



ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«ΕΥΕΛΙΚΤΕΣ ΜΟΡΦΕΣ ΔΙΟΙΚΗΣΗΣ»

«ΜΕΤΑΒΙΒΑΣΗ ΕΜΠΙΣΤΟΣΥΝΗΣ ΣΕ ΦΟΡΗΤΕΣ ΕΦΑΡΜΟΓΕΣ
ΕΥΡΕΙΑΣ ΧΡΗΣΗΣ»

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
ΜΠΑΝΙΑ ΑΡΕΤΗ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΑΝΘΟΠΟΥΛΟΣ ΛΕΩΝΙΔΑΣ

ΛΑΡΙΣΑ, ΔΕΚΕΜΒΡΙΟΣ 2021

Υπεύθυνη δήλωση

«Δηλώνω υπεύθυνα ότι η συγκεκριμένη μεταπτυχιακή διπλωματική εργασία για τη λήψη του μεταπτυχιακού τίτλου σπουδών του ΠΜΣ Πλήρους Φοίτησης του Πανεπιστημίου Θεσσαλίας «Ευέλικτες Μέθοδοι Διοίκησης» έχει συγγραφεί από εμένα προσωπικά και δεν έχει υποβληθεί ούτε έχει εγκριθεί στο πλαίσιο κάποιου άλλου μεταπτυχιακού ή προπτυχιακού τίτλου σπουδών, στην Ελλάδα ή στο εξωτερικό. Η εργασία αυτή έχοντας εκπονηθεί από εμένα, αντιπροσωπεύει τις προσωπικές μου απόψεις επί του θέματος και το κείμενο είναι γραμμένο με τα δικά μου λόγια και δεν αποτελεί προϊόν λογοκλοπής από τρίτες πηγές. Οι πηγές στις οποίες ανέτρεξα για την εκπόνηση της συγκεκριμένης διπλωματικής αναφέρονται στο σύνολό τους, δίνοντας πλήρεις αναφορές στους συγγραφείς, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο».

Η Δηλούσα

Μπανιά Αρετή

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα Καθηγητή μου κ. Ανθόπουλο Λεωνίδα για την πολύτιμη καθοδήγησή και στήριξή του στην περάτωση της διπλωματικής μου εργασίας, καθώς και όλους τους καθηγητές του μεταπτυχιακού «Ευέλικτες Μορφές Διοίκησης» του Πανεπιστημίου Θεσσαλίας για τις γνώσεις που απρόσκοπτα μας μετέδωσαν.

Στο πατέρα μου που έφυγε νωρίς...

Περίληψη

Τα τελευταία χρόνια, όλο και περισσότερες κυβερνήσεις παγκοσμίως ενσωματώνουν νέες τεχνολογίες στις ψηφιακές κυβερνητικές στρατηγικές τους για τον εκσυγχρονισμό της δημόσιας διοίκησης και τη βελτίωση των δημοσίων υπηρεσιών. Τα Κράτη, πλέον, εστιάζουν στην ανάπτυξη αντίστοιχων ψηφιακών χαρτοφυλακίων, ως συμπληρωματικό κανάλι παροχής των προσφερόμενων υπηρεσιών τους στον πολίτη. Σε αυτό το πλαίσιο, οι φορητές εφαρμογές αποτελούν μια ευέλικτη υπηρεσία στα πλαίσια της δημόσιας διοίκησης και διακυβέρνησης, καθώς προσφέρουν έναν αποτελεσματικό τρόπο ανταλλαγής πληροφοριών σε πραγματικό χρόνο και σε ένα ευρύ φάσμα χρηστών, μειώνοντας το λειτουργικό κόστος και βελτιώνοντας, παράλληλα, τις συναλλαγές των πολιτών με το κράτος.

Ωστόσο, λόγω της σχετικής τους καινοτομίας, δεν έχει καταστεί ακόμα σαφές ο τρόπος με τον οποίο μπορεί να μεταβιβαστεί η εμπιστοσύνη από τους πολίτες προς τις κρατικές εφαρμογές και ποιοι είναι εκείνοι οι παράγοντες που ενισχύουν την εμπιστοσύνη των πολιτών στη αποδοχή και χρήση αυτών των εφαρμογών. Μάλιστα, σε μια περίοδο όπου οι τεχνολογίες αυτές γίνονται ολοένα και περισσότερο πολύπλοκες, εγείρονται ανησυχίες σχετικά με την ασφάλεια χρήσης των εφαρμογών, την προστασία των προσωπικών δεδομένων, τη συλλογή και επεξεργασία των δεδομένων και την κοινωνική επιτήρηση των πολιτών από το Κράτος.

Στόχος, συνεπώς της παρούσας εργασίας είναι να εστιάσει στο θέμα της μεταβίβασης της εμπιστοσύνης από τους χρήστες σε φορητές εφαρμογές που έχουν δημιουργηθεί στα πλαίσια της δημόσιας διοίκησης και διακυβέρνησης. Ειδικότερα, θα επιχειρηθεί να αναδειχθεί ο ρόλος που η μεταβίβαση εμπιστοσύνης αποκτά σε σχέση με τους παράγοντες που ενισχύουν ή αποθαρρύνουν τους πολίτες να κάνουν χρήση αυτών των εφαρμογών, όπως η εμπιστοσύνη στο Κράτος, στα δεδομένα, στις συναλλαγές, στους θεσμούς, κ.α.. Με την ολοκλήρωση της εργασίας εκτιμάται ότι θα αποσαφηνιστούν οι τρόποι με τους οποίους το κράτος μπορεί να ενισχύσει την πρόθεση των πολιτών να χρησιμοποιήσουν τις κρατικές φορητές εφαρμογές.

Λέξεις-κλειδιά: Εμπιστοσύνη, Μεταβίβαση εμπιστοσύνης, Φορητές εφαρμογές, Ψηφιακή Διακυβέρνηση, COVID-19.

Abstract

In recent years, governments around the world are incorporating new technologies into their digital government strategies to improve public administration and its services. States focus now on developing respective digital portfolios, as a complementary distribution channel for their services to the citizen. In this context, mobile's applications are a viable option for public administration and governance, as they offer an effective way to exchange information in real time and to a wide range of users, reducing operating costs while improving citizens' transactions with the state.

However, due to their relative innovation, it is not clear yet how trust can be transferred to citizens and what are the factors that enhance citizens' trust in the acceptance and use of these applications. In fact, since these technologies are becoming increasingly sophisticated, concerns are raised about applications' security, citizens' privacy, protection of personal data, data collection and social surveillance of citizens by the State.

To that end, the aim of this study is to focus on the transfer of trust from users to mobile applications created within the public administration. In particular, it will be attempted to highlight the role that the transfer of trust acquires in relation to the factors that enhance or discourage citizens to make use of these applications, such as trust in the State, trust in data, trust in transactions, trust in institutions, etc. With the completion of this study, it is estimated that the ways in which the State can enhance citizens in their intention to use state-owned mobile applications will be clarified.

Key words: Trust, Trust Transfer, Mobile Applications, Digital Governance, COVID-19.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Υπεύθυνη δήλωση	2
Ευχαριστίες	3
Περίληψη	4
Abstract	5
ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ	6
Κατάλογος Πινάκων	9
Κατάλογος Εικόνων	10
ΚΕΦΑΛΑΙΟ 1: Εισαγωγή	11
1.1. Σημασία και σκοπός του υπό διερεύνηση θέματος	11
1.2. Θεωρητικό υπόβαθρο	13
1.3. Μεθοδολογία της έρευνας	16
1.4. Δομή εργασίας	17
ΚΕΦΑΛΑΙΟ 2: Βιβλιογραφική Επισκόπηση	19
2.1. Η έννοια της εμπιστοσύνης	19
2.1.1. Ορισμός της εμπιστοσύνης	19
2.1.2. Τα μοντέλα σχηματισμού εμπιστοσύνης	23
2.1.3. Η μεταβίβαση εμπιστοσύνης	27
2.2. Η χρήση φορητών εφαρμογών στη δημόσια διοίκηση	31
2.2.1. Η εμπιστοσύνη στη δημόσια διοίκηση και διακυβέρνηση	31
2.2.2. Οι φορητές εφαρμογές (Apps)	35
2.2.3. Η εμπιστοσύνη στις φορητές εφαρμογές	39
2.2.4. Η μεταβίβαση εμπιστοσύνης στη χρήση φορητών εφαρμογών	45
2.3. Προκλήσεις στη χρήση φορητών εφαρμογών	46
2.3.1. Κίνδυνοι ασφάλειας και απορρήτου	47
2.3.2. Έλεγχος και επιτήρηση των πολιτών	50

ΚΕΦΑΛΑΙΟ 3: Έρευνα πεδίου	55
3.1. Σκοπός και ερευνητικοί στόχοι της έρευνας	55
3.2. Μεθοδολογία	55
3.2.1. Συστηματική ανασκόπηση της βιβλιογραφίας	56
3.2.2. Χρήση Ερωτηματολογίου	58
3.3. Ερευνητικά ερωτήματα	60
3.4. Ερευνητικό μοντέλο	61
3.5. Ερευνητικές υποθέσεις	62
3.6. Το ερωτηματολόγιο της έρευνας	62
ΚΕΦΑΛΑΙΟ 4: Αποτελέσματα έρευνας	66
4.1. Η στατιστική ανάλυση	66
4.2. Έλεγχος αξιοπιστίας - Cronbach 's a	66
4.3. Περιγραφική στατιστική	68
4.3.1. Το προφίλ των συμμετεχόντων	68
4.3.2. Ποσοστά απαντήσεων ανά ενότητα	70
4.3.3. Αποτελέσματα περιγραφικής στατιστικής ανά ενότητα	71
4.4. Επαγωγική στατιστική	72
4.4.1. Παραγοντική ανάλυση – Factor Analysis	72
4.4.2. Ανάλυση Διαδρομών (Path Analysis) - Παλινδρόμηση (Regression)	78
4.5. Απαντήσεις στα ερευνητικά ερωτήματα	80
ΚΕΦΑΛΑΙΟ 5: Επίλογος	84
5.1. Σύγκριση ευρημάτων	84
5.2. Αποτελέσματα - Συμπεράσματα	86
5.3. Περιορισμοί της έρευνας	89
5.4. Μελλοντική έρευνα	90
ΒΙΒΛΙΟΓΡΑΦΙΑ	92

ΠΑΡΑΡΤΗΜΑ	99
I. Το ερωτηματολόγιο της έρευνας – Google Forms	99
II. Correlation Matrix	106

Κατάλογος Πινάκων

Πίνακας 1: Ορισμοί της εμπιστοσύνης.....	20
Πίνακας 2: Σχέσεις εμπιστοσύνης στην κοινωνία.....	22
Πίνακας 3: Το θεωρητικό πλαίσιο της μεταβίβασης εμπιστοσύνης	30
Πίνακας 4: Έλλειψη εμπιστοσύνης στους θεσμούς	32
Πίνακας 5: Κυβερνητικές εφαρμογές για την καταπολέμηση του COVID-19.....	37
Πίνακας 6: Η εμπιστοσύνη στις φορητές εφαρμογές.....	40
Πίνακας 7: Διατύπωση ερευνητικού ερωτήματος - SPIDER.....	57
Πίνακας 8: Εναλλακτικά σενάρια δείγματος έρευνας.....	60
Πίνακας 9: Το ερωτηματολόγιο της έρευνας	63
Πίνακας 10: Μέγεθος δείγματος, επίπεδο εμπιστοσύνης, περιθώρια σφάλματος	66
Πίνακας 11: Εσωτερική συνέπεια - Cronbach's Alpha	67
Πίνακας 12: Συνολικά στατιστικά.....	67
Πίνακας 13: Το προφίλ των συμμετεχόντων	69
Πίνακας 14: Ποσοστά απαντήσεων ανά ενότητα.....	70
Πίνακας 15: Αποτελέσματα περιγραφικής στατιστικής.....	71
Πίνακας 16: KMO and Bartlett's Test	73
Πίνακας 17: Communalities	74
Πίνακας 18: Total Variance Explained	75
Πίνακας 19: Component Matrix	76
Πίνακας 20: Rotated Component Matrix ^a	77
Πίνακας 21: Πρώτο επίπεδο Παλινδρόμησης -Model Summary	78
Πίνακας 22: Πρώτο επίπεδο Παλινδρόμησης - Coefficients	79
Πίνακας 23: Δεύτερο επίπεδο παλινδρόμησης - Model Summary	80
Πίνακας 24: Δεύτερο επίπεδο παλινδρόμησης- Coefficients.....	80

Κατάλογος Εικόνων

Εικόνα 1: Το μοντέλο αποδοχής τεχνολογίας -TAM (Davis et al., 1989)	23
Εικόνα 2: Μοντέλο αρχικού σχηματισμού εμπιστοσύνης (McKnight et al. 1998).....	24
Εικόνα 3: Το διαδικτυακό μοντέλο σχηματισμού εμπιστοσύνης (McKnight et al. 2002a).....	26
Εικόνα 4: Διαδικασία μεταφοράς εμπιστοσύνης (Lee et al., 2007)	29
Εικόνα 5: Εμπιστοσύνη πολιτών στη διαχείριση του COVID-19 από την Ε.Ε.	33
Εικόνα 6: Ερευνητικό πρωτόκολλο διπλωματικής εργασίας	56
Εικόνα 7: Ερευνητικό μοντέλο	61
Εικόνα 8: Ρυθμίσεις παραμέτρων Παραγοντικής Ανάλυσης στο SPSS.....	72

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ

1.1. Σημασία και σκοπός του υπό διερεύνηση θέματος

Η ραγδαία αύξηση της χρήσης των έξυπνων κινητών τηλεφώνων (smartphones) διαμόρφωσε πλέον ένα νέο πλαίσιο επικοινωνίας και διεκπεραίωσης καθημερινών συναλλαγών, τόσο στο δημόσιο όσο και στον ιδιωτικό τομέα. Βασικό χαρακτηριστικό των έξυπνων συσκευών είναι ότι παρέχουν προεγκατεστημένες εφαρμογές (applications ή εν συντομία apps), όπως εφαρμογές αποστολής και λήψης μηνυμάτων ηλεκτρονικού ταχυδρομείου, αναπαραγωγής πολυμέσων, πρόβλεψης καιρού κ.α., ενώ δίνεται και η δυνατότητα στον χρήστη να επισκεφτεί ένα κατάστημα εφαρμογών (π.χ. Apple Store) και να επιλέξει κάποια εφαρμογή, δωρεάν ή επί πληρωμή, μέσα από μια πληθώρα εφαρμογών.

Το 2021, κατεγράφησαν 3,48 εκατομμύρια εφαρμογές για Android κινητά, καθιστώντας το Google Play το κατάστημα με το μεγαλύτερο αριθμό διαθέσιμων εφαρμογών, ακολουθούμενη από το Apple App Store με 2,22 εκατομμύρια διαθέσιμες εφαρμογές για iOS κινητά (Statista, 2021). Οι φορητές εφαρμογές ακολουθούν διαφορετικά επιχειρησιακά μοντέλα και ανήκουν είτε απ' ευθείας στον πάροχο ενός ψηφιακού προϊόντος/υπηρεσίας, είτε σε κάτοχο πλατφόρμας που μεσολαβεί μεταξύ του χρήστη και του παρόχου του προϊόντος/υπηρεσίας. Επιτρέπουν δε, σε μια επιχείρηση/οργανισμό να αλληλεπιδρά σε πραγματικό χρόνο με τους αποδέκτες της αξίας της, συλλέγοντας δεδομένα που αξιοποιούνται άμεσα από τη Διοίκηση μετριάζοντας τις δαπάνες της μετά πώλησης (after-sales) περιόδου (Nel & Boshoff, 2017).

Καθώς οι εφαρμογές αυτές προσφέρουν έναν αποτελεσματικό τρόπο ανταλλαγής πληροφοριών σε πραγματικό χρόνο και σε ένα ευρύ φάσμα χρηστών, τα τελευταία χρόνια παρατηρείται αυξανόμενη χρήση τους και από τον δημόσιο τομέα. Ιδιαίτερα, η ενσωμάτωσή τους στη δημόσια διοίκηση στοχεύει στην απλοποιημένη αλληλεπίδραση των πολιτών με τις δημόσιες υπηρεσίες, τη δήλωση προβλημάτων στις πόλεις (complaints registration πχ. FixMyStreet), τις δημόσιες διαβουλεύσεις, την πρόσβαση σε υπηρεσίες μεταφορών (πχ. στάθμευση, bike sharing κλπ.), τις ηλεκτρονικές πληρωμές, την έξυπνη χρήση ενέργειας, έως και πιο πρόσφατα στην ιχνηλάτηση του ιού COVID-19 (Nah et al., 2005).

Παράλληλα, οι έννοιες της ασφάλειας και της ιδιωτικότητας στις φορητές εφαρμογές αποκτούν ιδιαίτερη σημασία, λόγω και των δυνατοτήτων διαρκούς καταγραφής της συμπεριφοράς του χρήστη, αποτύπωσης της θέσης του, εκχώρησης προσωπικών δεδομένων, κ.α.. Ειδικότερα, στις περιπτώσεις των φορητών εφαρμογών πλατφόρμας

(platform based), οι χρήστες παραχωρούν εμπιστοσύνη στην πλατφόρμα να αλληλεπιδρά με τον πάροχο της εκάστοτε υπηρεσίας (πχ. με τον οδηγό Uber, με τον εστιατόρα κλπ.). Όμοια, στην περίπτωση των δημόσιων εφαρμογών, οι χρήστες παραχωρούν εμπιστοσύνη στις εφαρμογές να αλληλεπιδράσουν με τους δημόσιους οργανισμούς (πχ. στην άυλη συνταγογράφηση φαρμάκων, στην ταυτοποίηση μέσω TAXIS κλπ.). Η οικοδόμηση εμπιστοσύνης συνεπώς, μεταξύ της δημόσιας διοίκησης και των πολιτών, αποτελεί καίριο παράγοντα στη χρήση αυτών των εφαρμογών (Belanche et al., 2014).

Σύμφωνα με μελέτες που έγιναν αναφορικά με τη δημόσια διοίκηση και την ηλεκτρονική διακυβέρνηση ανέδειξαν ότι η εμπιστοσύνη των πολιτών στην ηλεκτρονική διακυβέρνηση στηρίζεται σε δυο πυλώνες: 1) στην άποψη που έχουν για τη συγκεκριμένη οντότητα, π.χ. εμπιστοσύνη στην κυβέρνηση και 2) στην αξιοπιστία των τεχνολογικών μέσων που χρησιμοποιεί η συγκεκριμένη οντότητα, π.χ. εμπιστοσύνη στο διαδίκτυο. (Carter & Belanger, 2005). Αντίστοιχα, ο McKnight υποστηρίζει ότι απαιτείται a priori εμπιστοσύνη σε μια σχέση στην οποία ο πολίτης δεν έχει ακόμη αξιόπιστες ή σημαντικές πληροφορίες σχετικά με τον πάροχο ηλεκτρονικών υπηρεσιών (McKnight et al., 1998).

Ωστόσο, παρά τις αυξανόμενες επενδύσεις των κυβερνήσεων σε σύγχρονες και αξιόπιστες υπηρεσίες και εφαρμογές, οι πολίτες παρουσιάζονται διστακτικοί να κάνουν χρήση αυτών, επιλέγοντας παραδοσιακές μεθόδους εξυπηρέτησης, όπως επίσκεψη στις κατά τόπο υπηρεσίες. Καθοριστικός παράγοντας στη μη χρήση των εφαρμογών αναδεικνύεται η έλλειψη εμπιστοσύνης στην ασφάλεια των διαδικτυακών συναλλαγών και οι ανησυχίες που εγείρονται αναφορικά με τη χρήση των πληροφοριών και δεδομένων που υποβάλλονται ηλεκτρονικά (Bélanger & Carter, 2008). Η ανησυχία αυτή καταγράφηκε από τον κυβερνητικό οργανισμό Federal Trade Commission (FTC) των Ηνωμένων Πολιτειών, όπου το 2020, σημειώθηκαν 4,8 εκατομμύρια αναφορές κλοπής ταυτότητας και απάτης, με το 1/3 να εντοπίζεται σε κυβερνητικές υπηρεσίες (FTC, 2021).

Επιπλέον, έρευνα που διεξήχθη το 2020 αναφορικά με τις κρατικές εφαρμογές και τη χρήση τους από τους πολίτες, με αφορμή τον COVID-19, ανέδειξε ότι μόνο το 41% των πολιτών του Ηνωμένου Βασιλείου ήταν πρόθυμοι να μοιραστούν δεδομένα με την κυβέρνηση, στη Γαλλία, μόνο το 33% των ερωτηθέντων ήταν πρόθυμοι να κοινοποιήσουν οποιαδήποτε δεδομένα, ενώ στις ΗΠΑ, το 62% των πολιτών δήλωσε ότι δεν θα εμπιστευόταν τη διαχείριση των δεδομένων του στην κυβέρνηση (Howell, 2020). Ως εκ τούτου, αναδεικνύεται ότι ένα σημαντικό ποσοστό των πολιτών θεωρεί ότι η εκχώρηση

εμπιστοσύνης σε κρατικές εφαρμογές, εμπεριέχει τον κίνδυνο περιορισμού των συνταγματικών τους ελευθεριών, αντί της ενίσχυσης της εμπιστοσύνης τους σε αυτές (Stevens & Haines, 2020).

Σε αυτό το πλαίσιο, σκοπός της παρούσας ΜΔΕ είναι να εστιάσει στο θέμα της μεταβίβασης της εμπιστοσύνης από τους χρήστες σε φορητές εφαρμογές που έχουν δημιουργηθεί στα πλαίσια της ηλεκτρονικής διακυβέρνησης. Συγκεκριμένα, αξιοποιώντας τα δεδομένα που προέκυψαν παγκοσμίως από τη χρήση κρατικών εφαρμογών για την ιχνηλάτηση του COVID-19, θα επιχειρηθεί να αναδειχθεί ο ρόλος που η μεταβίβαση εμπιστοσύνης αποκτά και με ποιες προϋποθέσεις τα στοιχεία τα οποία δύνανται να συλλέξουν οι φορητές ενισχύουν ή αποθαρρύνουν τους πολίτες να κάνουν χρήση αυτών. Ειδικότερα, θα επιχειρηθεί να δοθεί απάντηση στα ακόλουθα ερευνητικά ερωτήματα:

E1: Ποια είναι η έννοια της μεταβίβασης εμπιστοσύνης σε φορητές εφαρμογές που έχουν δημιουργηθεί υπό κρατική αιγίδα;

E2: Τι κίνδυνοι απορρέουν από τη μεταβίβαση εμπιστοσύνης σε κρατικές φορητές εφαρμογές;

E3: Ποιοι παράγοντες θα μπορούσαν να επηρεάσουν την εμπιστοσύνη των πολιτών κατά τη χρήση φορητών εφαρμογών που έχουν υλοποιηθεί στα πλαίσια της δημόσιας διοίκησης και διακυβέρνησης;

Με την ολοκλήρωση της εργασίας εκτιμάται ότι, πέραν των απαντήσεων στα ερευνητικά ερωτήματα, θα έχουν αποσαφηνιστούν οι τρόποι με τους οποίους το κράτος μπορεί να ενισχύσει ή αποθαρρύνει τους πολίτες στην πρόθεσή τους να τις χρησιμοποιήσουν κρατικές εφαρμογές έξυπνων τηλεφώνων και σε ένα γενικότερο πλαίσιο να αποτυπωθεί ο τρόπος με τον οποίο αντιλαμβάνονται οι πολίτες στην Ελλάδα την έννοια της εμπιστοσύνης και της μεταβίβασής της κατά την χρήση κρατικών φορητών εφαρμογών.

1.2. Θεωρητικό υπόβαθρο

Η χρήση φορητών εφαρμογών, αποτελεί μια βιώσιμη επιλογή τόσο για τις επιχειρήσεις, που θέλουν να παραμείνουν ανταγωνιστικές σε μια άκρως μεταβαλλόμενη περίοδο, όσο και για τη δημόσια διοίκηση, μειώνοντας την γραφειοκρατία και προσφέροντας υπηρεσίες υψηλού επιπέδου στον πολίτη. Η τάση αυτή αποτυπώνεται και σε έρευνα της Ελληνικής Στατιστικής Αρχής, όπου 9 στους 10 πολίτες ηλικίας 16-74 ετών (88,9%) χρησιμοποιούν έξυπνα κινητά τηλέφωνα, με 8 στους 10 πολίτες (83,4%), να συνδέονται στο διαδίκτυο εν κινήσει από

φορητή συσκευή. Παράλληλα, 1 στους 2 πολίτες (52,9%) κάνει χρήση υπηρεσιών ηλεκτρονικής διακυβέρνησης, ενώ 1 στους 2 πολίτες (47,8%) πραγματοποιούν ηλεκτρονική αγορά ή παραγγελία αγαθών ή υπηρεσιών (ΕΛΣΤΑΤ, 2019).

Σύμφωνα με τον παγκόσμιο Οργανισμό για την Οικονομική Συνεργασία και Ανάπτυξη (ΟΟΣΑ), την τελευταία δεκαετία, οι κυβερνήσεις παγκοσμίως αξιοποιούν τις δυνατότητες που τους παρέχουν οι νέες τεχνολογίες και το Διαδίκτυο για τη βελτίωση των κυβερνητικών παροχών στους πολίτες. Χαρακτηριστικό παράδειγμα αποτελεί η εφαρμογή PetaBencana.id της κυβέρνησης της Ινδονησίας, για την ενημέρωση των πολιτών σχετικά με τις έκτακτες συνθήκες πλημμυρών, το Extreme Weather App των Ηνωμένων Αραβικών Εμιράτων για την πρόβλεψη αμμοθύελλων, το Wellbeing Project της Santa Monica - California, εφαρμογή η οποία βοηθάει την τοπική αυτοδιοίκηση να κατανοήσει και να ανταποκριθεί καλύτερα στις ανάγκες των κατοίκων της, κ.α. (OECD, 2017a).

Η επιτυχία, ωστόσο, αυτών των τεχνολογικών καινοτομιών εξαρτάται σε μεγάλο βαθμό από την αποδοχή και χρήση τους από τους πολίτες. Όπως αναφέρεται και στη διεθνή βιβλιογραφία, η εμπιστοσύνη ενός χρήστη σε μια εφαρμογή είναι υποκειμενική και εγγενώς δύσκολο να μετρηθεί. Δημιουργείται με την πάροδο του χρόνου και αλλάζει καθ' όλη τη διάρκεια χρήσης της εφαρμογή εξαιτίας της επίδρασης διαφόρων εξωγενών παραγόντων. Παράλληλα, απουσιάζουν έρευνες που εστιάζουν στη μελέτη της εμπιστοσύνης της χρήσης των εφαρμογών αυτών από την πλευρά του χρήστη, καθώς η πλειοψηφία αυτών επικεντρώνεται στην αξιολόγηση της συμπεριφοράς ή απόδοσής τους (Yan et al., 2010).

Σύμφωνα με τον Mayer, η εμπιστοσύνη αντικατοπτρίζει την προθυμία ενός προσώπου να είναι ευάλωτο στις ενέργειες κάποιου άλλου, με βάση την προσδοκία ότι το άλλο μέρος θα εκτελέσει τη συγκεκριμένη ενέργεια, ανεξάρτητα από τις δομές παρακολούθησης ή ελέγχου (Mayer et al., 1995). Ο Morgone επισημαίνει ότι η εμπιστοσύνη στηρίζεται σε δυο βασικούς πυλώνες: i) τις θετικές προσδοκίες που έχει μια οντότητα προς μια άλλη και ii) την αποδοχή της ευαλωτότητας σε ενδεχόμενο κίνδυνο ή αβέβαιων συνθηκών. Ομοίως, αναδεικνύονται διάφορες κατηγορίες σχέσεων εμπιστοσύνης, όπως μεταξύ των πολιτών, των πολιτών προς την κυβέρνηση, της κυβέρνησης προς τους πολίτες, κ.α.. (Morgone et al., 2009).

Αντίστοιχα, αρκετές μελέτες σημειώνουν ότι η εμπιστοσύνη μπορεί να μεταβιβαστεί μεταξύ διαφορετικών οντοτήτων, είτε πρόκειται για άτομα, αντικείμενα ή διαδικασίες. Ειδικότερα, η θεωρία μεταβίβασης εμπιστοσύνης υποστηρίζει ότι ένα άτομο αναπτύσσει εμπιστοσύνη

σε μια οντότητα λόγω της εμπιστοσύνης του σε μια άλλη συνδεδεμένη οντότητα (Belanche et al, 2014). Σύμφωνα με τους Doney και Cannon, η εμπιστοσύνη μπορεί να μεταφερθεί από μια αξιόπιστη πηγή σε ένα άλλο άτομο ή ομάδα με την οποία, το μέλος που εμπιστεύεται έχει μικρή ή καθόλου άμεση εμπειρία. Για παράδειγμα, ένας νέος πωλητής, που εκπροσωπεί μια εταιρεία που ο αγοραστής εμπιστεύεται, θα επωφεληθεί από την προηγούμενη εμπειρία του αγοραστή με την εταιρεία (Doney & Cannon, 1997).

Στο ίδιο πλαίσιο, ο μηχανισμός μεταβίβασης, μέσω του οποίου η παροχή υπηρεσιών μπορεί να επηρεάσει την εμπιστοσύνη σε δημόσιους οργανισμούς αναφέρεται στη διεθνή βιβλιογραφία ως υπόθεση μικρο-απόδοσης (micro-performance), δηλαδή η δυνατότητα των δημοσίων υπηρεσιών να παρέχουν καλύτερης ποιότητας υπηρεσίες, μπορούν να οδηγήσουν στην αύξηση της ικανοποίησης των πολιτών που χρησιμοποιούν τις δημόσιες εφαρμογές, αυξάνοντας κατ' επέκταση την εμπιστοσύνη στη δημόσια διοίκηση. Ως εκ τούτου, οι θετικές εμπειρίες που αποκομίζουν οι πολίτες από τη χρήση των αντίστοιχων εφαρμογών καθιστούν τη δημόσια διοίκηση αξιόπιστο «συνεργάτη» τους στη διεκπεραίωση γραφειοκρατιών υποθέσεων (OECD, 2017).

Εντούτοις, εγείρονται ερωτήματα αναφορικά με την επαρκή προστασία των δεδομένων των χρηστών των εφαρμογών έξυπνων τηλεφώνων και τη διασφάλιση της ηθικής χρήσης των συλλεγόμενων δεδομένων από τις κυβερνήσεις. Ιδίως, με αφορμή τον COVID-19, αρκετές κυβερνήσεις σε παγκόσμιο επίπεδο δημιούργησαν εφαρμογές για τον εντοπισμό των πολιτών που πιθανός ήρθαν σε επαφή με κάποιο επιβεβαιωμένο κρούσμα. Χαρακτηριστικό παράδειγμα αποτελεί η εφαρμογή TraceTogether η οποία δημιουργήθηκε από την κυβέρνηση της Σιγκαπούρης και χρησιμοποιεί την τεχνολογία Bluetooth για την ανταλλαγή προσωρινών αριθμών ταυτότητας (IDs) μεταξύ έξυπνων κινητών τηλεφώνων, που βρίσκονται σε κοντινή απόσταση. Όταν ένας πολίτης έχει ενεργοποιήσει την εφαρμογή και έχει διαγνωσθεί θετικός στον COVID-19, το Υπουργείο Υγείας έχει τη δυνατότητα να ανασύρει τα αποθηκευμένα δεδομένα του κινητού του και να κάνει ιχνηλάτηση των επαφών του (Stevens & Haines, 2020).

Σε αυτό το πλαίσιο, είναι απαραίτητο να διασφαλιστεί ότι τα δεδομένα που συλλέγονται μέσω φορητών εφαρμογών ευρείας χρήσης από την κυβέρνηση χρησιμοποιούνται μόνο για το σκοπό που οι χρήστες τα παραχωρούν και ότι λαμβάνονται μέτρα για τη διασφάλιση της ασφάλειάς τους.(Garg et al., 2020). Για την αποδοχή τους από τους πολίτες, απαιτείται μια πιο λεπτομερής διερεύνηση των παραγόντων που ενισχύουν την εμπιστοσύνη τους στη

κυβέρνηση και κατ' επέκταση στην ηλεκτρονική διακυβέρνηση. Ως εκ τούτου η οικοδόμηση εμπιστοσύνης, στις σχέσεις μεταξύ δημόσιας διοίκησης και πολιτών κρίνεται απαραίτητη ως μέσο για την αντιμετώπιση της αβεβαιότητας (Belanche et al., 2014).

Για να καλλιεργηθεί, συνεπώς, το κατάλληλο επίπεδο εμπιστοσύνης στους πολίτες μιας χώρας, απαιτείται τόσο εμπιστοσύνη των ιδίων στη κυβέρνηση όσο και εμπιστοσύνη στο διαδίκτυο. Μειωμένο επίπεδο εμπιστοσύνης στην κυβέρνηση σε συνδυασμό με υψηλό επίπεδο εμπιστοσύνης στο διαδίκτυο ελλοχεύει τον κίνδυνο οι πολίτες να μην εισάγουν αξιόπιστα δεδομένα στις εφαρμογές που χρησιμοποιούν. Αντίστοιχα, υψηλό επίπεδο εμπιστοσύνης στην κυβέρνηση, αλλά μειωμένο επίπεδο εμπιστοσύνης στο Διαδίκτυο υποδηλώνει την προθυμία των πολιτών να κάνουν χρήση των δημόσιων εφαρμογών, ωστόσο δεν θα αξιοποιηθούν στο έπακρο οι δυνατότητες της εφαρμογής (Colesca, 2009).

Κρίνεται, λοιπόν, απαραίτητο, οι πολίτες να γνωρίζουν ότι η κυβέρνηση διαθέτει τους απαραίτητους πόρους και την κατάλληλη τεχνογνωσία για τη διασφάλιση αυτών των εφαρμογών. Ενισχύοντας την εμπιστοσύνη των πολιτών στην κυβέρνηση, ενισχύεται παράλληλα και η πρόθεσή τους να συμμετάσχουν στην ηλεκτρονική διακυβέρνηση του κράτους, αξιοποιώντας τις αντίστοιχες εφαρμογές και παρέχοντας αξιόπιστα δεδομένα στην κυβέρνηση κατά τη χρήση αυτών (Warkentin et al., 2002).

1.3. Μεθοδολογία της έρευνας

Η έρευνα έχει ως στόχο της, μέσω της συστηματικής μελέτης και αντικειμενικής και εξακριβωμένης αναζήτησης πληροφοριών, την προαγωγή της επιστημονικής γνώσης, τη διερεύνηση νέων θεωριών και την επίλυση προβλημάτων (Παρασκευόπουλος, 1993). Αντίστοιχα, ο Δημητρόπουλος επισημαίνει ότι η μεθοδολογία έρευνας αφορά τις μεθοδολογικές προσεγγίσεις που θα επιλέξει ένας ερευνητής για να διεξάγει μια επιστημονική έρευνα (Δημητρόπουλος, 2004).

Η ερευνητική προσέγγιση της παρούσας διπλωματικής εργασίας ακολουθεί την προσέγγιση του θετικισμού, η οποία αποτελεί ένα από τα σημαντικότερα ρεύματα που οροθετούν το εύρος και τη μεθοδολογία της έρευνας και εξαρτάται από μετρήσιμες παρατηρήσεις που οδηγούν σε στατιστικές αναλύσεις. Αξίζει να σημειωθεί ότι ο θετικισμός, ως φιλοσοφία, είναι σύμφωνος με την εμπειρική άποψη ότι «η γνώση πηγάζει από την ανθρώπινη εμπειρία. Έχει μια ατομική, οντολογική άποψη του κόσμου που περιλαμβάνει διακριτά, παρατηρήσιμα στοιχεία και γεγονότα που αλληλεπιδρούν μεταξύ τους» (Collins, 2010).

Παράλληλα, επιλέχθηκε η ποσοτική μέθοδος, όπου μέσω της βιβλιογραφικής ανασκόπησης εξετάστηκαν τα υπό διερεύνηση ζητήματα, ενώ στη συνέχεια με τη χρήση ερωτηματολογίου συλλέχθηκαν τα δεδομένα, τα οποία χρησιμοποιήθηκαν για να απαντηθούν τα ερευνητικά ερωτήματα που τέθηκαν. Συγκεκριμένα, για να προσδιοριστούν τα ερευνητικά ερωτήματα E1 και E2, πραγματοποιήθηκε συστηματική ανασκόπηση της υπάρχουσας βιβλιογραφίας, ενώ για να προσδιοριστεί το ερευνητικό ερώτημα E3 χρησιμοποιήθηκε το ερωτηματολόγιο. Η ανάλυση και επεξεργασία των συλλεχθέντων δεδομένων έγινε με το πρόγραμμα SPSS.

Σύμφωνα με τη βιβλιογραφία, η ποσοτική έρευνα στοχεύει να δοκιμάσει υποθέσεις που έχουν ήδη εξεταστεί και από άλλους ερευνητές και να βρει στοιχεία που υποστηρίζουν ή δεν υποστηρίζουν μια υπάρχουσα υπόθεση. Καθώς το ζήτημα που διαπραγματεύεται η συγκεκριμένη διπλωματική εργασία απασχολεί την επιστημονική κοινότητα τα τελευταία χρόνια, κρίθηκε απαραίτητο να χρησιμοποιηθεί αυτή η μέθοδος ούτως ώστε να αποτυπωθεί η υφιστάμενη κατάσταση στο συγκεκριμένο πλαίσιο αναφοράς. Όπως χαρακτηριστικά αναφέρει και ο Creswell (2009), αν το πρόβλημα προσδιορίζει παράγοντες που επηρεάζουν ένα αποτέλεσμα, τότε μια ποσοτική προσέγγιση είναι προτιμότερη σε σχέση με την ποιοτική ή το συνδυασμό και των δυο.

Σε αυτό το σημείο, αξίζει να σημειωθεί ότι για τη διεξαγωγή της συστηματικής βιβλιογραφικής ανασκόπησης σχεδιάστηκε και ακολουθήθηκε συγκεκριμένο πρωτόκολλο έρευνας, το οποίο περιλάμβανε 6 βήματα: 1) Καθορισμός ερευνητικών ερωτημάτων, 2) Αναζήτηση σχετικών μελετών, 3) Εφαρμογή κριτηρίων ένταξης / αποκλεισμού, 4) Επιλογή σχετικών μελετών, 5) Εξαγωγή και σύνθεση δεδομένων, 6) Παρουσίαση ευρημάτων. Η χρήση ερευνητικού πρωτοκόλλου αποσκοπεί στην αξιολόγηση και, όπου είναι δυνατόν, στην ελαχιστοποίηση της προκατάληψης στα ευρήματα (Higgins & Thomas, 2021). Τόσο τα παραπάνω βήματα, όσο και η μεθοδολογία που ακολουθήθηκε παρουσιάζονται αναλυτικά στο Κεφάλαιο 3.

1.4. Δομή εργασίας

Το πρώτο κεφάλαιο αποτελεί το εισαγωγικό μέρος της παρούσας εργασίας, το οποίο συμπεριλαμβάνει τη σημασία και τον σκοπό του υπό διερεύνηση θέματος, ακολουθούμενο από το θεωρητικό υπόβαθρο πάνω στο οποίο στηρίχτηκε η ανάλυση της εργασίας, τη μεθοδολογία έρευνας, στην οποία αποτυπώνεται η ερευνητική προσέγγιση που επιλέχθηκε και τέλος τη διάρθρωση των κεφαλαίων της διπλωματικής εργασίας.

Το δεύτερο κεφάλαιο επικεντρώνεται στο να προσεγγίσει βιβλιογραφικά το υπό διερεύνηση θέμα και διαπραγματεύεται την έννοια της εμπιστοσύνης, τα μοντέλα σχηματισμού εμπιστοσύνης που χρησιμοποιήθηκαν στο ερευνητικό μέρος, την έννοια της μεταβίβασης εμπιστοσύνης, τη χρήση φορητών εφαρμογών στη δημόσια διοίκηση και διακυβέρνηση, τη μεταβίβαση εμπιστοσύνης στις φορητές εφαρμογές και τις προκλήσεις που αναδύονται κατά τη χρήση φορητών εφαρμογών.

Το τρίτο κεφάλαιο παρουσιάζει αναλυτικά το ερευνητικό πεδίο του υπό διερεύνηση θέματος και συμπεριλαμβάνει τις ενότητες που διαπραγματεύονται το σκοπό και τους ερευνητικούς στόχους της έρευνας, τη μεθοδολογία που ακολουθήθηκε ώστε να εξετασθεί, μέσω της συστηματική ανασκόπηση της βιβλιογραφίας, η υπάρχουσα κατάσταση και με τη βοήθεια του ερωτηματολογίου να αποτυπωθεί ποσοτικά η κατάσταση, τα ερευνητικά ερωτήματα, το ερευνητικό μοντέλο και τις ερευνητικές υποθέσεις, ενώ παρουσιάζεται συνοπτικά και το ερωτηματολόγιο της έρευνας.

Το τέταρτο κεφάλαιο επικεντρώνεται στην παρουσίαση των αποτελεσμάτων της έρευνας, η οποία διενεργήθηκε με το στατιστικό πρόγραμμα SPSS. Οι ενότητες του κεφαλαίου αποτελούνται από την στατιστική ανάλυση, τον έλεγχο αξιοπιστίας Cronbach α , την περιγραφική και επαγωγική στατιστική και ολοκληρώνεται με τις απαντήσεις στα ερευνητικά ερωτήματα.

Το πέμπτο κεφάλαιο, αποτελεί τον επίλογο της διπλωματικής εργασίας με τις ενότητές του να διαπραγματεύονται την παρουσίαση σχετικών, με το υπό διερεύνηση θέμα, ερευνών, τα συμπεράσματα της εργασίας, τους περιορισμούς της έρευνας και την προτεινόμενη μελλοντική έρευνα.

Η διπλωματική εργασία ολοκληρώνεται με την παράθεση της ξενόγλωσσης και ελληνικής βιβλιογραφίας που χρησιμοποιήθηκε για την εκπόνηση της και το Παράρτημα το οποίο περιλαμβάνει το ερωτηματολόγιο της ποσοτικής έρευνας και τον πίνακα συσχέτισης (correlation matrix) που χρησιμοποιήθηκε στην ανάλυση διαδρόμων (Path analysis).

ΚΕΦΑΛΑΙΟ 2: ΒΙΒΛΙΟΓΡΑΦΙΚΗ ΕΠΙΣΚΟΠΗΣΗ

2.1. Η έννοια της εμπιστοσύνης

Η έννοια της εμπιστοσύνης αποτελεί ένα αμφιλεγόμενο πεδίο έρευνας για τους μελετητές διαφόρων επιστημονικών κλάδων, όπως Ανθρωπολογίας, Οικονομίας, Ψυχολογίας, Κοινωνιολογίας, Πολιτικών επιστημών, κ.α., καθώς χρησιμοποιούνται διαφορετικές προσεγγίσεις και μέθοδοι, σχετικά με τη θεμελιώδη φύση της κοινής αυτής συνισταμένης. Αν και έχουν προταθεί αρκετοί ορισμοί και έχουν γίνει εκτενείς μελέτες πάνω σε διάφορα μοντέλα διαπροσωπικής και θεσμικής εμπιστοσύνης, δεν κατέστη εφικτό να παρουσιαστεί ένα κοινά αποδεκτό πλαίσιο της. Αδιαμφισβήτητο, ωστόσο, παραμένει το γεγονός ότι η εμπιστοσύνη αποτελεί μια από τις σημαντικότερες έννοιες, η οποία καθορίζει τις σχέσεις των ανθρώπων και τις συναλλαγές τους με επιχειρήσεις και κυβερνητικούς οργανισμούς.

2.1.1. Ορισμός της εμπιστοσύνης

Αν και η έννοια της εμπιστοσύνης έχει μελετηθεί εκτενώς από διάφορους επιστημονικούς κλάδους, πολύ πριν την ύπαρξη του διαδικτύου, των έξυπνων κινητών τηλεφώνων και της ηλεκτρονικής διακυβέρνησης, εντούτοις δεν υπάρχει ένας ευρέως αποδεκτός ορισμός της (Doney & Cannon, 1997). Σε ένα ευρύτερο εννοιολογικό πλαίσιο θα μπορούσε να ειπωθεί ότι η εμπιστοσύνη αντικατοπτρίζει την προθυμία ενός ανθρώπου να είναι ευάλωτος στις ενέργειες κάποιου άλλου, με βάση την προσδοκία ότι ο τελευταίος θα εκτελέσει μια συγκεκριμένη δράση, ανεξάρτητα από τις δομές παρακολούθησης ή ελέγχου (Mayer et al, 1995).

Αξίζει να σημειωθεί ότι παρά την πολυμορφία που παρατηρείται στη βιβλιογραφία σχετικά με τον ορισμό της, ένα βασικό ερώτημα, κοινό για όλες τις προσεγγίσεις, αποτελεί ο τρόπος με τον οποίο αναπτύσσεται η εμπιστοσύνη. Οι Lewicki και Bunker προτείνουν την κατηγοριοποίησή της με βάση τον τρόπο με τον οποίο αντιμετωπίζεται, είτε δηλαδή ως ατομικό χαρακτηριστικό, είτε ως χαρακτηριστικό των διαπροσωπικών συναλλαγών ή ως ένα θεσμικό φαινόμενο (Lewicki & Bunker, 1995). Οι ψυχολόγοι θεωρούν την εμπιστοσύνη ως ατομικό χαρακτηριστικό γνώρισμα. Οι κοινωνικοί ψυχολόγοι ορίζουν την εμπιστοσύνη ως προσδοκία σχετικά με τη συμπεριφορά των άλλων στις διαπροσωπικές επαφές, εστιάζοντας στους παράγοντες που την ενισχύουν ή την αναστέλλουν. Οι Οικονομολόγοι και Κοινωνιολόγοι εστιάζουν στον τρόπο με τον οποίο αναπτύσσεται η εμπιστοσύνη στις συναλλαγές μεταξύ αγνώστων (Bhattacharya et al., 1998).

Οι Barney και Hansen (1994), στην προσπάθειά τους να ενσωματώσουν το σύνολο των διαφορετικών απόψεων, υποστηρίζουν ότι υπάρχουν τρία διαφορετικά είδη εμπιστοσύνης: 1) η αδύναμη μορφή, 2) η ημι-ισχυρή μορφή, και 3) η ισχυρή μορφή. Η εμπιστοσύνη αδύναμης μορφής αναφέρεται σε εκείνου του είδους τις σχέσεις, όπου τα μέρη δεν παρουσιάζουν τρωτά σημεία τα οποία μπορούν να γίνουν αντικείμενο εκμετάλλευσης, οπότε και δεν απαιτείται καμία ενέργεια για το σχηματισμό της. Στην περίπτωση της ημι-ισχυρής μορφής εμπιστοσύνης, που υφίστανται τρωτά σημεία, απαιτείται η λήψη μέτρων ώστε να διασφαλιστεί η αξιοπιστία μεταξύ των συναλλασσόμενων μερών, ενώ στην ισχυρή της μορφή, όπου η ευαλωτότητα είναι σημαντική, ανεξάρτητα από τους μηχανισμούς ελέγχου, ο σχηματισμός εμπιστοσύνης μεταξύ των μελών καθίσταται αδύνατη.

Στον Πίνακα 1 αποτυπώνονται οι επικρατέστεροι ορισμοί της έννοιας της εμπιστοσύνης, σύμφωνα με τη διεθνή βιβλιογραφία.

Πίνακας 1: Ορισμοί της εμπιστοσύνης

Πηγή	Ορισμός
Rotter, (1980)	Η εμπιστοσύνη είναι μια γενικευμένη προσδοκία ενός ατόμου ότι μπορεί να βασιστεί στις λέξεις, την υπόσχεση ή τη δήλωση ενός άλλου ατόμου.
Lewis and Weigert (1985)	Η εμπιστοσύνη υπάρχει σε ένα κοινωνικό σύστημα στο βαθμό που τα μέλη αυτού του συστήματος ενεργούν σύμφωνα με αυτό.
Meyer et al. (1995)	Η εμπιστοσύνη αντικατοπτρίζει την προθυμία να είσαι ευάλωτος σε έναν άλλο.
Rousseau et al. (1998)	Μια ψυχολογική κατάσταση που περιλαμβάνει την πρόθεση ενός ατόμου να αποδεχτεί την ευαλωτότητα, διατηρώντας θετικές προσδοκίες για τις προθέσεις ή τη συμπεριφορά ενός άλλου.
Grandison and Sloman (2000)	Η εμπιστοσύνη είναι η σταθερή πίστη στην ικανότητα μιας οντότητας να ενεργεί αξιόπιστα και με ασφάλεια μέσα σε ένα συγκεκριμένο πλαίσιο.
Shekarpour and Katebi (2010)	Η εμπιστοσύνη ενός ατόμου A σε ένα άλλο άτομο B, για μια υπηρεσία X, είναι η μετρήσιμη πεποίθηση του A ότι το B συμπεριφέρεται αξιόπιστα σε σχέση με την υπηρεσία X.

Σύμφωνα με τους προαναφερθέντες ορισμούς, καθίσταται έκδηλο ότι η εμπιστοσύνη στηρίζεται σε δυο βασικούς πυλώνες: i) τις θετικές προσδοκίες που έχει μια οντότητα προς μια άλλη και ii) την αποδοχή της ευαλωτότητας σε ενδεχόμενο κίνδυνο ή αβέβαιων καταστάσεων. Ομοίως, αναδεικνύονται διάφορες κατηγορίες σχέσεων εμπιστοσύνης, όπως μεταξύ των πολιτών, των πολιτών προς την κυβέρνηση, της κυβέρνησης προς τους πολίτες, κ.α.. Αντίστοιχα η κατηγοριοποίηση των ανωτέρω σχέσεων περιλαμβάνει τα εξής δύο ευρύτερα σύνολα: i) τη διαπροσωπική εμπιστοσύνη, η οποία εμπεριέχει τις κοινωνικές αλληλεπιδράσεις και ii) τη συστημική ή θεσμική εμπιστοσύνη, η οποία αφορά τους δημόσιους και πολιτικούς θεσμούς (Morgone et al., 2009).

Ο Halpern σχετίζει τη διαπροσωπική εμπιστοσύνη με τα αποτελέσματα της αλληλεπίδρασης των ατόμων μέσα σε μια κοινωνία με κοινά ήθη, έθιμα και αξίες. Για παράδειγμα, ομάδες ατόμων με κοινό πολιτιστικό ή θρησκευτικό υπόβαθρο τείνουν να έχουν παρόμοια επίπεδα διαπροσωπικής εμπιστοσύνης (Halpern, 1999). Αντίστοιχα, ο Uslaner, διαχωρίζει την διαπροσωπική εμπιστοσύνη, την οποία χαρακτηρίζει με τον ορισμό γενικευμένη εμπιστοσύνη, σε στρατηγική εμπιστοσύνη, όταν δηλαδή ο Α εμπιστεύεται κάποιον που γνωρίζει προσωπικά και ηθικολογική (moralistic) εμπιστοσύνη, όταν ο Α εμπιστεύεται έναν άγνωστο (Uslaner, 2002).

Η συστημική ή θεσμική εμπιστοσύνη αντικατοπτρίζει το πλαίσιο εμπιστοσύνης η δυσπιστίας των πολιτών στην κυβέρνηση ή/και στους οργανισμούς σε σχέση με το ισχύον θεσμικό πλαίσιο. Σε μακρο-επίπεδο, επικεντρώνεται στην αλληλεπίδραση μεταξύ των πολιτών και της κυβέρνησης και δημιουργείται όταν οι πολίτες αξιολογούν τους δημόσιους οργανισμούς και την κυβέρνηση θετικά για την αποτελεσματικότητα και την ίση μεταχείριση. Όπως αναφέρεται και στη βιβλιογραφία, ένα άτομο Α εμπιστεύεται τον οργανισμό Β να κάνει την ενέργεια Χ, η οποία είναι συμβατική υποχρέωση του Β. Για παράδειγμα, ένας πολίτης εμπιστεύεται την κυβέρνηση για την προάσπιση των ατομικών/εθνικών του συμφερόντων. Σε μικρο-επίπεδο, ωστόσο, αυτός ο τύπος εμπιστοσύνης αναφέρεται και ως πολιτική εμπιστοσύνη των πολιτών σε συγκεκριμένους πολιτικούς ηγέτες. Υπό αυτό το πρίσμα, οι πολίτες εμπιστεύονται ή μη την κυβέρνηση και τους θεσμούς εξαιτίας της έγκρισης ή μη συγκεκριμένων πολιτικών ηγετών (Blind, 2007).

Στον Πίνακα 2 αποτυπώνονται οι κυριότερες σχέσεις εμπιστοσύνης που αναπτύσσονται στα πλαίσια της κοινωνίας και τα αποτελέσματα που αναδύονται από αυτή τη σχέση για κάθε μια από της κατηγορίες (OECD, 2017).

Πίνακας 2: Σχέσεις εμπιστοσύνης στην κοινωνία

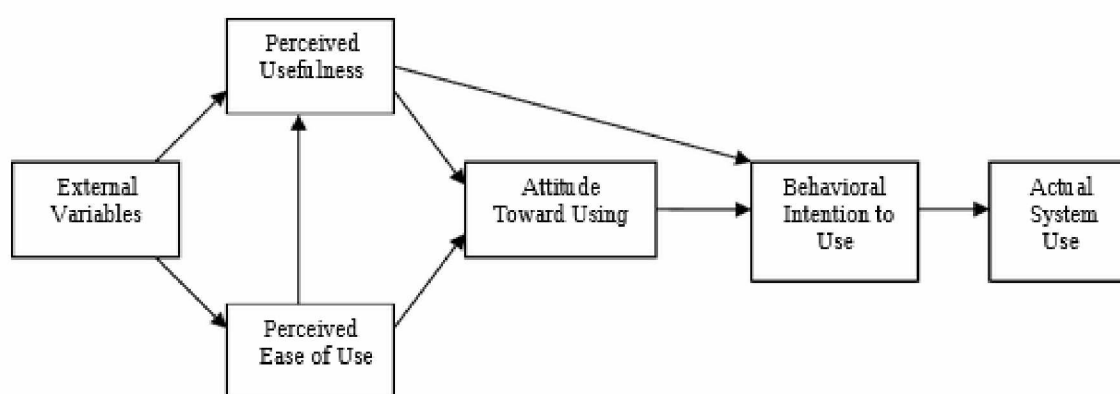
Σχέση εμπιστοσύνης	Αποτέλεσμα
Πολίτες προς πολίτες	<ul style="list-style-type: none">• Ενδυνάμωση του κοινωνικού κεφαλαίου• Αύξηση της συνοχής των κοινωνιών
Πολίτες προς Κυβέρνηση	<ul style="list-style-type: none">• Συμμόρφωση και υποστήριξη των πολιτών στα κυβερνητικά προγράμματα και πολιτικές• Μείωση στα κόστη εφαρμογής-επιβολής
Κυβέρνηση προς Πολίτες	<ul style="list-style-type: none">• Εξορθολογισμένες δημόσιες υπηρεσίες• Βελτιστοποίηση και αποτελεσματικότητα υπηρεσιών
Πολίτες προς πολιτικούς ηγέτες	<ul style="list-style-type: none">• Ευκολότερη εφαρμογή μέτρων• Μείωση πολιτικών αδιεξόδων
Επιχειρήσεις προς Κυβέρνηση	<ul style="list-style-type: none">• Προσέλκυση περισσότερων επενδύσεων• Συμμόρφωση με τους κανονισμούς και το νομικό πλαίσιο
Δομή κράτους	<ul style="list-style-type: none">• Αύξηση του επιπέδου συνεργασίας μεταξύ των κυβερνητικών υπηρεσιών• Αύξηση της αποτελεσματικότητας των υπηρεσιών

Αν και η διαπροσωπική εμπιστοσύνη με τη θεσμική εμπιστοσύνη δεν αλληλοαποκλείονται, εντούτοις, παρατηρείται μια διαφοροποίηση σχετικά με την αιτιότητα της σχέσης αυτής. Η διαπροσωπική εμπιστοσύνη επηρεάζεται από την αυξανόμενη κοινωνική συμμετοχή, καθώς η επαφή με άλλα μέλη της κοινότητας επιτρέπουν στους ανθρώπους να βελτιώνουν το επίπεδο εμπιστοσύνης όχι μόνο ανάμεσά τους, αλλά συχνά και με άλλους, άγνωστους, γι' αυτούς ανθρώπους (Fukuyama 1995, Levi 1997). Ωστόσο, η κοινωνική συμμετοχή δεν οδηγεί απαραίτητα στην αύξηση της θεσμικής εμπιστοσύνης. Ο Veenstra υποστηρίζει ότι, η κοινωνική συμμετοχή αυξάνει τη διαπροσωπική εμπιστοσύνη αλλά όχι τη θεσμική εμπιστοσύνη, ενώ ο Blind τονίζει ότι μια αξιόπιστη κυβέρνηση δημιουργεί τη διαπροσωπική εμπιστοσύνη και όχι το αντίστροφο (Veenstra 2002, Blind 2007).

2.1.2. Τα μοντέλα σχηματισμού εμπιστοσύνης

Σύμφωνα με τη βιβλιογραφία, αν και έχουν προταθεί διάφορα μοντέλα εμπιστοσύνης για να διερευνηθούν τη διαπροσωπική και θεσμική εμπιστοσύνη, λίγοι ερευνητές έχουν προσπαθήσει να κατανοήσουν το τρόπο με τον οποίο δημιουργείται η εμπιστοσύνη ενός χρήστη απέναντι σε ένα συγκεκριμένο πληροφοριακό σύστημα. Για δεκαετίες, η έρευνα στο πεδίο διαχείρισης πληροφοριακών συστημάτων επικεντρώθηκε στην αποδοχή των συστημάτων αυτών, σε σχέση με την ευκολία χρήσης τους, τη χρησιμότητα και τα τεχνικά χαρακτηριστικά. Πρόσφατες, ωστόσο, έρευνες αναγνώρισαν τη σημασία της εμπιστοσύνης ως υποκειμενικής αντίληψης, που επηρεάζει την αποδοχή ενός συστήματος από τους χρήστες, προτείνοντας το Μοντέλο Αποδοχής Τεχνολογίας (Technology Acceptance Model -TAM) (Davis et al., 1989).

Στόχος του συγκεκριμένου μοντέλου είναι να διερευνηθεί και να προβλέψει την αποδοχή των πληροφοριακών συστημάτων και ευρύτερα της τεχνολογίας από τους χρήστες και να καθορίσει τους παράγοντες αποδοχής. Βασίζεται στη Θεωρία της δικαιολογημένης δράσης (Theory of Reasoned Action - TRA), η οποία χρησιμοποιείται κυρίως για να προβλέψει πώς θα συμπεριφερθεί ένα άτομο με βάση προϋπάρχουσες στάσεις και προθέσεις συμπεριφοράς. Ουσιαστικά, η απόφαση ενός ατόμου να εκδηλώσει μια συγκεκριμένη συμπεριφορά βασίζεται στα αποτελέσματα που το άτομο αναμένει ότι θα προκύψουν ως αποτέλεσμα αυτής της συμπεριφοράς. Στην Εικόνα 1 αποτυπώνεται το μοντέλο αποδοχής TAM καθώς και οι κύριες συνιστώσες του (Davis et al., 1989).

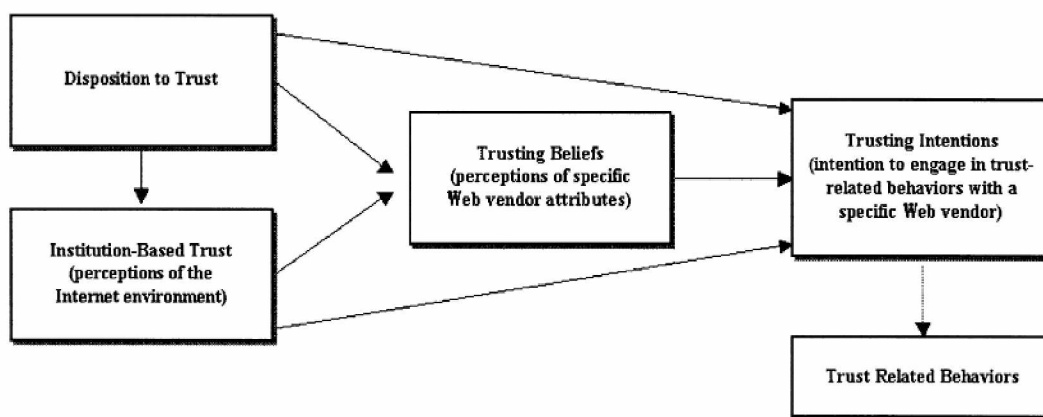


Εικόνα 1: Το μοντέλο αποδοχής τεχνολογίας -TAM (Davis et al., 1989)

Ειδικότερα, καθοριστικοί παράγοντες στην αποδοχή και χρήση ενός πληροφοριακού συστήματος αποτελούν: 1) η Αντιληπτή Ευκολία Χρήσης (Perceived Ease of Use), δηλαδή «ο βαθμός με τον οποίο ο χρήστης θεωρεί ότι η χρήση του συστήματος δεν απαιτεί επιπλέον

προσπάθεια» και 2) η Αντιληπτή Χρησιμότητα (Perceived Usefulness), δηλαδή «ο βαθμός με τον οποίο ένας χρήστης πιστεύει ότι η χρήση του συγκεκριμένου συστήματος θα αυξήσει την απόδοσή του». Επιμέρους παράγοντες του μοντέλου αυτού είναι: 1) η Στάση προς τη Χρήση (Attitude Towards Use): η άποψη που σχηματίζει ο χρήστης ως προς τη χρήση της εφαρμογής και 2) η Συμπεριφορική Πρόθεση για Χρήση (Behavioral Intention to Use): η πιθανότητα ο χρήστης να χρησιμοποιήσει την εφαρμογή. Τέλος, η Πραγματική Χρήση (Actual Use), υπολογίζεται από τη χρονική διάρκεια ή τη συχνότητα χρήσης μια συγκεκριμένης εφαρμογής από τους χρήστες (Legris et al., 2003).

Αντίστοιχα, το μοντέλο σχηματισμού εμπιστοσύνης του McKnight είναι ένα από τα πιο ευρέως διαδεδομένα μοντέλα, που επικεντρώνεται στην διαμόρφωση της εμπιστοσύνη ενός πληροφοριακού συστήματος πριν αυτό εισαχθεί σε ένα οργανισμό και πριν οι χρήστες αλληλεπιδράσουν άμεσα με αυτό και βρίσκει εφαρμογή κυρίως στα πλαίσια του ηλεκτρονικού εμπορίου. Σύμφωνα με το μοντέλο αυτό, η αρχική εμπιστοσύνη ορίζεται ως η εμπιστοσύνη σε μια άγνωστη οντότητα στην οποία το άτομο που εμπιστεύεται δεν έχει αξιόπιστη, ουσιαστική εμπειρία, γνώση ή συναισθηματικούς δεσμούς με το αντικείμενο εμπιστοσύνης. Στην Εικόνα 2 αποτυπώνεται το μοντέλο αρχικού σχηματισμού εμπιστοσύνης με τις βασικές συνιστώσες του (McKnight et al. 1998, McKnight et al. 2002a).



Εικόνα 2: Μοντέλο αρχικού σχηματισμού εμπιστοσύνης (McKnight et al. 1998)

Οι τέσσερις βασικές συνιστώσες του μοντέλου αυτού είναι:

- **Η ροπή ενός ανθρώπου να εμπιστεύεται (Disposition to trust):**

Η συγκεκριμένη συνιστώσα αναφέρεται στο βαθμό με τον οποίο ένα άτομο εμφανίζει την τάση να εμπιστεύεται και να εξαρτάται από τους άλλους. Τα δυο κύρια στοιχεία που χαρακτηρίζουν τη ροπή ενός ανθρώπου να εμπιστεύεται είναι: 1) Πίστη στην ανθρωπότητα,

δηλαδή η πεποίθηση η ότι οι άνθρωποι είναι συνήθως σωστοί, καλοπροαίρετοι και αξιόπιστοι και 2) Στάση εμπιστοσύνης, δηλαδή ανεξάρτητα από το τι πιστεύει κάποιος για τη φύση των ανθρώπων, υποθέτει ότι θα προκύψουν καλύτερα αποτελέσματα, αν αντιμετωπίζει τους ανθρώπους ως αξιόπιστους.

Αξίζει να σημειωθεί ότι οι στρατηγικές οικοδόμησης εμπιστοσύνης ενδέχεται να διαφέρουν μεταξύ των ατόμων με χαμηλή και υψηλή ροπή εμπιστοσύνης. Για παράδειγμα, οι υπερσύνδεσμοι γνωστών ιστότοπων ενδέχεται να ενισχύσουν την εμπιστοσύνη ενός καταναλωτή με υψηλή ροπή εμπιστοσύνης να περιηγηθεί σε αυτούς, αλλά μπορεί να απομακρύνουν κάποιον με χαμηλή ροπή εμπιστοσύνης.

- **Η θεσμική εμπιστοσύνη (Institution Based Trust):**

Η θεσμική εμπιστοσύνη καθορίζεται από την τάση που έχουν οι άνθρωποι να εμπιστεύονται (Disposition to trust) και αναφέρεται στην πεποίθηση ότι υπάρχουν οι απαραίτητες διαρθρωτικές συνθήκες για να ενισχυθεί η πιθανότητα επίτευξης σχηματισμού εμπιστοσύνης. Για παράδειγμα, η ύπαρξη τεχνολογικών και νομικών εγγυήσεων, που ενισχύουν την θεσμική εμπιστοσύνη, είναι σημαντικές για την ενίσχυση της εμπιστοσύνης των χρηστών στο Διαδίκτυο.

Οι δύο παράμετροι που χαρακτηρίζουν τη θεσμική εμπιστοσύνη είναι: 1) η διαρθρωτική διασφάλιση (Structural Assurance), η οποία αναφέρεται στην πεποίθηση ότι οι εγγυήσεις, οι κανονισμοί, οι νομικές προσφυγές ή άλλες παρόμοιες διαδικασίες, μπορούν να ενισχύσουν την εμπιστοσύνη και 2) η κανονικότητα της κατάστασης (Situational Normality), η οποία αναφέρεται στην πεποίθηση ότι θα υπάρξει θετικό αποτέλεσμα εξαιτίας της φυσιολογικής ή ευνοϊκής κατάστασης.

- **Πεποιθήσεις (Trusting Beliefs):**

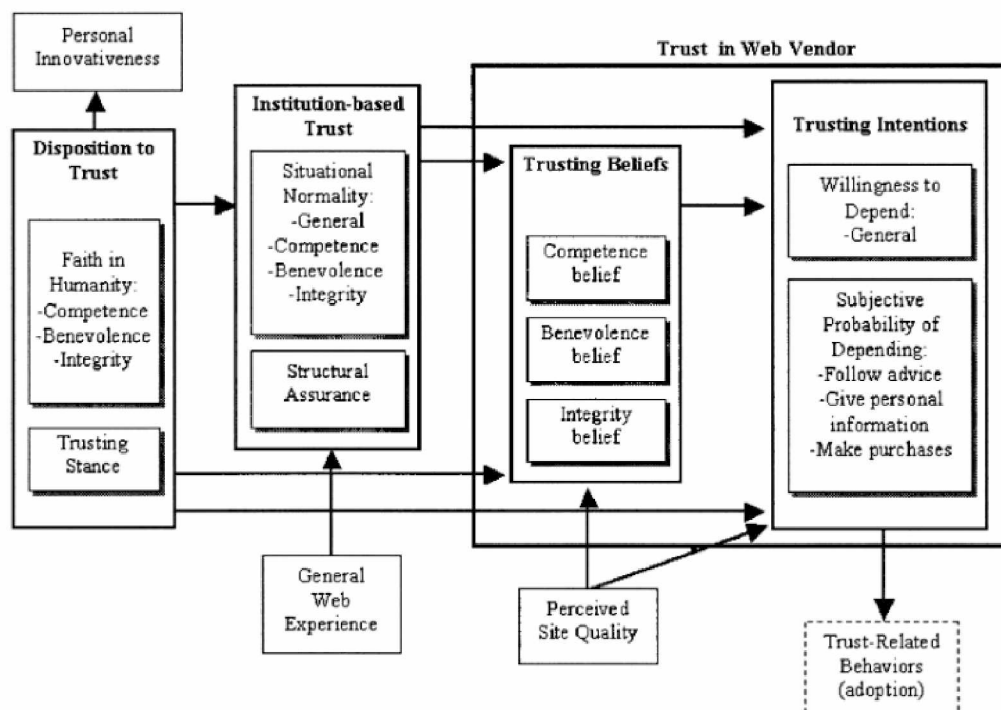
Οι πεποιθήσεις αναφέρονται στις υποκείμενες αντιλήψεις ότι το αντικείμενο εμπιστοσύνης έχει χαρακτηριστικά που είναι ευεργετικά για το άτομο που εμπιστεύεται. Τα τρία κύρια χαρακτηριστικά που αντιπροσωπεύουν αυτή την κατηγορία του μοντέλου είναι: 1) Ικανότητα (Competence): εμπιστοσύνη στην ικανότητα του αντικειμένου να κάνει ό, τι χρειάζεται το υποκείμενο, 2) Καλή πρόθεση (Benevolence): εμπιστοσύνη στα κίνητρα του αντικειμένου ότι θα δράσει προς το συμφέρον του υποκειμένου και 3) Ακεραιότητα (integrity): εμπιστοσύνη στην ειλικρίνεια του αντικειμένου και την τήρηση των υποσχέσεων

του. Οι πεποιθήσεις καθορίζουν την αμέσως επόμενη συνιστώσα του μοντέλου του McKnight, την Πρόθεση Εμπιστοσύνης.

- Πρόθεση εμπιστοσύνης (Trusting Intentions):

Η πρόθεση εμπιστοσύνης υποστηρίζει ότι ένα άτομο είναι πρόθυμο να εμπιστευτεί ή σκοπεύει να εμπιστευτεί το αντικείμενο εμπιστοσύνης. Στην πρώτη περίπτωση το άτομο προτίθεται να θέσει τον εαυτό του ευάλωτο, ενώ στη δεύτερη περίπτωση εκφράζει την αντιληπτή πιθανότητα το ένα μέλος να εξαρτάται από το άλλο.

Στην Εικόνα 3, αποτυπώνεται το διαδικτυακό μοντέλο σχηματισμού εμπιστοσύνης McKnight και οι συνδέσεις μεταξύ των δομών που σχηματίζουν την εμπιστοσύνη ενός χρήστη. Το δομικό στοιχείο “Ροπή ενός ανθρώπου να εμπιστευτεί” επιδρά άμεσα στις πεποιθήσεις και στις θεσμικές αντιλήψεις ενός ατόμου, ωστόσο η σύνδεσή του με το δομικό στοιχείο «Πρόθεση εμπιστοσύνης» δεν είναι άμεση, καθώς παρεμβάλλονται τα άλλα δυο δομικά στοιχεία. Για παράδειγμα, εάν ένας χρήστης αποκτήσει εμπειρία με έναν συγκεκριμένο διαδικτυακό προμηθευτή, η εμπειρία μπορεί να είναι η κυρίαρχη επιρροή στις πεποιθήσεις εμπιστοσύνης, αντί για τη θεσμική εμπιστοσύνη (McKnight et al., 1998).



Εικόνα 3: Το διαδικτυακό μοντέλο σχηματισμού εμπιστοσύνης (McKnight et al. 2002a)

Αντίστοιχα, η θεσμική εμπιστοσύνη σχετίζεται θετικά τόσο με τις πεποιθήσεις όσο και με τη πρόθεση εμπιστοσύνης. Όταν μια κατάσταση προκαλεί αισθήματα ασφάλειας, οι

άνθρωποι έχουν την τάση να θεωρούν ότι και παρόμοιες συσχετιζόμενες καταστάσεις έχουν τα ίδια αξιόπιστα χαρακτηριστικά. Συνεπώς, ένας χρήστης που αισθάνεται ασφάλεια με τη χρήση του διαδικτύου είναι πιθανό να αναπτύξει υψηλή εμπιστοσύνη σε έναν συγκεκριμένο προμηθευτή. Για παράδειγμα, η αντίληψη ότι ο πωλητής είναι ειλικρινής, ενθαρρύνει τον καταναλωτή να παράσχει προσωπικές πληροφορίες (Davis et al., 1989).

2.1.3. Η μεταβίβαση εμπιστοσύνης

Η έννοια της εμπιστοσύνης, όπως παρουσιάστηκε αναλυτικά στις προηγούμενες ενότητες, αντικατοπτρίζει την προθυμία ενός ατόμου να είναι ευάλωτος στις ενέργειες κάποιου άλλου, με βάση την προσδοκία ότι ο τελευταίος θα εκτελέσει μια συγκεκριμένη δράση, ανεξάρτητα από τις δομές παρακολούθησης ή ελέγχου (Mayer et al, 1995). Ουσιαστικά, η έννοια της εμπιστοσύνης εμπεριέχει μια δυαδική σχέση μεταξύ δύο μελών, δηλαδή του μέλους που εμπιστεύεται (trustor) και του μέλους στο οποίο εκχωρείται η εμπιστοσύνη (trustee). Για παράδειγμα, στο πλαίσιο του ηλεκτρονικού εμπορίου, δύναται να εξετασθεί ο ρόλος που διαδραματίζει η εμπιστοσύνη ενός αγοραστή σε σχέση π.χ. με τον διαδικτυακό προμηθευτή ή τη διαδικασία διαδικτυακών αγορών (Papadopoulou et al., 2010).

Αντίστοιχα, η μεταβίβαση εμπιστοσύνης, είναι μια γνωστική διαδικασία κατά την οποία ένα άτομο αναπτύσσει εμπιστοσύνη σε μια οντότητα λόγω της εμπιστοσύνης της σε μια συγγενή οντότητα (Belanche et al., 2014). Σύμφωνα με τους Doney και Cannon, η εμπιστοσύνη μπορεί να μεταφερθεί από μια αξιόπιστη πηγή σε μια άλλη οντότητα, με το μέλος που εμπιστεύεται να έχει μικρή ή καθόλου άμεση εμπειρία με το αντικείμενο εμπιστοσύνης. Για παράδειγμα, ένας νέος πωλητής, που εκπροσωπεί μια εταιρεία που ο αγοραστής εμπιστεύεται, θα επωφεληθεί από την προηγούμενη εμπειρία του αγοραστή με την εταιρεία ή αντίστοιχα η προηγούμενη εμπειρία ενός αγοραστή με πωλητές οδηγεί συχνά σε μια αρχική κατάσταση δυσπιστίας για τους επόμενους πωλητές (Doney & Cannon, 1997).

Ωστόσο, η μεταβίβαση εμπιστοσύνης, σε αντίθεση με την έννοια της εμπιστοσύνης, εμπεριέχει μια σχέση μεταξύ τριών μελών, δηλαδή του μέλους που εμπιστεύεται (trustor), του μέλους στο οποίο εκχωρείται η εμπιστοσύνη (trustee) και ενός τρίτου μέλους (third party) (Stewart, 2003). Ειδικότερα, το μέλος που εμπιστεύεται (trustor) αξιολογεί αν εμπιστεύεται τα μέλη με τα οποία συνδιαλέγεται. Το μέλος στο οποίο εκχωρείται η εμπιστοσύνη (trustee) αξιολογείται με βάση την αξιοπιστία του, ενώ το τρίτο μέλος κατέχει τον ρόλο του διαμεσολαβητή.

Ο μηχανισμός μεταβίβασης που ισχύει σε αυτή την περίπτωση βασίζεται στην εξής αρχή: όταν το μέλος που εμπιστεύεται (trustor) αξιολογεί το διαμεσολαβητή (third party) ως αξιόπιστο και υπάρχει στενή σχέση μεταξύ του διαμεσολαβητή (third party) και του μέλους στο οποίο εκχωρείται η εμπιστοσύνη (trustee), τότε η εμπιστοσύνη του μέλους που εμπιστεύεται (trustor), μεταβιβάζεται στο άλλο μέλος (trustee) (Wang et al., 2013).

Σύμφωνα με τους Lee, Kang και McKnight (2007), η μεταβίβαση εμπιστοσύνης μπορεί να πραγματοποιηθεί μεταξύ συναφών ή μη οντοτήτων. Ειδικότερα, η μεταφορά εμπιστοσύνης μεταξύ συναφών οντοτήτων στο ίδιο κανάλι χαρακτηρίζεται ως μεταφορά εμπιστοσύνης εντός καναλιού (Intra-channel trust transfer), ενώ η μεταφορά εμπιστοσύνης μεταξύ δύο οντοτήτων που σχετίζονται αλλά βρίσκονται σε διαφορετικά κανάλια αποτελεί τη διακαναλική μεταφορά εμπιστοσύνης (Inter-channel trust transfer). Αντίστοιχη μελέτη τονίζει ότι η μεταφορά εμπιστοσύνης εντός καναλιού αναφέρεται στην εμπιστοσύνη ενός ατόμου σε μια οντότητα (π.χ. προϊόντα ή οργανισμούς) που μεταφέρεται σε άλλη σχετική οντότητα στο ίδιο κανάλι, ενώ η δεύτερη περίπτωση αναφέρεται στη μεταφορά εμπιστοσύνης από το ένα περιβάλλον στο άλλο, όπως π.χ. τη μεταφορά από offline σε online περιβάλλοντα (Lin et al., 2011).

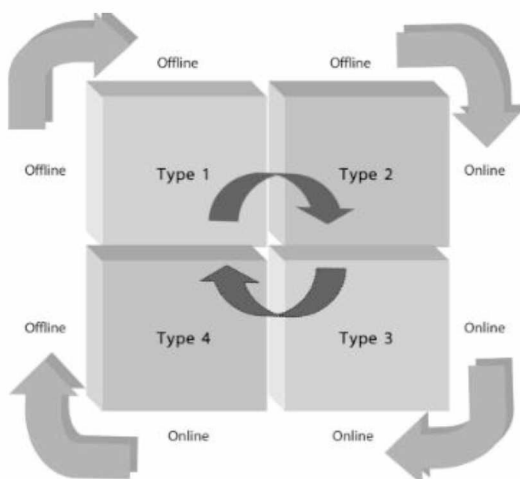
Η μεταβίβαση εμπιστοσύνης εντός καναλιού περιλαμβάνει δύο τύπους: 1) εκτός διαδικτύου (offline to offline) και 2) εντός διαδικτύου (online to online) (Stewart 2003). Ο πρώτος τύπος εξετάζει τη μεταφορά εμπιστοσύνης στο κανάλι εκτός διαδικτύου και αφορά κυρίως το παραδοσιακό περιβάλλον μάρκετινγκ. Ενδεικτικά, οι καταναλωτές που εμπιστεύονται υπολογιστές Apple που αγοράστηκαν σε ένα κατάστημα λιανικής μπορεί να εμπιστευτεί ένα προϊόν Apple που κυκλοφόρησε πρόσφατα και πωλείται σε κάποιο άλλο κατάστημα.

Ο δεύτερος τύπος επικεντρώνεται στη μεταφορά εμπιστοσύνης εντός του διαδικτυακού καναλιού, επισημαίνοντας ότι καθίσταται εφικτή η μεταφορά από μια έμπιστη διαδικτυακή πηγή σε μια άγνωστη μέσω των υπερσυνδέσεων που χρησιμοποιούν (hyperlinks). Ενδεικτικά, μια άγνωστη διαδικτυακή εταιρεία μπορεί να βελτιώσει την εμπιστοσύνη των καταναλωτών και την πρόθεση αγοράς, συνδέοντας τον εαυτό της με μια γνωστή διαδικτυακή εταιρεία (Stewart, 2006).

Στο ίδιο πλαίσιο, η διακαναλική μεταφορά εμπιστοσύνης εστιάζει στη μεταφορά εμπιστοσύνης από το ένα περιβάλλον στο άλλο, ειδικότερα από ένα κανάλι εκτός διαδικτύου (offline) σε ένα διαδικτυακό κανάλι (online). Για παράδειγμα, η εμπιστοσύνη των πελατών

στις εκτός δικτύου υπηρεσίες μιας επιχειρήσει μπορεί να επηρεάσει την αντίληψη του πελάτη για τις υπηρεσίες που προσφέρονται από την ίδια εταιρεία διαδικτυακά. Σχετικές μελέτες, μάλιστα, συνηγορούν, στο γεγονός ότι η εμπιστοσύνη των καταναλωτών σε μια εταιρεία με φυσική παρουσία στην αγορά επηρεάζει θετικά τις αντιλήψεις τους για τις διαδικτυακές υπηρεσίες της (Lin et al., 2011).

Αντίστοιχη μελέτη, αναφορικά με την μεταφορά εμπιστοσύνης από ένα περιβάλλον σε ένα άλλο προτείνεται η εξής κατηγοριοποίηση της διαδικασίας: 1) Μεταφορά εμπιστοσύνης από κανάλι εκτός διαδικτύου σε κανάλι εκτός διαδικτύου, 2) Μεταφορά εμπιστοσύνης από κανάλι εκτός διαδικτύου σε κανάλι εντός διαδικτύου, 3) Μεταφορά εμπιστοσύνης από κανάλι εντός διαδικτύου σε κανάλι εντός διαδικτύου και 4) Μεταφορά εμπιστοσύνης από κανάλι εντός διαδικτύου σε κανάλι εκτός διαδικτύου. Στην Εικόνα 4 αποτυπώνεται η σχετική κατηγοριοποίηση (Lee et al., 2007).



Εικόνα 4: Διαδικασία μεταφοράς εμπιστοσύνης (Lee et al., 2007)

Στην πρώτη περίπτωση, η εμπιστοσύνη των καταναλωτών, σε μια εταιρεία με φυσική παρουσία στην αγορά, μπορεί να επεκταθεί και στα υπόλοιπα προϊόντα ή υπηρεσίες. Χαρακτηριστικό παράδειγμα αποτελεί η εταιρεία General Electric, όπου η εμπιστοσύνη των πελατών της σε αυτή μεταβιβάζεται και σε όλους τους υπόλοιπους τομείς που δραστηριοποιείται, όπως υγειονομική περίθαλψη, ανανεώσιμη ενέργεια, κ.α.. Στην δεύτερη περίπτωση, η εμπιστοσύνη των καταναλωτών, σε μια εταιρεία με φυσική παρουσία στην αγορά μεταβιβάζεται ταυτόχρονα και στις υπηρεσίες που προσφέρει διαδικτυακά, π.χ. η Samsung Electronics Corporation διατηρεί την εμπιστοσύνη των πελατών της τόσο στην πώληση των προϊόντων σε φυσικό κατάστημα όσο και μέσω διαδικτύου.

Η τρίτη περίπτωση εστιάζει στην παρουσία εταιρειών μόνο μέσω διαδικτύου, χωρίς φυσική παρουσία στην αγορά. Αν και πολλές αμιγείς διαδικτυακές εταιρείες δεν κατόρθωσαν να συνεχίσουν την λειτουργία τους αποκλειστικά διαδικτυακά, εταιρείες με ισχυρό “brand name”, όπως η Dell Computer συνεχίζουν με επιτυχία τη λειτουργία τους διαδικτυακά. Ωστόσο, αν οι υπάρχουσες διαδικτυακές εταιρείες επιθυμούν να επεκτείνουν τα διαδικτυακά προϊόντα τους και υπηρεσίες, θα πρέπει να διατηρήσουν ή να αυξήσουν το επίπεδο εμπιστοσύνης των καταναλωτών, ώστε να παραμείνουν ανταγωνιστικές. Τέλος, η τέταρτη περίπτωση, αν και αποτελεί σπάνιο φαινόμενο, εστιάζει στην μεταφορά της εμπιστοσύνης πελατών από διαδικτυακά κανάλια σε κανάλια εκτός διαδικτύου, με τις εταιρείες να εκμεταλλεύονται τη διαδικτυακή τους φήμη (Lee et al., 2007).

Στον Πίνακα 3, αποτυπώνονται οι δυο κατηγορίες της μεταβίβασης εμπιστοσύνης, ακολουθούμενες από το θεωρητικό πλαίσιο και τη σχετική βιβλιογραφία. Σε αυτό το σημείο αξίζει να σημειωθεί, ότι η αναζήτηση σχετικών άρθρων σε έγκυρα περιοδικά ή βάσεις δεδομένων επέστρεψε ικανοποιητικό πλήθος δημοσιεύσεων, ωστόσο επιλέχθηκαν τα πιο συχνά αναφερόμενα άρθρα για κάθε κατηγορία.

Πίνακας 3: Το θεωρητικό πλαίσιο της μεταβίβασης εμπιστοσύνης

Μεταβίβαση εμπιστοσύνης	Θεωρητικό πλαίσιο	Σχετική βιβλιογραφία
Μεταβίβαση εμπιστοσύνης από οντότητα	1) Μεταβίβαση εμπιστοσύνης από οντότητα σε οντότητα εντός καναλιού (Intra-channel trust transfer) 2) Μεταβίβαση εμπιστοσύνης από οντότητα σε περιβάλλον	Ballester and Espallardo (2008), Perk and Halliday (2003), Stewart (2006)
Μεταβίβαση εμπιστοσύνης από περιβάλλον	1) Μεταβίβαση εμπιστοσύνης από περιβάλλον σε οντότητα 2) Διακαναλική μεταβίβαση εμπιστοσύνης (Inter-channel trust transfer) από περιβάλλον σε περιβάλλον <ul style="list-style-type: none"> • Offline to Offline • Offline to Online • Online to Online • Online to Offline 	Belanche et al. (2014), Doney and Cannon (1997), Lee et al. (2007), Lin et al. (2011), Wang et al. (2013), Stewart (2003)

2.2. Η χρήση φορητών εφαρμογών στη δημόσια διοίκηση

Σύμφωνα με τη Βίβλο του ψηφιακού μετασχηματισμού 2020-2025, στόχος του κυβερνητικού σχεδιασμού για μια πολιτοκεντρική Δημόσια Διοίκηση αποτελεί η παροχή εύχρηστων ψηφιακών υπηρεσιών προσανατολισμένων τόσο στις ανάγκες των πολιτών όσο και στις επιχειρήσεις που δραστηριοποιούνται στην Ελλάδα. Πολύ περισσότερο, σε μια περίοδο που οι κυβερνήσεις παγκοσμίως ήρθαν αντιμέτωπες με τη διαχείριση του COVID-19, κατέστη αναγκαίο να επιταχυνθεί ο ψηφιακός μετασχηματισμός του κρατικού μηχανισμού, αντικαθιστώντας τις υπάρχουσες γραφειοκρατικές διαδικασίες, με πιο ευέλικτα καινοτόμα μοντέλα βασισμένα στις νέες τεχνολογίες, επιτυγχάνοντας με αυτόν τον τρόπο την αδιάλειπτη λειτουργία του κράτους και της οικονομίας (Υπουργείο Ψηφιακής Διακυβέρνησης, 2020).

Ο κρατικός μηχανισμός στην Ελλάδα, παρά τις υφιστάμενες παθογένειες της Δημόσιας διοίκησης, κατόρθωσε να αντιμετωπίσει άμεσα τις προκλήσεις που αναδύθηκαν από την πανδημία του COVID-19, υλοποιώντας ένα σύνολο από ψηφιακές πρωτοβουλίες. Ενδεικτικά, το Υπουργείο Ψηφιακής Διακυβέρνησης έθεσε σε λειτουργία το ePresence, πλατφόρμα τηλεδιάσκεψης και απομακρυσμένης εργασίας για τη συνέχιση της λειτουργίας των υπηρεσιών μέσω τηλεργασίας. Το Υπουργείο Παιδείας παρείχε ψηφιακή πλατφόρμα για την εξ αποστάσεως εκπαίδευση των μαθητών όλων των βαθμίδων και των φοιτητών. Το Υπουργείο Υγείας, έθεσε σε λειτουργία την Πλατφόρμα Διαχείρισης Συνεδριών Εμβολιασμού κατά του COVID-19 και την εφαρμογή για την έκδοση πιστοποιητικών εμβολιασμού.

Επιπλέον, το Υπουργείο Εργασίας και Κοινωνικών Υποθέσεων, μέσω του πληροφοριακού συστήματος «Εργάνη», έδωσε τη δυνατότητα στους εργοδότες να δηλώσουν τους εργαζομένους που βρίσκονται σε αναστολή εργασίας και οι εργαζόμενοι μέσω της ηλεκτρονικής πλατφόρμας του ειδικού μηχανισμού στήριξης (supportemployees.services.gov.gr) να υπέβαλλαν τα αιτήματά τους για οικονομική στήριξη. Τέλος, η ψηφιοποίηση των δημόσιων υπηρεσιών επιταχύνεται πλέον με την έναρξη της λειτουργίας της κυβερνητικής πύλης «gov.gr» παρέχοντας περισσότερες από 500 ηλεκτρονικές υπηρεσίες (European Commission, 2020).

2.2.1. Η εμπιστοσύνη στη δημόσια διοίκηση και διακυβέρνηση

Η ψηφιακή διακυβέρνηση αναγνωρίζεται όλο και περισσότερο ως βασικός παράγοντας για τον μετασχηματισμό και εκσυγχρονισμό της δημόσιας διοίκησης και διακυβέρνησης. Παρά

τις τεράστιες επενδύσεις των κυβερνήσεων στην υλοποίηση ψηφιακών μέσων που θα ενισχύσουν την πρωτοβουλία αυτή, οι πολίτες εμφανίζονται απρόθυμοι να τις χρησιμοποιήσουν κατά τις συναλλαγές τους με τις δημόσιες υπηρεσίες και φορείς. Καθίσταται αξιοσημείωτο συνεπώς το γεγονός ότι ενώ οι ίδιοι πολίτες συμμετέχουν σε μέσα κοινωνικής δικτύωσης (facebook, Instagram, twitter), χρησιμοποιούν εφαρμογές ηλεκτρονικού εμπορίου (amazon, ebay), πραγματοποιούν τις τραπεζικές τους συναλλαγές online (e-banking), διστάζουν ωστόσο να χρησιμοποιήσουν τις κυβερνητικές εφαρμογές για να διεκπεραιώσουν υποθέσεις που σχετίζονται με τις δημόσιες αρχές.

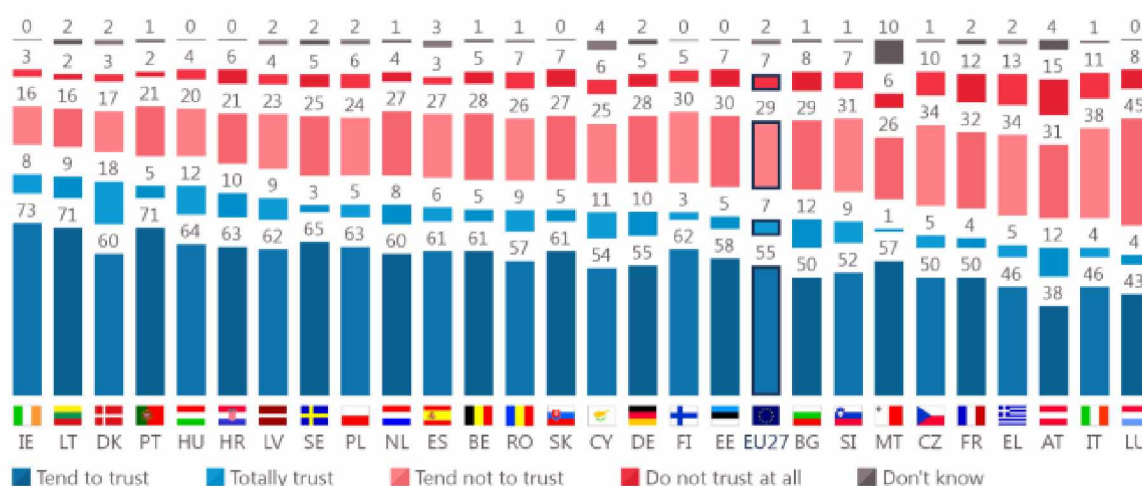
Έρευνα της Κομισιόν τα έτη 2019-2021, αναφορικά με την εμπιστοσύνη των Ευρωπαίων πολιτών 27 κρατών μελών της Ε.Ε, αναδεικνύει τη γενικευμένη μείωση του ποσοστού δυσπιστίας, με το έλλειμα εμπιστοσύνης ωστόσο να παραμένει σε υψηλά επίπεδα και την Ελλάδα να καταγράφει τα υψηλότερα ποσοστά πανευρωπαϊκά (European Commission 2019). Αν και το 2021 παρατηρείται μια μικρή αύξηση του ποσοστού εμπιστοσύνης, οι Έλληνες συνεχίζουν να δείχνουν δυσπιστία στη Δημόσια Διοίκηση (European Commission 2021). Στον Πίνακα 4, αποτυπώνονται τα ποσοστά που κατεγράφησαν σχετικά με την έλλειψη εμπιστοσύνης των Ελλήνων στους θεσμούς, με τα Πολιτικά κόμματα να παρουσιάζουν το υψηλότερο ποσοστό δυσπιστίας, ακολουθούμενα από τη Δημόσια διοίκηση, τη Βουλή των Ελλήνων και την Κυβέρνηση.

Πίνακας 4: Έλλειψη εμπιστοσύνης στους θεσμούς (European Commission 2019)

	Ευρωβαρόμετρο 92 (2019-2020)		Ευρωβαρόμετρο 94 (2020-2021)	
	Ελλάδα	M.O. EU.	Ελλάδα	M.O. EU
Πολιτικά κόμματα	92%	75%	88%	75%
Κυβέρνηση	71%	60%	71%	60%
Βουλή	75%	58%	73%	60%
Δημόσια Διοίκηση	75%	46%	76%	46%

Σε αυτό το σημείο αξίζει να σημειωθεί ότι οι συγκεκριμένες έρευνες διεξήχθησαν το διάστημα κατά οποίο όλες οι χώρες παγκοσμίως κλήθηκαν να διαχειριστούν την υγειονομική κρίση που επέφερε ο COVID-19. Σε έρευνα μάλιστα που πραγματοποιήθηκε το 2020, η πλειοψηφία των ευρωπαίων πολιτών (62%) δήλωσε ότι θα εμπιστευόταν την

Ευρωπαϊκή Ένωση στη λήψη μελλοντικών αποφάσεων για τη διαχείριση του COVID-19. Ωστόσο σε επίπεδο κρατών, η Ελλάδα συνεχίζει να παρουσιάζει υψηλά ποσοστά δυσπιστίας κατατάσσοντάς την στις τελευταίες θέσεις της λίστας των 26 χωρών-μελών της Ευρωπαϊκής ένωσης. Στην Εικόνα 5 αποτυπώνεται η τάση εμπιστοσύνης των Ευρωπαίων πολιτών των 26 χωρών στη διαχείριση του COVID-19 από την Ε.Ε. (European Commission, 2020).



Εικόνα 5: Εμπιστοσύνη πολιτών στη διαχείριση του COVID-19 από την Ε.Ε.¹

Ανεξάρτητα ωστόσο από τα επίπεδα εμπιστοσύνης που εκφράζουν οι ευρωπαίοι πολίτες στους θεσμούς, η εμπιστοσύνη αποτελεί αδιαμφισβήτητα μια σημαντική έννοια, η οποία υποστηρίζει τις περισσότερες συλλογικές και ατομικές αλληλεπιδράσεις, από τις συναλλαγές και το εμπόριο έως τα συστήματα πρόνοιας και την εκπαίδευση. Σε όλες αυτές τις περιπτώσεις, η εμπιστοσύνη επιτρέπει στα μέλη που συνδιαλέγονται, είτε πρόκειται για ανθρώπους, επιχειρήσεις ή δημόσιους οργανισμούς, να λαμβάνουν αποφάσεις χωρίς να χρειάζεται να επαναδιαπραγματευθούν ή/και να παρέχουν διαβεβαιώσεις για κάθε αλληλεπίδραση που πραγματοποιείται ανάμεσά τους. Αυτό οδηγεί στην μείωση του κόστους των επιχειρήσεων - οργανισμών και αυξάνει την ταχύτητα των κοινωνικών αλληλεπιδράσεων (OECD, 2017).

Η μεταστροφή από την παραδοσιακή μορφή διακυβέρνησης στη ψηφιακή διακυβέρνηση, η οποία ορίζεται από τα Ηνωμένα Έθνη (UN) ως η χρήση τεχνολογιών πληροφοριών και επικοινωνιών για την επίτευξη αποτελεσματικότερης διακυβέρνησης, επιφέρει σταδιακά σημαντικές αλλαγές στις δομές της δημόσιας διοίκησης. Η βασική της αρχή είναι η βελτίωση και αναδιοργάνωση του δημόσιου τομέα, μειώνοντας το οικονομικό κόστος και

¹ Πηγή: European Commission 2020

τους χρόνους συναλλαγών, αξιοποιώντας αποτελεσματικά το υπάρχον ανθρώπινο δυναμικό και τους πόρους. Ως εκ τούτου, οι κυβερνήσεις έχουν τη δυνατότητα να είναι πιο αποτελεσματικές, να παρέχουν καλύτερες υπηρεσίες και να ανταποκρίνονται στις ανάγκες των πολιτών άμεσα και με διαφάνεια (United Nations, 2020).

Παράλληλα, στόχος της ψηφιακής διακυβέρνησης είναι να προσφέρει μια ποικιλία διαδικτυακών υπηρεσιών στους πολίτες με αποτελεσματικό και οικονομικό τρόπο και να ενισχύσει την αλληλεπίδραση των ανθρώπων με την κυβέρνηση ως καταναλωτές δημοσίων υπηρεσιών και ως πολίτες. Η ενσωμάτωσή συνεπώς των φορητών εφαρμογών ευρείας χρήσης στη δημόσια διοίκηση αποβλέπει στην απλοποιημένη αλληλεπίδραση των πολιτών με τις δημόσιες υπηρεσίες, τη δήλωση προβλημάτων στις πόλεις (complaints registration), τις δημόσιες διαβουλεύσεις, την πρόσβαση σε υπηρεσίες μεταφορών (πχ. στάθμευση, bike sharing κλπ.), τις ηλεκτρονικές πληρωμές, έως και πιο πρόσφατα στην ιχνηλάτηση του ιού COVID-19 και την έκδοση πιστοποιητικών εμβολιασμού και νόσησης.

Όπως επισημαίνεται και σε έρευνα του OECD, η ψηφιακή διακυβέρνηση δεν επικεντρώνεται πλέον μόνο στη διαδικτυακή ενημέρωση και την παροχή υπηρεσιών στους πολίτες, αλλά έχει τη δυνατότητα να χρησιμοποιηθεί ως μέσο μετασχηματισμού των δομών, των διαδικασιών και της κουλτούρας του δημοσίου και να το καταστήσουν πιο αποτελεσματικό, προσανατολισμένο και διαφανές στους πολίτες. Η παροχή, συνεπώς, φορητών εφαρμογών, βασισμένων σε μοντέλα του ιδιωτικού τομέα, όπως η Uber, η Airbnb, κ.α., αποτελεί πρόκληση για κάθε κυβέρνηση, καθώς οι πολίτες αναμένουν παρόμοιες εφαρμογές από τις δημόσιες υπηρεσίες όσον αφορά τη χρηστικότητα, την προσβασιμότητα, την ευκολία και αποτελεσματικότητα (OECD, 2019).

Ειδικότερα, από τις αρχές του 2020, έτος που όλες οι χώρες του πλανήτη ήρθαν αντιμέτωπες με τον COVID-19, ο ρόλος της ψηφιακής διακυβέρνησης απέκτησε νέα δυναμική, καθώς η χρήση ψηφιακών κυβερνητικών υπηρεσιών γίνεται ευρέως διαδεδομένη στους πολίτες, αντικαθιστώντας, σε μεγάλο ποσοστό, τον συμβατικό τρόπο εξυπηρέτησης των πολιτών. Χώρες με ισχυρή και ευέλικτη ψηφιακή διακυβέρνηση κατόρθωσαν, μέσω των εθνικών τους πυλών, και των φορητών για κινητά, να παρέχουν στους πολίτες έγκυρη πληροφόρηση, μειώνοντας σημαντικά την παραπληροφόρηση και τις ψευδείς ειδήσεις. Αντιστοίχως, κυβερνήσεις που δεν είχαν επενδύσει σημαντικά σε αυτή κατόρθωσαν, σε σύντομο χρονικό διάστημα, να αναπτύξουν αντίστοιχες διαδικτυακές υπηρεσίες για την καταπολέμηση του COVID-19 (United Nations, 2020).

Σε αυτό το πλαίσιο, μελέτες που έγιναν αναφορικά με τη δημόσια διοίκηση και την ψηφιακή διακυβέρνηση ανέδειξαν ότι η εμπιστοσύνη των πολιτών στηρίζεται σε δυο πυλώνες: 1) στην άποψη που έχουν για τη συγκεκριμένη οντότητα, π.χ. εμπιστοσύνη στην κυβέρνηση και 2) στην αξιοπιστία των τεχνολογικών μέσων που χρησιμοποιεί η συγκεκριμένη οντότητα, π.χ. εμπιστοσύνη στο διαδίκτυο. (Carter & Belanger, 2005). Αντίστοιχα, ο McKnight υποστηρίζει ότι απαιτείται α ρίοφι εμπιστοσύνη σε μια σχέση στην οποία ο πολίτης δεν έχει ακόμη αξιόπιστες ή σημαντικές πληροφορίες σχετικά με τον πάροχο ηλεκτρονικών υπηρεσιών (McKnight et al., 1998).

Για να καλλιεργηθεί, συνεπώς, το κατάλληλο επίπεδο εμπιστοσύνης στους πολίτες μιας χώρας, απαιτείται τόσο εμπιστοσύνη των ιδίων στη κυβέρνηση όσο και εμπιστοσύνη στο διαδίκτυο. Μειωμένο επίπεδο εμπιστοσύνης στην κυβέρνηση σε συνδυασμό με υψηλό επίπεδο εμπιστοσύνης στο διαδίκτυο ελλοχεύει τον κίνδυνο οι πολίτες να μην εισάγουν αξιόπιστα δεδομένα στις εφαρμογές που χρησιμοποιούν. Αντίστοιχα, υψηλό επίπεδο εμπιστοσύνης στην κυβέρνηση, αλλά μειωμένο επίπεδο εμπιστοσύνης στο Διαδίκτυο υποδηλώνει την προθυμία των πολιτών να κάνουν χρήση των δημόσιων εφαρμογών, ωστόσο δεν θα αξιοποιηθούν στο έπακρο οι δυνατότητες τους (Colesca, 2009).

Ωστόσο, η έλλειψη εμπιστοσύνης των πολιτών, που προκαλείται από την καινοτομία και την αβεβαιότητα των διαδικτυακών συναλλαγών, έχει καταστεί ένα από τα σημαντικότερα εμπόδια στην ευρεία αποδοχή των δημόσιων φορητών εφαρμογών ηλεκτρονικής διακυβέρνησης. Παρά τις αυξανόμενες επενδύσεις των κυβερνήσεων σε σύγχρονες και αξιόπιστες ηλεκτρονικές υπηρεσίες και εφαρμογές, οι πολίτες παρουσιάζονται διστακτικοί να κάνουν χρήση αυτών, επιλέγοντας παραδοσιακές μεθόδους εξυπηρέτησης, όπως επίσκεψη στις κατά τόπου υπηρεσίες. Καθοριστικός παράγοντας στη μη χρήση των εφαρμογών αναδεικνύεται η έλλειψη εμπιστοσύνης στην ασφάλεια των διαδικτυακών συναλλαγών και οι ανησυχίες που εγείρονται αναφορικά με τη χρήση των πληροφοριών και δεδομένων που υποβάλλονται ηλεκτρονικά (Bélanger & Carter, 2008).

2.2.2. Οι φορητές εφαρμογές (Apps)

Οι εφαρμογές για έξυπνα κινητά τηλέφωνα, που συχνά αναφέρονται και ως συστήματα λογισμικού που λειτουργούν σε φορητές συσκευές, εξελίσσονται τα τελευταία χρόνια ραγδαία. Το 2021, κατεγράφησαν 3,48 εκατομμύρια εφαρμογές για Android κινητά, καθιστώντας το Google Play το κατάστημα με το μεγαλύτερο αριθμό διαθέσιμων εφαρμογών, ακολουθούμενη από το Apple App Store με 2,22 εκατομμύρια διαθέσιμες

εφαρμογές για iOS κινητά (Statista, 2021). Το αποτέλεσμα αυτής της αυξανόμενης τάσης, οδήγησε τις επιχειρήσεις και τους οργανισμούς να εστιάσουν στην εφαρμογή ψηφιακών στρατηγικών και να αναπτύξουν αντίστοιχα χαρτοφυλάκια, ως συμπληρωματικό κανάλι διανομής στις προσφερόμενες υπηρεσίες τους. Ωστόσο, λόγω της σχετικής τους καινοτομίας, δεν είναι ακόμη σαφές τι οδηγεί τη συμπεριφορά αποδοχής και χρήσης τους από τους πολίτες ή τους καταναλωτές (Nel & Boshoff, 2017).

Οι χρήστες έξυπνων κινητών τηλεφώνων μπορούν να χρησιμοποιήσουν διαφορετικούς τύπους εφαρμογών για κινητά, όπως τις «εγγενείς εφαρμογές» και τις «υβριδικές εφαρμογές» (Budiu 2013). Οι εγγενείς εφαρμογές εγκαθίστανται μέσω ενός καταστήματος εφαρμογών (app store) και αναπτύσσονται για μια συγκεκριμένη πλατφόρμα (π.χ. iOS ή Android), π.χ. WhatsApp, Spotify. Οι χρήστες εισέρχονται στην εφαρμογή μέσω των εικονιδίων που εγκαθίστανται στην αρχική οθόνη της συσκευής και έχουν πολλές δυνατότητες που τους διακρίνουν από τις εφαρμογές ιστού για κινητά, οι οποίες είναι απλώς ιστότοποι που έχουν σχεδιαστεί με διεπαφή χρήστη βελτιστοποιημένη για φορητές συσκευές. Οι υβριδικές εφαρμογές είναι εν μέρει εγγενείς εφαρμογές, εν μέρει υπηρεσίες κινητών και οι χρήστες μπορούν να έχουν πρόσβαση σε αυτές είτε μέσω ενός προγράμματος περιήγησης ιστού (browser) είτε μέσω των κατάστημα εφαρμογών, π.χ. Twitter, Gmail, Uber. (Lutes 2012, Nel & Boshoff 2017)

Οι φορητές εφαρμογές ακολουθούν διαφορετικά επιχειρησιακά μοντέλα και ανήκουν είτε απ' ευθείας στον πάροχο ενός ψηφιακού προϊόντος/υπηρεσίας, είτε σε κάτοχο πλατφόρμας που μεσολαβεί μεταξύ του χρήστη και του παρόχου του προϊόντος/υπηρεσίας. Επιτρέπουν δε, σε μια επιχείρηση ή οργανισμό να αλληλεπιδρά σε πραγματικό χρόνο με τους αποδέκτες της αξίας της, συλλέγοντας δεδομένα που αξιοποιούνται άμεσα από τη Διοίκηση μετριάζοντας τα κόστη της μετά πώλησης (after-sales) περιόδου. Ως εκ τούτου, οι εφαρμογές αυτές προσφέρουν έναν αποτελεσματικό τρόπο ανταλλαγής πληροφοριών σε πραγματικό χρόνο και σε ένα ευρύ φάσμα χρηστών, βελτιώνοντας την παροχή των υπηρεσιών των οργανισμών προς αυτούς. Αντίστοιχα, οι χρήστες των φορητών εφαρμογών, μπορούν να διεξάγουν τις συναλλαγές τους εν κινήσει και με ευελιξία, οποτεδήποτε και οπουδήποτε, παράλληλα με τη διεκπεραίωση άλλων δραστηριοτήτων (Nah et al., 2005).

Τα τελευταία χρόνια, όλο και περισσότερες κυβερνήσεις παγκοσμίως έχουν αρχίσει να ενσωματώνουν νέες τεχνολογίες στις ψηφιακές κυβερνητικές στρατηγικές τους για την αποτελεσματικότερη παροχή δημοσίων υπηρεσιών. Δεδομένου της πρόσφατης

υγειονομικής κρίσης, οι κυβερνήσεις στράφηκαν στην αναζήτηση νέων καινοτόμων μέσων για τον αποτελεσματικό περιορισμό της επιδημίας του COVID-19, δημιουργώντας ειδικές εφαρμογές ηλεκτρονικής διακυβέρνησης, όπως: 1) τις πύλες πληροφόρησης για τον COVID-19, 2) ηλεκτρονικές υπηρεσίες για την προμήθεια ιατρικών προϊόντων, 3) εικονικά ιατρικά ραντεβού (virtual doctors), 4) εφαρμογές αυτοδιάγνωσης (Chatbots), 5) ηλεκτρονικές άδειες μετακίνησης (online permits), 6) εφαρμογές παρακολούθησης (track and trace) και εφαρμογές για εργασία και εκμάθηση από το σπίτι (e-learning portals) (United Nations, 2020).

Ενδεικτικές καινοτόμες ψηφιακές κυβερνητικές απαντήσεις στην αντιμετώπιση του COVID-19 αποτελούν οι διαδικτυακοί πίνακες ελέγχου (dashboards) στον Καναδά και την Αυστραλία για την ανταλλαγή πληροφοριών και την παρακολούθηση της πορείας του. Στην Κίνα, τα chatbots χρησιμοποιούνται για την εκτίμηση του κινδύνου μόλυνσης των ασθενών και εφαρμόζεται μια υπηρεσία υγείας βάση κωδικών QR, όπου μέσω δημόσιων πλατφορμών για κινητά επαληθεύονται τα δεδομένα υγείας που εισάγουν οι πολίτες της. Στην Εσθονία και στη Βουλγαρία, ανέπτυξαν μια εφαρμογή που επιτρέπει στις τοπικές κυβερνήσεις να αλληλεπιδρούν άμεσα με τους κατοίκους, για την ανταλλαγή αξιόπιστων πληροφοριών και οδηγιών. Στο Λονδίνο, η χρήση, αισθητήρων και αλγορίθμων τεχνητής νοημοσύνης, που συνήθως προορίζονται για τον έλεγχο της κυκλοφορίας, χρησιμοποιούνται για τον έλεγχο της κοινωνικής απόστασης (United Nations, 2020).

Στον Πίνακα 5 αποτυπώνονται εφαρμογές που υλοποιήθηκαν στα πλαίσια της αντιμετώπισης τους COVID-19 από τις κυβερνήσεις διαφόρων κρατών της Ευρωπαϊκής Ένωσης. Στο σύνολό τους οι εφαρμογές είναι διαθέσιμες τόσο για κινητά Android όσο και για IOS, ενώ στο σύνολό τους στοχεύουν στην ανίχνευση των επαφών που έχουν έρθει σε επαφή με επιβεβαιωμένο κρούσμα.

Πίνακας 5: Κυβερνητικές εφαρμογές για την καταπολέμηση του COVID-19²

Χώρα	Όνομα εφαρμογής	Λειτουργικό σύστημα	Λειτουργικότητα
Αυστρία	Stopp Corona	Android, iOS	Ανίχνευση επαφών
Βέλγιο	Coronalert	Android, iOS	Ανίχνευση επαφών

² Πηγή: eHealth Network: https://ec.europa.eu/health/sites/default/files/ehealth/docs/covid-19_apps_en.pdf και Wikipedia: https://en.wikipedia.org/wiki/COVID-19_apps#cite_note-229

Χώρα	Όνομα εφαρμογής	Λειτουργικό σύστημα	Λειτουργικότητα
Τσεχία	eRouška	Android, iOS	Ανίχνευση επαφών
Κύπρος	CovTracer	Android, iOS	Ανίχνευση επαφών
Γερμανία	Corona-Warn-App	Android, iOS	Ανίχνευση επαφών
Γαλλία	TousAntiCovid	Android, iOS	Ανίχνευση επαφών
Ελλάδα	DOCANDU Covid Free GR	Android, iOS, Web-based	Αυτοδιάγνωση & Έκδοση πιστοποιητικών
Ιταλία	Immuni	Android, iOS	Ενημέρωση
Ολλανδία	CoronaMelder	Android, iOS	Ανίχνευση επαφών
Ισπανία	Radar COVID	Android, iOS	Ανίχνευση επαφών
Παγκόσμια	WHO Covid-19 App	Android, iOS	Ενημέρωση

Ειδικότερα στην Ελλάδα, η πρώτη εφαρμογή για έξυπνα κινητά που υλοποιήθηκε και εκτιμά τον κίνδυνο ένας πολίτης να έχει προσβληθεί από τον κορωνοϊό προκειμένου να αναζητήσει ιατρική βοήθεια, υλοποιήθηκε από Περιφέρεια Αττικής και τον Ιατρικό Σύλλογο Αθηνών και είναι διαθέσιμη στο Google Play store και στο Apple App Store. Επίσης, από τον Ιούλιο του 2021 είναι διαθέσιμη στους πολίτες, η πρώτη επίσημη κυβερνητική εφαρμογή για έξυπνα κινητά εφαρμογή «Covid Free GR», η οποία μπορεί να εγκατασταθεί σε οποιαδήποτε συσκευή χρησιμοποιεί λογισμικό iOS/Android και να χρησιμοποιηθεί για την επαλήθευση των Ευρωπαϊκών Ψηφιακών Πιστοποιητικών COVID καθώς και των ελληνικών βεβαιώσεων του gov.gr, μέσω της σάρωσης του QR Code (Ελληνική Δημοκρατία, 2021).

Όπως αναφέρεται και σε κείμενο της Commission, η πανδημία του COVID-19 έχει δημιουργήσει μια άνευ προηγουμένου πρόκληση για την Ευρωπαϊκή Ένωση και τα Κράτη-Μέλη της σε σχέση με τα συστήματα υγειονομικής περίθαλψης, την οικονομική σταθερότητα των κρατών και τον τρόπο ζωής των πολιτών. Οι ψηφιακές τεχνολογίες, συνεπώς, αποτελούν σημαντικό όπλο των κυβερνήσεων στην καταπολέμηση του COVID-19, με τις εφαρμογές για έξυπνα κινητά να υποστηρίζουν τόσο τις αρχές δημόσιας υγείας των κρατών στην παρακολούθηση και τον περιορισμό της πανδημίας, όσο και στην παροχή

απευθείας καθοδήγησης των πολιτών και στον εντοπισμό ατόμων που έχουν έρθει σε επαφή με επιβεβαιωμένο κρούσμα. (European Commission, 2020a)

Σημαντική προϋπόθεση, ωστόσο, για την αποδοχή και τη χρήση τους από τους πολίτες αποτελεί η διαβεβαίωση των κυβερνήσεων ότι οι εφαρμογές χρησιμοποιούνται αποκλειστικά για ειδικά καθορισμένους σκοπούς, ότι δεν χρησιμοποιούνται για μαζική παρακολούθηση και ότι οι χρήστες θα διατηρούν τον έλεγχο ως προς τα δεδομένα τους. Ενισχύοντας συνεπώς την εμπιστοσύνη των πολιτών τόσο στην κυβέρνηση ενισχύεται παράλληλα και η πρόθεσή τους να συμμετάσχουν στην ψηφιακή διακυβέρνηση του κράτους, αξιοποιώντας τις αντίστοιχες εφαρμογές και παρέχοντας αξιοπιστία δεδομένα στην κυβέρνηση κατά τη χρήση αυτών (Warkentin et al., 2002)

2.2.3. Η εμπιστοσύνη στις φορητές εφαρμογές

Κοινό χαρακτηριστικό της έννοιας της εμπιστοσύνης σε όλους τους επιστημονικούς κλάδους που την μελετούν είναι ότι εμπεριέχει μια δυαδική σχέση μεταξύ δύο μελών, δηλαδή του μέλους που εμπιστεύεται και του μέλους στο οποίο εκχωρείται η εμπιστοσύνη. Το μέλος στο οποίο εκχωρείται η εμπιστοσύνη παίζει καθοριστικό ρόλο στον προσδιορισμό του τι είναι η εμπιστοσύνη και στη διάκριση των διαφορετικών πτυχών από τις οποίες αποτελείται. Για παράδειγμα, στο πλαίσιο του ηλεκτρονικού εμπορίου, δύναται να εξετασθεί ο ρόλος που διαδραματίζει η εμπιστοσύνη σε σχέση με τον διαδικτυακό προμηθευτή, το Διαδίκτυο, το σύστημα ηλεκτρονικού εμπορίου, το θεσμικό περιβάλλον (Papadopoulou et al., 2010).

Καθίσταται συνεπώς σαφές ότι η έννοια της εμπιστοσύνης είναι πολλαπλή και μπορεί να διερευνηθεί σε σχέση με πολλά διαφορετικά μέλη στο οποίο εκχωρείται, όπως για παράδειγμα της εμπιστοσύνης του πολίτη στο Κράτος, στις υπηρεσίες ηλεκτρονικής διακυβέρνησης, στο πληροφοριακό σύστημα ηλεκτρονικής διακυβέρνησης και της εμπιστοσύνης στους θεσμούς. Στον Πίνακα 6 αποτυπώνονται οι διάφορες πτυχές της εμπιστοσύνης σε σχέση με την ηλεκτρονική διακυβέρνηση και τη χρήση φορητών εφαρμογών που την υποστηρίζουν. Κάθε ένας από τους τύπος εμπιστοσύνης που παρουσιάζονται θέτουν ένα σύνολο απαιτήσεων που πρέπει να πληρούνται για τη δημιουργία του αντίστοιχου τύπου εμπιστοσύνης (Papadopoulou et al., 2010).

Πίνακας 6: Η εμπιστοσύνη στις φορητές εφαρμογές³

Τύπος Εμπιστοσύνης	Περιγραφή
Εμπιστοσύνη στα δεδομένα	Ο βαθμός εμπιστοσύνης ενός πολίτη ότι τα δεδομένα που συλλέγονται και αποθηκεύονται από την κυβέρνηση μέσω πληροφοριακών συστημάτων προστατεύονται αποτελεσματικά (Horst et al., 2007).
Εμπιστοσύνη στις συναλλαγές	Ο βαθμός εμπιστοσύνης ενός πολίτη ότι τα δεδομένα που καταχωρεί μέσω μιας εφαρμογής προστατεύονται, όσον αφορά την ακεραιότητα και το απόρρητο των δεδομένων (Horst et al. 2007, Carter & Belanger 2005).
Εμπιστοσύνη στις υπηρεσίες	Ο βαθμός εμπιστοσύνης ενός πολίτη ότι το σύστημα ηλεκτρονικής διακυβέρνησης θα προσφέρει τις απαιτούμενες υπηρεσίες και ότι το αίτημά του θα διεκπεραιωθεί (Horst et al. 2007, Carter & Weerakkody, 2008).
Εμπιστοσύνη στην πληροφορία	Ο βαθμός εμπιστοσύνης ενός πολίτη ότι οι πληροφορίες που λαμβάνει διαδικτυακά είναι αξιόπιστες και ακριβείς (Gilbert et al., 2004).
Εμπιστοσύνη στο σύστημα	Ο βαθμός εμπιστοσύνης ενός πολίτη ότι η λειτουργία του συστήματος ηλεκτρονικής διακυβέρνησης δεν μπορεί να παραβιαστεί (Hung et al., 2006).
Εμπιστοσύνη στην Κυβέρνηση	Ο βαθμός εμπιστοσύνης ενός πολίτη ότι η Κυβέρνηση διαθέτει τα μέσα για να προσφέρει online υπηρεσίες (Carter & Belanger 2005, Horst et al. 2007).
Θεσμική εμπιστοσύνη	Ο βαθμός εμπιστοσύνης ενός πολίτη στην κυβέρνηση σε σχέση με το ισχύον θεσμικό πλαίσιο (Luhmann 1979, Lewis & Weigert1985).

³ Πηγή: Papadopoulou et al., 2010

▪ **Εμπιστοσύνη στα δεδομένα**

Η εμπιστοσύνη στα δεδομένα αντικατοπτρίζει το βαθμό εμπιστοσύνης ενός πολίτη ότι τα δεδομένα που συλλέγονται και αποθηκεύονται από την κυβέρνηση μέσω των πληροφοριακών συστημάτων προστατεύονται αποτελεσματικά (Horst et al., 2007). Τα επιμέρους στοιχεία που συνθέτουν την εμπιστοσύνη στα δεδομένα είναι:

- Πιστοποίηση (Authentication): Η επαλήθευση της ταυτότητας του πολίτη.
- Αυθεντικότητα (Authenticity): Η επαλήθευση της πραγματικής ταυτότητας του πολίτη, ότι είναι αυτός που ισχυρίζεται.
- Εξουσιοδότηση (Authorization): Έλεγχος πρόσβασης στα αποθηκευμένα δεδομένα των πολιτών ώστε να επιτρέπεται μόνο στους δικαιούχους.
- Εμπιστευτικότητα (Confidentiality): Διασφάλιση της προστασίας των δεδομένων από μη εξουσιοδοτημένη πρόσβαση.
- Απόρρητο (Privacy): Η διασφάλιση ότι τα δεδομένα που συλλέγονται θα χρησιμοποιούνται αποκλειστικά για τον σκοπό που συλλέχθηκαν.
- Ακεραιότητα (Integrity): Διασφάλιση ότι τα αποθηκευμένα δεδομένα προστατεύονται από μη εξουσιοδοτημένο χειρισμό ή αλλοίωση.

Συνεπώς, για να ενισχυθεί η εμπιστοσύνη των πολιτών στη χρήση εφαρμογών, μέσω έξυπνων κινητών τηλεφώνων κρίνεται απαραίτητο η κυβέρνηση να υιοθετήσει τεχνολογικά μέσα, όπως η πιστοποίηση των χρηστών με κωδικούς περιορισμένης διάρκειας, η έκδοση ψηφιακών πιστοποιητικών με τη χρήση Δημόσιου Κλειδιού (Public Key Infrastructure, PKI), βιομετρικές συσκευές, κ.α..

▪ **Εμπιστοσύνη στις συναλλαγές**

Η εμπιστοσύνη στις συναλλαγές αντικατοπτρίζει το βαθμό εμπιστοσύνης ενός πολίτη ότι τα δεδομένα που καταχωρεί μέσω μιας εφαρμογής προστατεύονται, όσον αφορά την ακεραιότητα και το απόρρητο των δεδομένων (Horst et al. 2007, Carter & Belanger 2005). Τα επιμέρους στοιχεία που συνθέτουν την εμπιστοσύνη στις συναλλαγές είναι:

- Εμπιστευτικότητα (Confidentiality): Διασφάλιση της προστασίας των δεδομένων από μη εξουσιοδοτημένη πρόσβαση.
- Ακεραιότητα (Integrity): Διασφάλιση της προστασίας των δεδομένων.
- Μη αποποίηση (Non-repudiation): Διασφάλιση ότι κανένα από τα εμπλεκόμενα μέλη της συναλλαγής δεν μπορεί να αμφισβητήσει την εγκυρότητα της.

- Απόρρητο (Privacy): Διασφάλιση ότι τα δεδομένα δεν συλλέγονται ή κοινοποιούνται χωρίς τη συγκατάθεση του πολίτη.
- Ασφάλεια (Security): Διασφάλιση ότι τα δεδομένα δεν παραποιούνται.

Για την ενίσχυση της εμπιστοσύνης των πολιτών στις συναλλαγές απαιτείται οι φορητές εφαρμογές να χρησιμοποιούν τα τυπικά πρωτόκολλα ασφαλείας, όπως SSL, TLS, HTTPS, S-HTTP και S/ MIME, τις ψηφιακές υπογραφές, την κρυπτογράφηση και την έκδοση ψηφιακών πιστοποιητικών με τη χρήση Δημόσιου Κλειδιού (PKI). Οι μηχανισμοί αυτοί θεωρούνται αποτελεσματικοί στη διασφάλιση των συναλλαγών και κατά συνέπεια στην αύξηση της εμπιστοσύνης των πολιτών.

▪ **Εμπιστοσύνη στις υπηρεσίες**

Η εμπιστοσύνη στις υπηρεσίες αντικατοπτρίζει το βαθμό εμπιστοσύνης ενός πολίτη ότι το σύστημα ηλεκτρονικής διακυβέρνησης μπορεί να προσφέρει τις απαιτούμενες υπηρεσίες και ότι το αίτημά του θα διεκπεραιωθεί (Horst et al. 2007, Carter & Weerakkody, 2008). Τα επιμέρους στοιχεία που συνθέτουν την εμπιστοσύνη στις υπηρεσίες μέσω μιας εφαρμογής έξυπνου κινητού τηλεφώνου είναι:

- Ανταπόκριση (Responsiveness): Οι προσφερόμενες υπηρεσίες θα ανταποκρίνονται αποτελεσματικά στα αιτήματα του πολίτη.
- Διαφάνεια (Transparency): Οι προσφερόμενες υπηρεσίες θα ενισχύουν την κυβερνητική λογοδοσία και τη διαφανή ενημέρωση των πολιτών.
- Αποδοτικότητα (Efficiency): Οι υπηρεσίες θα παρέχονται στους πολίτες άμεσα.
- Επικοινωνία (Communication): Οι προσφερόμενες υπηρεσίες θα υποστηρίζουν την αμφίδρομη επικοινωνία μεταξύ της κυβέρνησης και του πολίτη.
- Χρησιμότητα (Usefulness): Οι προσφερόμενες υπηρεσίες θα προσφέρουν στους πολίτες χρήσιμες πληροφορίες και λύσεις στην διεκπεραίωση αιτημάτων.
- Ευκολία χρήσης (Easy of use): Η εμπιστοσύνη στην παροχή εύκολων στη χρήση υπηρεσιών από τους πολίτες.

Για να ενισχυθεί, συνεπώς, η εμπιστοσύνη των πολιτών στη χρήση φορητών εφαρμογών θα πρέπει να διασφαλιστεί ότι οι υπηρεσίες του κράτους ανταποκρίνονται αποτελεσματικά, με διαφάνεια και δυνατότητα αμφίδρομης επικοινωνίας στα αιτήματα του πολίτη, που προσφέρονται διαδικτυακά ή με φυσική παρουσία στις κατά τόπους υπηρεσίες. Ο πολίτης, αντίστοιχα, θα πρέπει να εκλαμβάνει μια κρατική ηλεκτρονική υπηρεσία ως χρήσιμη,

αποτελεσματική, εύκολη στη χρήση και άμεση στην διεκπεραίωση των αιτημάτων του ώστε να την εμπιστευτεί και να συνεχίσει να την χρησιμοποιεί.

▪ **Εμπιστοσύνη στην πληροφορία**

Η εμπιστοσύνη στην πληροφορία αντικατοπτρίζει το βαθμό εμπιστοσύνης ενός πολίτη ότι οι πληροφορίες που λαμβάνει διαδικτυακά είναι αξιόπιστες και ακριβείς (Gilbert et al., 2004). Τα επιμέρους στοιχεία που συνθέτουν την εμπιστοσύνη στην πληροφορία είναι:

- Αξιοπιστία πληροφοριών: Η παροχή έγκυρων και αξιόπιστων πληροφοριών στους πολίτες.
- Επάρκεια πληροφόρησης: Η παροχή επαρκών πληροφοριών στους πολίτες σχετικά με το αίτημά τους.
- Συνάφεια πληροφοριών: Η παροχή σχετικών πληροφοριών στους πολίτες που σχετίζονται με το αίτημά τους.
- Κατανόηση πληροφοριών: Η παροχή κατανοητών πληροφοριών στους πολίτες.
- Ακρίβεια πληροφοριών: Η ακριβής παροχή πληροφοριών στους πολίτες.

Οι πληροφορίες που προορίζονται να διαμοιραστούν στις φορητές εφαρμογές θα πρέπει να είναι έγκυρες, συνεπείς και πλήρεις σε σχέση με τις πληροφορίες που αναρτώνται στο σύνολο των δημοσίων οργανισμών είτε μέσω ιστοσελίδων ή είτε μέσω πιο παραδοσιακών μηχανισμών. Για παράδειγμα, η χρήση χρονικών σφραγίδων τελευταίας τροποποίησης είναι ένας μηχανισμός που μπορεί να ενισχύσει την εγκυρότητα των πληροφοριών και να αυξήσει την εμπιστοσύνη των πολιτών.

▪ **Εμπιστοσύνη στο σύστημα**

Η εμπιστοσύνη στο σύστημα αντικατοπτρίζει το βαθμό εμπιστοσύνης ενός πολίτη ότι η σωστή λειτουργία του συστήματος ηλεκτρονικής διακυβέρνησης δεν μπορεί να παραβιαστεί (Hung et al., 2006). Τα επιμέρους στοιχεία που συνθέτουν την εμπιστοσύνη στο σύστημα είναι:

- Σωστή λειτουργία: Η διασφάλιση ότι το σύστημα λειτουργεί σωστά.
- Διαθεσιμότητα (Availability): Η διασφάλιση ότι το σύστημα είναι πλήρως λειτουργικό και προστατεύεται από τις κυβερνοεπιθέσεις (π.χ. Denial of Service).
- Ασφάλεια (Security). Η διασφάλιση ότι το σύστημα προστατεύεται από απειλές.
- Αποτυχία συστήματος (Failure): Η διασφάλιση ότι το σύστημα προστατεύει τα δεδομένα του χρήστη σε περίπτωση αποτυχίας του συστήματος.

- Λογοδοσία (Accountability): Η διασφάλιση ότι το σύστημα προβαίνει σε όλους τους απαραίτητους ελέγχους για την ανίχνευση και πρόληψη κυβερνοεπιθέσεων.
- Χρόνος απόκρισης (Response time): Η διασφάλιση ότι το σύστημα ανταποκρίνεται στα αιτήματα μέσα σε αποδεκτό χρονικό περιθώριο.

Η σωστή λειτουργία του συστήματος ηλεκτρονικής διακυβέρνησης παίζει εξίσου καθοριστικό ρόλο στην ενίσχυση της εμπιστοσύνης των πολιτών. Το κράτος οφείλει να φροντίσει για τη διαλειτουργικότητα των πληροφοριακών του συστημάτων, τη χρήση αρχείων καταγραφής ελέγχου (audit logs), μηχανισμού ανίχνευσης κυβερνοεπιθέσεων, προγραμμάτων ανάκτησης δεδομένων και λογισμικού προστασίας από ιούς.

▪ **Εμπιστοσύνη στην Κυβέρνηση**

Η εμπιστοσύνη στην Κυβέρνηση αντικατοπτρίζει το βαθμό εμπιστοσύνης ενός πολίτη ότι η Κυβέρνηση μέσω των πληροφοριακών της συστημάτων μπορεί να προσφέρει online υπηρεσίες (Carter & Belanger 2005, Horst et al. 2007). Τα επιμέρους στοιχεία που συνθέτουν την εμπιστοσύνη στην Κυβέρνηση είναι:

- Ικανότητα (Competence): Η εμπιστοσύνη του πολίτη στην ικανότητα της Κυβέρνησης να προσφέρει τις υπηρεσίες της απρόσκοπτα.
- Καλή πρόθεση (Benevolence): Η εμπιστοσύνη του πολίτη στην πρόθεση της Κυβέρνησης να ενεργεί με βάση το συμφέρον του και όχι καιροσκοπικά.
- Ακεραιότητα (integrity): Η εμπιστοσύνη του πολίτη στην ακεραιότητα της Κυβέρνησης ότι θα τηρήσει τις υποσχέσεις της.

Η εμπιστοσύνη στην Κυβέρνηση αποτελεί ένα σύνθετο ζήτημα και πρέπει να εξεταστεί σε ένα ενιαίο πλαίσιο. Μια τέτοια προσέγγιση περιλαμβάνει τη διάθεση όλων των υπηρεσιών της προς τους πολίτες, τόσο στο διαδίκτυο όσο εκτός σύνδεσης και την εφαρμογή ειδικά διαμορφωμένων πολιτικών σχετικά με τις διαδικασίες που θα ακολουθούνται.

▪ **Θεσμική εμπιστοσύνη**

Η θεσμική εμπιστοσύνη αντικατοπτρίζει το βαθμός εμπιστοσύνης ενός πολίτη στην κυβέρνηση ή/και στους οργανισμούς σε σχέση με το ισχύον θεσμικό πλαίσιο (Luhmann 1979, Lewis & Weigert 1985). Τα επιμέρους στοιχεία που συνθέτουν την θεσμική εμπιστοσύνη είναι:

- Νομικό και κανονιστικό πλαίσιο. Η εμπιστοσύνη του πολίτη για την ύπαρξη και εφαρμογή νόμων και κανονισμών σχετικά με διαδικτυακές συναλλαγές.

- Διεθνή πρότυπα. Η εμπιστοσύνη του πολίτη για τη χρήση διεθνών πρωτοκόλλων, προτύπων και μηχανισμών για τις online συναλλαγές.
- Ευρωπαϊκές οδηγίες: Η εμπιστοσύνη του πολίτη για τη χρήση ευρωπαϊκών οδηγιών αναφορικά με τις διαδικτυακές συναλλαγές.

Για την ενίσχυση της θεσμικής εμπιστοσύνης είναι απαραίτητο ο κρατικός μηχανισμός να προσδιορίσει τις νομικές απαιτήσεις σε σχέση με τις φορητές εφαρμογές, να διερευνήσει την επάρκεια του υφιστάμενου θεσμικού πλαισίου και να προτείνει πρόσθετα μέτρα ώστε να διασφαλίσει ότι οι παρεχόμενες υπηρεσίες μέσω των εφαρμογών πληρούν το νομικό πλαίσιο, τα διεθνή πρότυπα και τις ευρωπαϊκές οδηγίες (Papadopoulou et al., 2010).

2.2.4. Η μεταβίβαση εμπιστοσύνης στη χρήση φορητών εφαρμογών

Η ταχεία ανάπτυξη των έξυπνων τηλεφώνων και η επέκταση του ασύρματου δικτύου έχει δημιουργήσει μια κοινωνία που βρίσκεται πάντα «online», μέσω των διαφόρων εφαρμογών που είναι διαθέσιμες στο Google Play store και στο Apple App Store. Εφαρμογές για τραπεζικές συναλλαγές, ανταλλαγής μηνυμάτων και βιντεοκλήσεων, ψυχαγωγίας, υγείας, αγοράς αγαθών και χρήσης υπηρεσιών έχουν αλλάξει πολύ τον τρόπο που οι άνθρωποι ψωνίζουν, εργάζονται, διασκεδάζουν και σε ευρύτερο πλαίσιο ζουν. Παρά την ευρεία χρήση των φορητών εφαρμογών και των πλεονεκτημάτων που την συνοδεύουν, το θεωρητικό πλαίσιο και οι εμπειρικές έρευνες που μελετούν τον μηχανισμό μεταβίβασης εμπιστοσύνης είναι ακόμα σε πρώιμο στάδιο.

Όπως παρουσιάστηκε στην ενότητα 2.1.3, η μεταφορά εμπιστοσύνης ενός ατόμου σε έναν τομέα επηρεάζει τις στάσεις και τις αντιλήψεις του σε ένα άλλο τομέα. Για παράδειγμα, η εμπιστοσύνη των καταναλωτών σε ένα οργανισμό ή εταιρεία με φυσική παρουσία επηρεάζει θετικά τις αντιλήψεις τους για τις διαδικτυακές υπηρεσίες της (Lin et al., 2011). Ο μηχανισμός μεταβίβασης της εμπιστοσύνης εμπεριέχει, ουσιαστικά, μια σχέση μεταξύ τριών μελών: 1) του μέλους που εμπιστεύεται (trustor), 2) του μέλους στο οποίο εκχωρείται η εμπιστοσύνη (trustee) και 3) ενός διαμεσολαβητή (third party) (Stewart, 2003). Το μέλος που εμπιστεύεται (trustor), αξιολογεί το διαμεσολαβητή (third party) ως αξιόπιστο. Ο διαμεσολαβητής (third party), εμπιστεύεται το μέλος στο οποίο θα εκχωρηθεί η εμπιστοσύνη (trustee), οπότε η εμπιστοσύνη του μέλους που εμπιστεύεται (trustor) μεταβιβάζεται στο τρίτο μέλος (trustee) (Wang et al., 2013).

Αντίστοιχα, οι περισσότερες πρόσφατες έρευνες, αναφορικά με τη μεταβίβαση εμπιστοσύνης, εστιάζουν στον τρόπο με τον οποίο οι καταναλωτές μεταβιβάζουν την εμπιστοσύνη τους από ένα κατάστημα με φυσική παρουσία σε μια πλατφόρμα ηλεκτρονικού επιχειρείν της ίδιας εταιρείας. Αυτού του είδους η μεταφορά εμπιστοσύνης, από το ένα κανάλι στο άλλο, αναφέρεται στη βιβλιογραφία ως «διακαναλική μεταφορά εμπιστοσύνης» και επικεντρώνεται στη μεταφορά εμπιστοσύνης από κανάλι εκτός διαδικτύου σε κανάλι εντός διαδικτύου και στη μεταφορά εμπιστοσύνης από διαδικτυακό σε κανάλι για κινητά (Lin et al., 2011).

Ειδικότερα, η σταδιακή ανάπτυξη υπηρεσιών που βασίζονται σε φορητές συσκευές καθιστούν τη μεταφορά εμπιστοσύνης στο πλαίσιο του διαδικτυακού εμπορίου πιο περίπλοκη. Μελέτη των Lin et al. (2011) σχετικά με το ρόλο της διακαναλικής μεταφοράς εμπιστοσύνης στα πλαίσια της κινητής τηλεφωνίας ανέδειξε ότι η εμπιστοσύνη στις διαδικτυακές υπηρεσίες συμβάλλει άμεσα στη μεταβίβαση εμπιστοσύνης στις αντίστοιχες υπηρεσίες κινητής τηλεφωνίας. Μελέτη των Lee et al. (2011) αναφέρει ότι η εμπιστοσύνη σε τραπεζικές υπηρεσίες εκτός σύνδεσης επιδρά θετικά στις διαδικτυακές τραπεζικές συναλλαγές. Η Stewart (2003) σε μελέτη σχετικά με τον μηχανισμό μεταβίβασης εμπιστοσύνης από τα παραδοσιακά κανάλια αγορών, π.χ. φυσικό κατάστημα, σε ένα διαδικτυακό κανάλι επισημαίνει ότι η πρόθεση εμπιστοσύνης για αγορά από έναν διαδικτυακό κανάλι θα ήταν υψηλότερη, εάν εμφανιζόταν στον ιστότοπο μια εικόνα φυσικής τοποθεσίας που δημιουργεί περισσότερη εμπιστοσύνη στον καταναλωτή.

2.3. Προκλήσεις στη χρήση φορητών εφαρμογών

Η αυξανόμενη εξέλιξη των τεχνολογιών πληροφοριών και επικοινωνιών (ICT) τα τελευταία χρόνια, όπως τα έξυπνα κινητά τηλέφωνα, η Τεχνητή Νοημοσύνη (AI) και το Διαδίκτυο των Πραγμάτων (Internet of Things- IoT), αδιαμφισβήτητα βελτιώνουν την ποιότητα των καθημερινών εμπειριών των ανθρώπων. Ωστόσο, καθώς αυτές οι τεχνολογίες γίνονται ολοένα και περισσότερο πολύπλοκες, εγείρονται ανησυχίες σχετικά με την επαρκή προστασία των δεδομένων των χρηστών, τη διασφάλιση της ηθικής χρήσης των συλλεγόμενων δεδομένων και την κοινωνική επιτήρηση των πολιτών από τις κυβερνήσεις. Μάλιστα, σε πρόσφατη έρευνα, επισημαίνεται ότι οι χρήστες έχουν περιορισμένη γνώση για το είδος των προσωπικών δεδομένων που συλλέγονται και τον τρόπο που χρησιμοποιούνται ή διαμοιράζονται, συχνά εν αγνοία τους κατά τη χρήση των φορητών εφαρμογών (Yun et al., 2019).

Ειδικότερα, σε μια περίοδο που τόσο ο αριθμός των χρηστών έξυπνων κινητών όσο και ο αριθμός των εφαρμογών για έξυπνα κινητά αυξάνεται συνεχώς, οι κίνδυνοι του απορρήτου δεδομένων που ενδέχεται να θέτουν αυτές οι εφαρμογές δεν έχουν διερευνηθεί επαρκώς. Ως εκ τούτου, σημαντική προϋπόθεση για την αποδοχή τους από τους πολίτες αποτελεί η διαβεβαίωση των κυβερνήσεων ότι τα συλλεγόμενα δεδομένα χρησιμοποιούνται αποκλειστικά για ειδικά καθορισμένους σκοπούς, ότι δεν χρησιμοποιούνται για μαζική παρακολούθηση και ότι οι χρήστες θα διατηρούν τον έλεγχο ως προς αυτά (Warkentin et al., 2002).

2.3.1. Κίνδυνοι ασφάλειας και απορρήτου

Οι φορητές εφαρμογές αποτελούν πλέον αναπόσπαστο μέρος της ψηφιακής ζωής των ανθρώπων στη σημερινή κοινωνία, καθώς κατόρθωσαν να αλλάξουν τον τρόπο με τον οποίο αλληλεπιδρούν, επικοινωνούν και συνδιαλέγονται, τόσο με τις επιχειρήσεις όσο και με το δημόσιο τομέα. Ωστόσο, με τον συνεχώς αυξανόμενο όγκο δεδομένων που συλλέγονται, αποθηκεύονται και ενδεχομένως διαμοιράζονται με τρίτα μέρη, εγείρονται ανησυχίες από τους χρήστες για τον τρόπο συλλογής και διαχείρισης των προσωπικών τους πληροφοριών. Ανησυχητικό είναι επίσης το γεγονός ότι ακόμη και όταν οι χρήστες ενημερώνονται για μη εξουσιοδοτημένη πρόσβαση και κατάχρηση των προσωπικών τους πληροφοριών, όπως συνέβη στην περίπτωση των χρηστών του Facebook και της εταιρείας Cambridge Analytica, η πλειοψηφία τους εξακολουθεί να μην αλλάζει τις ρυθμίσεις για την ανταλλαγή πληροφοριών (Belanger & Crossler, 2019).

Ωστόσο, υπάρχουν σημαντικές διαφορές μεταξύ της χρήσης έξυπνων κινητών τηλεφώνων και των φορητών ή επιτραπέζιων υπολογιστών, ιδίως ότι αφορά τη διαμόρφωση των ρυθμίσεων που χρησιμοποιούνται. Για παράδειγμα, τα έξυπνα κινητά τείνουν να έχουν πολλές ρυθμίσεις «ενεργοποιημένες» για ευκολία, όπως το Bluetooth, που απαιτείται για τον συγχρονισμό ή τη σύνδεση του κινητού με άλλες φορητές συσκευές. Επιπλέον, τα λειτουργικά των έξυπνων κινητών, δεν διαθέτουν δομικά στοιχεία ασφαλείας, όπως π.χ. λογισμικό προστασίας από ιούς, τείχος προστασίας κλπ. και σε συνδυασμό με το γεγονός ότι βρίσκονται συνεχώς στην κατοχή του χρήστη και χρησιμοποιούνται σε πολλούς δημόσιους χώρους, αυξάνονται οι πιθανές απειλές παραβίασης της συσκευής και υποκλοπής των αποθηκευμένων δεδομένων (Belanger & Crossler, 2019)

Παράλληλα, οι χρήστες των έξυπνων κινητών τηλεφώνων, για να αξιοποιήσουν πλήρως τις δυνατότητες αυτών των συσκευών, επιλέγουν να κατεβάζουν από τα ηλεκτρονικά

καταστήματα διάφορες εφαρμογές στηριζόμενοι μόνο στις κριτικές και στις αξιολογήσεις άλλων χρηστών, παραβλέποντας το γεγονός ότι οι εφαρμογές είναι εκτελέσιμα αρχεία που μπορούν να χρησιμοποιηθούν για παράνομες ενέργειες ή για ανεπιθύμητη κοινή χρήση των πληροφοριών τους. Ταυτόχρονα, έρευνες αναδεικνύουν ότι η πλειονότητα των χρηστών δεν διαχειρίζονται επαρκώς τις ρυθμίσεις απορρήτου των εφαρμογών που χρησιμοποιούν και δεν διαφυλάσσουν την ασφάλεια του κινητού τους, πραγματοποιώντας τις προγραμματισμένες ενημερώσεις του λειτουργικού συστήματος της συσκευής (Crossler & Bélanger, 2017).

Σύμφωνα με τη βιβλιογραφία, οι φορητές εφαρμογές έχουν τη δυνατότητα να συλλέγουν κάθε είδους προσωπικά δεδομένα, όπως δεδομένα τοποθεσίας, προσωπικά δεδομένα, δεδομένα υγείας, δεδομένα από κάμερα, κ.α.. Παράλληλα, το σύνολο των έξυπνων κινητών τηλεφώνων διαθέτουν ενσωματωμένους διάφορους αισθητήρες, όπως μικρόφωνο, κάμερα, GPS, Wifi, κλπ., οι οποίοι αποτελούν πηγή για τη δημιουργία δεδομένων και μεταδεδομένων (metadata), σε σχέση με την τοποθεσία, το χρόνο, τη θερμοκρασία, κ.α. Αν και το μεγαλύτερο μέρος των προσωπικών δεδομένων συλλέγεται, εκ πρώτης όψεως, με τη ρητή άδεια του χρήστη, στην περίπτωση των μεταδεδομένων συμβαίνει χωρίς τη συγκατάθεση τους, εξαιτίας της προεπιλογής που υπάρχει στις ρυθμίσεις των αισθητήρων των κινητών (Mathur & Maheshwari, 2021).

Η χρήση, ωστόσο, των φορητών εφαρμογών επισκιάζεται από την ανησυχία των χρηστών ως προς την ασφάλεια και το απόρρητο των προσωπικών δεδομένων κατά τη χρήση αυτών των εφαρμογών. Χαρακτηριστικό παράδειγμα αποτελεί η εφαρμογή της εταιρεία Starbucks, όπου το 2015 παραβιάστηκαν οι λογαριασμοί των πελατών της, με αποτέλεσμα πελάτες να απεγκαταστήσουν την εφαρμογή (Balapour et al., 2020). Επιπλέον, σε έρευνα που διεξήχθη σε 940 εφαρμογές διαπιστώθηκε ότι το ένα τρίτο εξ αυτών ζητούσε από τους χρήστες να συναινέσουν στην παραχώρηση περισσότερων δικαιωμάτων από όσα είναι απαραίτητα για τη χρήση της εφαρμογής, ενώ σε έλεγχο 30 δημοφιλών εφαρμογών, οι μισές από αυτές παραχωρούσαν την τοποθεσία των χρηστών σε άλλους διακομιστές και τα δύο τρίτα χρησιμοποιούσαν τα προσωπικά δεδομένα με ύποπτο τρόπο (Herbster et al., 2016).

Σε αυτό το σημείο αξίζει να σημειωθεί ότι η αντιληπτή ασφάλεια των εφαρμογών για κινητά ορίζεται ως η αντίληψη των χρηστών ότι η λειτουργία του συστήματος δεν μπορεί να παραβιαστεί (Hung et al., 2006). Η αντίληψη, δηλαδή, ενός ατόμου για την ασφάλεια είναι το δομικό στοιχείο εμπιστοσύνης απέναντι σε οποιαδήποτε μορφή ηλεκτρονικής

συναλλαγής, η οποία μπορεί να τροφοδοτήσει τις συμπεριφορές των χρηστών, όπως η πρόθεσή τους για την παραχώρηση προσωπικών δεδομένων σε εφαρμογές κινητών. Μελέτη των Johnson et al. (2018) ανέδειξε ότι η αντίληψη των χρηστών σχετικά με την ασφάλεια των έξυπνων κινητών τηλεφώνων διαδραματίζει σημαντικό ρόλο στη διαμόρφωση της εμπιστοσύνης τους στις τραπεζικές εφαρμογές, ενώ η μελέτη των Ooi και Tan (2016) υποστηρίζει ότι η αντίληψη των χρηστών για την ασφάλεια των φορητών εφαρμογών αποτελεί έναν από τους βασικότερους παράγοντες που ενισχύουν την πρόθεση χρήσης τους.

Αντίστοιχα, το αντιληπτό απόρρητο των προσωπικών δεδομένων των εφαρμογών για κινητά ορίζεται ως η ικανότητα του ατόμου να ελέγχει πότε, πώς και σε ποιο βαθμό, οι προσωπικές του πληροφορίες κοινοποιούνται σε εφαρμογές για κινητά. Πρόσφατες μελέτες συνηγορούν στο γεγονός ότι η διασφάλιση των προσωπικών δεδομένων μπορεί να επηρεάσει, τόσο τη στάση των χρηστών σχετικά με την αποδοχή και τη χρήση των εφαρμογών για κινητά, όσο και την προθυμία τους να παραχωρήσουν τις προσωπικές τους πληροφορίες σε αυτές. Σε αντίστοιχη έρευνα που πραγματοποιήθηκε από τους Wottrich et al., (2018) διαφάνηκε ότι οι ανησυχίες των χρηστών σχετικά με την παραχώρηση των προσωπικών τους δεδομένων σε εφαρμογές επηρέασε αρνητικά τις προθέσεις τους να εγκρίνουν αιτήματα άδειας της εφαρμογής για πρόσβαση στα προσωπικά τους δεδομένα.

Στο ίδιο πλαίσιο, μελέτη των Johnson et al. (2018) σε σχέση με την πρόθεση των χρηστών να προβούν σε πληρωμές μέσω των φορητών εφαρμογών ανέδειξαν ότι η αντιληπτή ασφάλεια (perceived security) έχει θετικό αντίκτυπο στις προθέσεις των χρηστών προς τις εφαρμογές πληρωμών μέσω κινητού. Μελέτη των Balapour et al. (2020), σχετικά με τους παράγοντες που ενισχύουν ή αποθαρρύνουν τους χρήστες στο να χρησιμοποιήσουν αυτές τις εφαρμογές, αναδεικνύει ότι οι κίνδυνοι απορρήτου που συνοδεύουν τις εφαρμογές αποτελούν ανασταλτικό παράγοντα, τόσο στο να κάνουν χρήση αυτών όσο και να παραχωρήσουν τα προσωπικά τους δεδομένα σε αυτές. Ωστόσο, αν και η έννοια της ασφάλειας και η έννοια της προστασίας των προσωπικών δεδομένων είναι διακριτές, εντούτοις είναι αλληλένδετες και επηρεάζουν η μία την άλλη.

Ειδικότερα, οι ανησυχίες που εγείρονται από τους πολίτες, περί απορρήτου και ασφάλειας, επηρεάζουν σε μεγάλο βαθμό την αποδοχή και χρήση νέων τεχνολογικών καινοτομιών. Αν και στη βιβλιογραφία, η προστασία των προσωπικών δεδομένων έχει μελετηθεί ανεξάρτητα και σε συνδυασμό με την ασφάλεια, προκύπτει ότι αποτελούν εξίσου σημαντικοί παράγοντες, στη διαδικασία διαμοιρασμού ευαίσθητων πληροφοριών κατά τη χρήση του

διαδικτύου. Σχετικές μελέτες αναφορικά με τις επιπτώσεις της ασφάλειας και της ιδιωτικής ζωής, σε ατομικό και συλλογικό επίπεδο, επισημαίνουν ότι η ασφάλεια επηρεάζει θετικά την εμπιστοσύνη και στα δύο επίπεδα, αλλά η ιδιωτικότητα επηρεάζει αρνητικά την εμπιστοσύνη μόνο σε ατομικό επίπεδο (Kim et al., 2008).

Επιπρόσθετα, σε μελέτη των Belanger και Crossler (2019) διαφαίνεται ότι οι χρήστες συχνά παρουσιάζονται απρόθυμοι να εγκαταστήσουν διάφορες εφαρμογές στα κινητά τους, με τον φόβο ότι προσωπικές τους πληροφορίες μπορεί να αποκαλυφθούν και να χρησιμοποιηθούν από κακόβουλες εφαρμογές χωρίς την άδειά τους. Τα ίδια ζητήματα απορρήτου και ασφαλείας έχουν τεθεί επίσης και για τις εφαρμογές υγείας (mHealth) οι οποίες, για να παρέχουν οφέλη στους χρήστες, απαιτούν την εισαγωγή πιο ευαίσθητων προσωπικών δεδομένων, όπως π.χ. το ιατρικό ιστορικό. Ως εκ τούτου, οι χρήστες εφαρμογών υγείας αντιλαμβάνονται υψηλότερα επίπεδο κινδύνου όταν τους ζητείται να μοιραστούν πληροφορίες υγείας σε σύγκριση με άλλους τύπους πληροφοριών (Tran & Nguyen, 2021).

Ιδιαίτερα, στα πλαίσια περιορισμού του COVID-19, οι κυβερνήσεις παγκοσμίως συνεργάστηκαν με ιδιωτικές εταιρείες τεχνολογίας για τη δημιουργία συστημάτων παρακολούθησης και επιτήρησης, γεγονός που μπορεί να οδηγήσει μελλοντικά στη θέσπιση ενός ελαστικότερου νομοθετικού πλαισίου για την ασφάλεια και την προστασία των προσωπικών δεδομένων. Στο ίδιο πνεύμα, μελέτη των Brough και Martin (2021) επισημαίνει ότι νομικά, ηθικά και κοινωνικά ζητήματα, τα οποία σχετίζονται με τη χρήση συστημάτων υγείας από τους πολίτες, όπως οι εφαρμογές mMobile, πρέπει να λαμβάνονται υπόψη από τις κυβερνήσεις. Στην επιστημονική κοινότητα, μάλιστα, ήδη εγείρονται ανησυχίες ότι τα προσωπικά δεδομένα των πολιτών που χρησιμοποιούνται από την κυβέρνηση για την καταπολέμηση του COVID-19 θα συνεχίσουν να χρησιμοποιούνται και μετά το τέλος της πανδημίας.

2.3.2. Έλεγχος και επιτήρηση των πολιτών

Ο κρατικός έλεγχος και η επιτήρηση, σύμφωνα με τη βιβλιογραφία, περιλαμβάνει την παρακολούθηση, τη συλλογή και την επεξεργασία δεδομένων προσωπικού χαρακτήρα των πολιτών από το Κράτος. Αυτό μπορεί να περιλαμβάνει την παρακολούθηση της διαδικτυακής δραστηριότητας, της τοποθεσίας, των οικονομικών συναλλαγών, τη συλλογή βιομετρικών δεδομένων, κ.α., με την πλειονότητα των δεδομένων που συλλέγονται να εμπίπτουν στην κατηγορία των προσωπικών δεδομένων.

Επιστημονικοί κλάδοι, όπως η κοινωνιολογία, οι οικονομικές και οι πολιτικές επιστήμες και η φιλοσοφία θεωρούν ότι η κρατική επιτήρηση είναι θεμελιώδης τόσο για τη διακυβέρνηση όσο και για τον κοινωνικό έλεγχο, καθώς διασφαλίζει την κοινωνική τάξη. Ιδιαίτερα στα αυταρχικά καθεστώτα, αποτελεί εργαλείο εντοπισμού των εσωτερικών πολιτικών απειλών και καταστολής των διαφωνιών και επιβολή της τάξης (Eck & Hatz, 2020).

Παρόμοιες προκλήσεις αναδύονται και από την χρήση των κρατικών φορητών εφαρμογών από τους πολίτες, καθώς η εκχώρηση εμπιστοσύνης σε αυτές, εμπεριέχει τον κίνδυνο περιορισμού των συνταγματικών τους ελευθεριών. Στο δυτικό κόσμο, ιδιαίτερα έπειτα από την τρομοκρατική επίθεση της 11^{ης} Σεπτεμβρίου στην Αμερική, η δημόσια συζήτηση για την ενίσχυση της επιτήρησης των πολιτών επικεντρώθηκε στον τρόπο με τον οποίο ένας πολίτης είναι διατεθειμένος να θυσιάσει την ιδιωτικότητά του στο όνομα της ασφάλειας. Με το ξέσπασμα, ωστόσο, της πανδημίας του COVID-19 και έπειτα, το ερώτημα που πλέον τίθεται είναι έως ποιο σημείο είναι ένας πολίτης πρόθυμος να θυσιάσει την ιδιωτικότητά του για να βοηθήσει το Κράτος και τον συνάνθρωπό του (Barriga, et al., 2020).

Οι κυβερνήσεις παγκοσμίως, σε μια πρωτοφανή κίνηση για την καταπολέμηση της επιδημίας COVID-19, υιοθέτησαν συστήματα παρακολούθησης και επιτήρησης των πολιτών τους, μέσω φορητών εφαρμογών, λογισμικού αναγνώρισης προσώπου, κ.α.. Η πρώτη εφαρμογή για έξυπνα κινητά που αναπτύχθηκε το 2020, από την κυβέρνηση της Σιγκαπούρης, είναι η εφαρμογή «Trace Together». Η εφαρμογή χρησιμοποιεί την τεχνολογία Bluetooth για να αποθηκεύει πληροφορίες, όπως προσωρινούς αριθμούς ταυτότητας (IDs) και διάρκεια εγγύτητας των κινητών. Όταν ένας πολίτης έχει ενεργοποιήσει την εφαρμογή και έχει διαγνωσθεί θετικός στον COVID-19, το Υπουργείο Υγείας ανασύρει τα αποθηκευμένα δεδομένα για να κάνει ιχνηλάτηση των επαφών του. Έκτοτε, δημιουργήθηκαν διάφοροι άλλοι τύποι εφαρμογών εντοπισμού επαφών, καθεμία από τις οποίες χρησιμοποιεί διαφορετικές μεθόδους συλλογής δεδομένων.

Για παράδειγμα, στο Ηνωμένο Βασίλειο, οι τεχνολογίες «έξυπνων πόλεων» που σχεδιάστηκαν για να εξομαλύνουν τη ροή της κυκλοφορίας, χρησιμοποιούνται πλέον και για τη συμμόρφωση των πολιτών σύμφωνα με τα πρωτόκολλα κοινωνικής απόστασης (Brough & Martin, 2021). Στο Ισραήλ, αναπτύχθηκαν εφαρμογές για έξυπνα κινητά που εστιάζουν στην παρακολούθηση και ιχνηλάτηση των πολιτών, ενώ η κυβέρνηση του Ισραήλ ενδέχεται να νομιμοποιήσει αυτή της την πρωτοβουλία, ώστε να καταστεί δυνατή αυτή η μορφή επιτήρησης και στην μετα-COVID εποχή. Στην Πολωνία, μέσω της πρόσφατης

τροπολογίας που εγκρίθηκε, οι εταιρείες τηλεπικοινωνιών υποχρεώνονται να συλλέγουν και να δίνουν πρόσβαση σε δεδομένα τοποθεσίας ατόμων που έχουν μολυνθεί με COVID-19 ή είναι σε καραντίνα, με τα μέτρα αυτά να παραμείνουν σε ισχύ μέχρι το τέλος της πανδημίας.

Η κυβέρνηση της Βουλγαρίας, σύμφωνα με το νομοθετικό της πλαίσιο, υποχρεώνει τις εταιρείες τηλεπικοινωνιών να παρέχουν μεταδεδομένα στις αρμόδιες αρχές, συμπεριλαμβανομένης της αστυνομίας, για την παρακολούθηση της συμμόρφωσης των πολιτών στα μέτρα που έχουν επιβληθεί για τον περιορισμό του COVID-19. Αν και το νομοθετικό πλαίσιο καθορίζει ότι δεν απαιτείται δικαστική εντολή, ωστόσο δεν διευκρινίζει το χρονικό πλαίσιο ισχύς των μέτρων, ούτε προβλέπει την άρση τους έπειτα το πέρας της υγειονομικής κρίσης.

Η κυβέρνηση της Κροατίας στην προσπάθειά της να εισαγάγει παρόμοιες νομοθετικές τροποποιήσεις που θα επέτρεπαν την επεξεργασία δεδομένων τοποθεσίας για την «προστασία της εθνικής και δημόσιας ασφάλειας» και θα υποχρέωνε τους τηλεπικοινωνιακούς φορείς να μοιράζονται τα δεδομένα ήρθε αντιμέτωπη με την έντονη κριτική της αντιπολίτευσης και πολλών οργανώσεων για την απόσυρση του νομοσχεδίου. Αν και το νομοσχέδιο αποσύρθηκε, αυτού του είδους οι κινήσεις αναδεικνύουν την προσπάθεια πολλών κρατών να νομιμοποιήσουν, με κάθε δυνατή ευκαιρία, τον έλεγχο και την επιτήρηση των πολιτών τους (Rodriguez et al. 2020).

Αλλά ακόμη και σε χώρες, όπως η Κίνα ή η Νότια Κορέα, όπου οι πολίτες είναι πιο εξοικειωμένοι με τον κρατικό έλεγχο, χρησιμοποιήθηκαν κράνη τεχνητής νοημοσύνης για τη μέτρηση της θερμοκρασίας, μη επανδρωμένα αεροσκάφη, με δυνατότητα αναγνώρισης προσώπου για να ειδοποιήσουν όσους δεν φορούσαν μάσκες και εφαρμογές για κινητά για τον έλεγχο των μετακινήσεων των πολιτών (Brough & Martin, 2021). Ειδικότερα η Νότια Κορέα, έχει περιορίσει δραματικά το δικαίωμα των πολιτών της στην ιδιωτικότητα, καθώς η αστυνομία μπορεί να κατασχέσει τα προσωπικά δεδομένα των πολιτών που συλλέγονται στην προσπάθεια καταπολέμησης του COVID-19, όπως διευθύνσεις κατοικίας, αριθμούς τηλεφώνου, συνταγογραφήσεις, αρχεία ιατρικής περίθαλψης, χωρίς τη συγκατάθεση των πολιτών και χωρίς δικαστική επίβλεψη.

Παράλληλα όμως με την τεχνολογική ανάπτυξη των εφαρμογών αυτών, εντείνονται και οι ανησυχίες για την ιδιωτικότητα των πολιτών, τις ατομικές ελευθερίες και τη δημοκρατία. Μελέτες υποστηρίζουν ότι σε περιόδους παγκόσμιας κρίσης δικαιολογούνται ακόμη και τα

πιο ακραία αντίμετρα και ότι οι εκτεταμένες προσπάθειες των Κυβερνήσεων να ελέγξουν τις κινήσεις των πολιτών ίσως είναι προτιμότερες από τους περιορισμούς της ατομικής ελευθερίας και από το οικονομικό κόστος που απορρέει από τη συνεχή διακοπή λειτουργίας των αγορών (Abeler et al., 2020). Μάλιστα, έχει παρατηρηθεί ότι κατά τη διάρκεια καταστάσεων έκτακτης ανάγκης, ορισμένες κυβερνήσεις παρακάμπτουν τις νομοθετικές διαδικασίες και ενεργούν με βάση την εκτελεστική εξουσία, καθιστώντας τα μέτρα που λαμβάνουν λιγότερο διαφανή και δημοκρατικά νόμιμα (Rodríguez et al., 2020).

Σε αυτό το πλαίσιο, η πεποίθηση ότι η συλλογή περισσότερων δεδομένων, μέσω των φορητών εφαρμογών, θα οδηγήσει σε πιο έγκαιρη και αποτελεσματική αντιμετώπιση της υγειονομικής κρίσης του COVID-19, οδήγησε τις κυβερνήσεις να παραβλέψουν συνταγματικά κατοχυρωμένα δικαιώματα των πολιτών, ώστε να διασφαλίσουν την υγεία τους και να ελαχιστοποιήσουν τις οικονομικές απώλειες. Ωστόσο, ακόμα και αν αυτά τα αντισταθμιστικά μέτρα οδηγήσουν τα κράτη στην έξοδο από την κρίση, δεν διασφαλίζεται ότι αυτές οι τεχνολογίες δεν θα συνεχίσουν να χρησιμοποιούνται από τις κυβερνήσεις ως μέσο ελέγχου των πολιτών. Πολύ περισσότερο σε χώρες με απολυταρχικά καθεστώτα, τα μέτρα επιτήρησης και ελέγχου δύναται να ενισχύσουν την πολιτική επιτήρηση των πολιτών (Barriga et al., 2020).

Αξίζει, ωστόσο σε αυτό το σημείο να ειπωθεί ότι η επιτυχία των Κυβερνήσεων της Νότιας Κορέας, της Ταϊβάν και της Σιγκαπούρης ενάντια του COVID-19 έγκειται περισσότερο στην προθυμία των πολιτών τους να κάνουν σωστή χρήση των φορητών εφαρμογών, παραχωρώντας μέσω αυτών αληθή δεδομένα, παρά στην επιβολή των κυβερνητικών μέτρων ελέγχου και επιτήρησης των πολιτών τους. Εντούτοις, για να επιτευχθεί αυτό το επίπεδο συμμόρφωσης και συνεργασίας, στις δυτικές κοινωνίες απαιτείται εμπιστοσύνη των πολιτών στην επιστήμη, στις δημόσιες αρχές και στην τεχνολογία. Μόνο αν οι άνθρωποι εμπιστεύονται ένα σύστημα, ότι δεν τους «κατασκοπεύει», το σύστημα θα βρει ευρεία υποστήριξη στον πληθυσμό (Abeler et al., 2020).

Αδιαμφισβήτητο, ωστόσο, παραμένει το γεγονός ότι η χρήση συγκεκριμένων μέτρων παρακολούθησης δημιουργεί συγκεκριμένα είδη κοινωνικών και πολιτικών σχέσεων και συγκεκριμένα είδη πολιτών. Ένα κράτος, που έχει καλλιεργήσει την εμπιστοσύνη στους πολίτες του, ενημερώνοντάς τους με πλήρη διαφάνεια είναι πιο αποτελεσματικό από ένα αστυνομούμενο κράτος. Ωστόσο, εάν δεν υφίσταται αυτή η συνέργεια μεταξύ κράτους και πολίτη ενδέχεται τα επόμενα χρόνια η υφιστάμενη υγειονομική κρίση να αποτελέσει

κομβικό σημείο στο φαινόμενο της επιτήρησης των πολιτών. Όχι μόνο επειδή θα μπορούσε να νομιμοποιηθεί η χρήση εφαρμογών μαζικής επιτήρησης, αλλά πολύ περισσότερο γιατί θα σηματοδοτήσει μια δραματική μετάβαση από την επιτήρηση στην έννομη παρακολούθηση (Harari, 2020).

ΚΕΦΑΛΑΙΟ 3: ΈΡΕΥΝΑ ΠΕΔΙΟΥ

3.1. Σκοπός και ερευνητικοί στόχοι της έρευνας

Η ηλεκτρονική διακυβέρνηση ενός κράτους δεν μπορεί να λειτουργήσει αποτελεσματικά χωρίς την εμπιστοσύνη και την συμμετοχή των πολιτών της σε αυτή. Αν και σημαντικός αριθμός ερευνών έχει διεξαχθεί αναφορικά με το ρόλο που διαδραματίζει η εμπιστοσύνη στο ηλεκτρονικό εμπόριο (π.χ., Hoffman et al., 1999, Belanger et al., 2002, McKnight and Chervany, 2002, Van Slyke et al., 2004), μελέτες που να διερευνούν το ρόλο της εμπιστοσύνης και κατ' επέκταση την μεταβίβασή της στην υιοθέτηση της ηλεκτρονικής διακυβέρνησης βρίσκονται ακόμα σε πρώιμο στάδιο (Carter και Belanger, 2005, Welch et al., 2005, Belanger and Hiller, 2006). Ειδικότερα, σε αναζήτηση σχετικών μελετών στη διεθνή βιβλιογραφία αναδείχθηκε το περιορισμένο εύρος διερεύνησης θεμάτων που άπτονται σε ζητήματα μεταβίβασης της εμπιστοσύνης από τους χρήστες σε φορητές εφαρμογές.

Συνεπώς, υπό το πρίσμα της απροθυμίας των πολιτών να μεταβούν από τον παραδοσιακό τρόπο αλληλεπίδρασης με το Κράτος στην υιοθέτηση εφαρμογών ηλεκτρονικής διακυβέρνησης, σκοπός της παρούσας έρευνας είναι πρωτίστως να αναδειχθεί ο ρόλος της μεταβίβασης εμπιστοσύνης σε φορητές κρατικές εφαρμογές και αφετέρου να διερευνηθεί πώς οι αντιλήψεις των πολιτών σχετικά με το βαθμό εμπιστοσύνης που προσδίδουν σε αυτές και τους κινδύνους που εμπεριέχουν καθίστανται βαρόμετρο στο να ενθαρρύνουν ή να εμποδίσουν την υιοθέτηση τους.

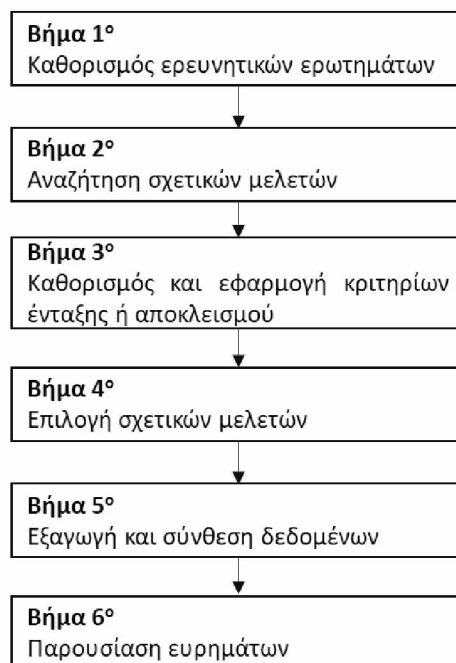
Σε αυτό το πλαίσιο, με την ολοκλήρωση της εργασίας, εκτιμάται ότι θα έχουν αποσαφηνιστεί οι παράγοντες που ενισχύουν ή αποθαρρύνουν την εμπιστοσύνη των πολιτών στη χρήση των φορητών εφαρμογών (π.χ. εμπιστοσύνη στην κυβέρνηση, εμπιστοσύνη στο διαδίκτυο).

3.2. Μεθοδολογία

Για την εκπόνηση της παρούσας μεταπτυχιακής εργασίας επιλέχθηκε η ποσοτική έρευνα, διενεργώντας: (i) Συστηματική ανασκόπηση της βιβλιογραφίας, ώστε να εξετασθεί, μέσω επιλεγμένων δημοσιεύσεων, η υπάρχουσα κατάσταση και (ii) έρευνα με τη χρήση ερωτηματολογίου, ώστε να αποτυπωθεί ποσοτικά η κατάσταση σε ένα πεπερασμένο αριθμό συμμετεχόντων.

3.2.1. Συστηματική ανασκόπηση της βιβλιογραφίας

Σύμφωνα με τη διεθνή βιβλιογραφία, για την επίτευξη υψηλής ποιότητας συστηματικών ανασκοπήσεων απαιτείται η συμμόρφωση με συγκεκριμένες αρχές, ώστε να αποφευχθούν συστηματικά και τυχαία σφάλματα. Ως εκ τούτου, σχεδιάστηκε και ακολουθήθηκε το πρωτόκολλο έρευνας, το οποίο περιλαμβάνει τα εξής 6 βήματα: 1) Καθορισμός ερευνητικών ερωτημάτων, 2) Αναζήτηση σχετικών μελετών, 3) Καθορισμός κριτηρίων ένταξης ή αποκλεισμού, 4) Επιλογή σχετικών μελετών, 5) Εξαγωγή και σύνθεση δεδομένων, 6) Παρουσίαση ευρημάτων. Σε καθένα από τα προαναφερθέντα βήματα εκτελέστηκαν συγκεκριμένες διεργασίες. Στην Εικόνα 6 αποτυπώνεται στο ερευνητικό πρωτόκολλο που ακολουθήθηκε.



Εικόνα 6: Ερευνητικό πρωτόκολλο διπλωματικής εργασίας

Βήμα 1: Καθορισμός ερευνητικών ερωτημάτων

Ο καθορισμός των ερευνητικών ερωτημάτων αποτελεί ένα από τα σημαντικότερα στάδια, καθώς καθοδηγούν την στρατηγική αναζήτησης σχετικών μελετών με το υπό διερεύνηση θέμα. Στην παρούσα μελέτη χρησιμοποιήθηκε ως εργαλείο για τη διατύπωση των ερευνητικών ερωτημάτων το πλαίσιο SPIDER, το οποίο αποτυπώνεται στον Πίνακα 7, σε σχέση με το ερευνητικό ερώτημα: «Ποιοι παράγοντες θα μπορούσαν να επηρεάσουν την εμπιστοσύνη των πολιτών κατά τη χρήση φορητών εφαρμογών που έχουν υλοποιηθεί στα πλαίσια της δημόσιας διοίκησης και διακυβέρνησης;»

Πίνακας 7: Διατύπωση ερευνητικού ερωτήματος - SPIDER

Sample	Πολίτες
Phenomenon of Interest	Παράγοντες που επηρεάζουν επηρεάσουν την εμπιστοσύνη των πολιτών κατά τη χρήση φορητών εφαρμογών
Design	Συστηματική ανασκόπηση της υπάρχουσας βιβλιογραφίας και χρήση ερωτηματολογίου
Evaluation	Καταγραφή παραγόντων
Research type	Ποσοτική

Βήμα 2: Αναζήτηση σχετικών μελετών

Κατά τον σχεδιασμό μιας ποσοτικής μελέτης, η αναζήτηση σχετικών μελετών χρησιμοποιείται για να εισαγάγει ένα πρόβλημα ή για να περιγράψει λεπτομερώς την υπάρχουσα βιβλιογραφία (Creswell, 2009). Η αναζήτηση, σχετικών με το υποδιερεύνηση θέμα, δημοσιευμένων ερευνών πραγματοποιήθηκε αξιοποιώντας τη βάση δεδομένων των Google Scholar, Scopus, Web of Science, κ.α.. Οι λέξεις κλειδιά που χρησιμοποιήθηκαν, για την εύρεση άρθρων, είναι: transfer of trust AND mobile apps (AND COVID-19), ή transfer of trust OR mobile apps (AND COVID-19), transfer of trust AND e-governance (AND COVID-19).

Βήμα 3: Καθορισμός και εφαρμογή κριτηρίων ένταξης ή αποκλεισμού

Τα κριτήρια ένταξης των άρθρων που επιλέχθηκαν είναι τα εξής: 1) Άρθρα επιστημονικών περιοδικών (Articles), 2) Άρθρα επιστημονικών συνεδρίων (Conference Papers), 3) Ανασκοπήσεις (Reviews) και 4) Κεφάλαια βιβλίων (Book chapters). Τα κριτήρια απόρριψης που θέσαμε αφορούν: 1) Άρθρα που αποτελούν ανασκοπήσεις συνεδρίων και 2) Άρθρα που είναι δημοσιευμένα σε περιοδικό με χαμηλό impact factor. Για τα επιλεγμένα άρθρα πραγματοποιήθηκε έλεγχος στο Scimago Journal & Country Rank – SJR⁴, ώστε να εξακριβωθεί ο impact factor.

Βήμα 4: Επιλογή σχετικών μελετών

Σε αυτό το στάδιο, κατεγράφησαν τα άρθρα που συγκεντρώθηκαν και διεγράφησαν τα διπλότυπα. Στη συνέχεια, για κάθε ένα από τα επιλεγμένα άρθρα, εξετάστηκε η περίληψη

⁴ <https://www.scimagojr.com>

τους και έγινε γρήγορη ανάγνωση του περιεχομένου τους. Με βάση τα προαναφερθέντα κριτήρια πραγματοποιήθηκε εκ νέου διαχωρισμός των άρθρων που τελικώς χρησιμοποιήθηκαν στα πλαίσια της διπλωματικής εργασίας.

Βήμα 5: Εξαγωγή και σύνθεση δεδομένων

Σε αυτό το στάδιο εξετάστηκαν τα επιλεγμένα άρθρα διεξοδικά και για κάθε ένα από αυτά πραγματοποιήθηκε η περίληψη τους και στη συνέχεια παράχθηκε η σύνθεση των περιλήψεων τους.

Βήμα 6: Παρουσίαση ευρημάτων

Η σύνθεση των άρθρων, κατόπιν επεξεργασίας, αποτέλεσε τη βιβλιογραφική ανασκόπηση της παρούσας μελέτης.

3.2.2. Χρήση Ερωτηματολογίου

Για τη διερεύνηση της εμπιστοσύνη που δείχνουν οι πολίτες στην Ελλάδα σε φορητές εφαρμογές ευρείας χρήσης καθώς και για την αξιολόγηση των παραγόντων που θα αυξήσουν την εμπιστοσύνη τους, χρησιμοποιήθηκε ως μέθοδος συλλογής δεδομένων το ερωτηματολόγιο. Η επιλογή του συγκεκριμένου εργαλείου προσφέρει τη δυνατότητα συλλογής δεδομένων από πολίτες διαφόρων περιοχών της Ελλάδας, ελαχιστοποιεί την πιθανότητα εσφαλμένης εισαγωγής δεδομένων, διευκολύνει την επεξεργασία τους και δεν είναι μεροληπτικό ή κατευθυνόμενο στις απαντήσεις των συμμετεχόντων.

Ειδικότερα, το ερωτηματολόγιο, το οποίο υλοποιήθηκε με τη χρήση του Google forms, περιέχει ένα ικανοποιητικό αριθμό σαφώς διατυπωμένων ερωτήσεων που καλύπτει σε αξιόλογο βαθμό τα ερευνητικά ερωτήματα και τους στόχους της έρευνας. Για τη σύνταξη του ερωτηματολογίου, αξιοποιήθηκαν αυτούσιες ερωτήσεις που έχουν χρησιμοποιηθεί σε αντίστοιχες έρευνες ενώ κάποιες εξ αυτών προσαρμόστηκαν στα ερευνητικά ζητήματα της συγκεκριμένης μελέτης. Σε αυτό το σημείο, αξίζει να σημειωθεί ότι κατά το σχεδιασμό του ερωτηματολογίου, λήφθηκε ιδιαίτερη μέριμνα ώστε η κάθε ερώτηση να είναι διατυπωμένη με τέτοιο τρόπο ώστε να μην επιδέχεται παρερμηνείες από τον ερωτώμενο και η απάντηση που θα δίνεται από τον ερωτώμενο να είναι σαφώς διατυπωμένη ώστε ο ερευνητής να καταλαβαίνει αυτό ακριβώς που θέλει να πει ο ερωτώμενος» (Saunders et al., 2015).

Αναφορικά με τον τύπο των ερωτήσεων χρησιμοποιήθηκαν ερωτήσεις κλειστού τύπου, συγκεκριμένα ερωτήσεις διαβαθμισμένης κλίμακας με τη χρήση βαθμολόγησης

συγκεκριμένης κλίμακας: 1 (Διαφωνώ απόλυτα), 2 (Διαφωνώ), 3 (Ουδέτερος), 4 (Συμφωνώ), 5 (Συμφωνώ απόλυτα).

Επιπλέον, ιδιαίτερη έμφαση δόθηκε i) στην ανωνυμία των ερωτηθέντων και στα προσωπικά τους δεδομένα, ii) στην αποφυγή χρήσης λέξεων και φράσεων που θίγουν θρησκευτικές, ιδεολογικές, φυλετικές, κ.α. πεποιθήσεις και έννοιες, (iii) στην αποφυγή ερωτήσεων που εμπεριέχουν άρνηση, (iv) στη σειρά των ερωτήσεων (πιο απλές στην αρχή, πιο σύνθετες ερωτήσεις στη μέση και κατηγοριοποίηση σε σαφείς ενότητες). Παράλληλα στην αρχή του ερωτηματολόγιου συμπεριλαμβάνεται ένα κείμενο με βάση τις οδηγίες της Αρχής Προστασίας Δεδομένων για την ανώνυμη συλλογή και επεξεργασία των δεδομένων που θα εισάγουν οι ερωτώμενοι.

Για το βαθμό κατανόησης των ερωτήσεων και της αποτελεσματικότητας του ερωτηματολογίου έγινε πιλοτικός διαμοιρασμός του σε ένα σύνολο 10 ερωτώμενων, ώστε να διενεργηθεί μια πρόιμη εκτίμηση της εγκυρότητας και της αξιοπιστίας του. Συγκεκριμένα, η εγκυρότητα αποτυπώνει το βαθμό που ένα ερωτηματολόγιο υπολογίζει τη μεταβλητή την οποία διατείνεται ότι μετρά, ενώ η αξιοπιστία τη συνέπεια με την οποία το ερωτηματολόγιο υπολογίζει την υποδιερεύνηση μεταβλητή. Καθώς τα ερωτηματολόγια πρέπει να χαρακτηρίζονται από υψηλή εγκυρότητα και αξιοπιστία (μείωση συστηματικού και τυχαίου σφάλματος), αναλόγως της ανατροφοδότησης που λάβαμε προβήκαμε σε διορθωτικές κινήσεις ως προς το σχεδιασμό του και στη συνέχεια ακολούθησε ο διαμοιρασμός του μέσω κοινωνικών δικτύων και mail.

Ο πληθυσμός της έρευνας αποτελείται από πολίτες, άνω των 18 έως 65 ετών που έχουν λογαριασμό σε κοινωνικά δίκτυα, όπως π.χ. Facebook. Αναφορικά με τη μέθοδο δειγματοληψίας επιλέχθηκε η δειγματοληψία χωρίς πιθανότητες ή δειγματοληψία κρίσης και συγκεκριμένα η δειγματοληψία της χιονόμπαλας η οποία χρησιμοποιείται ευρέως σε περιπτώσεις που δεν υπάρχει διαθέσιμο δειγματοληπτικό πλαίσιο που να καταγράφει όλα τα στοιχεία του πληθυσμού. Αυτή η τεχνική δειγματοληψίας μπορεί να συνεχίζεται έως ότου ο ερευνητής έχει αρκετά δεδομένα για να αναλύσει ώστε να παραχθούν αποτελέσματα που μπορούν να οδηγήσουν σε τεκμηριωμένες αποφάσεις (Λαγουμιντζής κ.α., 2015).

Για τον υπολογισμό του συνιστώμενου μεγέθους δείγματος χρησιμοποιήθηκε το online εργαλείο Raosoft⁵, το οποίο δίνει την δυνατότητα υπολογισμού του ελάχιστου

⁵ <http://www.raosoft.com/samplesize.html>

προτεινόμενου μέγεθους που θα πρέπει να έχει μια ποσοτική έρευνα. Θέτοντας το επίπεδο εμπιστοσύνης στο 95%, το επίπεδο απόκρισης στο 50% και το περιθώριο σφάλματος στο 5%, ο αριθμός των ερωτηματολογίων ανέρχεται σε 377. Στον Πίνακα 8 αποτυπώνονται τα εναλλακτικά σενάρια σε σχέση με το περιθώριο σφάλματος και το επίπεδο εμπιστοσύνης. Αξίζει να σημειωθεί ότι όσο αυξάνεται το μέγεθος του δείγματος μειώνεται το περιθώριο σφάλματος, ενώ όσο αυξάνεται η εμπιστοσύνη, αυξάνεται το μέγεθος δείγματος.

Πίνακας 8: Εναλλακτικά σενάρια δείγματος έρευνας

Μέγεθος δείγματος	100	200	300	Επίπεδο εμπιστοσύνης	90%	95%	99%
Περιθώριο σφάλματος	9.78%	6.89%	5.62%	Μέγεθος δείγματος	267	377	643

Τέλος, για τη στατιστική ανάλυση των δεδομένων, χρησιμοποιήθηκε το πρόγραμμα SPSS (Statistical Package for the Social Sciences) καθώς δίνει στο χρήστη τη δυνατότητα δημιουργίας αναφορών, μοντελοποίησης και ανάλυσης δεδομένων αλλά και τη γραφική αναπαράσταση αυτών.

3.3. Ερευνητικά ερωτήματα

Τα ερευνητικά ερωτήματα αποτελούν ένα από τα βασικότερα στοιχεία μια έρευνας, είτε αυτή είναι ποσοτική, είτε ποιοτική, καθώς εστιάζουν στον σκοπό και στους ερευνητικούς στόχους που έχει θέσει εξ αρχής ένας ερευνητής. Σε αυτό το πλαίσιο, καθώς ο σκοπός της παρούσας έρευνας είναι να διερευνηθεί ο ρόλος της μεταβίβασης εμπιστοσύνης σε φορητές κρατικές εφαρμογές και να καταγραφούν οι αντιλήψεις των πολιτών σχετικά με το βαθμό εμπιστοσύνης που προσδίδουν σε αυτές, διαμορφώθηκαν τα εξής ερευνητικά ερωτήματα:

E1: Ποια είναι η έννοια της μεταβίβασης εμπιστοσύνης σε φορητές εφαρμογές;

E2: Τι κίνδυνοι απορρέουν από τη μεταβίβαση εμπιστοσύνης;

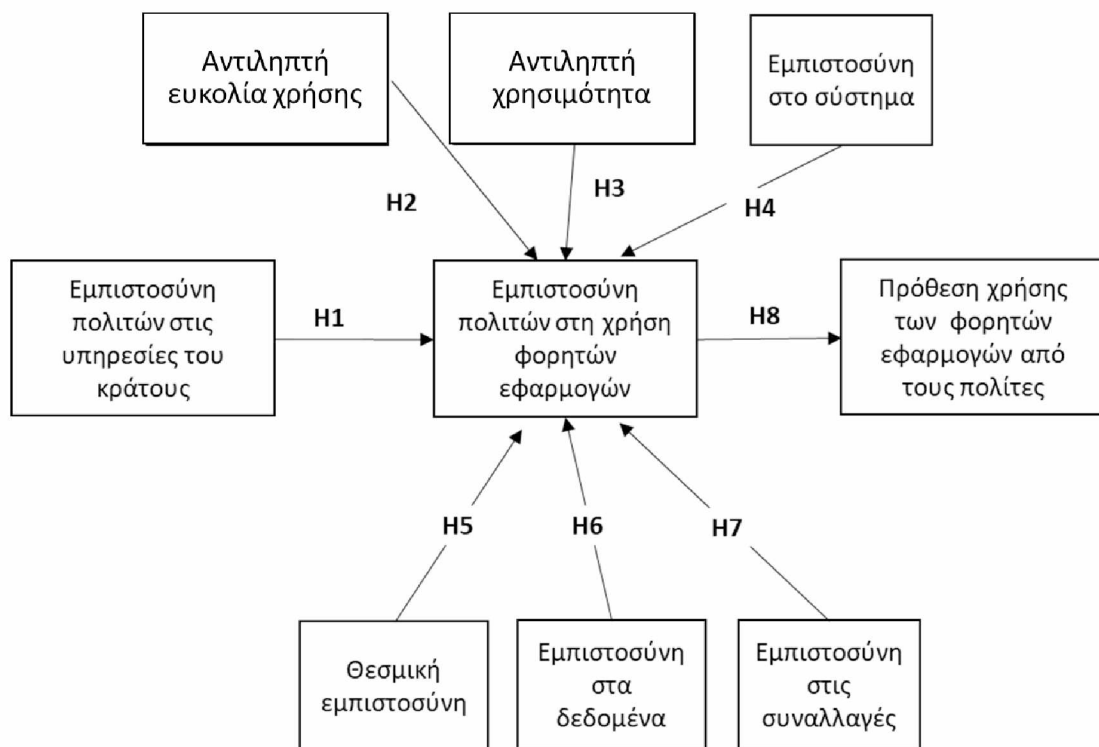
E3: Ποιοι παράγοντες θα μπορούσαν να επηρεάσουν την εμπιστοσύνη των πολιτών κατά τη χρήση φορητών εφαρμογών που έχουν υλοποιηθεί υπό κρατική αιγίδα

Για να απαντηθούν τα ερευνητικά ερωτήματα E1 και E2, διεξήχθη συστηματική ανασκόπηση της υπάρχουσας διεθνούς βιβλιογραφίας ώστε να αποτυπωθεί το πλαίσιο του υπό διερεύνηση θέματος. Για το ερευνητικό ερώτημα E3, επιλέχθηκε η χρήση του

ερωτηματολογίου, καθώς οι παράγοντες που καθορίζουν το επίπεδο εμπιστοσύνης των πολιτών στις φορητές εφαρμογές που δημιουργούνται υπό κρατική αιγίδα, αποτελούν βαρόμετρο στο να ενθαρρύνουν ή να εμποδίσουν την υιοθέτηση τους.

3.4. Ερευνητικό μοντέλο

Στην Εικόνα 7 παρουσιάζεται το ερευνητικό μοντέλο της διπλωματικής εργασίας, το οποίο βασίζεται στο μοντέλο Αποδοχής Τεχνολογίας (Technology Acceptance Model-TAM) (Davis et al., 1989) και στο μοντέλο αρχικού σχηματισμού εμπιστοσύνης McKnight (1998), τα οποία παρουσιάστηκαν εκτενώς στο Κεφάλαιο 2. Επιπρόσθετα, το ερευνητικό μοντέλο στηρίζεται στη θεωρία της μεταβίβασης εμπιστοσύνης από ένα κανάλι εκτός διαδικτύου (offline) σε ένα διαδικτυακό κανάλι (online), σύμφωνα με την οποία η μεταβίβαση εμπιστοσύνης μπορεί να επηρεάσει θετικά την αντίληψη ενός χρήστη για τις υπηρεσίες που προσφέρονται από το ίδιο κανάλι διαδικτυακά (Lin et al., 2011). Αντίστοιχα, η έννοια της εμπιστοσύνης σε ένα online περιβάλλον μπορεί να διερευνηθεί σε σχέση με δομικά στοιχεία, όπως η εμπιστοσύνη στις υπηρεσίες, στο σύστημα, στις συναλλαγές, στα δεδομένα και στη θεσμική εμπιστοσύνη και το ρόλο που διαδραματίζουν στην πρόθεση ενός πολίτη να χρησιμοποιήσει ή μη τις φορητές εφαρμογές (Paradourou et al., 2010).



Εικόνα 7: Ερευνητικό μοντέλο

3.5. Ερευνητικές υποθέσεις

Οι ερευνητικές υποθέσεις αποτελούν δηλώσεις σχετικά με το αναμενόμενο αποτέλεσμα του υπό διερεύνηση ερευνητικού ερωτήματος. Ως εκ τούτου, για να εξεταστεί το ερευνητικό ερώτημα Ε3 και να αποσαφηνιστούν οι παράγοντες που ενισχύουν την εμπιστοσύνη των πολιτών και κατ' επέκταση την πρόθεση ενός πολίτη να χρησιμοποιήσει ή μη τις φορητές εφαρμογές δημιουργήθηκαν οι εξής υποθέσεις:

Ερευνητική Υπόθεση Η1: Η εμπιστοσύνη ενός πολίτη στην Κυβέρνηση επηρεάζει θετικά την εμπιστοσύνη του στη χρήση φορητών εφαρμογών (TGS).

Ερευνητική Υπόθεση Η2: Η ευκολία χρήσης των φορητών εφαρμογών επηρεάζει θετικά την εμπιστοσύνη των πολιτών στις φορητές εφαρμογές ευρείας χρήσης (PEU).

Ερευνητική Υπόθεση Η3: Η χρησιμότητα των φορητών εφαρμογών επηρεάζει θετικά την εμπιστοσύνη των πολιτών στις φορητές εφαρμογές ευρείας χρήσης (PU).

Ερευνητική Υπόθεση Η4: Η εμπιστοσύνη ενός πολίτη ότι η λειτουργία του συστήματος ηλεκτρονικής διακυβέρνησης δεν μπορεί να παραβιαστεί επηρεάζει θετικά την εμπιστοσύνη στις φορητές εφαρμογές ευρείας χρήσης (TSY) .

Ερευνητική Υπόθεση Η5: Η εμπιστοσύνη των πολιτών ότι τα δεδομένα που συλλέγονται και αποθηκεύονται ηλεκτρονικά προστατεύονται επηρεάζει θετικά την εμπιστοσύνη στις φορητές εφαρμογές ευρείας χρήσης (TD).

Ερευνητική Υπόθεση Η6: Η εμπιστοσύνη ενός πολίτη ότι τα δεδομένα που καταχωρεί μέσω μιας εφαρμογής δεν παραποιούνται, επηρεάζει θετικά την εμπιστοσύνη στις φορητές εφαρμογές ευρείας χρήσης (TT).

Ερευνητική Υπόθεση Η7: Η εμπιστοσύνη των πολιτών στο ισχύον νομικό και θεσμικό πλαίσιο επηρεάζει θετικά την εμπιστοσύνη στις φορητές εφαρμογές ευρείας χρήσης (IT).

Ερευνητική Υπόθεση Η8: Η εμπιστοσύνη των πολιτών στη χρήση φορητών εφαρμογών έχει θετικό αντίκτυπο στην πρόθεσή τους να τα χρησιμοποιήσουν (IU).

3.6. Το ερωτηματολόγιο της έρευνας

Η δημιουργία ερωτήσεων που μετρούν με ακρίβεια τις απόψεις, τις εμπειρίες και τις συμπεριφορές του πληθυσμού μιας έρευνας αποτελεί κομβικό στοιχείο για την επιτυχή διεξαγωγή της. Η αναζήτηση στη βιβλιογραφία σταθμισμένου ερωτηματολογίου, σχετικού

με το υπό διερεύνηση θέμα, δεν επέστρεψε ικανοποιητικά αποτελέσματα, ως εκ τούτου σχεδιάστηκε εξ' αρχής νέο ερωτηματολόγιο βασισμένο σε παρόμοιες έρευνες των: Bélanger & Carter 2008, Belanche et al. 2014, Colesca 2009, Davis 1989, Lee et al. 2007 και Ayyash et al. 2011. Στον Πίνακα 9 αποτυπώνεται το ερωτηματολόγιο της έρευνας.

Πίνακας 9: Το ερωτηματολόγιο της έρευνας

Κοινωνιοδημογραφικοί παράγοντες	
Ηλικία	18-30 31-40 41-50 51-65
Φύλο	Άντρας Γυναίκα
Εκπαίδευση	Γυμνάσιο Λύκειο ΙΕΚ ΑΕΙ/ΤΕΙ Μεταπτυχιακό Διδακτορικό
Επάγγελμα	Φοιτητής Άνεργος Δημόσιος Υπάλληλος Ιδιωτικός Υπάλληλος Ελεύθερος Επαγγελματίας
Εμπειρία στη χρήση του διαδικτύου	Καθόλου Λίγο Πολύ Πάρα πολύ
Εμπιστοσύνη στις υπηρεσίες του κράτους -TGS	TGS1 Οι πολίτες εμπιστεύονται τις υπηρεσίες του κράτους για τη διεκπεραίωση των αιτημάτων τους. TGS2 Οι ηλεκτρονικές υπηρεσίες του κράτους ανταποκρίνονται αποτελεσματικά στα αιτήματα του πολίτη.

Αντιλαμβανόμενη Ευκολία Χρήσης	PEU1	Οι ηλεκτρονικές υπηρεσίες του κράτους είναι εύκολες στη χρήση.
	PEU2	Οι ηλεκτρονικές υπηρεσίες του κράτους παρέχουν κατανοητές οδηγίες για τον τρόπο χρήσης των υπηρεσιών.
	PEU3	Οι ηλεκτρονικές υπηρεσίες του κράτους είναι εύκολα προσβάσιμες από το κινητό.
	PEU4	Οι ηλεκτρονικές υπηρεσίες του κράτους είναι εύκολες στην πλοήγηση από κινητό.
	PEU5	Οι ηλεκτρονικές υπηρεσίες του κράτους δεν απαιτούν επιπλέον χρόνο και κόπο σε σχέση με την αυτοπρόσωπη εξυπηρέτηση στις κατά τόπους υπηρεσίες.
Αντιλαμβανόμενη Χρησιμότητα - PU	PU1	Οι ηλεκτρονικές υπηρεσίες του κράτους παρέχουν χρήσιμες πληροφορίες στον πολίτη.
	PU2	Οι ηλεκτρονικές υπηρεσίες του κράτους ενισχύουν την αμφίδρομη επικοινωνία πολίτη-κράτους.
	PU3	Οι ηλεκτρονικές υπηρεσίες του κράτους διεκπεραιώνουν αποτελεσματικά τα ζητήματα των πολιτών χωρίς να απαιτείται φυσική παρουσία.
Εμπιστοσύνη στο σύστημα -TSY	TSY1	Αισθάνομαι ότι είναι ασφαλές να χρησιμοποιήσω μια υπηρεσία ηλεκτρονικής διακυβέρνησης.
	TSY2	Η Κυβέρνηση λαμβάνει όλα τα απαραίτητα μέτρα για τη σωστή λειτουργία των πληροφοριακών της συστημάτων.
	TSY3	Η Κυβέρνηση λαμβάνει όλα τα απαραίτητα μέτρα για την προστασία των πληροφοριακών συστημάτων της από απειλές.
	TSY4	Πιστεύω ότι οι κίνδυνοι υπερτερούν των οφελών από τη χρήση μιας υπηρεσίας ηλεκτρονικής διακυβέρνησης.

Εμπιστοσύνη στα δεδομένα - TD	TD1	Η κυβέρνηση διασφαλίζει την προστασία των προσωπικών μου δεδομένων από μη εξουσιοδοτημένη πρόσβαση.
	TD2	Η κυβέρνηση διασφαλίζει ότι τα δεδομένα που συλλέγονται θα χρησιμοποιούνται αποκλειστικά για τον σκοπό που συλλέχθηκαν.
Εμπιστοσύνη στις συναλλαγές TT	TT1	Η κυβέρνηση διασφαλίζει ότι τα δεδομένα που συλλέγονται δεν κοινοποιούνται σε άλλους φορείς/υπηρεσίες χωρίς τη συγκατάθεση μου.
Θεσμική εμπιστοσύνη – IT	IT1	Η κυβέρνηση λαμβάνει όλα τα απαραίτητα νομικά μέτρα για την προστασία μου.
Πρόθεση Χρήσης – IU	IU	Σκοπεύω να χρησιμοποιήσω τις κρατικές φορητές εφαρμογές.

ΚΕΦΑΛΑΙΟ 4: ΑΠΟΤΕΛΕΣΜΑΤΑ ΕΡΕΥΝΑΣ

4.1. Η στατιστική ανάλυση

Για τη στατιστική ανάλυση των δεδομένων που συλλέχθηκαν χρησιμοποιήθηκε το Statistical Package for the Social Sciences – SPSS, το οποίο αποτελεί ένα πακέτο λογισμικού που χρησιμοποιείται από αρκετά επιστημονικά πεδία, για τη διαχείριση σύνθετων στατιστικών αναλύσεων. Η ανάγκη για ένα στατιστικό πακέτο προκύπτει λόγω της πολυπλοκότητας των υπολογισμών που περιλαμβάνονται σε αυτό, καθώς δίνει στο χρήστη τη δυνατότητα δημιουργίας αναφορών, μοντελοποίησης και ανάλυσης δεδομένων αλλά και τη γραφική αναπαράσταση αυτών. Για την ολοκλήρωση της παρούσας έρευνας χρησιμοποιήθηκε η IBM SPSS Statistics v26 έκδοση για λειτουργικά συστήματα Windows 32bit.

Ο πληθυσμός της έρευνας αποτελείται από πολίτες, άνω των 18 έως 65 ετών που έχουν λογαριασμό σε κοινωνικά δίκτυα, όπως π.χ. Facebook. Για τον υπολογισμό του συνιστώμενου μεγέθους δείγματος, όπως αναλύθηκε στην Ενότητα 3.2.2., χρησιμοποιήθηκε το online εργαλείο Raosoft, θέτοντας το επίπεδο εμπιστοσύνης στο 95%, το επίπεδο απόκρισης στο 50% και το περιθώριο σφάλματος στο 5%, υποδεικνύοντας το μέγεθος δείγματος του σε 377. Ωστόσο, στο διάστημα από 18/10- 25/10 που το ερωτηματολόγιο ήταν αναρτημένο συγκεντρώθηκαν 353 απαντήσεις. Στον Πίνακα 10 αποτυπώνεται το επίπεδο εμπιστοσύνης και το περιθώριο σφάλματος σε σχέση με το επιτευχθέν μέγεθος δείγματος, τα οποία παρουσιάζουν αποκλίσεις σε σχέση με τις εκτιμώμενες προβλέψεις, παραμένοντας όμως σε ικανοποιητικά επίπεδα.

Πίνακας 10: Μέγεθος δείγματος, επίπεδο εμπιστοσύνης, περιθώρια σφάλματος

Μέγεθος δείγματος	Επίπεδο εμπιστοσύνης	Περιθώριο σφάλματος
353	94.2%	5.16%

4.2. Έλεγχος αξιοπιστίας - Cronbach 's a

Στον Πίνακα 11, αποτυπώνεται η τιμή του δείκτη Cronbach's a στο σύνολο των 20 ερωτήσεων που τέθηκαν στην έρευνα, ο οποίος στην παρούσα εργασία, αποδείχθηκε εξαιρετικά υψηλός (Cronbach's a= 0,915), γεγονός που αναδεικνύει ότι το ερωτηματολόγιο διαθέτει εσωτερική συνέπεια. Σύμφωνα με τη βιβλιογραφία για να θεωρηθεί ένα

ερωτηματολόγιο αξιόπιστο θα πρέπει ο δείκτης αξιοπιστίας Cronbach's α να είναι μεγαλύτερος του 0,70 και για την εξαγωγή αξιόπιστων συμπερασμάτων τουλάχιστον $\alpha \geq 0,9$ (Nunnally & Bernstein, 1994).

Πίνακας 11: Εσωτερική συνέπεια - Cronbach's Alpha

Reliability Statistics	
Cronbach's Alpha	N of Items
,915	20

Στον Πίνακα 12, στη στήλη «Corrected Item-Total Correlation» περιλαμβάνεται η συσχέτιση κάθε ερώτησης με το συνολικό άθροισμα των υπολοίπων ερωτήσεων. Η συσχέτιση έχει υπολογιστεί με το δείκτη γραμμικής συσχέτισης r του Pearson. Παράλληλα, η τελευταία στήλη του Πίνακα «Cronbach's Alpha if Item deleted» αποτυπώνει την τιμή που θα λάβει ο δείκτης α του Cronbach, για κάθε ερώτηση, σε περίπτωση που επιλεγθεί να μην συμπεριληφθεί στην ανάλυση. Εάν η αφαίρεση κάποιας ερώτησης αναμένεται να βελτιώσει σημαντικά την τιμή του δείκτη αξιοπιστίας, τότε θα μπορούσε αυτή να μπορούσε να αφαιρεθεί. Ωστόσο, σύμφωνα με τα αποτελέσματα οι τιμές του δείκτη κυμαίνονται από 0,906 έως 0,927, οπότε δεν κρίνεται σκόπιμο να παραλειφθεί κάποια ερώτηση.

Πίνακας 12: Συνολικά στατιστικά

Item-Total Statistics				
	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
TGS1	68,04	129,967	,612	,909
TGS2	68,16	131,562	,631	,909
PEU1	68,00	134,974	,535	,911
PEU2	68,08	134,309	,509	,912
PEU3	68,18	131,967	,554	,911
PEU4	68,48	131,006	,560	,911

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
PEU5	67,46	134,334	,443	,913
PU1	67,58	135,426	,559	,911
PU2	68,23	131,681	,543	,911
PU3	67,76	132,970	,490	,912
TSY1	67,93	129,370	,625	,909
TSY2	68,35	127,036	,724	,906
TSY3	68,36	128,117	,717	,907
TSY4	69,28	142,748	,017	,927
TD1	68,34	126,856	,718	,907
TD2	68,47	127,653	,681	,907
TT1	68,44	126,395	,685	,907
TT2	68,03	128,939	,685	,908
IT1	68,38	127,287	,737	,906
IU1	67,50	134,779	,474	,912

4.3. Περιγραφική στατιστική

Η περιγραφική στατιστική (descriptive statistics) αποτελεί μια συνοπτική και αποτελεσματική παρουσίαση των δεδομένων μιας στατιστικής έρευνας. Για κάθε ενότητα του ερωτηματολογίου αποτυπώνεται σε πίνακα το ποσοστό απαντήσεων των συμμετεχόντων και τα αποτελέσματα της περιγραφικής στατιστικής, όπως την: Ελάχιστη τιμή, Μέγιστη τιμή, Μέση τιμή και την Τυπ. Απόκλιση.

4.3.1. Το προφίλ των συμμετεχόντων

Στον Πίνακα 13 αποτυπώνονται τα αποτελέσματα των δημογραφικών των συμμετεχόντων.

Πίνακας 13: Το προφίλ των συμμετεχόντων

	Συχνότητα	Ποσοστό
Φύλο		
Άνδρας	157	44,5%
Γυναίκα	196	55,5%
Ηλικία		
18-30	39	11,0%
31-40	100	28,3%
41-50	160	45,3%
51-65	54	15,3%
Εκπαίδευση		
Γυμνάσιο	6	1,7%
Λύκειο	17	4,8%
ΙΕΚ	21	5,9%
ΑΕΙ/ΤΕΙ	142	40,2%
Μεταπτυχιακό	141	39,9%
Διδακτορικό	26	7,4%
Επάγγελμα		
Φοιτητής	8	2,3%
Άνεργος	20	5,7%
Δημόσιος Υπάλληλος	121	34,3%
Ιδιωτικός Υπάλληλος	102	28,9%
Ελεύθερος Επαγγελματίας	95	26,9%
Οικιακά	2	0,6%
Συνταξιούχος	2	0,6%
Εμπειρία		
Καθόλου	0	0
Λίγο	16	4,5%
Μέτρια	48	13,6%
Πολύ	124	35,1%
Πάρα πολύ	165	46,7%

4.3.2. Ποσοστά απαντήσεων ανά ενότητα

Στον Πίνακα 14 αποτυπώνονται οι απαντήσεις των συμμετεχόντων ανά ενότητα.

Πίνακας 14: Ποσοστά απαντήσεων ανά ενότητα

	1 (Διαφωνώ απόλυτα).	2 (Διαφωνώ)	3 (Ουδέτερος)	4 (Συμφωνώ)	5 (Συμφωνώ απόλυτα)
TGS1	4 (1,1%)	45 (12,7%)	85 (24,1%)	137 (38,8%)	82 (23,2%)
TGS2	3 (0,8%)	31 (8,8%)	128 (36,3%)	141 (39,9%)	50 (14,2%)
PEU1	2 (0,6%)	11 (3,1%)	112 (31,7%)	179 (50,7%)	49 (13,9%)
PEU2	2 (0,6%)	34 (9,6%)	91 (25,8%)	182 (51,6%)	44 (12,5%)
PEU3	7 (2,0%)	35 (9,9%)	123 (34,8%)	130 (36,8%)	58 (16,4%)
PEU4	13 (3,7%)	65 (18,4%)	131 (37,1%)	104 (29,5%)	40 (11,3%)
PEU5	4 (1,1%)	20 (5,7%)	37 (10,5%)	105 (29,7%)	187 (53%)
PU1	0	6 (1,7%)	43 (12,2%)	194 (55%)	110 (31,2%)
PU2	2 (0,6%)	59 (16,7%)	109 (30,9%)	122 (34,6%)	61 (17,3%)
PU3	2 (0,6%)	30 (8,5%)	69 (19,5%)	126 (37,5%)	126 (37,5%)
TSY1	8 (2,3%)	40 (11,3%)	54 (15,3%)	159 (45%)	92 (26,1%)
TSY2	11 (3,1%)	57 (16,1%)	125 (35,4%)	105 (29,7%)	55 (15,6%)
TSY3	7 (2%)	54 (15,3%)	141 (39,9%)	100 (28,3%)	51 (14,4%)
TSY4	96 (27,2%)	117 (33,1%)	51 (14,4%)	60 (17%)	29 (8,2%)
TD1	12 (3,4%)	50 (14,2%)	141 (39,9%)	85 (24,1%)	65 (18,4%)
TD2	17 (4,8%)	59 (16,7%)	138 (39,1%)	90 (25,5%)	49 (13,9%)
TT1	18 (5,1%)	70 (19,8%)	113 (32%)	92 (26,1%)	60 (17%)
TT2	2 (0,6%)	31 (8,8%)	126 (35,7%)	103 (29,2%)	91 (25,8%)
IT1	14 (4%)	44 (12,5%)	144 (40,8%)	102 (28,9%)	49 (13,9%)
IU1	0	16 (4,5%)	48 (13,6%)	124 (35,1%)	165 (46,7%)

4.3.3. Αποτελέσματα περιγραφικής στατιστικής ανά ενότητα

Στον Πίνακα 14 αποτυπώνονται το πλήθος των απαντήσεων, η ελάχιστη και μέγιστη τιμή, η μέση τιμή και η τυπική απόκλιση για το σύνολο των ενοτήτων.

Πίνακας 15: Αποτελέσματα περιγραφικής στατιστικής

	N	Ελάχιστη τιμή	Μέγιστη τιμή	Μέση τιμή	Τυπ. απόκλιση
TGS1	353	1	5	3,70	1,000
TGS2	353	1	5	3,58	0,869
PEU1	353	1	5	3,74	0,753
PEU2	353	1	5	3,66	0,839
PEU3	353	1	5	3,56	0,946
PEU4	353	1	5	3,26	1,006
PEU5	353	1	5	4,28	0,943
PU1	353	2	5	4,16	0,692
PU2	353	1	5	3,51	0,983
PU3	353	1	5	3,97	0,972
TSY1	353	1	5	3,81	1,019
TSY2	353	1	5	3,39	1,030
TSY3	353	1	5	3,38	0,976
TSY4	353	1	5	2,46	1,277
TD1	353	1	5	3,40	1,048
TD2	353	1	5	3,27	1,049
TT1	353	1	5	3,30	1,121
TT2	353	1	5	3,71	0,967
IT1	353	1	5	3,36	0,999
IU1	353	2	5	4,24	0,854

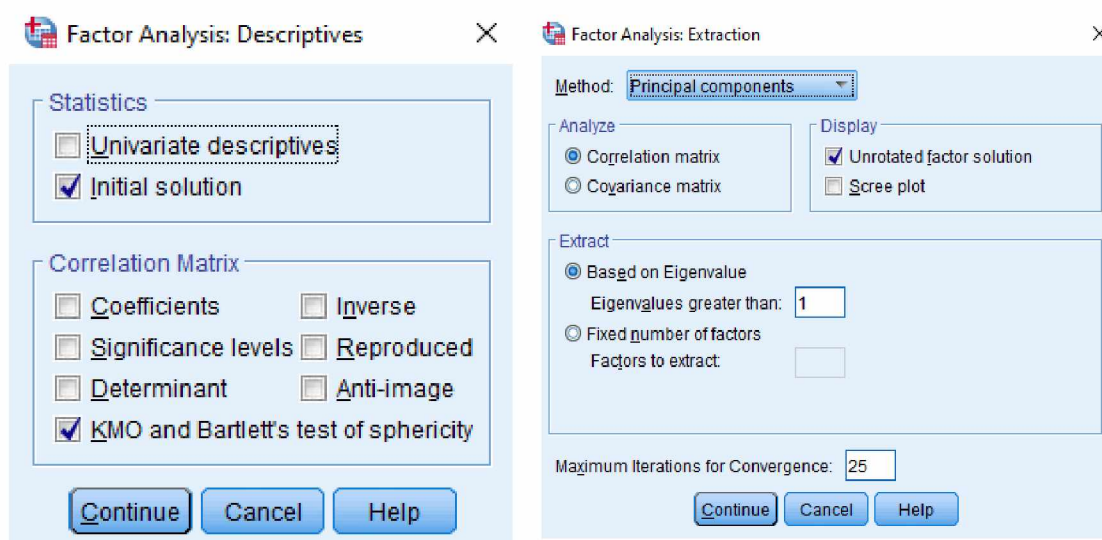
4.4. Επαγωγική στατιστική

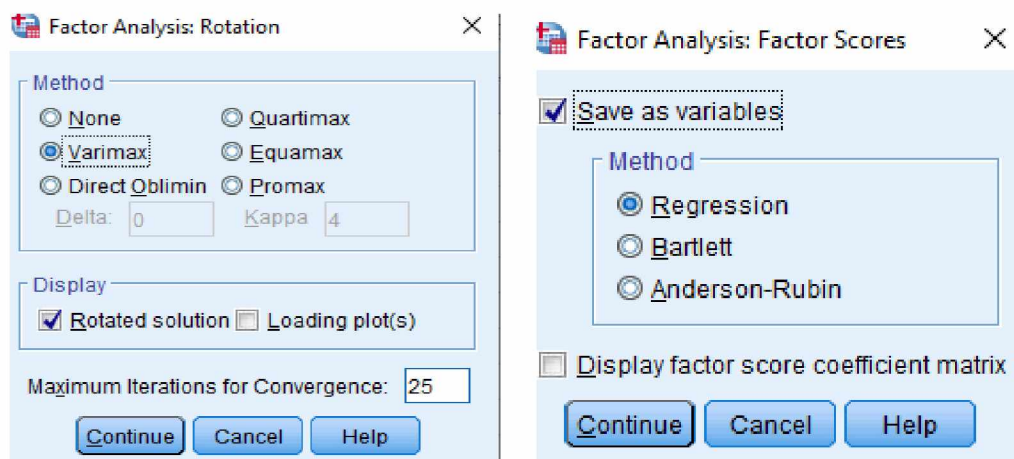
Η επαγωγική στατιστική συμπεριλαμβάνει την ανάλυση και εξαγωγή αντίστοιχων συμπερασμάτων, ώστε να απαντηθούν οι ερευνητικές υποθέσεις. Σε αυτό το πλαίσιο, διενεργήθηκε Παραγοντική ανάλυση (Factor Analysis) και Ανάλυση διαδρομών (Path analysis) με τη μέθοδο της παλινδρόμησης (Regression), χρησιμοποιώντας ως δεδομένα εισόδου τα αποτελέσματα του πίνακα Component Correlation Matrix της παραγοντικής ανάλυσης (ο πίνακας περιλαμβάνεται στο Παράρτημα II). Στις επόμενες ενότητες παρουσιάζονται αναλυτικά αυτές οι δυο αναλύσεις.

4.4.1. Παραγοντική ανάλυση – Factor Analysis

Στη συγκεκριμένη έρευνα, ως μεταβλητές χρησιμοποιήθηκαν οι 20 ερωτήσεις- καταστάσεις του ερωτηματολογίου, στις οποίες οι συμμετέχοντες κλήθηκαν να δηλώσουν πόσο συμφωνούν ή διαφωνούν ανάμεσα από τις εξής επιλογές της πεντάβαθμης κλίμακας: 1 (Διαφωνώ απόλυτα), 2 (Διαφωνώ), 3 (Ουδέτερος), 4 (Συμφωνώ), 5 (Συμφωνώ απόλυτα). Για το σύνολο αυτών των μεταβλητών: TGS1, TGS2, PEU1, PEU2, PEU3, PEU4, PEU5, PU1, PU2, PU3, TSY1, TSY2, TSY3, TSY4, TD1, TD2, TT1, TT2, IT1, IU, καθίσταται αναγκαία η χρήση της Παραγοντικής Ανάλυσης (Factor Analysis), μεθόδου που στοχεύει στη μείωση της διάστασης του προβλήματος και παράγει ανεξάρτητες μεταβλητές βάσει των αρχικών μεταβλητών. Στη Εικόνα 8 αποτυπώνονται οι ρυθμίσεις που χρησιμοποιήθηκαν κατά την εφαρμογή της Παραγοντικής Ανάλυσης στο SPSS.

Εικόνα 8: Ρυθμίσεις παραμέτρων Παραγοντικής Ανάλυσης στο SPSS





Για να εξεταστεί αν η παραγοντική ανάλυση είναι η κατάλληλη στατιστική μέθοδος σε σχέση με τα παρεχόμενα δεδομένα της έρευνας διενεργήθηκαν τα τεστ Kaiser-Meyer-Olkin και Bartlett. Συγκεκριμένα, η μέτρηση της επάρκειας δειγματοληψίας Kaiser-Meyer-Olkin (KMO) είναι μια μέτρηση που υποδεικνύει το ποσοστό διακύμανσης στις μεταβλητές που μπορεί να προκαλείται από υποκείμενους παράγοντες. Οι υψηλές τιμές (κοντά στο 1,0) υποδεικνύουν γενικά ότι μια παραγοντική ανάλυση μπορεί να είναι χρήσιμη, ενώ αν η τιμή είναι $< 0,50$, η μέθοδος αυτή δεν είναι αποτελεσματική.

Αντίστοιχα ο έλεγχος σφαιρικότητας του Bartlett χρησιμοποιείται για να εξετάσει αν τα δεδομένα προέρχονται από πληθυσμούς με ίσες διακυμάνσεις. Μικρές τιμές $< 0,05$ του επιπέδου σημαντικότητας υποδεικνύουν ότι μια παραγοντική ανάλυση μπορεί να είναι χρήσιμη σε σχέση με τα δεδομένα. Στον Πίνακα 16 αποτυπώνονται τα αποτελέσματα των δυο αυτών μετρήσεων, αναδεικνύοντας ότι τα δεδομένα είναι κατάλληλα για τη διεξαγωγή παραγοντικής ανάλυσης ($KMO=0.894 > 0.5$, Bartlett's test of sphericity < 0.05).

Πίνακας 16: KMO and Bartlett's Test

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		,894
Bartlett's Test of Sphericity	Approx. Chi-Square	4556,999
	df	190
	Sig.	,000

Στον Πίνακα 17, αποτυπώνεται το ποσοστό διακύμανσης κάθε μεταβλητής σε σχέση με τους παράγοντες που προέκυψαν κατά την παραγοντική ανάλυση (Communalities). Σύμφωνα με

τα αποτελέσματα του Πίνακα μπορεί να εξαχθεί το συμπέρασμα ότι το προσαρμοσμένο μοντέλο ερμηνεύει το 0,604 (60,4%) της πρώτης ερώτησης (TGS1), το 0,558 (55,8%) της δεύτερης ερώτησης, κ.ο.κ.. Όλες οι τιμές της στήλης Extraction παρουσιάζουν ικανοποιητικές τιμές, υποδηλώνοντας ότι η διακύμανση των αντίστοιχων μεταβλητών εξηγείται ικανοποιητικά.

Πίνακας 17: Communalities

Communalities		
	Initial	Extraction
TGS1	1,000	,604
TGS2	1,000	,558
PEU1	1,000	,650
PEU2	1,000	,730
PEU3	1,000	,510
PEU4	1,000	,693
PEU5	1,000	,704
PU1	1,000	,430
PU2	1,000	,384
PU3	1,000	,588
TSY1	1,000	,574
TSY2	1,000	,609
TSY3	1,000	,677
TSY4	1,000	,368
TD1	1,000	,800
TD2	1,000	,764
TT1	1,000	,758
TT2	1,000	,728
IT1	1,000	,731
IU1	1,000	,604

Extraction Method: Principal Component Analysis.

Στον Πίνακα 18 αποτυπώνονται οι Ιδιοτιμές (Eigenvalues) και τα ποσοστά της συνολικής μεταβλητότητας που ερμηνεύουν οι παράγοντες που προέκυψαν πριν και μετά την περιστροφή των αξόνων. Σύμφωνα με τις παραμέτρους που επιλέξαμε αρχικά, μόνο τρεις παράγοντες στην αρχική λύση έχουν ιδιοτιμές μεγαλύτερες από την τιμή 1 και αντιπροσωπεύουν σχεδόν το 61,7% της συνολικής μεταβλητότητας.

Πίνακας 18: Total Variance Explained

Component	Total Variance Explained								
	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	8,330	41,650	41,650	8,330	41,650	41,650	5,992	29,959	29,959
2	2,496	12,478	54,128	2,496	12,478	54,128	4,300	21,499	51,457
3	1,512	7,561	61,689	1,512	7,561	61,689	2,046	10,231	61,689
4	,977	4,886	66,574						
5	,844	4,218	70,792						
6	,792	3,959	74,751						
7	,725	3,623	78,374						
8	,658	3,291	81,665						
9	,556	2,782	84,447						
10	,517	2,585	87,032						
11	,473	2,365	89,398						
12	,370	1,851	91,249						
13	,331	1,655	92,904						
14	,302	1,508	94,412						
15	,235	1,176	95,588						
16	,226	1,132	96,720						
17	,205	1,024	97,744						
18	,170	,849	98,593						
19	,148	,740	99,333						
20	,133	,667	100,000						

Extraction Method: Principal Component Analysis.

Ο Πίνακας 19 αποτυπώνει τους συντελεστές συσχέτισης κάθε πρότασης με τον παράγοντα στον οποίο ανήκουν, πριν γίνει η περιστροφή των αξόνων. Για παράδειγμα, οι μεταβλητές «Αντιλαμβανόμενη ευκολίας χρήσης» – PEU1, PEU2, PEU3, PEU4 παρουσιάζει την υψηλότερη τιμή στον παράγοντα 1, κ.ο.κ..

Πίνακας 19: Component Matrix

	Component		
	1	2	3
PEU1	,555	,528	,129
PEU2	,543	,472	,201
PEU3	,590	,140	,531
PEU4	,595	,013	,613
PEU5	,494	,414	-,308
TGS1	,643	,475	-,231
TGS2	,660	,469	-,221
PU1	,601	,246	,089
PU2	,583	,191	-,084
PU3	,532	,473	-,284
TSY1	,702	-,184	-,219
TSY2	,780	-,022	,022
TSY3	,776	-,262	,079
TSY4	,015	,286	,535
TD1	,786	-,428	,009
TD2	,750	-,449	,006
TT1	,748	-,443	,037
TT2	,753	-,396	-,060
IT1	,800	-,301	,030
IU1	,544	-,152	-,399

Extraction Method: Principal Component Analysis.
a. 3 components extracted.

Προκειμένου όμως να αυξηθεί η ερμηνευτική ικανότητα του μοντέλου και να εξαχθούν ασφαλέστερα συμπεράσματα αξιολογούνται οι επιβαρύνσεις των παραγόντων μετά την

περιστροφή των αξόνων. Ο Πίνακας 20 περιέχει τις συσχετίσεις των τριών παραγόντων της ανάλυσης με τα στοιχεία που συμμετέχουν. Να σημειωθεί ότι σε κάθε παράγοντα θεωρούμε ότι συμμετέχουν τα στοιχεία που παρουσιάζουν τις υψηλότερες τιμές.

Πίνακας 20: Rotated Component Matrix^a

	Component		
	1	2	3
PEU1	,092	,656	,406
PEU2	,115	,581	,455
PEU3	,351	,244	,683
PEU4	,432	,124	,727
PEU5	,131	,700	-,045
TGS1	,206	,802	,081
TGS2	,222	,804	,094
PU1	,307	,492	,305
PU2	,334	,506	,125
PU3	,123	,757	,003
TSY1	,667	,352	-,069
TSY2	,616	,426	,217
TSY3	,764	,228	,205
TSY4	-,187	,017	,577
TD1	,878	,139	,098
TD2	,864	,104	,081
TT1	,858	,096	,110
TT2	,836	,169	,034
IT1	,808	,231	,155
IU1	,531	,352	-,269

Extraction Method: Principal Component Analysis, Rotation Method: Varimax with Kaiser Normalization, a. Rotation converged in 5 iterations.

Συνολικά θα μπορούσε να ειπωθεί ότι ένας από τους κυριότερους λόγους που εφαρμόζεται η μέθοδος της παραγοντικής ανάλυσης, είναι η δημιουργία νέων μεταβλητών οι οποίες ερμηνεύουν, όσο το δυνατόν μεγαλύτερο ποσοστό των αρχικών μεταβλητών με τη μικρότερη απώλεια πληροφορίας. Ως εκ τούτου, από τα 20 στοιχεία που αποτελούν την αρχική κλίμακα καταλήξαμε σε 3 παράγοντες, μειώνοντας τη διάσταση του προβλήματος. Παράλληλα, σύμφωνα με τον Πίνακα 20, κάθε στοιχείο εμπίπτει σε έναν και μόνο παράγοντα, γεγονός που συνάδει με τις απαιτήσεις της δομικής εγκυρότητας.

4.4.2. Ανάλυση Διαδρομών (Path Analysis) - Παλινδρόμηση (Regression)

Για την Ανάλυση Διαδρομών (Path Analysis) χρησιμοποιήθηκε η μέθοδος της παλινδρόμησης (Regression), χρησιμοποιώντας ως δεδομένα εισόδου τα αποτελέσματα του Component Correlation Matrix (ο πίνακας περιλαμβάνεται στο Παράρτημα II) της παραγοντικής ανάλυσης.

- **Πρώτο επίπεδο Παλινδρόμησης**

Στο πρώτο επίπεδο παλινδρόμησης εξετάζουμε την εξαρτημένη μεταβλητή TGS2 σε σχέση με τους υπόλοιπους συντελεστές, δηλαδή: TGS1, PEU1, PEU2, PEU3, PEU4, PEU5, PU1, PU2, PU3, IT, TSY1, TSY2, TSY3, TSY4, TD1, TD2, TT1, TT2, →TGS2. Στον Πίνακα 21 αποτυπώνεται η συσχέτιση του μοντέλου με τους συντελεστές.

Πίνακας 21: Πρώτο επίπεδο Παλινδρόμησης - Model Summary

Model Summary		
Model	R	R Square
1	,952 ^a	,906

a. Predictors: (Constant), IT1, PU2, PEU2, PEU3, PEU5, PU1, PU3, TSY2, PEU1, TSY1, TGS1, PEU4, TT1, TSY3, TSY4, TT2, TD1, TD2

Η τιμή "e" (διακύμανση σφάλματος) υπολογίζεται ως $\sqrt{(1-R^2)}$, δηλαδή:

$$e_{TGS2} = \sqrt{(1 - .906)} = .306.$$

Αντίστοιχα στον Πίνακα 22, οι συντελεστές διαδρομής Beta για το πρώτο επίπεδο παλινδρόμησης. Συγκεκριμένα: TGS1= ,425, PEU1= ,021, PEU2= ,202, PEU3= ,136, PEU4= -,053, PEU5= ,370, PU1= ,175, PU2= -,064, PU3= ,575, TSY1= ,670, TSY2= -,448, TSY3= ,488, TSY4= ,694, TD1= ,116, TD2= ,372, TT1= -,096, TT2= ,021, IT1= -,376.

Πίνακας 22: Πρώτο επίπεδο Παλινδρόμησης - Coefficients

Coefficients^a						
Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	-,457	,840		-,544	,683
	TGS1	,417	,914	,425	,456	,727
	PEU1	,021	,575	,021	,037	,976
	PEU2	,201	,623	,202	,322	,802
	PEU3	,134	,984	,136	,136	,914
	PEU4	-,051	,970	-,053	-,053	,967
	PEU5	,350	,638	,370	,549	,680
	PU1	,197	,590	,175	,334	,795
	PU2	-,074	,497	-,064	-,150	,905
	PU3	,523	,917	,575	,571	,670
	TSY1	,576	,882	,670	,652	,632
	TSY2	-,433	1,056	-,448	-,411	,752
	TSY3	,413	1,000	,488	,413	,751
	TSY4	,552	,985	,694	,560	,675
	TD1	,085	1,220	,116	,070	,955
	TD2	,271	1,272	,372	,213	,866
	TT1	-,072	1,256	-,096	-,057	,964
	TT2	,016	1,141	,021	,014	,991
	IT1	-,306	1,046	-,376	-,292	,819

a. Dependent Variable: TGS2

- **Δεύτερο επίπεδο παλινδρόμησης: TG2 → IU**

Στο δεύτερο επίπεδο παλινδρόμησης εξετάζουμε την εξαρτημένη μεταβλητή TGS2 με τον συντελεστή IU. Στον Πίνακα 23 αποτυπώνεται το δεύτερο επίπεδο παλινδρόμησης.

Πίνακας 23: Δεύτερο επίπεδο παλινδρόμησης - Model Summary

Model Summary		
Model	R	R Square
1	,027 ^a	,001

a. Predictors: (Constant), TGS2

Η διακύμανση σφάλματος e υπολογίζεται χρησιμοποιώντας το αποτέλεσμα R^2 του Πίνακα 23, δηλαδή: $e_{IU1} = \sqrt{(1-R^2)} = \sqrt{(1 - .906)} = .306$.

Πίνακας 24: Δεύτερο επίπεδο παλινδρόμησης- Coefficients

Coefficients ^a						
Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	0,314	,131		2,396	,028
	TGS2	,054	,291	,045	0,187	,910

a. Dependent Variable: IU1

Όπως αποτυπώνεται στον Πίνακα 24, ο συντελεστής διαδρομής για το TGS2, για το δεύτερο επίπεδο παλινδρόμησης, προκύπτει από την τιμή του Beta: TGS2= ,025.

4.5. Απαντήσεις στα ερευνητικά ερωτήματα

Η ενότητα αυτή επικεντρώνεται στο να παρουσιάσει, με βάση τους στατιστικούς υπολογισμούς που προηγήθηκαν, τις απαντήσεις στις ερευνητικές υποθέσεις.

- **Ερευνητική Υπόθεση H1:** *Η εμπιστοσύνη ενός πολίτη στην Κυβέρνηση επηρεάζει θετικά την εμπιστοσύνη του στη χρήση φορητών εφαρμογών.*

Σύμφωνα με τα αποτελέσματα, ο συντελεστής διαδρομής beta που συνδέει την εμπιστοσύνη των πολιτών στις υπηρεσίες του κράτους (TGS1) με την εμπιστοσύνη των πολιτών στη χρήση φορητών εφαρμογών (TGS2) είναι ,425 και η τιμή του στατιστικού t ισούται με ,456,

γεγονός που αναδεικνύει ότι η εμπιστοσύνη ενός πολίτη στην Κυβέρνηση επηρεάζει θετικά την εμπιστοσύνη του στη χρήση φορητών εφαρμογών.

- **Ερευνητική Υπόθεση H2:** *Η ευκολία χρήσης των φορητών εφαρμογών επηρεάζει θετικά την εμπιστοσύνη των πολιτών στις φορητές εφαρμογές ευρείας χρήσης.*

Στη δεύτερη ερευνητική υπόθεση, εξετάστηκαν οι επιμέρους ερωτήσεις που σχετίζονται με την ευκολία χρήσης των φορητών εφαρμογών. Η υπόθεση PEU1 – «Οι ηλεκτρονικές υπηρεσίες του κράτους είναι εύκολες στη χρήση» δεν επηρεάζει σημαντικά την εμπιστοσύνη των πολιτών στη χρήση φορητών εφαρμογών ($\beta = ,021$ $t = ,037$).

Σχετικά με την υπόθεση PEU2 – «Οι ηλεκτρονικές υπηρεσίες του κράτους παρέχουν κατανοητές οδηγίες για τον τρόπο χρήσης των υπηρεσιών», τα αποτελέσματα ($\beta = ,202$ $t = ,322$) αναδεικνύουν ότι η εμπιστοσύνη των πολιτών στη χρήση φορητών εφαρμογών επηρεάζεται θετικά, όταν το κράτος παρέχει αναλυτικές οδηγίες χρήσης των εφαρμογών.

Αντίστοιχα, η υπόθεση PEU3 – «Οι ηλεκτρονικές υπηρεσίες του κράτους είναι εύκολα προσβάσιμες από το κινητό» παρουσιάζει θετικό αντίκτυπο στην εμπιστοσύνη των πολιτών στη χρήση φορητών εφαρμογών με τα αποτελέσματα να κυμαίνονται: $\beta = ,136$ και $t = ,136$.

Ωστόσο η υπόθεση PEU4 – «Οι ηλεκτρονικές υπηρεσίες του κράτους είναι εύκολες στην πλοήγηση από κινητό», των οποίων τα αποτελέσματα παρουσιάζουν αρνητικές τιμές ($\beta = -,053$ και $t = -,053$) αναδεικνύει ότι οι πολίτες δεν θεωρούν εύκολη την πλοήγηση από κινητό και παρουσιάζονται διστακτικοί στη χρήση αυτών μέσω κινητού τηλεφώνου.

Τα αποτελέσματα της υπόθεσης PEU5 – «Οι ηλεκτρονικές υπηρεσίες του κράτους δεν απαιτούν επιπλέον χρόνο και κόπο σε σχέση με την αυτοπρόσωπη εξυπηρέτηση στις κατά τόπους υπηρεσίες» ($\beta = ,370$ και $t = ,549$) έχουν θετικό αντίκτυπο στην εμπιστοσύνη των πολιτών στη χρήση φορητών εφαρμογών.

- **Ερευνητική Υπόθεση H3:** *Η χρησιμότητα των φορητών εφαρμογών επηρεάζει θετικά την εμπιστοσύνη των πολιτών στις φορητές εφαρμογές ευρείας χρήσης.*

Σύμφωνα με τα αποτελέσματα της υπόθεσης PU1 – «Οι ηλεκτρονικές υπηρεσίες του κράτους παρέχουν χρήσιμες πληροφορίες στον πολίτη» ($\beta = ,175$, $t = ,334$) διαφαίνεται ότι η χρησιμότητα των φορητών εφαρμογών έχει θετικό αντίκτυπο στην εμπιστοσύνη των πολιτών.

Σχετικά με την υπόθεση PU2 – «Οι ηλεκτρονικές υπηρεσίες του κράτους ενισχύουν την αμφίδρομη επικοινωνία πολίτη-κράτους», τα αποτελέσματα ($\beta = -,064$ και $t = -,150$) αναδεικνύουν ότι η υπόθεση αυτή δεν υποστηρίζεται καθώς οι πολίτες εμφανίζονται διχασμένοι σχετικά με το αν προάγεται η μη η αμφίδρομη επικοινωνία.

Αντίστοιχα, η υπόθεση PU3 – «Οι ηλεκτρονικές υπηρεσίες του κράτους διεκπεραιώνουν αποτελεσματικά τα ζητήματα των πολιτών χωρίς να απαιτείται φυσική παρουσία» παρουσιάζει ιδιαίτερα θετικό αντίκτυπο στην εμπιστοσύνη των πολιτών στη χρήση φορητών εφαρμογών με τα αποτελέσματα να κυμαίνονται: $\beta = ,575$ και $t = ,571$.

- **Ερευνητική Υπόθεση H4:** *Η εμπιστοσύνη ενός πολίτη ότι η λειτουργία του συστήματος ηλεκτρονικής διακυβέρνησης δεν μπορεί να παραβιαστεί επηρεάζει θετικά την εμπιστοσύνη στις φορητές εφαρμογές ευρείας χρήσης.*

Σχετικά με τα αποτελέσματα της υπόθεσης TSY1 – «Αισθάνομαι ότι είναι ασφαλές να χρησιμοποιήσω μια υπηρεσία ηλεκτρονικής διακυβέρνησης» ($\beta = ,670$ και $t = ,652$), διαφαίνεται ότι το αίσθημα ασφάλειας των πολιτών έχει ιδιαίτερα θετικό αντίκτυπο στην εμπιστοσύνη των πολιτών στη χρήση φορητών εφαρμογών έχει θετικό αντίκτυπο

Αντίστοιχα, τα αποτελέσματα ($\beta = -,448$ και $t = -,411$) για την υπόθεση TSY2 – «Η Κυβέρνηση λαμβάνει όλα τα απαραίτητα μέτρα για τη σωστή λειτουργία των πληροφοριακών της συστημάτων», αναδεικνύουν ότι η υπόθεση αυτή δεν υποστηρίζεται καθώς οι πολίτες θεωρούν ότι δεν λαμβάνονται όλα τα απαραίτητα μέτρα.

Αντίστοιχα, η υπόθεση TSY3 – «Η Κυβέρνηση λαμβάνει όλα τα απαραίτητα μέτρα για την προστασία των πληροφοριακών συστημάτων της από απειλές» παρουσιάζει ιδιαίτερα θετικό αντίκτυπο στην εμπιστοσύνη των πολιτών στη χρήση φορητών εφαρμογών με τα αποτελέσματα να κυμαίνονται: $\beta = ,488$ και $t = ,413$.

Τέλος, τα αποτελέσματα της υπόθεσης TSY4 – «Πιστεύω ότι τα οφέλη υπερτερούν των κινδύνων από τη χρήση μιας υπηρεσίας ηλεκτρονικής διακυβέρνησης» ($\beta = ,694$ και $t = ,560$) έχουν ιδιαίτερα θετικό αντίκτυπο στην εμπιστοσύνη των πολιτών.

- **Ερευνητική Υπόθεση H5:** *Η εμπιστοσύνη των πολιτών ότι τα δεδομένα που συλλέγονται και αποθηκεύονται ηλεκτρονικά προστατεύονται επηρεάζει θετικά την εμπιστοσύνη στις φορητές εφαρμογές ευρείας χρήσης.*

Σύμφωνα με τα αποτελέσματα της υπόθεσης TD1 – «Οι ηλεκτρονικές υπηρεσίες του κράτους παρέχουν χρήσιμες πληροφορίες στον πολίτη» ($\beta = ,116$, $t = ,070$). διαφαίνεται ότι η υπόθεση υποστηρίζεται, ωστόσο δεν έχει ιδιαίτερο αντίκτυπο στην εμπιστοσύνη των πολιτών στη χρήση φορητών εφαρμογών.

Σχετικά με την υπόθεση TD2 – «Η κυβέρνηση διασφαλίζει ότι τα δεδομένα που συλλέγονται θα χρησιμοποιούνται αποκλειστικά για τον σκοπό που συλλέχθηκαν», τα αποτελέσματα ($\beta = ,372$ και $t = ,213$) αναδεικνύουν ότι η υπόθεση αυτή υποστηρίζεται και παρουσιάζει θετικό αντίκτυπο στην εμπιστοσύνη των πολιτών στη χρήση φορητών εφαρμογών

- **Ερευνητική Υπόθεση H6:** *Η εμπιστοσύνη ενός πολίτη ότι τα δεδομένα που καταχωρεί μέσω μιας εφαρμογής δεν παραποιούνται, επηρεάζει θετικά την εμπιστοσύνη στις φορητές εφαρμογές ευρείας χρήσης.*

Τα αποτελέσματα για την υπόθεση TT1 – «Η κυβέρνηση διασφαλίζει ότι τα δεδομένα που συλλέγονται δεν κοινοποιούνται χωρίς τη συγκατάθεση μου», ($\beta = -,096$ και $t = -,057$), αναδεικνύουν ότι η υπόθεση δεν υποστηρίζεται καθώς οι πολίτες θεωρούν ότι το προσωπικά τους δεδομένα πιθανόν να κοινοποιούνται μεταξύ των υπηρεσιών του δημοσίου.

Σχετικά με τα αποτελέσματα της υπόθεσης TT2 – «Η κυβέρνηση διασφαλίζει ότι τα δεδομένα που εισάγω δεν παραποιούνται» ($\beta = ,021$ και $t = ,014$). διαφαίνεται ότι δεν επηρεάζει σημαντικά την εμπιστοσύνη των πολιτών στη χρήση φορητών εφαρμογών.

- **Ερευνητική Υπόθεση H7:** *Η εμπιστοσύνη των πολιτών στο ισχύον νομικό και θεσμικό πλαίσιο επηρεάζει θετικά την εμπιστοσύνη στις φορητές εφαρμογές ευρείας χρήσης.*

Τα αποτελέσματα για την υπόθεση IT1 – «Η κυβέρνηση λαμβάνει όλα τα απαραίτητα νομικά μέτρα για την προστασία μου», ($\beta = -,376$ και $t = -,292$), αναδεικνύουν ότι η υπόθεση αυτή δεν υποστηρίζεται καθώς οι πολίτες διαφαίνεται ότι δεν εμπιστεύονται το ισχύον νομικό πλαίσιο αναφορικά με τη χρήση φορητών εφαρμογών.

- **Ερευνητική Υπόθεση H8:** *Η εμπιστοσύνη των πολιτών στη χρήση φορητών εφαρμογών έχει θετικό αντίκτυπο στην πρόθεσή τους να τα χρησιμοποιήσουν.*

Τα αποτελέσματα της υπόθεσης IU – «Σκοπεύω να χρησιμοποιήσω τις κρατικές φορητές εφαρμογές» ($\beta = ,045$ και $t = ,0187$). αναδεικνύουν ότι η υπόθεση αυτή υποστηρίζεται και διαφαίνεται ότι οι πολίτες είναι θετικοί στη χρήση φορητών εφαρμογών και ότι σκοπεύουν να τις χρησιμοποιήσουν.

ΚΕΦΑΛΑΙΟ 5: ΕΠΙΛΟΓΟΣ

5.1. Σύγκριση ευρημάτων

Η διερεύνηση των παραγόντων που ενισχύουν ή αποθαρρύνουν τους πολίτες στο να χρησιμοποιήσουν τις κρατικές φορητές εφαρμογές αποτελεί ένα σχετικά νέο πεδίο ερευνών, καθώς η ραγδαία ανάπτυξη των έξυπνων κινητών τηλεφώνων και των εφαρμογών είναι ένα γεγονός που απέκτησε ιδιαίτερη σημασία κυρίως τα τελευταία χρόνια. Σύμφωνα με τη βιβλιογραφία, παρατηρείται ότι έχουν προταθεί διάφορα μοντέλα σχηματισμού εμπιστοσύνης στην ηλεκτρονική διακυβέρνηση, τα οποία εξετάζουν την εμπιστοσύνη είτε ως μια ενιαία δομή της ηλεκτρονικής διακυβέρνησης είτε αναφέρονται σε συγκεκριμένα ζητήματα που σχετίζονται με αυτή διερευνώντας πτυχές όπως η αξιοπιστία των τεχνολογικών μέσων.

Για παράδειγμα, στην μελέτη των Warkentin (2002) και Davis (1989) ο σχηματισμός εμπιστοσύνης παρουσιάζεται ως μια συνολική πεποίθηση που επηρεάζει την πρόθεση της συμμετοχής στην ηλεκτρονική διακυβέρνηση. Η μελέτη των Horst (2007) εξετάζεται την εμπιστοσύνη ως προγνωστικό στοιχείο της αντίληψης της χρησιμότητας των υπηρεσιών ηλεκτρονικής διακυβέρνησης, ενώ η μελέτη των McKnight (2002) διερευνά το σχηματισμό της εμπιστοσύνης ενός πληροφοριακού συστήματός πριν αυτό εισαχθεί σε ένα οργανισμό. Απουσιάζουν, ωστόσο, έρευνες που εστιάζουν στη μεταβίβαση εμπιστοσύνης και στους παράγοντες που ενισχύουν ή αποθαρρύνουν την εμπιστοσύνη ενός πολίτη στις φορητές εφαρμογές.

Παρόμοια έρευνα με την παρούσα διπλωματική εργασία διενεργήθηκε από τους Luo et al. (2017) στο πλαίσιο των επιχειρήσεων. Ειδικότερα, εξετάζεται η μεταβίβαση της εμπιστοσύνης από μια επιχείρηση με φυσική παρουσία σε ένα διαδικτυακό κανάλι της ίδιας επιχείρησης και τον τρόπο με τον οποίο διαμορφώνεται η εμπιστοσύνη του καταναλωτή σε αυτή τη διαδικασία. Σε αυτό το σημείο να σημειωθεί ότι αν και η συγκεκριμένη έρευνα επικεντρώνεται στις επιχειρήσεις, χρησιμοποιείται το ίδιο βιβλιογραφικό και ερευνητικό υπόβαθρο με την παρούσα εργασία. Συγκεκριμένα το ερευνητικό της μοντέλο βασίζεται τόσο στη μεταβίβαση εμπιστοσύνης, όσο και στο Μοντέλο Αποδοχής Τεχνολογίας (Technology Acceptance Model -TAM).

Το ερευνητικό της μέρος διεξήχθη με τη μορφή ερωτηματολογίου και με τη συμμετοχή 210 ερωτώμενων πολιτών της Κίνας, συγκεντρώνοντας 159 έγκυρα ερωτηματολόγια. Το περιεχόμενο των ερωτήσεων και η στατιστική ανάλυση των δεδομένων είναι παραπλήσια

με την παρούσα μελέτη, ενώ με τη χρήση του SPSS διενεργήθηκε η περιγραφική στατιστική ανάλυση των δημογραφικών χαρακτηριστικών του δείγματος, για τον βαθμό αξιοπιστίας εξετάστηκε ο δείκτης Cronbach's α , για τη συσχέτιση των μεταβλητών επιλέχθηκε η παραγοντική ανάλυση και για την εύρεση των συντελεστών διαδρομής του δομικού μοντέλου χρησιμοποιήθηκε το LISREL 8.7.

Τα αποτελέσματα της μελέτη των Luo et al. (2017) για το πρώτο ερευνητικό ερώτημα (TGS) αναδεικνύουν ότι η εμπιστοσύνη των καταναλωτών σε επιχειρήσεις με φυσική παρουσία, δεν έχει ιδιαίτερο αντίκτυπο στην εμπιστοσύνη τους στα διαδικτυακά κανάλια, γεγονός που αποδίδεται στη δύναμη της συνήθειας του αγοραστικού κοινού. Σχετικά με την ευκολία χρήσης των διαδικτυακών καναλιών (PU) οι συμμετέχοντες στην πλειοψηφία τους υποστηρίζουν ότι δεν έχει σημαντικό αντίκτυπο στην εμπιστοσύνη τους σε αυτά, καθώς θεωρούν ότι εξυπηρετούνται το ίδιο εύκολα και από τους υπαλλήλους των καταστημάτων. Ωστόσο, η χρησιμότητα των διαδικτυακών καναλιών (PEU) παρουσιάζεται να έχει θετικό αντίκτυπο στην εμπιστοσύνη των καταναλωτών.

Αντίστοιχα, η διασφάλιση ασφάλειας και απορρήτου (TSY, TD, TT) διαφαίνεται ότι δεν επιδρά σημαντικά στην ενίσχυση της εμπιστοσύνη των καταναλωτών στα διαδικτυακά κανάλια. Σύμφωνα με τους συγγραφείς αυτό αποδίδεται στο γεγονός ότι το καταναλωτικό κοινό της Κίνας δεν δίνει ιδιαίτερη έμφαση σε θέματα ασφαλείας κατά τις διαδικτυακές τους συναλλαγές. Τέλος, σχετικά με την πρόθεση χρήσης διαδικτυακών καναλιών, η εμπιστοσύνη των καταναλωτών στα διαδικτυακά κανάλια έχει θετικό αντίκτυπο στην πρόθεσή τους να τα χρησιμοποιήσουν.

Στο ίδιο πλαίσιο, η έρευνα της Colesca (2009), μέσω ερωτηματολογίου 793 κατοίκων της Ρουμανίας, ανέδειξε ότι η ανησυχία των πολιτών για την προστασία της ιδιωτικότητάς τους παίζει σημαντικό ρόλο στην εμπιστοσύνη τους στην ηλεκτρονική διακυβέρνηση. Μάλιστα το σύνολο των συμμετεχόντων πολιτών εξέφρασε την πεποίθηση ότι θα επιθυμούσαν τα προσωπικά τους δεδομένα να χρησιμοποιούνται από το Κράτος μόνο για το σκοπό που οι ίδιοι τα παραχωρούν και ότι θα πρέπει να λαμβάνονται μέτρα για τη διασφάλιση της ασφάλειας τους. Η έρευνα καταλήγει στη διαπίστωση ότι, δεδομένου του γεγονότος ότι η ψηφιακή διακυβέρνηση αποτελεί ένας από τους βασικούς πυλώνες για την αποκατάσταση της εμπιστοσύνης των πολιτών στο Κράτος, καθίσταται πλέον επιτακτική η ανάγκη μετάβασης από την παραδοσιακή μορφή διακυβέρνησης σε πιο διαφανής και πολιτοκεντρικές διαδικασίες που θα διασφαλίζουν το απόρρητο και την ασφάλεια.

Παρεμφερή ευρήματα, αναφορικά με τους παράγοντες που ενισχύουν ή αποθαρρύνουν τη εμπιστοσύνη των πολιτών στις κρατικές φορητές εφαρμογές, καταγράφονται στη μελέτη των Tran & Nguyen (2021), η οποία διαπραγματεύεται τη σχέση μεταξύ του αντιλαμβανόμενου κινδύνου για την υγεία, του αντιληπτού κινδύνου απορρήτου, της αντιληπτής αξίας και της εφαρμογής ανίχνευσης επαφών COVID-19. Συγκεκριμένα, διαφαιίνεται ότι οι πολίτες διστάζουν να εγκαταστήσουν εφαρμογές υγείας εξαιτίας των ανησυχιών τους για το απόρρητο, την ασφάλεια και την εσφαλμένη αντίληψη σχετικά με τις εφαρμογές εντοπισμού επαφών για τον COVID-19. Η έρευνα αυτή καταλήγει στο συμπέρασμα ότι για να αμβλυνθούν οι ανησυχίες και να οικοδομηθεί η εμπιστοσύνη στις φορητές εφαρμογές υγείας θα πρέπει να υπάρξει διαφάνεια των δικαιωμάτων τόσο στο απόρρητο χρήσης όσο και στο χειρισμό των δεδομένων από το κράτος.

Ειδικότερα, σε σχέση με τις ανησυχίες που εγείρονται σχετικά με τις εφαρμογές για τον COVID-19, τον βαθμό επιτήρησης της ιδιωτικής ζωής των πολιτών και της παραβίασης, ή μη των θεμελιωδών τους δικαιωμάτων, έρευνα των Barriga et al. (2020) σημειώνει ότι η απροθυμία των πολιτών στη χρήση εφαρμογών σχετίζεται τόσο με τον φόβο παραβίασης της ιδιωτικής τους ζωής, όσο και με τη χρήση των προσωπικών τους δεδομένων για πολιτικούς ή εμπορικούς σκοπούς. Όπως χαρακτηριστικά, επισημαίνεται το ζήτημα της ανωνυμίας αποτελεί τροχοπέδι στη χρήση των φορητών εφαρμογών, π.χ., τα προσωπικά δεδομένα υγείας μπορούν να χρησιμοποιηθούν από ασφαλιστικές εταιρείες ή αν δεν καταστραφούν, ενδέχεται να ιδιοποιηθούν από άλλες ψηφιακές πλατφόρμες ή άλλες υπηρεσίες του κράτους.

5.2. Αποτελέσματα - Συμπεράσματα

Τα συμπεράσματα που προκύπτουν, τόσο από την ανασκόπηση της βιβλιογραφίας, όσο και από την ερευνητική ανάλυση των δεδομένων και τη συγκριτική έρευνα που προηγήθηκε, αναδεικνύουν, σε ένα γενικότερο πλαίσιο, ότι η έλλειψη εμπιστοσύνης των πολιτών έχει καταστεί ένα από τα σημαντικότερα εμπόδια στην ευρεία αποδοχή των δημόσιων φορητών εφαρμογών. Καθοριστικός παράγοντας στη μη χρήση των φορητών εφαρμογών αναδεικνύεται η έλλειψη εμπιστοσύνης στην ασφάλεια των διαδικτυακών συναλλαγών και οι ανησυχίες που εγείρονται αναφορικά με τη χρήση των δεδομένων που υποβάλλονται ηλεκτρονικά.

Ειδικότερα, τα συμπεράσματα που απορρέουν από την παρούσα διπλωματική εργασία επικεντρώνονται στις ακόλουθες παρατηρήσεις:

A) Η εμπιστοσύνη αποτελεί αδιαμφισβήτητα μια από τις σημαντικότερες έννοιες στην αλληλεπίδραση των πολιτών με το Κράτος για τη διεκπεραίωση των υποθέσεών τους με τις διοικητικές υπηρεσίες, καθώς επιτρέπει στα μέλη που συνδιαλέγονται, να λαμβάνουν αποφάσεις χωρίς να χρειάζεται να επαναδιαπραγματευθούν ή/και να παρέχουν διαβεβαιώσεις για κάθε αίτημα ή συνδιαλλαγή του πολίτη με το Κράτος.

B) Η διαδικασία μεταβίβασης της εμπιστοσύνης του πολίτη από ένα οργανισμό με φυσική παρουσία σε μια ψηφιακή πλατφόρμα του ίδιου οργανισμού και εν τέλει στη χρήση των ψηφιακών υπηρεσιών από τον πολίτη, αποτελεί μια σύνθετη διαδικασία. Μπορεί να διερευνηθεί σε σχέση με διάφορους παράγοντες στους οποίους εκχωρείται η εμπιστοσύνη, όπως για παράδειγμα της εμπιστοσύνης του πολίτη στις υπηρεσίες ηλεκτρονικής διακυβέρνησης, στο πληροφοριακό σύστημα ηλεκτρονικής διακυβέρνησης, της διαχείρισης δεδομένων που εισάγει και της εμπιστοσύνης στους θεσμούς.

Γ) Η ψηφιακή διακυβέρνηση αναγνωρίζεται όλο και περισσότερο ως βασικός παράγοντας για τον μετασχηματισμό και εκσυγχρονισμό της δημόσιας διοίκησης και διακυβέρνησης. Η ενσωμάτωσή των φορητών εφαρμογών στη δημόσια διοίκηση αποβλέπει στην απλοποιημένη αλληλεπίδραση των πολιτών με τη δημόσιες υπηρεσίες, στην άμεση εξυπηρέτηση των αιτημάτων των πολιτών χωρίς να απαιτείται αυτοπρόσωπη παρουσία τους.

Δ) Οι ανησυχίες που εγείρονται από τους πολίτες, περί απορρήτου και ασφάλειας, επηρεάζουν σε μεγάλο βαθμό την αποδοχή και χρήση νέων τεχνολογικών καινοτομιών. Ενισχύοντας την εμπιστοσύνη των πολιτών τόσο στην κυβέρνηση όσο και στο σύνολο των δομών που απαρτίζουν ένα πληροφοριακό σύστημα ή μια εφαρμογή, ενισχύεται παράλληλα και η πρόθεσή τους να συμμετάσχουν στην ψηφιακή διακυβέρνηση του κράτους, αξιοποιώντας τις αντίστοιχες εφαρμογές.

Ε) Σημαντικά ερωτήματα αναδύονται επίσης και σχετικά με τον κρατικό έλεγχο και την επιτήρηση των πολιτών κατά τη χρήση κρατικών φορητών εφαρμογών, καθώς η εκχώρηση εμπιστοσύνης σε αυτές, εμπεριέχει τον κίνδυνο περιορισμού των συνταγματικών τους ελευθεριών. Μάλιστα, με αφορμή την πανδημία του COVID-19 το ερώτημα που πλέον τίθεται, σε παγκόσμιο επίπεδο, είναι έως ποιο σημείο ένας πολίτης είναι πρόθυμος να θυσιάσει την ιδιωτικότητά του.

ΣΤ) Σημαντική προϋπόθεση για την αποδοχή και χρήση των κρατικών εφαρμογών από τους πολίτες αποτελεί η διαβεβαίωση του Κράτους ότι τα δεδομένα που εισάγουν οι πολίτες στις κρατικές εφαρμογές θα χρησιμοποιούνται αποκλειστικά για το σκοπό που παραχωρούνται, δίνοντας στους πολίτες τη δυνατότητα ελέγχου αυτών, ότι λαμβάνονται όλα τα απαραίτητα μέτρα ασφάλειας για την απρόσκοπτη λειτουργία των υπηρεσιών τους διαδικτυακά και ότι δεν θα αποτελέσουν μελλοντικά μέσο μαζικής παρακολούθησης στο μέλλον.

Αναφορικά με τα αποτελέσματα του ερευνητικού μέρους της παρούσας εργασίας σε σχέση με τους παράγοντες που ενισχύουν ή αποτρέπουν τη χρήση κρατικών φορητών εφαρμογών διαφαίνεται ότι:

- Η εμπιστοσύνη ενός πολίτη στο Κράτος επηρεάζει θετικά την εμπιστοσύνη του στη χρήση φορητών εφαρμογών.
- Η εμπιστοσύνη των πολιτών στη χρήση φορητών εφαρμογών επηρεάζεται θετικά, όταν το κράτος παρέχει αναλυτικές οδηγίες χρήσης των εφαρμογών.
- Η χρησιμότητα των φορητών εφαρμογών έχει θετικό αντίκτυπο στην εμπιστοσύνη των πολιτών.
- Η εμπιστοσύνη των πολιτών ότι οι ηλεκτρονικές υπηρεσίες του κράτους θα διεκπεραιώσουν αποτελεσματικά τα ζητήματα τους χωρίς να απαιτείται φυσική παρουσία επηρεάζει θετικά την πρόθεσή τους να τις χρησιμοποιήσουν.
- Η πεποίθηση ότι οι εφαρμογές δεν απαιτούν επιπλέον χρόνο και κόπο σε σχέση με την αυτοπρόσωπη εξυπηρέτηση στις κατά τόπους υπηρεσίες έχουν θετικό αντίκτυπο στην εμπιστοσύνη των πολιτών στη χρήση φορητών εφαρμογών.
- Η ευκολία πρόσβασης των υπηρεσιών από το κινητό παρουσιάζει θετικό αντίκτυπο στην εμπιστοσύνη των πολιτών στη χρήση φορητών εφαρμογών.
- Οι πολίτες δεν θεωρούν εύκολη την πλοήγηση από κινητό και παρουσιάζονται διστακτικοί στη χρήση αυτών μέσω κινητού τηλεφώνου.
- Οι πολίτες θεωρούν ότι το προσωπικά τους δεδομένα πιθανόν να κοινοποιούνται μεταξύ των υπηρεσιών του δημοσίου.
- Οι πολίτες θεωρούν ότι δεν λαμβάνονται από το Κράτος όλα τα απαραίτητα μέτρα για τη σωστή λειτουργία των πληροφοριακών της συστημάτων.
- Οι πολίτες διαφαίνεται ότι δεν εμπιστεύονται το ισχύον νομικό πλαίσιο αναφορικά με τη χρήση φορητών εφαρμογών.

- Οι πολίτες θεωρούν ότι τα οφέλη υπερτερούν των κινδύνων από τη χρήση μιας υπηρεσίας ηλεκτρονικής διακυβέρνησης γεγονός που έχει ιδιαίτερα θετικό αντίκτυπο στην εμπιστοσύνη των πολιτών στη χρήση φορητών εφαρμογών.
- Οι πολίτες παρουσιάζονται θετικοί στη χρήση φορητών εφαρμογών και ότι σκοπεύουν να τις χρησιμοποιήσουν, παρά τις ανησυχίες αναφορικά με τα προσωπικά τους δεδομένα και την ασφάλεια των εφαρμογών.

Εν κατακλείδι, η μεταβίβαση της εμπιστοσύνης των πολιτών στις εφαρμογές ηλεκτρονικής διακυβέρνησης είναι μια σύνθετη διαδικασία η οποία θα πρέπει να αντιμετωπίζεται πολυδιάστατα και σε σχέση με τους διάφορους παράγοντες στους οποίους εκχωρείται η εμπιστοσύνη. Ως εκ τούτου, οι παράγοντες εμπιστοσύνης που ενισχύουν ή αποτρέπουν τον πολίτη να χρησιμοποιήσει τις εφαρμογές, αν και σε διαφορετικό βαθμό, απαιτούν μια προσέγγιση που θα συνδυάζει τόσο τεχνολογικές όσο και θεσμικές λύσεις. Συγκεκριμένα, η εμπιστοσύνη των πολιτών στα αποθηκευμένα δεδομένα, και το σύστημα μπορεί να δημιουργηθεί και ενισχυθεί με τη χρήση της τρέχουσα τεχνολογίας, ενώ η εμπιστοσύνη στις υπηρεσίες και η θεσμική εμπιστοσύνη απαιτεί από το Κράτος τη διαμόρφωση του κατάλληλου θεσμικού και νομικού πλαισίου.

5.3. Περιορισμοί της έρευνας

Κατά τη διάρκεια εκπόνησης της διπλωματικής εργασίας ένας από τους κυριότερους περιορισμούς που κληθήκαμε να αντιμετωπίσουμε ήταν η εύρεση βιβλιογραφίας που να επικεντρώνεται στη μεταβίβαση εμπιστοσύνης σε φορητές εφαρμογές. Καθώς το συγκεκριμένο πεδίο είναι σχετικά καινούριο, οι περισσότερες μελέτες εξετάζουν τη μεταβίβαση εμπιστοσύνης κυρίως σε σχέση με τις επιχειρήσεις που διατηρούν τόσο φυσικό κατάστημα όσο και διαδικτυακό καθώς και τους παράγοντες που ενισχύουν την εμπιστοσύνη των καταναλωτών στο να στραφούν στις διαδικτυακές αγορές.

Παράλληλα, ο ίδιος περιορισμός παρουσιάστηκε και στην εύρεση σταθμισμένου ερωτηματολογίου που να ανταποκρίνεται στις ανάγκες της παρούσας εργασίας, παρά την εκτεταμένη ανασκόπηση της υπάρχουσας βιβλιογραφίας. Τα υφιστάμενα ερωτηματολόγια που εξετάστηκαν δεν επικεντρωνόταν στους παράγοντες που επιθυμούσαμε να διερευνήσουμε, ως εκ τούτου σχεδιάστηκε εξ' αρχής ένα νέο ερωτηματολόγιο βασιζόμενο σε παρόμοιες έρευνες, όπως των Luo et al. (2017), κ.α., ώστε να καλύψουμε το ερευνητικό μοντέλο και τις ερευνητικές υποθέσεις της παρούσας διπλωματικής εργασίας.

Αναφορικά με το ερωτηματολόγιο, καθώς το διάστημα διαμοιρασμού στα κοινωνικά δίκτυα ήταν περιορισμένο, δεν επιτεύχθηκε ο στόχος των 377 συμμετεχόντων και συγκεντρώθηκαν 353 απαντήσεις, με το περιθώριο σφάλματος και το επίπεδο εμπιστοσύνης να παρουσιάζουν πολύ μικρές αποκλείσεις σε σχέση με τις εκτιμώμενες προβλέψεις, παραμένοντας όμως σε ικανοποιητικά επίπεδα. Δόκιμο λοιπόν θα ήταν η έρευνα να μπορούσε να επεκταθεί σε ένα ευρύτερο σύνολο συμμετεχόντων, ώστε να διεξαχθούν σαφή συμπεράσματα για τους παράγοντες που ενισχύουν ή αποθαρρύνουν την εμπιστοσύνη των πολιτών.

Τέλος, εξαιτίας των υγειονομικών συνθηκών και του διαστήματος κατά το οποίο διαμοιράστηκε το ερωτηματολόγιο, δεν κατέστη δυνατό να υπάρξει διαθέσιμο δειγματοληπτικό πλαίσιο που να καταγράφει όλα τα στοιχεία του πληθυσμού. Συνεπώς, επιλέχθηκε η δειγματοληψία της χιονόμπαλας, τεχνική δειγματοληψίας κατά την οποία ο ερευνητής καθορίζει το πότε έχει αρκετά δεδομένα ώστε να παραχθούν αποτελέσματα που μπορούν να οδηγήσουν σε τεκμηριωμένες αποφάσεις.

5.4. Μελλοντική έρευνα

Η παρούσα διπλωματική εργασία επικεντρώθηκε στη διαδικασία μεταβίβασης της εμπιστοσύνης των πολιτών στις φορητές εφαρμογές και είχε ως στόχο της να αναδείξει τους παράγοντες που ενισχύουν ή αποθαρρύνουν τους πολίτες στη χρήση αυτών. Η έρευνα επικεντρώθηκε στο έλεγχο συγκεκριμένων παραμέτρων, όπως η εμπιστοσύνη στα δεδομένα, στις συναλλαγές, στις υπηρεσίες, στην πληροφορία, στο σύστημα, στην Κυβέρνηση, στη Θεσμική εμπιστοσύνη και στην αντιλαμβανόμενη ευκολία χρήσης και χρησιμότητας.

Περαιτέρω συνεισφορά στην έρευνα θα μπορούσε να αποτελέσει ο συσχετισμός των δημογραφικών στοιχείων των συμμετεχόντων σε σχέση με τους προαναφερθέντες παράγοντες εμπιστοσύνης. Συγκεκριμένα, η διερεύνηση της εμπιστοσύνης σε σχέση με το φύλο, την ηλικία, την εκπαίδευση, το επάγγελμα και την εμπειρία, θα μπορούσε να προσφέρει μια πληρέστερη εικόνα αναφορικά με τους τρόπους που θα μπορούσε το Κράτος να ενισχύσει την εμπιστοσύνη των πολιτών στη χρήση των φορητών εφαρμογών. Παράλληλα, μια πανελλαδική έρευνα, θα μπορούσε να αποτυπώσει πληρέστερα την υπάρχουσα κατάσταση και να εξαχθούν συμπεράσματα που θα καλύπτουν ένα ευρύτερο κοινωνικό πλαίσιο.

Σε αυτό το σημείο αξίζει να σημειωθεί ότι η παροχή κρατικών φορητών εφαρμογών, βασισμένες σε μοντέλα του ιδιωτικού τομέα, όπως η Uber, η Airbnb, κ.α., αποτελεί πρόκληση για κάθε κυβέρνηση, καθώς οι πολίτες αναμένουν παρόμοιες εφαρμογές από τις δημόσιες υπηρεσίες όσον αφορά τη χρηστικότητα, την προσβασιμότητα, την ευκολία και την αποτελεσματικότητα. Ως εκ τούτου, σε μελλοντική έρευνα θα ήταν χρήσιμο να διερευνηθούν οι παράγοντες που καθιστούν τις ιδιωτικές φορητές εφαρμογές ευρέως αποδεχτές από τους πολίτες, ώστε αντίστοιχα να υλοποιηθούν παρόμοιες ολιστικές προτάσεις από το Κράτος που θα εναρμονίζουν τις κρατικές εφαρμογές σε σχέση με τις πραγματικές ανάγκες των πολιτών.

BIBΛΙΟΓΡΑΦΙΑ

- Abeler, J., Backer, M., Buermeyer, U., & Zillessen, H. (2020). COVID-19 Contact Tracing and Data Protection Can Go Together. *JMIR Mhealth Uhealth, Vol 8, No 4*. doi:10.2196/19359
- Ayyash, M., Ahmad, K., & Singh, D. (2011). A Questionnaire Approach for User Trust Adoption in Palestinian E-Government Initiative. *American Journal of Applied Sciences, 8 (11): 1202-1208*. doi:10.3844/AJASSP.2011.1202.1208
- Balapour, A., Nikkhah, H., & Sabherwal, R. (2020). Mobile application security: Role of perceived privacy as the predictor of security perception. *International Journal of Information Management, Volume 52*. doi:10.1016/j.ijinfomgt.2019.102063
- Ballester, E., & Espallardo, M. (2008). Effect of brand associations on consumer reactions to unknown on-line brands. *International Journal of Electronic Commerce, 12(3):81-113*. doi:10.2753/JEC1086-4415120305
- Barney, J., & Hansen, M. (1994). Trustworthiness as a source of competitive advantage. *Strategic Management Journal, Vol. 15 (Special issue): 175-190*. doi:10.1002/smj.4250150912
- Barriga, A., Martins, A., Simoes, M., & Faustino, D. (2020). The COVID-19 pandemic: Yet another catalyst for governmental mass surveillance? *Social Sciences & Humanities Open, Volume 2, Issue 1*. doi:10.1016/j.ssaho.2020.100096
- Belanche, D., Casalo, L. V., Flavián, C., & Schepers, J. (2014). Trust transfer in the continued usage of public e-services. *Information & Management, 51(6), 627-640*. doi:10.1016/j.im.2014.05.016
- Bélanger, F., & Carter, L. (2008). Trust and risk in e-government adoption. *The Journal of Strategic Information Systems(17(2), 165-176.)*. doi:10.1016/j.jsis.2007.12.002
- Belanger, F., & Crossler, R. (2019). Dealing with digital traces: understanding protective behaviors on mobile devices. *The Journal of Strategic Information Systems, Volume 28, Issue 1, p. 34-49*. doi:10.1016/j.jsis.2018.11.002
- Belanger, F., & Hiller, J. (2006). A framework for e-government: privacy implications. *Business Process Management Journal, Vol. 12, No. 1, σσ. 48-60*. doi:https://doi.org/10.1108/14637150610643751
- Belanger, F., Hiller, J., & Smith, W. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *The Journal of Strategic Information Systems, Volume 11, Issues 3-4, σσ. 245-270*. doi:https://doi.org/10.1016/S0963-8687(02)00018-5
- Bhattacharya, R., Devinney, T., & Pillutla, M. (1998). A Formal Model of Trust Based on Outcomes. *The Academy of Management Review, 23(3), 459*. doi:doi:10.2307/259289
- Blind, P. (2007). Building Trust in Government in the Twenty-First Century: Review of Literature and Emerging Issues. *7th Global Forum on Reinventing Government, Building Trust in Government*.
- Brough, A., & Martin, K. (2021). Consumer privacy during (and after) the COVID-19 pandemic. *Journal of Public Policy & Marketing, Volume 40, issue 1, p. 108-110*. doi:10.1177/0743915620929999
- Carter, L., & Belanger, F. (2005). The utilization of e-government services: citizen trust, innovation and acceptance factors. *Information Systems Journal, 15 (1), 5-25*.

- Carter, L., & Weerakkody, V. (2008). E-government adoption: A cultural comparison. *Information systems*, 10, pp. 473-482. doi:10.1007/s10796-008-9103-6
- Colesca, S. (2009). Increasing e-trust: A solution to minimize risk in e-government adoption. *Journal of Applied Quantitative Methods*, Volume 4, Issue 1.
- Collins, H. (2010). *Creative Research: The Theory and Practice of Research for the Creative Industries*. AVA Publications.
- Creswell, J. (2009). *Research Design: Qualitative, Quantitative, and Mixed-Method Approaches*. Sage Publications.
- Crossler, R., & Bélanger, F. (2017). The Mobile Privacy-Security Knowledge Gap Model: Understanding Behaviors. *Proceedings of the 50th Hawaii International Conference on System Sciences*. doi:10.24251/HICSS.2017.491
- Davis, F. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340. doi:10.2307/249008
- Davis, F., Bagozzi, R., & Warshaw, P. (1989). User acceptance of computer technology: a comparison of two theoretical models. *Management Science*, 35 (8), 982–1003.
- Doney, P., & Cannon, J. (1997). An Examination of the Nature of Trust in Buyer-Seller Relationships. *Journal of Marketing*, 61(2), 35-51. doi:10.2307/1251829
- Eck, K., & Hatz, S. (2020). State surveillance and the COVID-19 crisis. *Journal of Human Rights*, Volume 19, Issue 5, p.603-612. doi:10.1080/14754835.2020.1816163
- European Commission . (2020). *Standard Eurobarometer 93: The EU and the coronavirus outbreak*. doi:10.2775/652700
- European Commission. (2019). *Standard Eurobarometer 92*. Ανάκτηση 29/8/2021, από <https://europa.eu/eurobarometer/surveys/detail/2255>
- European Commission. (2020). *Digital Economy and Society Index (DESI) 2020*. Ανάκτηση 11/9/2021, από <https://digital-strategy.ec.europa.eu/en/policies/desi-greece>
- European Commission. (2020a). Communication from the Commission Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection. *Official Journal of the European Union*(2020/C 124 I/01). Ανάκτηση 5/9/2021, από <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020XC0417%2808%29>
- European Commission. (2021). *Standard Eurobarometer 94*. Ανάκτηση 29/8/2021, από <https://europa.eu/eurobarometer/surveys/detail/2355>
- FTC. (2021). *Consumer Sentinel Network Data Book 2020*. Ανάκτηση 20/7/2021, από Federal Trade Commission: https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf
- Fukuyama, F. (1995). Social Capital and the Global Economy: A Redrawn Map of the World. *Foreign Affairs*, Volume 75, No. 4.
- Garg S, Bhatnagar N, Gangadharan N. (2020). A Case for Participatory Disease Surveillance of the COVID-19 Pandemic in India. *JMIR Public Health Surveill*. doi:10.2196/18795

- Gilbert, D., Balestrini, P., & Littleboy, D. (2004). Barriers and Benefits in the adoption of e-government. *The International Journal of Public Sector Management*, Vol. 17, No. 4, pp.296-301. doi:10.1108/09513550410539794
- Grandison, T., & Sloman, M. (2000). A survey of trust in internet applications. *IEEE Communications Surveys & Tutorials*, vol. 3, no. 4, pp. 2-16. doi:10.1109/COMST.2000.5340804
- Halpern, D. (1999). *Social Capital: the New Golden Goose*. Cambridge: Faculty of Social and Political Sciences, Cambridge University.
- Harari, Y. (2020). The world after coronavirus. *The Financial Times*. Ανάκτηση 4/10/2021, από https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75?fbclid=IwARlucVmXDQapaiS2_Lo0IDyqCkzCahpU0WU0gr06MJTYQ47pBgdM-4eoEV0
- Herbster, R., DellaTorre, S., Druschel, P., & Bhattacharjee, B. (2016). Privacy Capsules: Preventing Information Leaks by Mobile Apps. *Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services Companion - ACM MobiSys*, p.399-411. doi:10.1145/2906388.2906409
- Higgins, J., & Thomas, J. (2021). *Cochrane Handbook for Systematic Reviews of Interventions (Version 6.2)*. Ανάκτηση 26/7/2021, από Cochrane: www.training.cochrane.org/handbook
- Hoffman, D., Novak, T., & Peralta, M. (1999). Building consumer trust online. *Commun. ACM*, 42, 4, σσ. 80–85. doi:<https://doi.org/10.1145/299157.299175>
- Horst, M., Kuttschreuter, M., & Gutteling, J. (2007). Perceived usefulness, personal experiences, risk perception and trust as determinants of adoption of e-government services in The Netherlands. *Computers in Human Behavior*, 23(4), 1838–1852. doi:10.1016/j.chb.2005.11.003
- Howell, D. (2020). A Pandemic Of Data Sharing? Silicon UK [online]. Ανάκτηση 12/7/2021, από <https://www.silicon.co.uk/e-regulation/governance/a-pandemic-of-data-sharing-346438>
- Hung, S., Chang, C., & Yu, T. (2006). Determinants of user acceptance of the e-Government services: The case of online tax filing and payment system. *Government Information Quarterly*, 23, pp. 97–122. doi:10.1016/j.giq.2005.11.005
- Johnson, V., Kiser, A., Washington, R., & Torres, R. (2018). Limitations to the rapid adoption of M-payment services: Understanding the impact of privacy risk on M-payment services. *Computers in Human Behavior*, Volume 79, p. 111-122. doi:10.1016/j.chb.2017.10.035
- Kim, D., Steinfield, C., & Lai, Y. (2008). Revisiting the role of web assurance seals in business-to-consumer electronic commerce. *Decision Support Systems*, 44 (4), p. 1000-1015. doi:10.1016/j.dss.2007.11.007
- Klassen, T., Jadad, A., & Moher, D. (1998). Guides for reading and interpreting systematic reviews: I. Getting started. *Arch Pediatr Adolesc Med*. 152(7):700-4.
- Lee, K., Kang, I., & McKnight, D. (2007). Modeling Initial and Repeat Online Trust in B2C E-Commerce. *IEEE Transactions on Engineering Management*, 54 (4): 729–741. doi:10.1109/TEM.2007.906851

- Legris, P., Ingham, J., & Colletrette, P. (2003). Why do people use information technology? A critical review of the technology acceptance model. *Information & Management, Volume 40, Issue 3, Pages 191-204*. doi:[https://doi.org/10.1016/S0378-7206\(01\)00143-4](https://doi.org/10.1016/S0378-7206(01)00143-4)
- Levi, M. (1997). *Consent, Dissent and Patriotism*. Cambridge University Press, New York. .
- Lewicki, R., & Bunker, B. (1995). *Trust in relationships: A model of trust development and decline*. In B. Bunker & J. Rubin (Eds.)*Conflict, cooperation and justice: . San Francisco: Jossey-Bass*.
- Lewis, J., & Weigert, A. (1985). Trust as a Social Reality. *Social Forces, 63(4), 967-985*. doi:10.2307/2578601
- Li, X., Valacich, J., & Hess, T. (2004). Predicting User Trust in Information Systems: A Comparison of Competing Trust. *Proceedings of the 37th Hawaii International Conference on System Sciences, Vol. 8*. doi:10.1109/HICSS.2004.1265619
- Lin, J., Lu, Y., Wang, B., & Wei, K. (2011). The role of inter-channel trust transfer in establishing mobile commerce trust. *Electronic Commerce Research and Applications, 10, 615-625*. doi:10.1016/j.elerap.2011.07.008.
- Luhmann, N. (1979). *Trust and Power*. New York: John Wiley & Sons.
- Luo, H., Yu, Y., Huang, W., Liang, J., & Yang, L. (2017). Empirical research on the influencing factors of consumers' trust transfer from offline to online channel. *International Conference on Service Systems and Service Management, pp. 1-5*. doi:10.1109/ICSSSM.2017.7996200
- Lutes, K. (2012). Cross-Platform Mobile App Software. *Journal of Issues in Informing Science and Information Technology (IISIT), 9:115-124*.
- Mathur, A., & Maheshwari, G. (2021). The state of data privacy in the mobile apps space. *Sunday Guardian*. Ανάρτηση 28/9/2021, από <https://www.sundayguardianlive.com/legally-speaking/state-data-privacy-mobile-apps-space>
- Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An Integrative Model Of Organizational Trust. *Academy of Management Review, 20(3), 709-734*. doi:10.5465/amr.1995.9508080335
- McKnight, D., & Chervany, N. (2002). What trust means in e-commerce customer relationships: an interdisciplinary conceptual. *International Journal of Electronic Commerce, Volume 6, Issue 2*. doi:<https://doi.org/10.1080/10864415.2001.11044235>
- Mcknight, D., Choudhury, V., & Kacmar, C. (2002a). Developing and Validating Trust Measures for e-Commerce: An Integrative Typology. *Information Systems Research, 13(3):334-359*. doi:10.1287/isre.13.3.334.81
- McKnight, D., Cummings, L., & Chervany, N. (1998). Initial trust formation in new organizational relationships. *Academy of Management Review(23 (3), 473-490)*.
- Morrone, A., Tontoranelli, N., & Ranuzzi, G. (2009). How Good is Trust? Measuring Trust and its role for the progress of societies. *OECD Statistics Working Papers 2009/03*. doi:<https://dx.doi.org/10.1787/220633873086>
- Nah, F., Siau, K., & Sheng, H. (2005). The Value of Mobile Applications: A Utility Company Study. *Communications of the ACM, 48 (2): 85-90*. doi:doi:10.1145/1042091.1042095

- Nel, J., & Boshoff, C. (2017). Development of application-based mobile-service trust and online trust transfer: an elaboration likelihood model perspective. *Behaviour & Information Technology*. doi:10.1080/0144929X.2017.1296493
- Nel, J., & Boshoff, C. (2017). Development of application-based mobile-service trust and online trust transfer: an elaboration likelihood model perspective. *Behaviour & Information Technology*, 36(8), 809–826. doi:10.1080/0144929X.2017.1296493
- Nunnally, J., & Bernstein, I. (1994). *Psychometric Theory (3rd ed.)*. New York: McGraw-Hill, Inc.
- OECD. (2017). Trust and Public Policy: How Better Governance Can Help Rebuild Public Trust. *OECD Public Governance Reviews*, OECD Publishing. doi:http://dx.doi.org/10.1787/9789264268920-en
- OECD. (2017a). *Embracing Innovation in Government - Global Trends*. Ανάκτηση 20/7/2021, από Organisation for Economic Cooperation and Development: <https://www.oecd.org/gov/innovative-government/embracing-innovation-in-government.pdf>
- OECD. (2019). *Strengthening Digital Government*. OECD Going Digital Policy Note. Ανάκτηση 1/9/2021, από www.oecd.org/goingdigital/strengthening-digital-government.pdf
- Ooi, K., & Tan, G. (2016). Mobile technology acceptance model: An investigation using mobile users to explore smartphone credit card. *Expert Systems with Applications, Volume 59*, p. 33-46. doi: 10.1016/j.eswa.2016.04.015
- Papadopoulou, P., Nikolaidou, M., & Martakos, D. (2010). What Is Trust in E-Government? A Proposed Typology. *43rd Hawaii International Conference on System Sciences*, pp. 1-10. doi:10.1109/HICSS.2010.491
- Pavlou, P. (2002). Institution-based trust in interorganizational exchange relationships: the role of online B2B marketplaces on trust formation. *The Journal of Strategic Information Systems, Volume 11, Issues 3–4*, 215-243. doi:10.1016/S0963-8687(02)00017-3
- Perk, H., & Halliday, S. (2003). Sources, signs and signaling for fast trust creation in organizational relationships. *European Management Journal, Volume 21, Issue 3*, p. 338-350. doi:10.1016/S0263-2373(03)00049-5
- Rodriguez, K., Windwehr, S., & Schoen, S. (2020). International Proposals for Warrantless Location Surveillance To Fight COVID-19. *Electronic Frontier Foundation, EFF*. doi:https://www.eff.org/deeplinks/2020/05/global-contact-tracing-international-proposals-track-COVID-19
- Roth, F. (2006). Trust and Economic Growth: Conflicting Results Between Cross-Sectional and Panel. *Ratio Working Papers 102*. The Ratio Institute.
- Rotter, J. (1980). Interpersonal trust, trustworthiness, and gullibility. *American Psychologist*, 35(1), 1–7. doi:https://doi.org/10.1037/0003-066X.35.1.1
- Rousseau, D., Sitkin, S., Burt, R., & Camerer, C. (1998). Not So Different After All: A Cross-discipline View of Trust. *Academy of Management Review*, 23(3). doi:10.5465/AMR.1998.926617
- Shapiro, S. (1987). The Social Control of Impersonal Trust. *American Journal of Sociology*, Vol. 93, No.3, 623 - 658.

- Shekarpour, S., & Katebi, S. (2010). Modeling and evaluation of trust with an extension in semantic web . *Journal of Web Semantics, Vol. 8. Issue 1, p. 26-36.*
doi:10.1016/j.websem.2009.11.003
- Statista. (2021). *Number of apps available in leading app stores 2021.* Statista Research Department. Ανάκτηση 18/9/2021, από <https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/>
- Stevens, W. and Haines, M.B. (2020). TraceTogether: Pandemic response, democracy, and technology. *East Asian Science Technology and Society an International Journal.*
doi:10.1215/18752160-8698301
- Stewart, K. (2003). Trust transfer on the World Wide Web. *Organization Science, 14(1):5-17.*
doi:0.1287/orsc.14.1.5.12810
- Stewart, K. (2006). How hypertext links influence consumer perceptions to build and degrade trust online. *Journal of Management Information Systems., 23, 1, 183–210.*
doi:10.2753/MIS0742-1222230106
- Tran, C., & Nguyen, T. (2021). Health vs. privacy? The risk-risk tradeoff in using COVID-19 contact-tracing apps. *Technology in Society, Volume 67.*
doi:10.1016/j.techsoc.2021.101755
- United Nations. (2020). *UN e-Government Survey 2020. Digital Government in the Decade of Action for Sustainable Development.* Department of Economic and Social Affairs, Division for Public Institutions and Digital Government. Ανάκτηση 2/9/2021, από <https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2020>
- Uslaner, E. (2002). *The Moral Foundations of Trust.* Cambridge: Cambridge University Press.
- Van Slyke, C., Belanger, F., & Comunale, C. (2004). Adopting business-to-consumer electronic commerce: the effects of trust and perceived innovation characteristics. *The Data Base for Advances in Information Systems, Volume 35(Issue 2), σσ. 32-49.*
- Veenstra, G. (2002). Explicating Social Capital: Trust and Participation in the Civil Space. *Canadian Journal of Sociology, Vol. 27, Nr. 4, pp. 547-572.*
- Wang, N., Shen, X., & Sun, Y. (2013). Transition of electronic word-of-mouth services from web to mobile context: A trust transfer perspective. *Decision Support Systems, 54(3):1394–1403.* doi:10.1016/j.dss.2012.12.015
- Warkentin, M., Gefen, D., Pavlou, P., & Rose, G. (2002). Encouraging Citizen Adoption of e-Government by Building Trust. *Electronic Markets(12. 157-162).*
doi:10.1080/101967802320245929.
- Welch, E., Hinnant, C., & Moon, M. (2004). Linking Citizen Satisfaction with E-Government and Trust in Government. *Journal of Public Administration Research and Theory, 15, σσ. 371-391.* doi:<https://doi.org/10.1093/JOPART/MUI021>
- Wottrich, V., Van Reijmersdal, E., & Smit, E. (2018). The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. *Decision Support Systems, Volume 106, p. 44-52.* doi:10.1016/j.dss.2017.12.003
- Yan, Z., Dong, Y., Niemi, V., & Yu, G. (2010). Exploring Trust of Mobile Applications Based on User Behaviors. *Lecture Notes in Computer Science., 212–226.* doi:10.1007/978-3-642-14597-1_13

- Yun, H., Lee, G., & Kim, D. (2019). A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs. *Information & Management, Volume 56, Issue 4, p. 570-601*. doi:10.1016/j.im.2018.10.001
- Δημητρόπουλος, Ε. (2004). *Εισαγωγή στη μεθοδολογία της επιστημονικής έρευνας: Προς ένα συστηματικό δυναμικό μοντέλο μεθοδολογίας επιστημονικής έρευνας*. Αθήνα: ΕΛΛΗΝ.
- Ελληνική Δημοκρατία. (2021). Διαθέσιμη η εφαρμογή «Covid Free GR». ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΠΟΛΙΤΙΚΗΣ, ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ & ΕΝΗΜΕΡΩΣΗΣ. Ανάκτηση 5/9/2021, από <https://government.gov.gr/diathesimi-efarmogi-covid-free-gr/>
- ΕΛΣΤΑΤ. (2019). Έρευνα Χρήσης Τεχνολογιών Πληροφόρησης και Επικοινωνίας από Νοικοκυριά και Άτομα, 2020. *Ελληνική Στατιστική Αρχή*. Ανάκτηση 13/7/2021, από <https://www.statistics.gr/el/infographic-information-technologies-2019>
- Λαγουμιντζής, Γ., Βλαχόπουλος, Γ., & Κουτσογιάννης, Κ. (2015). *Μέθοδοι Συλλογής Δεδομένων. [Κεφάλαιο Συγγράμματος]. Στο Λαγουμιντζής, Γ., Βλαχόπουλος, Γ., Κουτσογιάννης, Κ. 2015. Μεθοδολογία της έρευνας στις επιστήμες υγείας. [ηλεκτρ. βιβλ.]. Αθήνα: Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών. κεφ. 4. Ανάκτηση από <http://hdl.handle.net/11419/5360>*
- Παρασκευόπουλος, Ι. (1993). *Μεθοδολογία επιστημονικής έρευνας. Έννοια, Χαρακτηριστικά, Είδη και Στάδια της Επιστημονικής Έρευνας (Τόμ. Ι)*. ΑΘΗΝΑ.
- Υπουργείο Ψηφιακής Διακυβέρνησης. (2020). *Βίβλος Ψηφιακού Μετασχηματισμού 2020-2025*. Ελληνική Δημοκρατία. Ανάκτηση 11/9/2021, από <http://www.opengov.gr/digitalandbrief/wp-content/uploads/downloads/2020/12/digitalstrategy.pdf>

ΠΑΡΑΡΤΗΜΑ

I. Το ερωτηματολόγιο της έρευνας – Google Forms

11/11/21, 10:04 μ.μ.

Ερωτηματολόγιο Διπλωματικής Εργασίας

Ερωτηματολόγιο Διπλωματικής Εργασίας

Το ερωτηματολόγιο συντάχθηκε στο πλαίσιο της εκπόνησης Διπλωματικής Εργασίας με τίτλο "Μεταβίβαση εμπιστοσύνης σε φορητές εφαρμογές ευρείας χρήσης" για το Πρόγραμμα Μεταπτυχιακών Σπουδών "Ευέλικτες Μέθοδοι Διοίκησης" του Τμήματος Διοίκησης Επιχειρήσεων του Πανεπιστημίου Θεσσαλίας.

Η συμμετοχή σ' αυτή την έρευνα είναι εθελοντική και διασφαλίζεται η ανωνυμία των συμμετεχόντων και η εμπιστευτικότητα των δεδομένων, σύμφωνα με τις απαιτήσεις του ν.4624/2019 περί προστασίας προσωπικών δεδομένων (GDPR). Τα δεδομένα που θα συλλεχθούν θα χρησιμοποιηθούν αποκλειστικά για τους σκοπούς της έρευνας.

Ο απαιτούμενος χρόνος για την συμπλήρωσή του είναι περίπου 5 λεπτά.

Σας ευχαριστώ για την ανταπόκριση.

* Απαιτείται

Στόχος έρευνας

Στόχος της παρούσας έρευνας είναι να εξετάσει το κατά πόσο η εμπιστοσύνη των πολιτών στο Κράτος μπορεί να μεταβιβαστεί στις online υπηρεσίες που παρέχονται στον πολίτη για την διακπαρσίωση των υποθέσεών του με το δημόσιο, όπως π.χ. την άμεση έκδοση πιστοποιητικών και ποιοι είναι οι παράγοντες που επηρεάζουν ή αποθαρρύνουν τους πολίτες στην πρόθεσή τους να τις χρησιμοποιήσουν.

1. 1. Οι ηλεκτρονικές υπηρεσίες του κράτους είναι εύκολες στη χρήση. *

Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Διαφωνώ απόλυτα	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Συμφωνώ απόλυτα

2. 2. Οι ηλεκτρονικές υπηρεσίες του κράτους παρέχουν κατανοητές οδηγίες για τον τρόπο χρήσης των υπηρεσιών. *

Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Διαφωνώ απόλυτα	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Συμφωνώ απόλυτα

<https://docs.google.com/forms/d/1P0laHoDnVdL5dyLTxP20gV6M/W/viewform?edit>

1/8

3. 3. Οι ηλεκτρονικές υπηρεσίες του κράτους είναι εύκολα προσβάσιμες από το κινητό. *

Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Διαφωνώ απόλυτα	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Συμφωνώ απόλυτα

4. 4. Οι ηλεκτρονικές υπηρεσίες του κράτους είναι εύκολες στην πλοήγηση από κινητό. *

Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Διαφωνώ απόλυτα	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Συμφωνώ απόλυτα

5. 5. Οι ηλεκτρονικές υπηρεσίες του κράτους δεν απαιτούν επιπλέον χρόνο και κόπο σε σχέση με την αυτοπρόσωπη εξυπηρέτηση στις κατά τόπους υπηρεσίες. *

Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Διαφωνώ απόλυτα	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Συμφωνώ απόλυτα

6. 6. Οι ηλεκτρονικές υπηρεσίες του κράτους παρέχουν χρήσιμες πληροφορίες στον πολίτη. *

Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Διαφωνώ απόλυτα	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Συμφωνώ απόλυτα

7. 7. Οι ηλεκτρονικές υπηρεσίες του κράτους ενισχύουν την αμφίδρομη επικοινωνία πολίτη-κράτους. *

Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Διαφωνώ απόλυτα	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Συμφωνώ απόλυτα

8. 8. Οι πολίτες εμπιστεύονται τις υπηρεσίες του κράτους για τη διεκπεραίωση των αιτημάτων τους. *

Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Διαφωνώ απόλυτα	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Συμφωνώ απόλυτα

9. 9. Οι ηλεκτρονικές υπηρεσίες του κράτους παρέχουν στους πολίτες άμεσες λύσεις στην διεκπεραίωση αιτημάτων τους. *

Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Διαφωνώ απόλυτα	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Συμφωνώ απόλυτα

10. 10. Οι ηλεκτρονικές υπηρεσίες του κράτους ανταποκρίνονται αποτελεσματικά στα αιτήματα του πολίτη. *

Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Διαφωνώ απόλυτα	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Συμφωνώ απόλυτα

11. 11. Αισθάνομαι ότι είναι ασφαλές να χρησιμοποιήσω μια υπηρεσία ηλεκτρονικής διακυβέρνησης. *

Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Διαφωνώ απόλυτα	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Συμφωνώ απόλυτα

12. 12. Η Κυβέρνηση λαμβάνει όλα τα απαραίτητα μέτρα για τη σωστή λειτουργία των πληροφοριακών της συστημάτων. *

Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Διαφωνώ απόλυτα	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Συμφωνώ απόλυτα

13. 13. Η Κυβέρνηση λαμβάνει όλα τα απαραίτητα μέτρα για την προστασία των πληροφοριακών συστημάτων της από απειλές. *

Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Διαφωνώ απόλυτα	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Συμφωνώ απόλυτα

14. 14. Η κυβέρνηση διασφαλίζει την προστασία των προσωπικών μου δεδομένων από μη εξουσιοδοτημένη πρόσβαση. *

Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Διαφωνώ απόλυτα	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Συμφωνώ απόλυτα

15. 16. Η κυβέρνηση διασφαλίζει ότι τα δεδομένα που συλλέγονται θα χρησιμοποιούνται αποκλειστικά για τον σκοπό που συλλέχθηκαν.*

Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Διαφωνώ απόλυτα	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Συμφωνώ απόλυτα

16. 16. Η κυβέρνηση διασφαλίζει ότι τα δεδομένα που συλλέγονται δεν κοινοποιούνται σε άλλους φορείς/υπηρεσίες χωρίς τη συγκατάθεση μου.*

Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Διαφωνώ απόλυτα	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Συμφωνώ απόλυτα

17. 17. Η κυβέρνηση διασφαλίζει ότι τα δεδομένα που εισάγω δεν παραποιούνται.*

Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Διαφωνώ απόλυτα	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Συμφωνώ απόλυτα

18. 18. Η κυβέρνηση λαμβάνει όλα τα απαραίτητα νομικά μέτρα για την προστασία μου.*

Να επισημαίνεται μόνο μία έλλειψη.

	1	2	3	4	5	
Διαφωνώ απόλυτα	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Συμφωνώ απόλυτα

II. Correlation Matrix

	TGS1	TGS2	PEU1	PEU2	PEU3	PEU4	PEU5	PU1	PU2	PU3	TSY1	TSY2	TSY3	TSY4	TD1	TD2	TT1	TT2	IT1	IU1
TGS1	1,000	,728	,494	,413	,341	,267	,459	,400	,430	,673	,400	,478	,300	,092	,274	,296	,313	,357	,387	,297
TGS2	,728	1,000	,510	,471	,356	,261	,500	,407	,413	,606	,472	,474	,424	,085	,332	,281	,294	,330	,343	,306
PEU1	,494	,510	1,000	,584	,394	,341	,441	,497	,363	,406	,255	,352	,257	,188	,228	,203	,227	,252	,321	,212
PEU2	,413	,471	,584	1,000	,410	,377	,397	,425	,341	,376	,227	,426	,361	,116	,240	,225	,146	,220	,345	,143
PEU3	,341	,356	,394	,410	1,000	,767	,249	,366	,238	,238	,359	,449	,410	,112	,379	,315	,380	,306	,362	,195
PEU4	,267	,261	,341	,377	,767	1,000	,159	,329	,294	,219	,303	,442	,450	,167	,398	,414	,438	,386	,456	,171
PEU5	,459	,500	,441	,397	,249	,159	1,000	,374	,266	,401	,314	,358	,225	-,047	,218	,186	,209	,223	,249	,354
PU1	,400	,407	,497	,425	,366	,329	,374	1,000	,425	,280	,311	,442	,384	,064	,357	,287	,361	,353	,436	,259
PU2	,430	,413	,363	,341	,238	,294	,266	,425	1,000	,409	,425	,405	,365	,102	,360	,373	,327	,349	,357	,303
PU3	,673	,606	,406	,376	,238	,219	,401	,280	,409	1,000	,210	,404	,268	,019	,241	,221	,192	,249	,319	,278
TSY1	,400	,472	,255	,227	,359	,303	,314	,311	,425	,210	1,000	,561	,583	-,159	,581	,520	,524	,544	,524	,476
TSY2	,478	,474	,352	,426	,449	,442	,358	,442	,405	,404	,561	1,000	,733	-,046	,633	,598	,475	,450	,595	,308
TSY3	,300	,424	,257	,361	,410	,450	,225	,384	,365	,268	,583	,733	1,000	-,008	,743	,633	,607	,603	,639	,388
TSY4	,092	,085	,188	,116	,112	,167	-,047	,064	,102	,019	-,159	-,046	-,008	1,000	-,052	-,054	,005	-,073	-,057	-,159
TD1	,274	,332	,228	,240	,379	,398	,218	,357	,360	,241	,581	,633	,743	-,052	1,000	,747	,734	,749	,745	,438
TD2	,296	,281	,203	,225	,315	,414	,186	,287	,373	,221	,520	,598	,633	-,054	,747	1,000	,796	,714	,730	,422
TT1	,313	,294	,227	,146	,380	,438	,209	,361	,327	,192	,524	,475	,607	,005	,734	,796	1,000	,765	,707	,479
TT2	,357	,330	,252	,220	,306	,386	,223	,353	,349	,249	,544	,450	,603	-,073	,749	,714	,765	1,000	,763	,440
IT1	,387	,343	,321	,345	,362	,456	,249	,436	,357	,319	,524	,595	,639	-,057	,745	,730	,707	,763	1,000	,384
IU1	,297	,306	,212	,143	,195	,171	,354	,259	,303	,278	,476	,308	,388	-,159	,438	,422	,479	,440	,384	1,000