την αντιμετώπιση του περιστατικού	
Περιγραφή των μέτρων που λήφθηκαν για την αντιμετώπιση της παραβίασης	
8.3 Διασυνοριακό περιστατικό και άλλα θέματα	
Η εν λόγω γνωστοποίηση αφορά περιστατικό παραβίασης που επηρεάζει πρόσωπα σε πολλά Κράτη Μέλη και υποβάλλεται στην επικεφαλής εποπτική Αρχή; (ΝΑΙ/ΟΧΙ)	
Γνωστοποιήσατε ή προτίθεστε να γνωστοποιήσετε το περιστατικό και σε άλλα επηρεαζόμενα Κράτη Μέλη; (ΝΑΙ/ΟΧΙ)	
Γνωστοποιήσατε ή προτίθεστε να γνωστοποιήσετε το περιστατικό και σε Αρχή Προστασίας Δεδομένων κράτους εκτός ΕΕ; (ΝΑΙ/ΟΧΙ)	
Γνωστοποιήσατε ή προτίθεστε να γνωστοποιήσετε το περιστατικό και σε άλλο Όργανο ή Αρχή βάσει διατάξεων άλλων από τον Κανονισμό (ΕΕ) 2016/679 (ΝΑΙ/ΟΧΙ)	

Εντούτοις, γνωστοποίηση στην εποπτική αρχή δεν απαιτείται εάν η παραβίαση των προσωπικών δεδομένων δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Ως τέτοιες παραβιάσεις νοούνται εκείνες που είτε τα δεδομένα είναι ήδη δημόσια προσιτά είτε αυτά έχουν καταστεί ουσιαστικά ακατάληπτα για μη εξουσιοδοτημένα πρόσωπα λόγω πχ της κατάλληλης κρυπτογράφησης [148].

Εν σχέσει δε με την ανακοίνωση της παραβίασης δεδομένων και στα υποκείμενα των δεδομένων, σύμφωνα με το άρθρο 34 του ΓΚΠΔ, προϋπόθεση για

την ενημέρωση τους είναι η ύπαρξη υψηλού κινδύνου για τα δικαιώματα και τις ελευθερίες των προσώπων των οποίων παραβιάζονται τα δεδομένα. Ο σκοπός της ανακοίνωσης είναι η παροχή ειδικής ενημέρωσης αναφορικά με τα μέτρα που πρέπει να λάβουν τα υποκείμενα των δεδομένων προκειμένου να αυτοπροστατευθούν ενώ θα πρέπει να προτιμάται εκείνη η μέθοδος ανακοίνωσης που μεγιστοποιεί τις πιθανότητες να γίνει γνωστή η σχετική πληροφορία σε όλα τα θιγόμενα υποκείμενα των δεδομένων[148].

Σύμφωνα με την παράγραφο 3 του άρθρου 34 του ΓΚΠΔ η ανακοίνωση μπορεί να παραλειφθεί εάν ο υπεύθυνος επεξεργασίας είχε ήδη πριν από την παραβίαση λάβει τα κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας ή λαμβάνει τέτοια μέτρα στη συνέχεια διασφαλίζοντας ότι δεν είναι πλέον πιθανό να επέλθει ο κίνδυνος.

6.3 Τήρηση αρχείου δραστηριοτήτων

Ο υπεύθυνος επεξεργασίας προκειμένου να μπορεί να αποδείξει τη συμμόρφωση του με τον ΓΚΠΔ, φέρει επίσης υποχρέωση τήρησης αρχείου δραστηριοτήτων επεξεργασίας το οποίο πρέπει να περιέχει, σύμφωνα με το άρθρο 30 του ΓΚΠΔ, τις ακόλουθες πληροφορίες: το όνομα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας, τους σκοπούς της επεξεργασίας, την περιγραφή των κατηγοριών υποκειμένων των δεδομένων και των κατηγοριών δεδομένων προσωπικού χαρακτήρα, τις κατηγορίες αποδεκτών στους οποίους πρόκειται να γνωστοποιηθούν ή γνωστοποιήθηκαν τα δεδομένα προσωπικού χαρακτήρα, όπου συντρέχει περίπτωση, τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό, συμπεριλαμβανομένων του προσδιορισμού της εν λόγω χώρας ή του διεθνούς οργανισμού, όπου είναι δυνατό τις προβλεπόμενες προθεσμίες διαγραφής των διάφορων κατηγοριών δεδομένων καθώς και όπου είναι δυνατό, γενική περιγραφή των τεχνικών και οργανωτικών μέτρων ασφαλείας. Το εν λόγω αρχείο φυλάσσεται υπό την ευθύνη του υπευθύνου επεξεργασίας και τίθεται στη διάθεση της εποπτικής αρχής σε περίπτωση που ζητηθεί.

6.4 Ορισμός Υπεύθυνου Προστασίας Προσωπικών Δεδομένων (Data Protection Officer - DPO)

Με το άρθρο 37 του ΓΚΠΔ εισάγεται ο θεσμός του Υπευθύνου Προστασίας Δεδομένων (ΥΠΔ), ο οποίος σύμφωνα με τις αναθεωρημένες το έτος 2017

Κατευθυντήριες Γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων της Ομάδας Εργασίας του άρθρου 29 για την προστασία προσωπικών δεδομένων [147] αποτελεί καίρια συνιστώσα του νέου συστήματος διακυβέρνησης δεδομένων. Σύμφωνα και με την αιτιολογική σκέψη 97 του ΓΚΠΔ, αποτελεί ένα πρόσωπο με ειδικές γνώσεις στο δίκαιο και τις πρακτικές προστασίας δεδομένων που παρέχει συνδρομή προς τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία κατά την παρακολούθηση της εσωτερικής συμμόρφωσης προς τον ΓΚΠΔ.

Δεδομένου μάλιστα ότι στο πλαίσιο της έξυπνης πανεπιστημιούπολης οι βασικές δραστηριότητες που πραγματοποιούνται απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα και συνιστούν ταυτόχρονα και μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα, ο διορισμός του υπευθύνου προστασίας δεδομένων είναι υποχρεωτικός για τον οργανισμό της έξυπνης πανεπιστημιούπολης, σύμφωνα με το άρθρο 37 παρ. 1 του ΓΚΠΔ.

Μεταξύ των καθηκόντων του ΥΠΔ ανήκουν κατ΄ελάχιστον, σύμφωνα με το άρθρο 39 του ΓΚΠΔ, τα ακόλουθα: i) συνεχής παροχή συμβουλών και ενημέρωσης προς τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία και τους υπαλλήλους αυτών σχετικά με τις υποχρεώσεις που απορρέουν από τον ΓΚΠΔ. Ο υπεύθυνος ή εκτελών την επεξεργασία δεν υποχρεούται να ακολουθήσει την συμβουλή του ΥΠΔ, η οποία άλλωστε είναι και μη δεσμευτική, αλλά στη περίπτωση αυτή, ενδείκνυται σύμφωνα με τις επιταγές της αρχής της λογοδοσίας, η έγγραφη τεκμηρίωση της αντίθετης θέσης από πλευράς του υπευθύνου επεξεργασίας και αντίστοιχα η από μέρους του ΥΠΔ έγγραφη ενημέρωση της ανώτερης διοίκησης [148], ii) παρακολούθηση της συμμόρφωσης του υπευθύνου και εκτελούντος την επεξεργασία με τον ΓΚΠΔ αλλά και με τις πολιτικές της επιχείρησης συμπεριλαμβανομένων αυτών της ανάθεσης αρμοδιοτήτων, ευαισθητοποίησης και κατάρτισης των υπαλλήλων που συμμετέχουν σε πράξεις επεξεργασίας. Η δυνατότητα του ΥΠΔ να προβαίνει σε προληπτικούς ελέγχους είναι απόρροια της ανεξαρτησίας και αντικειμενικότητας του ενώ σε περίπτωση μη συμμόρφωσης με τον ΓΚΠΔ αποτελεί καθήκον του να προβεί σε συστάσεις διορθωτικού περιεχομένου προς τον υπεύθυνο ή τον εκτελούντα την επεξεργασία λειτουργώντας σαν μια εσωτερική εποπτική αρχή [148], iii) συνεργασία με την εποπτική αρχή και ταυτόχρονα δράση ως σημείο επικοινωνίας για την εποπτική αρχή και την άσκηση των ερευνητικών - ελεγκτικών αρμοδιοτήτων της. Πρόκειται για δύο διακριτά

καθήκοντα που μπορούν όμως να συνδυασθούν και να ασκηθούν από κοινού καθώς αναφέρονται στον «μεσολαβητικό» και «διευκολυντικό» ρόλο του ΥΠΔ. Στη πρώτη περίπτωση ήτοι της συνεργασίας του ιδίου με την εποπτική αρχή, ο ΥΠΔ διευκολύνει την πρόσβαση της εποπτικής αρχής στα έγγραφα και τις πληροφορίες που σχετίζονται με την επιτέλεση των καθηκόντων της ενώ στη δεύτερη περίπτωση ο ΥΠΔ λειτουργεί για λογαριασμό της εποπτικής αρχής, ως μεσολαβητής με τον υπεύθυνο ή εκτελούντα την επεξεργασία καθώς και με τα υποκείμενα των δεδομένων για κάθε ζήτημα σχετικό με την επεξεργασία των δεδομένων τους και την άσκηση των δικαιωμάτων τους δυνάμει του ΓΚΠΔ έχοντας μάλιστα ταυτόχρονα ακόμη και αν δε προκύπτει ρητά από τον ΓΚΠΔ και ρόλο αποδοχής και διερεύνησης καταγγελιών παραβίασης της νομοθεσίας για τα προσωπικά δεδομένα [148]. Με τη παράγραφο 2 του άρθρου 39 που επιτάσσει στον ΥΠΔ να λαμβάνει δεόντως τον κίνδυνο που συνδέεται με τις πράξεις επεξεργασίας συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς επεξεργασίας, δεν εισάγεται ένα επιπλέον καθήκον αλλά ένας κανόνας αξιολόγησης και προτεραιοποίησης εξέτασης των πράξεων επεξεργασίας που συνδέονται με υψηλό κίνδυνο [148].

6.5 Μελέτη εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων

Ο ΓΚΠΔ στο άρθρο 35 αυτού προέβλεψε ως εργαλείο συμμόρφωσης του υπευθύνου επεξεργασίας με την αρχή της λογοδοσίας, την διενέργεια εκτίμησης αντικτύπου σχετικά με τη προστασία των προσωπικών δεδομένων στην οποία αναλύονται η φύση, το πεδίο εφαρμογής και οι σκοποί της επεξεργασίας, αποτιμώνται η αναγκαιότητα και αναλογικότητα της και εκτιμάται η σοβαρότητα των κινδύνων για τα δικαιώματα και τις ελευθερίες των ατόμων σε συνάρτηση με την πιθανότητα επέλευσης τους [150].

Υφίσταται υποχρέωση διενέργειας αυτής σε περιπτώσεις επεξεργασιών υψηλής επικινδυνότητας για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων και ιδίως στις ακόλουθες περιπτώσεις, σύμφωνα με την παράγραφο 3 του άρθρου 35 του ΓΚΠΔ: α) όταν υπάρχει συστηματική και εκτενής αξιολόγηση προσωπικών πτυχών σχετικά με φυσικά πρόσωπα, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία, περιλαμβανομένης της κατάρτισης προφίλ και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα σχετικά με το φυσικό πρόσωπο ή ομοίως επηρεάζουν σημαντικά το φυσικό πρόσωπο, β) όταν πρόκειται για μεγάλης κλίμακας επεξεργασία των ειδικών κατηγοριών δεδομένων

που αναφέρονται στο άρθρο 9 παρ. 1 ή γ) όταν αφορούν σε συστηματική παρακολούθηση δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα.

Ενόψει του γεγονότος ότι στο πλαίσιο της έξυπνης πανεπιστημιούπολης λαμβάνει χώρα συστηματική, εκτενής και σε μεγάλη κλίμακα επεξεργασία απλών αλλά και ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα με τη χρήση νέων τεχνολογιών που ενδέχεται να οδηγήσουν σε σημαντική αύξηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, καθίσταται σαφές πως η διενέργεια εκτίμησης αντικτύπου είναι υποχρεωτική.

Ο ΓΚΠΔ δεν επιβάλλει κάποια συγκεκριμένη μεθοδολογία για την εκπόνηση της Εκτίμησης Αντικτύπου, πλην όμως υπάρχει ένα διεθνές πρότυπο, το ISO/IEC 29134:2017 και σήμερα αναθεωρημένο ISO/IEC 29134:2023 [151] το οποίο παρέχει κατευθυντήριες γραμμές για την διαδικασία εκπόνησης, τη δομή και το περιεχόμενο μίας εκτίμησης αντικτύπου. Με απλά λόγια, η εκτίμηση αντικτύπου είναι ένα σύνολο ενεργειών με ορισμένα παραδοτέα, οι οποίες μπορεί να βασίζονται σε διαδικασίες και να αποτελούνται από πολλά βήματα. Ξεκινάει ήδη κατά την ανάπτυξη ενός συστήματος ή προγράμματος στο οποίο προβλέπεται επεξεργασία προσωπικών δεδομένων, έτσι ώστε να είναι δυνατή η επιρροή της στις τελικές επιλογές των χαρακτηριστικών και των μέσων επεξεργασίας, διασφαλίζοντας έτσι την προστασία δεδομένων ήδη από το σχεδιασμό [150].

Η εκτίμηση αντικτύπου πρέπει να περιλαμβάνει ορισμένα απαραίτητα τυπικά στοιχεία ήτοι: συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών επεξεργασίας, εκτίμηση αναγκαιότητας και αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους σκοπούς, εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων καθώς επίσης και τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων περιλαμβανομένων των εγγυήσεων, των μέτρων και μηχανισμών ασφαλείας ώστε να διασφαλίζεται η προστασία των δεδομένων προσωπικού χαρακτήρα και να αποδεικνύεται η συμμόρφωση με τον ΓΚΠΔ.

Εν κατακλείδι, η εκτίμηση αντικτύπου στην προστασία δεδομένων είναι ένα εργαλείο για τη συμμόρφωση του υπευθύνου επεξεργασίας με τον ΓΚΠΔ η οποία θα πρέπει να αναθεωρείται τακτικά και σε κάθε περίπτωση όταν επέρχεται κάποια σημαντική αλλαγή που επηρεάζει και αυξάνει τους επαπειλούμενους κινδύνους, όπως εάν χρησιμοποιηθούν νέα τεχνολογικά μέσα ή διευρυνθούν τα είδη των δεδομένων

που συλλέγονται ή οι παραλήπτες τους ή αν ακόμη αποκαλυφθούν αδυναμίες των τεχνικών μέσων επί των οποίων στηρίζεται η επεξεργασία [150].

ΚΕΦΑΛΑΙΟ 7 - ΣΥΜΠΕΡΑΣΜΑΤΑ

Η έξυπνη πανεπιστημιούπολη συνιστά έναν ζωντανό οργανισμό που αναπτύσσεται συνέχεια έχοντας ως συμμάχους της τις διαρκώς εξελισσόμενες τεχνολογίες. Η πλούσια βιβλιογραφία επί των προτεινόμενων υπηρεσιών ανά πυλώνα της έξυπνης πανεπιστημιούπολης φανερώνει αφενός τον ταχύ ρυθμό ενσωμάτωσης των νέων αυτών τεχνολογιών στο εσωτερικό της και αφετέρου το μεγάλο ενδιαφέρον των ερευνητών προς μία κατεύθυνση βελτιστοποίησης, αυτοματοποίησης και εν γένει αναβάθμισης των εκπαιδευτικών -και όχι μόνο- διαδικασιών που παρέχονται στο πλαίσιο αυτής. Από τα ευφυή συστήματα διαχείρισης κτιρίων έως την ανάλυση της μάθησης με βάση τα δεδομένα, η ενσωμάτωση των έξυπνων τεχνολογιών έχει ωθήσει τα εκπαιδευτικά ιδρύματα σε μια εποχή αυξημένης αποτελεσματικότητας, προσβασιμότητας και συνδεσιμότητας.

Η έξυπνη πανεπιστημιούπολη αποτελεί έναν κόμβο διασυνδεδεμένων συσκευών και συστημάτων που αξιοποιεί στο έπακρο τις σύγχρονες τεχνολογικές δυνατότητες. Τούτο συνεπάγεται μεταξύ άλλων, τη δημιουργία και τη χρήση τεράστιων ποσοτήτων δεδομένων, ορισμένων εκ των οποίων, προσωπικών και μάλιστα ευαίσθητων, με αποτέλεσμα να εγείρονται προβληματισμοί σχετικά με τη προστασία της ιδιωτικότητας των χρηστών.

Τους προβληματισμούς αυτούς επιλύει σε μεγάλο βαθμό ο ΓΚΠΔ, ο οποίος θεσπίζει ένα ισχυρό νομικό και θεσμικό πλέγμα ομοιόμορφων κανόνων για την προστασία των δεδομένων προσωπικού χαρακτήρα σε ευρωπαϊκό επίπεδο διαφυλάσσοντας τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων και ταυτόχρονα αυξάνοντας τις υποχρεώσεις του υπευθύνου επεξεργασίας, σε μία προσπάθεια αντιμετώπισης των προκλήσεων για την προστασία των προσωπικών δεδομένων που δημιούργησαν οι ραγδαίες τεχνολογικές εξελίξεις.

Ο ΓΚΠΔ θέτει πολλούς περιορισμούς και προϋποθέσεις ως προς τη νομιμότητα των πράξεων επεξεργασίας των προσωπικών δεδομένων των χρηστών. Οι αυστηρές αυτές προϋποθέσεις συνδυαστικά με τον αλματώδη ρυθμό ανάπτυξης της τεχνολογίας καθιστούν επιτακτική την αδιάλειπτη ερμηνεία και υπαγωγή των εννοιών του στα καινούρια τεχνολογικά δεδομένα προκειμένου να μη καταλείπεται περιθώριο καταστρατήγησης της νομοθεσίας καθώς όπως η ανάπτυξη της έξυπνης

πανεπιστημιούπολης αποτελεί μια διαρκώς εξελισσόμενη διαδικασία, έτσι ακριβώς και η συμμόρφωση με τις κανονιστικές επιταγές πρέπει να ελέγχεται συστηματικά και πάντοτε σε πραγματικό χρόνο.

Η αυστηρότητα των διατάξεων του ανωτέρω Κανονισμού θα έλεγε κανείς πως αποτελεί τροχοπέδη στην υλοποίηση μίας πολυδιάστατης έξυπνης πανεπιστημιούπολης όπως αναλύθηκε ως άνω, πλην όμως τούτο δεν ευσταθεί. Ο ΓΚΠΔ δεν θεσπίστηκε προκειμένου να αναχαιτίσει τη τεχνολογική πρόοδο, αλλά αντιθέτως προκειμένου να τη ρυθμίσει. Για το λόγο αυτό, θέτει άλλωστε και συγκεκριμένες υποχρεώσεις στους υπευθύνους επεξεργασίας, τηρουμένων των οποίων επιτυγχάνεται η συμμόρφωση τους με αυτόν.

Ειδικότερα, ο ΓΚΠΔ καθιστά επιβεβλημένη τη λήψη τεχνικών και οργανωτικών μέτρων καθώς επίσης και την τήρηση των αρχών επεξεργασίας των δεδομένων προσωπικού χαρακτήρα. Παρέχει μάλιστα ένα οπλοστάσιο δικαιωμάτων στα υποκείμενα των δεδομένων δίνοντας τους την δυνατότητα να διαδραματίζουν ενεργό ρόλο κατά τη διάρκεια των πράξεων επεξεργασίας των προσωπικών τους δεδομένων.

Αν και αποτελεί ένα αναλυτικό νομοθέτημα, δε παύει να αφήνει αρρύθμιστα και ορισμένα νομικά ζητήματα, τα οποία μεγεθύνονται με τη συνεχή εξέλιξη της τεχνολογίας. Για το λόγο αυτό περιέχει και αρκετές «ρήτρες ευελιξίας» και «ρήτρες ανοίγματος», αναγνωρίζοντας στα κράτη μέλη την ευχέρεια να εξειδικεύσουν τους κανόνες του με τη θέσπιση ειδικότερων νομοθετικών μέτρων πάντοτε σε συμμόρφωση με το γενικότερο πνεύμα αυτού.

Εξετάζοντας τα της ελληνικής έννομης τάξης, δεν εντοπίζονται ειδικότερες διατάξεις που να ρυθμίζουν τα ζητήματα ιδιωτικότητας στα πλαίσια της έξυπνης πανεπιστημιούπολης. Για το λόγο αυτό, θα πρέπει να διαπιστωθεί στην πράξη αν επαρκεί το ισχύον κανονιστικό πλαίσιο και αν κριθεί ότι χρειάζονται επιμέρους ρυθμίσεις, να υπάρξει η σχετική νομοθετική πρόβλεψη.

Σε κάθε δε περίπτωση, ο συνεχής διάλογος και η συνεργασία μεταξύ ακαδημαϊκών, επιστημόνων πληροφορικής και νομικής καθώς και ρυθμιστικών φορέων θα αποτελέσει ένα χρήσιμο εργαλείο προς τη συγκεκριμένη κατεύθυνση. Με την προώθηση μιας διεπιστημονικής προσέγγισης, τα έξυπνα εκπαιδευτικά ιδρύματα μπορούν να συμμετέχουν ενεργά στη διαμόρφωση πολιτικών, κατευθυντήριων γραμμών και βέλτιστων πρακτικών που προωθούν την καινοτομία και είναι σύμφωνες με τις αρχές του ΓΚΠΔ. Αυτή η συνεργατική προσπάθεια είναι

καθοριστική για την αντιμετώπιση των ιδιαιτεροτήτων της ψηφιακής εποχής, με μέλημα πάντοτε τη διαφύλαξη της προστασίας των προσωπικών δεδομένων.

Εν κατακλείδι, αποδεικνύεται πανηγυρικά ότι το θεωρητικό χάσμα μεταξύ της τεχνολογικής υποδομής της έξυπνης πανεπιστημιούπολης και της προστασίας των δεδομένων προσωπικού χαρακτήρα δεν υφίσταται στην πράξη, τηρουμένων των ανωτέρω. Εντούτοις, είναι σημαντικό οι αρμόδιοι για την υλοποίηση της έξυπνης πανεπιστημιούπολης φορείς να παρακολουθούν στενά τις εν γένει νομοθετικές εξελίξεις και να προσαρμόζουν τις υπηρεσίες και εφαρμογές στις επιταγές αυτών (βλ. σχετικώς νέες και υπό συζήτηση διατάξεις του Κανονισμού για τη Τεχνητή Νοημοσύνη).

ΚΕΦΑΛΑΙΟ 8 - ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Swilling, M.; Hajer, M.; Baynes, T.; Bergesen, J.; Labbé, F.; Musango, J.K.; Ramaswami, A.; Robinson, B.; Salat, S.; Suh, S.; et al. The Weight of Cities Resource Requirements Of Future Urbanization. Available online: https://europa.eu/capacity4dev/unep/documents/weight-cities-resource-requirements-future-urbanization (accessed on 1 April 2019).

[2] Dameri, R.P.; Cocchia, A. Smart City and Digital City: Twenty Years of Terminology Evolution. *X Conf. Ital. Chapter AIS, ITAIS 2013* , 1–8. Available online: http://www.itais.org/proceedings/itais2013/pdf/119.pdf (accessed on 4 October 2018).

[3] Gil-Garcia, J.R.; Pardo, T.A.; Nam, T. What Makes a City Smart? Identifying Core Components and Proposing an Integrative and Comprehensive Conceptualization. *Inf. Polity* 2015, *20*, 61–87.

[4] Nam, T.; Pardo, T.A. Conceptualizing Smart City with Dimensions of Technology, People, and Institutions. In Proceedings of the 12th Annual International Digital Government Research Conference: Digital Government Innovation in Challenging Times, College Park, MD, USA, 12–15 June 2018.

[5] H. M. A. P. K. Bandara, J. D. C. Jayalath, A. R. S. P. Rodrigo, A. U. Bandaranayake, Z. Maraikar, and R. G. Ragel, ‘‘Smart campus phase one: Smart parking sensor network,’’ in Proc. Manuf. Ind. Eng. Symp. (MIES), Oct. 2016, pp. 1–6, doi: 10.1109/MIES.2016.7780262.

[6] W. Muhamad, N. B. Kurniawan, Suhardi, and S. Yazid, ‘‘Smart campus features, technologies, and applications: A systematic literature review,’’ in Proc. Int. Conf. Inf. Technol. Syst. Innov. (ICITSI), Oct. 2017, pp. 384–391, doi: 10.1109/ICITSI.2017.8267975

[7] Zhang, X.M., Shen, J.J., Wu, P.J. and Sun, D.L. (2021) Research on the Application of Big Data Mining in the Construction of Smart Campus. Open Access Library Journal, 8: e8169. https://doi.org/10.4236/oalib.1108169

[8] Zhao Yang Dong, Yuchen Zhang, Christine Yip, Sharon Swift, Kim Beswick, “Smart campus: definition, framework, technologies, and services”, eISSN 2631-7680

Received on 31st August 2019 Revised 14th February 2020 Accepted on 19th February 2020 E-First on 10th March 2020 doi: 10.1049/iet smc.2019.0072 www.ietdl.org

[9] Kajarekar Sunit Pravin Aruna, Manjrekar Devesh Parag Bhagyashree, Kotian Siddhanth Jagdish Sarita, NFC and NFC Payments: A Review,IEEE, https://doi.org/10.1109/ICTBIG.2016.7892683

[10] R. Yasmin, M. Salminen, E. Gilman, J. Petäjäjärvi, K. Mikhaylov, M. Pakanen, A. Niemelä, J. Riekki, S. Pirttikangas, A. Pouttu. Combining IoT Deployment and Data Visualization: experiences within campus maintenance use-case. 9th International Conference on the Network of the Future (NOF), 2018.

[11] https://www.uctel.co.uk/blog/7-reasons-why-campuses-need-a-private-5g-network

[12] Fei Wanga, Hongxia Wangb, and Omid Ranjbar Dehghan, Machine Learning Techniques and Big Data Analysis for Internet of Things Applications: A Review Study, CYBERNETICS AND SYSTEMS: AN INTERNATIONAL JOURNALhttps://doi.org/10.1080/01969722.2022.2103231

[13] Hong Shu, Big Data Analytics: Six Techniques, Geo-spatial information science, 2016Vol. 19, no. 2, 119–128 http://dx.doi.org/10.1080/10095020.2016.1182307

[14]Tuncay Ercana, Effective use of cloud computing in educational institutions, 1877-0428 © 2010 Published by Elsevier Ltd, doi:10.1016/j.sbspro.2010.03.130

[15] Samancioglu, N., Nuere, S. A determination of the smartness level of university campuses: the Smart Availability Scale (SAS). J. Eng. Appl. Sci. 70, 10 (2023). https://doi.org/10.1186/s44147-023-00179-8

[16] Augusto JC, Callaghan V, Cook D, Kameas A, Satoh I (2013) Intelligent environments: A manifesto. HCIS 3(1). https://doi.org/10.1186/2192-1962-3-12

[17] Kulakov K, Petrina OB, Korzun DG, Varfolomeyev AG (2016) Towards an understanding of Smart Service: The case study for cultural heritage E-tourism. In: 2016 18th Conference of Open Innovations Association and Seminar on Information Security and Protection of Information Technology (FRUCT-ISPIT). https://doi.org/10.1109/fruct-ispit. 2016.7561520

[**18]** Akhrif O, Idrissi YEBE, Hmina N (2019) Service Oriented Computing and Smart University. In: Ben Ahmed M, Boudhir A, Younes A (eds) Innovations in Smart Cities Applications Edition 2. SCA 2018. Lecture Notes in Intelligent Transportation and Infrastructure. Springer, Cham. https://doi.org/10.1007/978-3-030-11196-0_3

[19] N. Chagnon-Lessard et al., Smart Campuses: Extensive Review of the Last Decade of Research and Current Challenges, Received July 26, 2021, accepted August 23, 2021, date of publication August 31, 2021, date of current version September 14, 2021. Digital Object Identifier 10.1109/ACCESS.2021.3109516

[20] Theodoros Anagnostopoulos, IoT-enabled Unobtrusive Surveillance Systems for Smart Campus Safety, IEEE Press WILEY, Hardback ISBN: 9781119903901

[21] H. Talei, B. Zizi, M. R. Abid, M. Essaaidi, D. Benhaddou, and N. Khalil, ‘‘Smart campus microgrid: Advantages and the main architectural components,’’ in Proc. 3rd Int. Renew. Sustain. Energy Conf. (IRSEC), Dec. 2015, pp. 1–7, doi: 10.1109/IRSEC.2015.7455093.

[22] B. Lamia and C. Adnen, "Integration of Renewable Energies into the Smart Grid Electricity network," 2023 IEEE International Conference on Artificial Intelligence & Green Energy (ICAIGE), Sousse, Tunisia, 2023, pp. 1-5, doi: 10.1109/ICAIGE58321.2023.10346488.

[23] Zhang, Yuchen & Yip, Christine & Lu, Erwan & Dong, Z.Y.. (2022). A Systematic Review on Technologies and Applications in Smart Campus: A Human-Centered Case Study. IEEE Access. 10. 16134-16149. 10.1109/ACCESS.2022.3148735.

[24] C.-T. Yang, S.-T. Chen, J.-C. Liu, R.-H. Liu, and C.-L. Chang, ‘‘On construction of an energy monitoring service using big data technology for the smart campus,’’ Cluster Comput., vol. 23, no. 1, pp. 265–288, Mar. 2020.

[25] Y. Weng, N. Zhang, and C. Xia, ‘‘Multi-agent-based unsupervised detection of energy consumption anomalies on smart campus,’’ IEEE Access, vol. 7, pp. 2169–2178, 2018, Digital Object Identifier 10.1109/ACCESS.2018.2886583

[26] Pandey, D., & Hanchate Author, S. (2018). Navigation based - Intelligent Parking Management System using Queuing theory and IOT. 2018 Second International Conference on Green Computing and Internet of Things (ICGCIoT). doi:10.1109/icgciot.2018.8753053

[27] Y. Bandung, M. F. N. Aldiansyah, M. R. Dwi Putra and M. I. I. Syiraaj, "Design and Implementation of IoT-Based Smart Parking System in Campus Area," 2023 10th International Conference on ICT for Smart Society (ICISS), Bandung, Indonesia, 2023, pp. 1-6, doi: 10.1109/ICISS59129.2023.10292040.

[28] Toutouh J, Arellano J, Alba E. BiPred: A Bilevel Evolutionary Algorithm for Prediction in Smart Mobility. Sensors (Basel). 2018 Nov 24;18(12):4123. doi: 10.3390/s18124123. PMID: 30477239; PMCID: PMC6308553.

[29] Joaquín Torres-Sospedra, Joan Avariento, David Rambla, Raúl Montoliu, Sven Casteleyn, Mauri Benedito-Bordonau, Michael Gould & Joaquín Huerta (2015): Enhancing integrated indoor/outdoor mobility in a smart campus, International Journal of Geographical Information Science, DOI: 10.1080/13658816.2015.1049541

[30] De Paola, A., Giammanco, A., lo Re, G., & Anastasi, G. (2019). Detection of Points of Interest in a Smart Campus. 2019 IEEE 5th International Forum on Research and Technology for Society and Industry (RTSI), doi: 10.1109/RTSI.2019.8895569

[31] L. Manqele, M. Dlodlo, L. Manqele, L. Coetzee, Q. Williams, and G. Sibiya, ‘‘Preference-based Internet of Things dynamic service selection for smart campus,’’ in Proc. AFRICON, Sep. 2015, pp. 1–5, doi: 10.1109/AFRCON.2015.7332047

[32] https://www.geeksforgeeks.org/supervised-unsupervised-learning/

[33] Kwon, Dongwoo; Kim, Hyeonwoo; An, Donghyeok; Ju, Hongtaek (2017). Container based testbed for gate security using open API mashup. Procedia Computer Science, 111(), 260–267. doi:10.1016/j.procs.2017.06.062

[34] B. Gadgay, D. C. Shubhangi and R. Abhijeet, "VTU campus surveillance and student smart accessibility system using IOT," 2021 IEEE International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS), Bangalore, India, 2021, pp. 1-6, doi: 10.1109/CSITSS54238.2021.9683672

[35] Chandra, Yakob Utama; Mahatmaputra Tedjojuwono, Samuel; David, ; Halim, Stievan Kurniadi; Al-Fath, Nashiruddin; Rebecca, Irene Teresa (2019). [IEEE 2019 International Conference on ICT for Smart Society (ICISS) - Bandung, Indonesia (2019.11.19-2019.11.20)] 2019 International Conference on ICT for Smart Society (ICISS) - Smart E-badge for Student Activities in Smart Campus. , (), 1–6. doi:10.1109/ICISS48059.2019.8969806

[36] N. Deepika, A. J. Sheela, P. S. Lakshmi, V. Lavanya, A. J. Gilda and L. J. Mary, "Android Application to Increase Faculty Performance using Gamified Leaderboard," 2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS), Trichy, India, 2022, pp. 1135-1140, doi: 10.1109/ICAISS55157.2022.10010879.

[37] L. Chamba-Eras and J. Aguilar, "Augmented Reality in a Smart Classroom—Case Study: SaCI," in IEEE Revista Iberoamericana de Tecnologias del Aprendizaje, vol. 12, no. 4, pp. 165-172, Nov. 2017, doi: 10.1109/RITA.2017.2776419.

[**38]** S. AlAwadhi et al., "Virtual reality application for interactive and informative learning," 2017 2nd International Conference on Bio-engineering for Smart Technologies (BioSMART), Paris, France, 2017, pp. 1-4, doi: 10.1109/BIOSMART.2017.8095336.

[39] W. Jia et al., "Smart Education Under 5G+," 2021 11th International Conference on Information Technology in Medicine and Education (ITME), Wuyishan, Fujian, China, 2021, pp. 582-585, doi: 10.1109/ITME53901.2021.00123.

[40] G.J. Hwang, H.C. Chu, C. Yin, H. Ogata, Transforming the educational settings: innovative designs and applications of learning technologies and learning environments. Interact. Learn. Environ. 23(2), 127–129 (2015)

[41] M. Spector, Conceptualizing the emerging field of smart learning environments. Smart Learn. Environ. 1(1), 2–10 (2014), Springer Open

[42] T. Zobel, T. Staubitz and C. Meinel, "Introducing a Smart Learning Assistant on a MOOC Platform: Enhancing Personalized Learning Experiences," 2023 IEEE 2nd German Education Conference (GECon), Berlin, Germany, 2023, pp. 1-6, doi: 10.1109/GECon58119.2023.10295099.

[43] Fotaris Panagiotis & Barbatsis, Kostas & Mastoras, Theodoros & Manitsaris, Athanasios. (2006). VRLAB: An interactive 3D learning environment. WSEAS Transactions on Computers. 5. 30-36.

[44] Murat Akçayır, Gökçe Akçayır, Hüseyin Miraç Pektaş, Mehmet Akif Ocak, Augmented reality in science laboratories: The effects of augmented reality on university students' laboratory skills and attitudes toward science laboratories, Computers in Human Behavior, Volume 57, 2016, Pages 334-342, ISSN 0747-5632, https://doi.org/10.1016/j.chb.2015.12.054.

[45] El-Haggar N, Amouri L, Alsumayt A, Alghamedy FH, Aljameel SS. The Effectiveness and Privacy Preservation of IoT on Ubiquitous Learning: Modern Learning Paradigm to Enhance Higher Education. Applied Sciences. 2023; 13(15):9003. https://doi.org/10.3390/app13159003

[46] G. Y. Shien, K. Shanmugam and M. E. Rana, "Automated Face Mask Detection using Artificial Intelligence and Video Surveillance Management," 2023 15th International Conference on Developments in eSystems Engineering (DeSE), Baghdad & Anbar, Iraq, 2023, pp. 233-236, doi: 10.1109/DeSE58274.2023.10099878.

[47] S. Thiprak and W. Kurutach, "Ubiquitous computing technologies and Context Aware Recommender Systems for Ubiquitous Learning," 2015 12th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), Hua Hin, Thailand, 2015, pp. 1-6, doi: 10.1109/ECTICon.2015.7206939.

[48] Shen, Chien-wen; Wu, Yen-Chun Jim; Lee, Tsung-che (2014). Developing a NFC-equipped smart classroom: Effects on attitudes toward computer science. Computers in Human Behavior, 30(), 731–738. doi:10.1016/j.chb.2013.09.002

[49] Huang, L.-S., Su, J.-Y., & Pao, T.-L. (2019). A Context Aware Smart Classroom Architecture for Smart Campuses. Applied Sciences, 9(9), 1837. doi:10.3390/app9091837

[50] X. Hu, J. Su, Y. Dai, J. Xiong, X. Yu and M. Zhang, "Research on the Application of Internet of Things and Artificial Intelligence Technology in Smart Classroom," 2022 International Conference on Applied Physics and Computing (ICAPC), Ottawa, ON, Canada, 2022, pp. 418-425, doi: 10.1109/ICAPC57304.2022.00088.

[51] C. -U. Lei, H. -N. Liang and K. L. Man, "Building a smart laboratory environment at a university via a cyber-physical system," Proceedings of 2013 IEEE

International Conference on Teaching, Assessment and Learning for Engineering (TALE), Bali, Indonesia, 2013, pp. 243-247, doi: 10.1109/TALE.2013.6654439.

[52] J. Yu, "Construction of Smart Library Based on the Big Data Mining and Knowledge Discovery," 2021 Smart City Challenges & Outcomes for Urban Transformation (SCOUT), Bhubaneswar, India, 2021, pp. 57-61, doi: 10.1109/SCOUT54618.2021.00023.

[53] A. Ozeer, Y. Sungkur and S. D. Nagowah, "Turning a Traditional Library into a Smart Library," 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), Dubai, United Arab Emirates, 2019, pp. 352-358, doi: 10.1109/ICCIKE47802.2019.9004242.

[54] S. D. Nagowah, H. Ben Sta and B. A. Gobin-Rahimbux, "An Ontology for an IoT-enabled Smart Library in a University Campus," 2021 IEEE 23rd Int Conf on High Performance Computing & Communications; 7th Int Conf on Data Science & Systems; 19th Int Conf on Smart City; 7th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys), Haikou, Hainan, China, 2021, pp. 1952-1957, doi: 10.1109/HPCC-DSS-SmartCity-DependSys53884.2021.00292.

[55] F. N. Purba and A. A. Arman, "A Systematic Literature Review of Smart Governance," 2022 International Conference on Information Technology Systems and Innovation (ICITSI), Bandung, Indonesia, 2022, pp. 70-75, doi: 10.1109/ICITSI56531.2022.9970796.

[56] Zhan, X., Lu, jiang, & Yuan, huabing. (2019). Research on the Application of Decision Support System on Smart Campus. 2019 International Conference on Computer Network, Electronic and Automation (ICCNEA). doi:10.1109/iccnea.2019.00091 10.1109/ICCNEA.2019.00091

[57] F. Wu, Q. Zheng, F. Tian, Z. Suo, Y. Zhou, K.-M. Chao, M. Xu, N. Shah, J. Liu, and F. Li, ‘‘Supporting poverty-stricken college students in smart campus,’’ Future Gener. Comput. Syst., vol. 111, pp. 599–616, Oct. 2020, doi: 10.1016/j.future.2019.09.017.

[58] V. Opranescu, I. Nedelcu and A. D. Ionita, "Automating Students’ Decision Processes in a Smart Campus," 2023 13th International Symposium on Advanced Topics in Electrical Engineering (ATEE), Bucharest, Romania, 2023, pp. 1-6, doi: 10.1109/ATEE58038.2023.10108094.

[59] Zhangbin Chen and Yang Liu. 2022. Research and Construction of University Data Governance Platform Based on Smart Campus Environment. In 2021 3rd International Conference on Artificial Intelligence and Advanced Manufacture (AIAM2021). Association for Computing Machinery, New York, NY, USA, 450–455. https://doi.org/10.1145/3495018.3495097

[60] P. Fraga-Lamas, M. Celaya-Echarri, P. Lopez-Iturri, L. Castedo, . Azpilicueta, E. Aguirre, M. Suárez-Albela, F. Falcone, and T. M. Fernández-Caramés, ‘‘Design and experimental validation of a LoRaWAN fog computing based architecture for IoT enabled smart campus applications,’’ Sensors, vol. 19, no. 15, p. 3287, Jul. 2019, doi: 10.3390/s19153287.

[61] S. -M. Zhang and X. Li, "Mobility patterns of human population among university campuses," 2016 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), Jeju, Korea (South), 2016, pp. 50-53, doi: 10.1109/APCCAS.2016.7803893.

[62] https://opendatahandbook.org/guide/el/why-open-data/

[63] Vasileva, R.; Rodrigues, L.; Hughes, N.; Greenhalgh, C.; Goulden, M.; Tennison, J. What Smart Campuses Can Teach Us about Smart Cities: User Experiences and Open Data. Information 2018, 9, 251. https://doi.org/10.3390/info9100251

[64] N. Verstaevel, J. Boes and M. -P. Gleizes, "From smart campus to smart cities issues of the smart revolution," 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), San Francisco, CA, USA, 2017, pp. 1-6, doi: 10.1109/UIC-ATC.2017.8397400.

[65] Prandi C, Monti L, Ceccarini C, Salomoni P (2020) Smart campus: Fostering the community awareness through an intelligent environment. Mob Netw Appl 25(3):945–952. https://doi.org/10.1007/s11036-019-01238-2

[66] Tarabieh KA, Elnabarawy IO, Mashaly IA, Rashed YM (2015) The power of data visualization: A prototype energy performance map for a university campus. In: Sustainable Human–Building Ecosystems, pp 194–203. https://ascelibrary.org/doi/abs/10.1061/9780784479681.021

[67] Ramachandran GS, Bogosian B, Vasudeva K, Sriramaraju SI, Patel J, Amidwar S, Malladi L, Shylaja RD, Kumar NRB, Krishnamachari B (2019) An immersive visualization of micro-climatic data using usc air (demo). In: Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services, MobiSys ’19, pp 675–676. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3307334.3328577

[68] Tomás Langebaek Carrizosa. 2022. Open IoT data platform for Uniandes campus. In Proceedings of SELF (Software Evolution Lab.). ACM, New York, NY, USA, 16 pages.

[69] A. Lizzio and K. Wilson. Student Participation in University Governance: The Role Conceptions and Sense of Efficacy of Student Representatives. Departmental Comités. Studies in Higher Education, 34(1), 69-84, 2009. DOI: https://doi.org/10.1080/03075070802602000

[70] J. Steffek and P. Nanz, Emergent Patterns of Civil Society Participation in Global and European Governance. In: Civil Society Participation in European and Global Governance. ¿A Cure for the Democratic Deficit?, Steffek, J., Kissling, C. and Nanz, P. (Eds) Palgrave Eds. 2008.

[71] J.P. Gibson, R. Krimmer, V. Teague and J. Pomares, A review of evoting: the past, present and future. ANN TELECOMMUN, 71(7-8), 279-286. 2016.DOI: DOI 10.1007/s12243-016-0525-8

[72] V. Peñafiel and J. M. Lavín, "Improving University Decision Making Through E-Participation," 2018 International Conference on eDemocracy & eGovernment (ICEDEG), Ambato, Ecuador, 2018, pp. 392-396, doi: 10.1109/ICEDEG.2018.8372371.

[73] P. M. Bhamare, P. P. Kulkarni, A. Mhetre, K. Shipra, S. Wani and V. Pai, "Revolutionizing College Elections with a Secure Blockchain Voting Solution," 2023 IEEE 5th International Conference on Cybernetics, Cognition and Machine Learning Applications (ICCCMLA), Hamburg, Germany, 2023, pp. 121-125, doi: 10.1109/ICCCMLA58983.2023.10346825.

[74] Razi, Qaiser & Devrani, Aryan & Abhyankar, Harshal & Chalapathi, GSS & Hassija, Vikas & Guizani, Mohsen. (2023). Non-Fungible Tokens (NFTs)-Survey of Current Applications, Evolution and Future Directions. IEEE Open Journal of the Communications Society. PP. 1-1. 10.1109/OJCOMS.2023.3343926.

[75] V. S. Sisodiya and H. Garg, "A Comprehensive study of Blockchain and its various Applications," 2020 International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC), Mathura, India, 2020, pp. 475-480, doi: 10.1109/PARC49193.2020.236659.

[76] Saad, A. & Roseli, Mohd & Zullkeply, Muhammad. (2014). A smart e-voting system using RFID authentication method for a campus electoral. Proceedings of the 8th International Conference on Ubiquitous Information Management and Communication, ICUIMC 2014. 10.1145/2557977.2557985.

[77] G. Rathee, R. Iqbal, O. Waqar and A. K. Bashir, "On the Design and Implementation of a Blockchain Enabled E-Voting Application Within IoT-Oriented Smart Cities," in IEEE Access, vol. 9, pp. 34165-34176, 2021, doi: 10.1109/ACCESS.2021.3061411.

[**78]** Singh, A.; Ganesh, A.; Patil, R.R.; Kumar, S.; Rani, R.; Pippal, S.K. Secure Voting Website Using Ethereum and Smart Contracts. Appl. Syst. Innov. 2023, 6, 70. https://doi.org/10.3390/asi6040070

[79] Wilkinson, M. D. et al. The FAIR Guiding Principles for scientific data management and stewardship. Sci. Data 3:160018 doi: 10.1038/sdata.2016.18 (2016).

[80] A. Sheth, «Transforming Big Data into Smart Data: Deriving value via harnessing Volume, Variety, and Velocity using semantic techniques and

technologies - IEEE Conference Publication», IEEE 30th International Conference on Data Engineering, 2014, pp. 2-2.

[81] A. Sheth, «Smart data - How you and I will exploit Big Data for personalized digital health and many other activities», en 2014 IEEE International Conference on Big Data (Big Data), 2014, pp. 2-3

[82] F. Ye, Y. Sun, and A. Rettig, ‘‘Authentication and access control for an IoT green roof monitoring system,’’ in Proc. IEEE 15th Int. Conf. Dependable, Autonomic Secure Comput., 15th Int. Conf. Pervas. Intell. Comput., 3rd Int. Conf. Big Data Intell. Comput. Cyber Sci. Technol. Congr. (DASC/PiCom/DataCom/CyberSciTech), Nov. 2017, pp. 251–256, doi: 10.1109/DASC-PICom-DataCom-CyberSciTec.2017.53.

[83] N. Yousefnezhad, M. Madhikermi, and K. Främling, ‘‘MeDI: Measurement-based device identification framework for Internet of Things,’’ in Proc. IEEE 16th Int. Conf. Ind. Informat. (INDIN), Jul. 2018, pp. 95–100, doi: 10.1109/INDIN.2018.8472080.

[84] L. Zheng, C. Song, N. Cao, Z. Li, W. Zhou, J. Chen, and L. Meng, ‘‘A new mutual authentication protocol in mobile RFID for smart campus,’’ IEEE Access, vol. 6, pp. 60996–61005, 2018, doi: 10.1109/ACCESS.2018.2875973.

[85] Li, S., Xu, L.D. & Zhao, S. The internet of things: a survey. Inf Syst Front 17, 243–259 (2015). https://doi.org/10.1007/s10796-014-9492-7

[86] R. Schamberger, G. Madlmayr and T. Grechenig, "Components for an interoperable NFC mobile payment ecosystem," 2013 5th International Workshop on Near Field Communication (NFC), Zurich, Switzerland, 2013, pp. 1-5, doi: 10.1109/NFC.2013.6482440.

[87] S. J. Danbatta and A. Varol, "Comparison of Zigbee, Z-Wave, Wi-Fi, and Bluetooth Wireless Technologies Used in Home Automation," 2019 7th International Symposium on Digital Forensics and Security (ISDFS), Barcelos, Portugal, 2019, pp. 1-5, doi: 10.1109/ISDFS.2019.8757472.

[88] R. Want, "An introduction to RFID technology," in IEEE Pervasive Computing, vol. 5, no. 1, pp. 25-33, Jan.-March 2006, doi: 10.1109/MPRV.2006.2.

[89] Y. Li, "Research on Building Smart Campus Based on Cloud Computing Technology," 2020 5th International Conference on Mechanical, Control and Computer Engineering (ICMCCE), Harbin, China, 2020, pp. 723-726, doi: 10.1109/ICMCCE51767.2020.00159.

[90] G. Lin et al., "Research on IoT Perception Technology of Renewable Energy Based on Edge Computing," 2022 IEEE 10th International Conference on Information, Communication and Networks (ICICN), Zhangye, China, 2022, pp. 36-40, doi: 10.1109/ICICN56848.2022.10006574.

[91] M. Al-Mekhlal and A. Ali Khwaja, "A Synthesis of Big Data Definition and Characteristics," 2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), New York, NY, USA, 2019, pp. 314-322, doi: 10.1109/CSE/EUC.2019.00067.

[92] D. Navani, S. Jain and M. S. Nehra, "The Internet of Things (IoT): A Study of Architectural Elements," 2017 13th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS), Jaipur, India, 2017, pp. 473-478, doi: 10.1109/SITIS.2017.83.

[93] S. Vashi, J. Ram, J. Modi, S. Verma and C. Prakash, "Internet of Things (IoT): A vision, architectural elements, and security issues," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2017, pp. 492-496, doi: 10.1109/I-SMAC.2017.8058399.

[94] A. Zhamanov, Z. Sakhiyeva, R. Suliyev and Z. Kaldykulova, "IoT smart campus review and implementation of IoT applications into education process of university," 2017 13th International Conference on Electronics, Computer and Computation (ICECCO), Abuja, Nigeria, 2017, pp. 1-4, doi: 10.1109/ICECCO.2017.8333334.

[95] Abuarqoub, A., Abusaimeh, H., Hammoudeh, M., Uliyan, D., Abu-Hashem, M. A., Murad, S.,& Al-Fayez, F. (2017, July). A survey on internet of things enabled smart campus applications. In Proceedings of the International Conference on Future Networks and Distributed Systems (pp. 1-7).

[96] Dangi R, Lalwani P, Choudhary G, You I, Pau G. Study and Investigation on 5G Technology: A Systematic Review. Sensors. 2022; 22(1):26. https://doi.org/10.3390/s22010026

[97] W. Roh et al., ‘‘Millimeter-wave beamforming as an enabling technology for 5G cellular communications: Theoretical feasibility and prototype results,’’ IEEE Commun. Mag., vol. 52, no. 2, pp. 106–113, Feb. 2014.

[98] Shweta Rajoria, Aditya Trivedi, W. Wilfred Godfrey,A comprehensive survey: Small cell meets massive MIMO,Physical Communication, Volume 26, 2018, Pages 40-49,ISSN 1874-4907,https://doi.org/10.1016/j.phycom.2017.11.004.

[99] W. Hong, K.-H. Baek, Y. Lee, Y. Kim, and S.-T. Ko, ‘‘Study and prototyping of practically large-scale mmWave antenna systems for 5G cellular devices,’’ IEEE Commun. Mag., vol. 52, no. 9, pp. 63–69, Sep. 2014.

[100] M. A. Wassay, K. Verma and S. Singla, "An Efficient IoT e-Environment System to Monitor and Control Pollution and Maintain Hygienics in Educational Institutions," 2022 International Conference on Computational Modelling, Simulation and Optimization (ICCMSO), Pathum Thani, Thailand, 2022, pp. 291-295, doi: 10.1109/ICCMSO58359.2022.00064.

[101] Vladimir Tanasiev, George Cristian Pătru, Daniel Rosner, Gabriela Sava, Horia Necula, Adrian Badea, Enhancing environmental and energy monitoring of residential buildings through IoT, Automation in Construction, Volume 126, 2021, 103662,ISSN 0926-5805, https://doi.org/10.1016/j.autcon.2021.103662.

[102] M. Agiwal, A. Roy and N. Saxena, "Next Generation 5G Wireless Networks: A Comprehensive Survey," in IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 1617-1655, thirdquarter 2016, doi: 10.1109/COMST.2016.2532458.

[103] Xiang, Haiyun. "Research on the application of 5G in smart campuses of universities." Scientific Journal of Economics and Management Research 3.6 (2021).

[104] D. M. K. Finkenzeller, RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication, 3rd ed. Chichester, U.K.: Wiley, Aug. 2010.

[105] https://edscoop.com/5g-making-the-connection-for-greater-student-and-faculty-success/

[106] C. Gong, J. Liu, Q. Zhang, H. Chen and Z. Gong, "The Characteristics of Cloud Computing," 2010 39th International Conference on Parallel Processing Workshops, San Diego, CA, USA, 2010, pp. 275-279, doi: 10.1109/ICPPW.2010.45.

[107] Chao Huang, On Study of Building Smart Campus under Conditions of Cloud Computing and Internet of Things, 2017 IOP Conf. Ser.: Earth Environ. Sci. 100 012118, DOI 10.1088/1755-1315/100/1/012118

[**108]** Khanzode, Ku Chhaya A., and Ravindra D. Sarode. "Advantages and disadvantages of artificial intelligence and machine learning: A literature review." International Journal of Library & Information Science (IJLIS) 9.1 (2020): 3.

[109] Ι. Βλαχάβας, Π. Κεφαλάς, Ν. Βασιλειάδης, Φ. Κόκκορας, Η. Σακελλαρίου, Τεχνητή Νοημοσύνη - Β' Έκδοση, Εκδόσεις Πανεπιστημίου Μακεδονίας

[110] T. Sutjarittham, H.H. Gharakheili, S.S. Kanhere and V. Sivaraman, ―Experiences with IoT and AI in a smart campus for optimizing classroom usage‖, IEEE Internet of Things Journal Vol.6, No.5, PP.7595–7607, 2019

[**111]** Althobaiti, Maha M. "Toward a smart campus based on smart technologies and best practices." International Journal of Advanced Research in Engineering and Technology (IJARET) 11.10: 1385-1394.

[112] Williams, R., McMahon, E., Samtani, S., Patton, M., Chen, H., 2017. Identifying vulnerabilities of consumer Internet of Things (IoT) devices: A scalable approach, in: 2017 IEEE International Conference on Intelligence and Security Informatics (ISI). Presented at the 2017 IEEE International Conference on Intelligence and Security Informatics (ISI), pp. 179–181. https://doi.org/10.1109/ISI.2017.8004904

[113] Ikrissi, G. and Tomader Mazri. “A STUDY OF SMART CAMPUS ENVIRONMENT AND ITS SECURITY ATTACKS.” The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences (2020), DOI:10.5194/isprs-archives-xliv-4-w3-2020-255-2020

[114] Andrea, I., Chrysostomou, C., Hadjichristofi, G., 2015. Internet of Things: Security vulnerabilities and challenges. pp. 180–187. https://doi.org/10.1109/ISCC.2015.7405513

[115] Anwaar AlDairi, Lo’ai Tawalbeh, Cyber Security Attacks on Smart Cities and Associated Mobile Technologies, Procedia Computer Science, Volume 109, 2017, Pages 1086-1091, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2017.05.391.

[116] Deogirikar, J., Vidhate, A., 2017. Security attacks in IoT: A survey, in: 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC). Presented at the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), pp. 32–37., https://doi.org/10.1109/I-SMAC.2017.8058363

[117] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, "Social phishing." Communications of the ACM 50, no. 10 (2007): 94-100.

[118] Rehman, S., Manickam, S., 2016. A Study of Smart Home Environment and it’s Security Threats. International Journal of Reliability, Quality and Safety Engineering 23. https://doi.org/10.1142/S0218539316400052

[119] Hezam, A., Konstantas, D., Mahyoub, M., 2018. A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Mode. International Journal of Advanced Computer Science and Applications Vol. 9, https://doi.org/10.14569/IJACSA.2018.090349

[120] Abomhara, M., Ien, G.M.K., 2015. Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. Journal of Cyber Security and Mobility 4, 65–88, https://doi.org/10.13052/jcsm2245-1439.414

[121] Farahat, I.S., Tolba, A.S., Elhoseny, M., Eladrosy, W., 2019. Data Security and Challenges in Smart Cities, in: Hassanien, A.E., Elhoseny, M., Ahmed, S.H., Singh, A.K. (Eds.), Security in Smart Cities: Models, Applications, and Challenges, Lecture Notes in Intelligent Transportation and Infrastructure. Springer International Publishing, Cham, pp. 117–142. https://doi.org/10.1007/978-3-030-01560-2_6

[122] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, Adopted on 2 April 2013, p. 45.

[123] Ο ΓΚΠΔ διαθέσιμος σε: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679.

[124] βλ. ενδεικτικά ορισμένους σκοπούς και νομικές βάσεις ορισμένων Ελληνικών Πανεπιστημίων οι οποίες ομοιάζουν και στο πλαίσιο της έξυπνης πανεπιστημιούπολης https://www.uom.gr/terms,

https://duth.gr/Portals/0/Enhmerosi%20kanonismos.pdf,
https://www.uoc.gr/files/items/7/7133/guidance_for_compliance_with_gdpr.pdf

[125] Γνώμη 2/2002 σχετικά με τη χρήση μοναδικών αναγνωριστικών σε τηλεπικοινωνιακό τερματικό εξοπλισμό: το παράδειγμα των IPv6 της Ομάδας εργασίας του άρθρου 29 για την προστασία των δεδομένων: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp58_en.pdf

[126] https://www.dpa.gr/el/enimerwtiko/nomothesia/proswpika/sxetikieu

[127] Εγχειρίδιο της European Union Agency for Fundamental Rights σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων - Έκδοση 2018, διαθέσιμο στην ιστοσελίδα: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_el.pdf

[128] Γνώμη 3/2010 σχετικά με την αρχή της λογοδοσίας της Ομάδας εργασίας του άρθρου 29 για την προστασία των δεδομένων: https://ec.europa.eu/justice/article-29/documentation/opinion recommendation/files/2010/wp173_el.pdf

[129] Κατευθυντήριες γραμμές για την αυτοματοποιημένη λήψη αποφάσεων και την κατάρτιση προφίλ για τους σκοπούς του κανονισμού 2016/679: https://www.dpa.gr/sites/default/files/2020-05/wp251rev01_el.pdf

[130] Φερενίκη Παναγοπούλου -Κουτνατζή, Διαδίκτυο των Πραγμάτων (Internet of Things – IoT): Αποικισμός της καθημερινής ζωής ή νέα τεχνολογική πρόκληση, δημοσιευμένο στο τεύχος Δίκαιο και Καινοτομία Innovation Law από το 5ο Πανελλήνιο Συνέδριο e-ΘΕΜΙΣ, ΝΟΜΙΚΗ ΒΙΒΛΙΟΘΗΚΗ, σελ. 147-174

[131] Γνώμη 3/2011 σχετικά με τις υπηρεσίες εντοπισμού γεωγραφικής θέσης που παρέχονται μέσω έξυπνων κινητών συσκευών της Ομάδας Εργασίας άρθρου 29 για την προστασία των δεδομένων: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp185_el.pdf

[132] Bannon, A. (2008). RFID: Radio Frequency Identification OR Real Frailty in Data Protection?', The Journal of Information, Law and Technology (JILT), available at: http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2008_1/bannon

[133] Γνώμη 5/2010 και Αναθεωρημένη αυτής 9/2011 της Ομάδας Εργασίας άρθρου 29 σχετικά με την πρόταση του κλάδου για ένα πλαίσιο εκπόνησης εκτιμήσεων των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων για τις εφαρμογές RFID: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp175_el.pdf, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp180_el.pdf

[134] Γνώμη 8/2014 σχετικά με τις πρόσφατες εξελίξεις στο Διαδίκτυο των Πραγμάτων της Ομάδας Εργασίας άρθρου 29 για την προστασία των δεδομένων:

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_el.pdf

[135] Οδηγία 1/2011 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) περί της χρήσης συστημάτων βιντεοεπιτήρησης για την προστασία προσώπων και αγαθών: https://www.dpa.gr/sites/default/files/2020-01/ODIGIA_CCTV_FINAL_1_2011.PDF

[136] Μαγδαληνή Σκόνδρα, Συστήματα Βιντεοεπιτήρησης, αναγνώριση προσώπου και προστασία προσωπικών δεδομένων, ΤΝΠ QUALEX, ΔiΜΕΕ, 1/2020, σελ. 45 – 56

[137] Κατευθυντήριες γραμμές υπ' αριθμ. 3/2019 του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω βιντεοσυσκευών:https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_el.pdf

[138] Κατευθυντήριες γραμμές υπ' αριθμ. 04/2020 του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων σχετικά με τη χρήση δεδομένων θέσης και εργαλείων ιχνηλάτησης επαφών στο πλαίσιο της έξαρσης της νόσου COVID-19 : https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_el_0.pdf

[139] Jansen W./Grance T., Guidelines on Security and Privacy in Public Cloud Computing, NIST Special Publication 800-144, 2011.

[140] Αφροδίτη Κουσουνή-Πανταζοπούλου, Νομικές διαστάσεις του Cloud computing, ΤΝΠ QUALEX, ΔiΜΕΕ, 2/2012, σελ. 177 – 185

[141] Γνώμη 05/2012 σχετικά με τη νεφοϋπολογιστική της Ομάδας Εργασίας του άρθρου 29 για την Προστασία των Δεδομένων, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_el.pdf

[142]https://www.europarl.europa.eu/news/el/headlines/society/20230601STO93804/praxi-technitis-noimosunis-tis-ee-protos-kanonismos-gia-tin-techniti-noimosuni, https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai

[143] https://data.europa.eu/en/publications/datastories/protecting-data-and-opening-data

[144] Analytical Report 3: Open Data and Privacy, Publications Office of the European Union, European Union, 2020, OA-BF-20-003-EN-N ISBN: 978-92-78-41895-3 ISSN: 2600-0601 doi: 10.2830/532195

[145]https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/asfaleia/asfaleiaepexergasias/tekmiriwsh_asfaleia_proswpikwn/metra_asgaleia_proswpikwn/texnika_metra

[**146]**https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/asfaleia/asfaleiaepexergasias/tekmiriwsh_asfaleia_proswpikwn/metra_asgaleia_proswpikwn/organotika_metra

[147] Κατευθυντήριες Γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων της Ομάδας Εργασίας του άρθρου 29 για τη προστασία των δεδομένων: https://ec.europa.eu/newsroom/article29/items/612048/en

[148] Γ.Γιαννόπουλος/Λ.Μήτρου/Γρ.Τσόλιας (ενότητα Υποχρεώσεις του υπευθύνου επεξεργασίας) σε σε Λ.Κοτσαλή, Κ.Μενουδάκο, Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (GDPR), Νομική Διάσταση και πρακτική εφαρμογή, 2018, ΝΟΜΙΚΗ ΒΙΒΛΙΟΘΗΚΗ

[149] Υπόδειγμα αντλημένο από την ιστοσελίδα της Ανεξάρτητης Αρχής ΠροστασίαςΠροσωπικώνΔεδομένων:https://www.dpa.gr/el/foreis/asfaleia_dedomenwn/gnwstopoiisi_paraviasis/upovoli_gnwstopoihshs_paraviashs

[150] Β. Ζορκάδης (ενότητα Εκτίμηση Αντικτύπου στην προστασία δεδομένων) σε Λ.Κοτσαλή, Κ.Μενουδάκο, Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (GDPR), Νομική Διάσταση και πρακτική εφαρμογή, 2018, ΝΟΜΙΚΗ ΒΙΒΛΙΟΘΗΚΗ

[151] https://www.iso.org/standard/86012.html

[152] https://skyrfid.com/RFID_Education.php]

[153] https://www.mouser.es/blog/zigbee-vs-z-wave-whats-the-difference

[154] Kumar, Vishal & Laghari, Asif & Karim, Shahid & Shaikh, Shakir & Brohi, Ali. (2019). Comparison of Fog Computing & Cloud Computing. International Journal of Mathematical Sciences and Computing. 5. 31-41. 10.5815/ijmsc.2019.01.03.