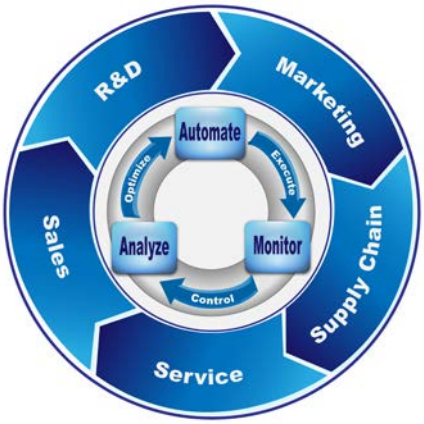
Πλοήγηση στο διαδίκτυο και ηλεκτρονικά προσωπικά δεδομένα
Μέτρηση βαθμού ικανοποίησης χρηστών της ιστοσελίδας και του newsletter της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Αϊδίνης Κωνσταντίνος

Πρόγραμμα Μεταπτυχιακών Σπουδών:

Αυτοματισμός Παραγωγής και Υπηρεσιών



ΔΙΑΤΡΙΒΗ

Πειραιάς, Φεβρουάριος 2018

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΑΥΤΟΜΑΤΙΣΜΟΥ
Π.ΡΑΛΛΗ & ΘΗΒΩΝ 250, 122 44, ΑΙΓΑΛΕΩ, ΑΘΗΝΑ, ΕΛΛΑΔΑ
ΤΗΛ.: +30-210-5381311, MSCAUTO1@TEIPIR.GR

Μεταπτυχιακή Διατριβή που υποβάλλεται στο καθηγητικό σώμα για την μερική εκπλήρωση των υποχρεώσεων απόκτησης του μεταπτυχιακού τίτλου του Μεταπτυχιακού Προγράμματος «Αυτοματισμός Παραγωγής και Υπηρεσιών» του Τμήματος Μηχανικών Αυτοματισμού του Ανώτατου Εκπαιδευτικού Ιδρύματος Πειραιώς Τεχνολογικού Τομέα.

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

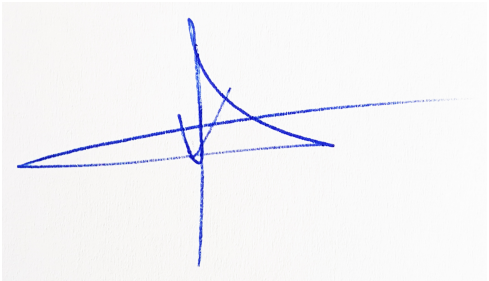
Ο κάτωθι υπογεγραμμένος **Αϊδίνης Κωνσταντίνος**, του **Γεωργίου**, με αριθμό μητρώου **33** φοιτητής του Τμήματος **Μηχανικών Αυτοματισμού Τ.Ε.** του Α.Ε.Ι. Πειραιά Τ.Τ. πριν αναλάβω την εκπόνηση της Πτυχιακής Εργασίας μου, δηλώνω ότι ενημερώθηκα για τα παρακάτω:

«Η Πτυχιακή Εργασία (Π.Ε.) αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο του συγγραφέα, όσο και του Ιδρύματος και θα πρέπει να έχει μοναδικό χαρακτήρα και πρωτότυπο περιεχόμενο.

Απαγορεύεται αυστηρά οποιοδήποτε κομμάτι κειμένου της να εμφανίζεται αυτούσιο ή μεταφρασμένο από κάποια άλλη δημοσιευμένη πηγή. Κάθε τέτοια πράξη αποτελεί προϊόν λογοκλοπής και εγείρει θέμα Ηθικής Τάξης για τα πνευματικά δικαιώματα του άλλου συγγραφέα. Αποκλειστικός υπεύθυνος είναι ο συγγραφέας της Π.Ε., ο οποίος φέρει και την ευθύνη των συνεπειών, ποινικών και άλλων, αυτής της πράξης.

Πέραν των όποιων ποινικών ευθυνών του συγγραφέα σε περίπτωση που το Ίδρυμα του έχει απονείμει Πτυχίο, αυτό ανακαλείται με απόφαση της Συνέλευσης του Τμήματος. Η Συνέλευση του Τμήματος με νέα απόφασης της, μετά από αίτηση του ενδιαφερόμενου, του αναθέτει εκ νέου την εκπόνηση της Π.Ε. με άλλο θέμα και διαφορετικό επιβλέποντα καθηγητή. Η εκπόνηση της εν λόγω Π.Ε. πρέπει να ολοκληρωθεί εντός τουλάχιστον ενός ημερολογιακού 6μήνου από την ημερομηνία ανάθεσης της. Κατά τα λοιπά εφαρμόζονται τα προβλεπόμενα στο άρθρο 18, παρ. 5 του ισχύοντος Εσωτερικού Κανονισμού.»

Ο Δηλών



Ημερομηνία
27/02/2018

«Αφιερωμένο στους γονείς μου,

στα παιδιά μου Μελίνα και Γιώργο

και στην σύζυγο μου Μαρία.…..»

ΠΕΡΙΛΗΨΗ

Τα τελευταία χρόνια η ανθρωπότητα ζει σε κλίμα αβεβαιότητας όσον αφορά την προστασία των προσωπικών δεδομένων. Η προστασία της ιδιωτικής ζωής θα αφορά, στο εξής, όχι μόνον το περιεχόμενο, αλλά και τα μεταδεδομένα που προκύπτουν από τις ηλεκτρονικές επικοινωνίες. Στην Ελλάδα η συμβολή της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) στη διαμόρφωση ενός φιλικού στην προστασία δεδομένων περιβάλλοντος είναι μεγάλη. Η μόνη βιώσιμη άμυνα έναντι των κινδύνων της ιδιωτικότητας είναι η ενδυνάμωση των «ψηφιακών πολιτών», η οποία επιτυγχάνεται μέσω της ενημέρωσης και της εκπαίδευσής τους για τους ψηφιακούς κινδύνους, τα δικαιώματα και τις υποχρεώσεις τους.

Με επίκεντρο λοιπόν τους «ψηφιακούς πολίτες», η συγκεκριμένη μελέτη έχει ως αντικείμενό της την προστασία της ιδιωτικής ζωής σε συνάρτηση με την ψηφιακή παγκοσμιοποίηση και την ραγδαία εξέλιξη των ηλεκτρονικών επικοινωνιών. Το βασικό ερώτημα στο οποίο θα προσπαθήσει να δώσει απάντηση η παρούσα εργασία είναι αν υπάρχει προστασία δεδομένων στην νέα εποχή των Τεχνολογιών Πληροφορικής και Επικοινωνιών που διανύει η ανθρωπότητα.

Πιο συγκεκριμένα, σκοπός της παρούσας διατριβής είναι να αντληθούν χρήσιμα συμπεράσματα σχετικά με το κατά πόσο οι πολίτες γνωρίζουν τη νομοθεσία για την προστασία προσωπικών δεδομένων, και κατέχουν τις απαραίτητες γνώσεις και δεξιότητες αναφορικά με την πλοήγηση στο διαδίκτυο και τη χρήση συναφών υπηρεσιών και μέσων κοινωνικής δικτύωσης.

Επίσης, επιχειρείται για πρώτη φορά η αξιολόγηση της ιστοσελίδας (www.dpa.gr) και του ενημερωτικού δελτίου (newsletter) της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και στο κατά πόσο οι πολίτες γνωρίζουν την ύπαρξή τους. Η αξιολόγηση αφορά στο ποια είναι η γνώμη των πολιτών για το περιεχόμενο, τη σχεδίαση και την πλοήγηση της ιστοσελίδας και την ανάγνωση του ενημερωτικού δελτίου.

Για την επίτευξη του ανωτέρου στόχου καταρτίσθηκε ειδικό ερωτηματολόγιο, που αποτέλεσε το κύριο μέσο άντλησης πληροφοριών για την υλοποίηση της μελέτης. Το ειδικό ερωτηματολόγιο αποτελείται από τρία μέρη: Α. Δημογραφικές ερωτήσεις, Β.

Βαθμός ενημέρωσης των πολιτών σχετικά με το ισχύον νομοθετικό πλαίσιο για την προστασία των προσωπικών δεδομένων και με τις γνώσεις και δεξιότητές τους αναφορικά με τη πλοήγηση στο διαδίκτυο και τη χρήση συναφών υπηρεσιών και μέσων κοινωνικής δικτύωσης, Γ. Αξιολόγηση της ιστοσελίδας και του ενημερωτικού δελτίου της Αρχής.

Η στατιστική ανάλυση πραγματοποιήθηκε με την χρήση του εξειδικευμένου στατιστικού λογισμικού Statistical Package for Social Sciences (SPSS22). Τα συμπεράσματα που εξήχθησαν από την στατιστική ανάλυση 153 ερωτηματολογίων που συμπληρώθηκαν θα επιφέρουν αποδοτικότερη διαχείριση των πόρων της Αρχής και ποιοτικότερες υπηρεσίες προς τους πολίτες, με σκοπό να δημιουργηθούν ικανές εγγυήσεις για την ιδιωτική ζωή και να διαμορφωθεί ένα ισχυρό πλαίσιο προστασίας.

Οι πολίτες, οι εκπαιδευτικοί, οι δημόσιοι υπάλληλοι, οι μελλοντικοί προγραμματιστές και επιστήμονες και, φυσικά, οι πολιτικοί και οι νομοθέτες θα πρέπει να είναι ενημερωμένοι για την προστασία της ιδιωτικής τους ζωής και τις επιπτώσεις των διαδικτυακών συμπεριφορών τους.

Λέξεις κλειδιά: *Προσωπικά Δεδομένα, Διαδίκτυο, Ιδιωτικότητα, SPSS*

ABSTRACT

In recent years, humanity has been living in a state of uncertainty regarding the protection of personal data. Protection of privacy will henceforth concern not only content but also metadata resulting from electronic communications. In Greece, the contribution of the Personal Data Protection Authority (DPA) to the development of a data friendly environment is great. The only sustainable defense against the dangers of privacy is the empowerment of "digital citizens", which is achieved through information and education about digital hazards, rights and obligations.

Focusing on "digital citizens", this study's scope is the protection of privacy in connection with digital globalization and accordingly the rapid development of electronic communications. The key question to be addressed in the present work is whether data protection actually exists in the new era of Information and Communication Technologies that mankind is experiencing.

More specifically, the purpose of this dissertation is to draw useful conclusions as to whether citizens are aware of the data protection legislation and possess the necessary knowledge and skills regarding navigation and the use of related services and social media.

It is also being attempted for the first time to evaluate the website (www.dpa.gr) and the newsletter of the Personal Data Protection Authority and to conclude whether citizens are aware of their existence. What is really evaluated, concerns the citizens' opinion about the content, design and navigation of the website as well as reading the newsletter.

In order to achieve this goal, a specific questionnaire was designed, from which information was obtained for the implementation of the study. The specific questionnaire consists of three parts: A. Demographic questions, B. Degree of informing citizens about the current legal framework for the protection of personal data and possession of the necessary knowledge and skills regarding navigation and the use of related services and social media, C. Evaluation of the Authority's website and newsletter.

The statistical analysis was conducted using the Statistical Package for Social Sciences (SPSS22). The conclusions drawn from the statistical analysis of 153 completed questionnaires will result in a more efficient management of the Authority's resources and in better services towards citizens in order to create adequate safeguards for privacy and a strong framework of protection.

Citizens, educators, civil servants, future developers and scientists and, of course, politicians and legislators should be aware of the protection of their privacy and the impact of their internet behaviors.

Keywords: *Personal Data, Internet, Privacy, SPSS*

ΠΡΟΛΟΓΟΣ

Φαίνεται πως διανύουμε μια νέα εποχή στις Τεχνολογίες Πληροφορικής και Επικοινωνιών. Εύκολα λοιπόν κάποιος μπορεί να συνειδητοποιήσει τις προκλήσεις, αλλά και τους κινδύνους που προκύπτουν από την ανταλλαγή οικονομικών και εμπορικών δεδομένων στο πλαίσιο της παγκοσμιοποίησης, την ανάπτυξη της ψηφιακής οικονομίας και την αλματώδη εξέλιξη των υπηρεσιών κοινωνικής δικτύωσης αλλά και των τεχνολογιών των «Μεγάλων Δεδομένων (Big Data) και Ανοικτών Δεδομένων – Open Data» και του «Διαδικτύου των Πραγμάτων» (Internet of things IoT)», τα οποία αποτελούν μια πραγματικότητα που έχει άμεσο αντίκτυπο στην ιδιωτική ζωή του καθενός. Καθίσταται πλέον επιβεβλημένη η ανάγκη θεσμοθέτησης ισχυρών κανόνων για την προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής του ατόμου.

Ορμώμενος λοιπόν από αυτές τις ραγδαίες εξελίξεις, αλλά και από την επαγγελματική μου ιδιότητα ως υπάλληλος Πληροφορικής της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, επέλεξα να ασχοληθώ διεξοδικά με την πλοήγηση στο διαδίκτυο και τα ηλεκτρονικά προσωπικά δεδομένα στο πλαίσιο ανάπτυξης της μεταπτυχιακής μου διατριβής. Για την ολοκλήρωσή της βοήθησαν πολλοί άνθρωποι τους οποίους οφείλω να ευχαριστήσω.

Πρώτα από όλα οφείλω πολλά ευχαριστώ στον καθηγητή κύριο Χρήστο Δρόσο για την άρτια συνεργασία, την υποστήριξη και την απεριόριστη υπομονή του.

Εν συνεχεία, οφείλω πολλά ευχαριστώ στους συναδέλφους μου που με βοήθησαν στη σύνταξη του ειδικού ερωτηματολογίου. Επίσης, θα ήθελα να ευχαριστήσω όλα τα άτομα εκείνα που είχαν την διάθεση και υπομονή να συμπληρώσουν το ειδικό αυτό ερωτηματολόγιο της έρευνας, βοηθώντας στην συγκέντρωση πολύτιμων πληροφοριών για την ολοκλήρωση της μεταπτυχιακής μου διατριβής.

Τέλος οφείλω πολλά ευχαριστώ στην οικογένεια μου για την αμέριστη συμπαράσταση και υπομονή που έδειξε κατά τη διάρκεια όλου του κύκλου των μεταπτυχιακών μου σπουδών καθώς και στο φίλο μου Ντόντο Κωνσταντίνο που με παρότρυνε να παρακολουθήσω το μεταπτυχιακό πρόγραμμα το οποίο αν και είχε τις δυσκολίες του, θεωρώ ότι με βοήθησε να διευρύνω τους ορίζοντες μου.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

1. ΕΙΣΑΓΩΓΗ

1.1. Προσωπικά δεδομένα

Όλες οι πληροφορίες που αναφέρονται σε ένα άτομο και μπορούν άμεσα ή έμμεσα να οδηγήσουν στην προσωποποίηση – αναγνώρισή του αποτελούν Προσωπικά Δεδομένα. Για παράδειγμα το ονοματεπώνυμο, η ημερομηνία γέννησης, τα στοιχεία επικοινωνίας (αριθμοί σταθερών και κινητών τηλεφωνικών συνδέσεων, λογαριασμοί ηλεκτρονικού ταχυδρομείου, emails), η διεύθυνση κατοικίας, ο αριθμός φορολογικού μητρώου (ΑΦΜ), ο αριθμός μητρώου κοινωνικής ασφάλισης (ΑΜΚΑ), ο αριθμός δελτίου ταυτότητας (ΑΔΤ), αλλά και όλα τα «ηλεκτρονικά» αποτυπώματά του, όπως ιστοσελίδες που έχει επισκεφθεί, τα «like's», τα «post» και κάθε είδους αναρτήσεις σε όλα τα δίκτυα κοινωνικής δικτύωσης (Facebook, Twitter, Instagram, LinkID, κλπ), οι φωτογραφίες και τα βίντεο που «τράβηξε» και «ανέβασε» με φιλικά πρόσωπα είναι κάποια μόνο ενδεικτικά παραδείγματα αναφορικά με το τι θεωρείται προσωπικό δεδομένο στην καθημερινή ζωή του ατόμου.

Τα προσωπικά δεδομένα αφορούν και σε ιδιαίτερα ευαίσθητα στοιχεία της ιδιωτικής ζωής, όπως στις πολιτικές πεποιθήσεις, στο θρήσκευμα, στην ερωτική ζωή και στο σεξουαλικό προσανατολισμό ή και στην υγεία. Είναι εύκολο να δει κανείς ότι η ιδιωτική ζωή είναι άμεσα συνυφασμένη με τα προσωπικά δεδομένα. Αρκεί να αναλογιστεί κανείς ότι για όλους υπάρχουν πληροφορίες που δεν θα ήθελαν να μοιραστούν με άλλους ανθρώπους (όχι απαραίτητα επειδή πρέπει να κρατηθούν κρυφές, αλλά επειδή, με απλά λόγια, αποτελούν αποκλειστικά προσωπική υπόθεση). Αν αυτές οι ιδιωτικές πληροφορίες βρεθούν σε λάθος χέρια, κανείς δεν ξέρει ποτέ πώς θα χρησιμοποιηθούν. Η ιδιωτικότητα είναι πολύτιμη: η προστασία της ιδιωτικότητας επιτυγχάνεται με την διαφύλαξη των προσωπικών δεδομένων[1].

Ο διαχωρισμός των προσωπικών δεδομένων σε απλά και ευαίσθητα σχετίζεται με τη διαδικασία συλλογής και επεξεργασίας αυτών. Για τη νόμιμη επεξεργασία των απλών δεδομένων αρκεί η προφορική συγκατάθεση του υποκειμένου και η γνωστοποίηση στην αρμόδια Αρχή (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα – ΑΠΔΠΧ). Αντίθετα, για τα ευαίσθητα δεδομένα θεσπίζεται η γενική

απαγόρευση της επεξεργασίας τους. Κατ΄ εξαίρεση επιτρέπεται η συλλογή και η επεξεργασία ευαίσθητων δεδομένων, καθώς και η ίδρυση και λειτουργία σχετικού αρχείου, ύστερα από άδεια της ΑΠΔΠΧ, όταν συντρέχουν μία ή περισσότερες από τις ακόλουθες προϋποθέσεις (αρ.7, ν.2472/1997):

- *Το υποκείμενο έδωσε τη γραπτή συγκατάθεσή του εκτός εάν η συγκατάθεση έχει αποσπασθεί με τρόπο που αντίκειται στο νόμο ή τα χρηστά ήθη ή νόμος ορίζει ότι η συγκατάθεση δεν αίρει την απαγόρευση.*
- *Η επεξεργασία είναι αναγκαία για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου ή προβλεπόμενου από το νόμο συμφέροντος τρίτου, εάν το υποκείμενο τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του.*
- *Η επεξεργασία αφορά δεδομένα που δημοσιοποιεί το ίδιο το υποκείμενο ή είναι αναγκαία για την αναγνώριση, άσκηση ή υπεράσπιση δικαιώματος ενώπιον δικαστηρίου ή πειθαρχικού οργάνου.*
- *Η επεξεργασία αφορά θέματα υγείας και εκτελείται από πρόσωπο που ασχολείται κατ' επάγγελμα με την παροχή υπηρεσιών υγείας και υπόκειται σε καθήκον εχεμύθειας ή σε συναφείς κώδικες δεοντολογίας, υπό τον όρο ότι η επεξεργασία είναι απαραίτητη για την ιατρική πρόληψη, διάγνωση, περίθαλψη ή τη διαχείριση υπηρεσιών υγείας.*
- *Η επεξεργασία εκτελείται από Δημόσια Αρχή και είναι αναγκαία είτε αα) για λόγους εθνικής ασφάλειας είτε ββ) για την εξυπηρέτηση των αναγκών εγκληματολογικής ή σωφρονιστικής πολιτικής και αφορά τη διακρίβωση εγκλημάτων, ποινικές καταδίκες ή μέτρα ασφαλείας είτε γγ) για λόγους προστασίας της δημόσιας υγείας είτε δδ) για την άσκηση δημόσιου φορολογικού ελέγχου ή δημόσιου ελέγχου κοινωνικών παροχών.*
- *Η επεξεργασία πραγματοποιείται για ερευνητικούς και επιστημονικούς αποκλειστικά σκοπούς και υπό τον όρο ότι τηρείται η ανωνυμία και λαμβάνονται όλα τα απαραίτητα μέτρα για την προστασία των δικαιωμάτων των προσώπων στα οποία αναφέρονται.*

- *Η επεξεργασία αφορά δεδομένα δημοσίων προσώπων, εφόσον αυτά συνδέονται με την άσκηση δημοσίου λειτουργήματος ή τη διαχείριση συμφερόντων τρίτων, και πραγματοποιείται αποκλειστικά για την άσκηση του δημοσιογραφικού επαγγέλματος. Η άδεια της αρχής χορηγείται μόνο εφόσον η επεξεργασία είναι απολύτως αναγκαία για την εξασφάλιση του δικαιώματος πληροφόρησης επί θεμάτων δημοσίου ενδιαφέροντος καθώς και στο πλαίσιο καλλιτεχνικής έκφρασης και εφόσον δεν παραβιάζεται καθ' οιονδήποτε τρόπο το δικαίωμα προστασίας της ιδιωτικής και οικογενειακής ζωής.*

Ακόμα πιο επιτακτική γίνεται όμως η προστασία των προσωπικών δεδομένων του ατόμου κατά την πλοήγησή του στο διαδίκτυο, καθώς η διαρκή εξέλιξή του τα τελευταία χρόνια, η ευρεία αποδοχή του και χρήση του από όλες σχεδόν τις

πληθυσμιακές ομάδες και οι νέες υπηρεσίες που παρέχει, δίνει τη δυνατότητα στους διαχειριστές (κακόβουλους και μη) των υποδομών του διαδικτύου να έχουν πρόσβαση στα προσωπικά δεδομένα των χρηστών. Η επεξεργασία των προσωπικών δεδομένων στο διαδίκτυο είναι πλέον πολύ συχνή (πολλές φορές εν αγνοία του υποκειμένου) και ουσιαστικά, αναπόφευκτη: για παράδειγμα, κάθε φορά κατά τη διαδικασία πρόσβασης στο διαδίκτυο με τη χρήση οποιασδήποτε «έξυπνης» συσκευής (υπολογιστή, φορητό υπολογιστή, κινητό τηλέφωνο, ταμπλέτα), ο πάροχος πρόσβασης διαδικτύου αναθέτει στη συσκευή αυτή έναν αριθμό που ονομάζεται διεύθυνση πρωτοκόλλου διαδικτύου (διεύθυνση IP). Η διεύθυνση IP είναι απαραίτητη για την πρόσβαση στο διαδίκτυο. Παρόλο που η εν λόγω συσκευή ενδεχομένως να χρησιμοποιείται από πολλά άτομα (π.χ. από όλα τα μέλη μιας οικογένειας) και παρά το γεγονός ότι η διεύθυνση IP είναι διαφορετική σε κάθε σύνδεση στο διαδίκτυο, εν τούτοις και αυτή αποτελεί προσωπικό δεδομένο, ακριβώς γιατί μπορεί, έστω και υπό προϋποθέσεις ή/και σε συνδυασμό με

άλλες πληροφορίες, να ταυτοποιήσει το χρήστη της συσκευής για κάποια δεδομένη χρονική στιγμή. Για όλους τους παραπάνω λόγους, λοιπόν, η λήψη κατάλληλων μέτρων για την προστασία των προσωπικών δεδομένων έχει αποκτήσει ιδιαίτερη βαρύτητα και σημασία[1].

1.2. Τι ισχύει για την προστασία των προσωπικών δεδομένων

Καθημερινά συλλέγονται, επεξεργάζονται και αναλύονται δεδομένα ατόμων. Ποια είναι η ορθή χρήση τους; Τι θα πρέπει να τηρείται κατά την συλλογή και την επεξεργασία τους, χωρίς να προσβάλλονται τα δικαιώματα των υποκειμένων των δεδομένων; Πώς μπορούν να προστατευθούν;

Αρχικά, η Ευρωπαϊκή Ένωση, με το άρθρο 8 του Χάρτη Θεμελιωδών Δικαιωμάτων, υποστήριξε το δικαίωμα των ατόμων στην προστασία των προσωπικών τους δεδομένων. Για το σκοπό αυτό, εξέδωσε και αντίστοιχη Οδηγία 95/46/ΕΚ. Ωστόσο, η σημαντική τεχνολογική πρόοδος που σημειώθηκε έκτοτε και συνεχίζει και μέχρι τις μέρες μας, αναγκάζει την Ευρωπαϊκή Ένωση να εγκρίνει και να επικαιροποιεί συνεχώς κανόνες που καθορίζουν τον τρόπο με τον οποίο πρέπει να προστατεύονται τα προσωπικά δεδομένα.

Στην Ελλάδα, όπως και στα υπόλοιπα κράτη μέλη της Ευρωπαϊκής Ένωσης, υπάρχει ειδική νομοθεσία που προστατεύει τα άτομα από την ανεξέλεγκτη χρήση των προσωπικών τους δεδομένων. Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα είναι ο αρμόδιος φορέας για την εφαρμογή αυτής της νομοθεσίας στην Ελλάδα (νόμοι 2472/1997 και 3471/2006).

Η σημερινή νομοθεσία θεσπίστηκε το 1995, μία εποχή εντελώς διαφορετική, με πολύ λιγότερες προκλήσεις για τα προσωπικά δεδομένα. Το διαδίκτυο βρισκόταν σε εμβρυακό επίπεδο ανάπτυξης, οι μηχανές αναζήτησης και τα δίκτυα κοινωνικής δικτύωσης δεν υπήρχαν ούτε καν σαν ιδέα στο μυαλό των δημιουργών τους.

Σήμερα, ο τρόπος συλλογής, υποβολής σε επεξεργασία και η πρόσβαση σε δεδομένα δεν μοιάζει σε τίποτα με τις μεθόδους που χρησιμοποιήθηκαν πριν από περίπου δύο δεκαετίες. Επιπλέον, σε κάθε ένα από τα 28 κράτη μέλη, οι εθνικές αρχές επιβολής του νόμου έχουν μεταφέρει τους κανόνες με διαφορετικό τρόπο στο

εσωτερικό τους και προσαρμόζουν το επίπεδο προστασίας προσωπικών δεδομένων σύμφωνα με την εκάστοτε υπόθεση (διασυνοριακή, εσωτερική, Europol, Eurojust, Prum). Το γεγονός αυτό οδηγεί σε απόκλιση στην εφαρμογή των κανόνων προστασίας των προσωπικών δεδομένων, ενώ ταυτόχρονα δημιουργεί σημαντικό διοικητικό φόρτο στις επιχειρήσεις, καθώς αυτή η πανευρωπαϊκή διαφορά είναι μη βιώσιμη[2].

Μέσα σε αυτή την τεχνολογική έκρηξη που βιώνει όλος ο κόσμος και με έντονη την απειλή της τρομοκρατίας και του οργανωμένου εγκλήματος, ξεκίνησαν συζητήσεις σε ευρωπαϊκό επίπεδο σχετικά με τον καλύτερο συνδυασμό του σεβασμού της ασφάλειας και της ιδιωτικής ζωής.

Η υιοθέτηση της ψηφιακής τεχνολογίας από τους πολίτες, σχεδόν για το σύνολο των αναγκών τους, συνεχίζεται με αμείωτο ρυθμό. Τα κοινωνικά μέσα δικτύωσης και μια μεγάλη σειρά άλλων ηλεκτρονικών υπηρεσιών είναι πλέον διαδεδομένη. Η ψηφιακή ταυτότητα γίνεται πλέον ένα σημαντικό κομμάτι της καθημερινότητας του ατόμου, γεγονός που αναπόφευκτα το οδηγεί να μοιραστεί τουλάχιστον κάποιες βασικές προσωπικές πληροφορίες του με τους παρόχους υπηρεσιών.

Μέσα σε αυτό το συνεχώς τεχνολογικά εξελισσόμενο περιβάλλον, οι κίνδυνοι είναι υπαρκτοί και εξελίσσονται ταυτόχρονα. Η σχετικά πρόσφατη αποκάλυψη υπόθεσης στην Ελλάδα, όπου ιδιώτης κατάφερε να υποκλέψει φορολογικά και άλλα προσωπικά δεδομένα 9.000.000 πολιτών, με σκοπό να τα πουλήσει σε ιδιωτικές εταιρίες, αποτελεί ένα τρανταχτό παράδειγμα της επιτακτικής ανάγκης για ένα πιο αυστηρό νομικό πλαίσιο του καθεστώτος προστασίας προσωπικών δεδομένων στην Ευρωπαϊκή Ένωση. Οι παρόντες κανόνες προστασίας στην Ευρωπαϊκή Ένωση θεωρούνται πλέον απαρχαιωμένοι[2].

Προκειμένου να εξελίξει τους κανόνες αυτούς, από το 2012 η Ευρωπαϊκή Επιτροπή (η Ευρωπαϊκή Επιτροπή είναι το πολιτικά ανεξάρτητο εκτελεστικό όργανο

της Ευρωπαϊκής Ένωσης. Είναι το μόνο αρμόδιο όργανο για την κατάρτιση προτάσεων για νέα ευρωπαϊκή νομοθεσία, και εφαρμόζει τις αποφάσεις του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της Ευρωπαϊκής Ένωσης[3]) συμμετέχει στη διαδικασία μεταρρύθμισης της προστασίας δεδομένων σε ολόκληρη την Ευρωπαϊκή Ένωση. Τα τελευταία έτη, η ολοκλήρωση αυτής της μεταρρύθμισης έχει καταστεί προτεραιότητα πολιτικού επιπέδου. Στόχος αυτής της μεταρρύθμισης είναι να ενισχυθούν τα δικαιώματα των ατόμων και να τους δοθεί η δυνατότητα να έχουν καλύτερο έλεγχο των δικών τους δεδομένων. Επιπροσθέτως, καθώς η Επιτροπή δίνει ιδιαίτερη βάση στην τόνωση της ψηφιακής ενιαίας αγοράς και στα οφέλη της ψηφιακής οικονομίας[4], η απλοποίηση του κανονιστικού πλαισίου για τις επιχειρήσεις ως προς τη χρήση των προσωπικών δεδομένων κρίνεται απαραίτητη.

Καθώς λοιπόν, η προστασία των προσωπικών δεδομένων είναι ένα πολύ ευαίσθητο θέμα για την ευρωπαϊκή κοινή γνώμη, γιατί αγγίζει την καθημερινότητα όλων, το βασικό στοιχείο της δέσμης μεταρρυθμίσεων για την προστασία των δεδομένων είναι ένας Γενικός Κανονισμός για την προστασία των δεδομένων (General Data Protection Regulation GDPR).

1.3. Γενικός Κανονισμός για την προστασία των προσωπικών δεδομένων GDPR

Την ριζική αναμόρφωση του νομικού πλαισίου προστασίας των προσωπικών δεδομένων επέβαλαν οι τεχνολογικές εξελίξεις. Σήμερα, η κοινωνία βρίσκεται μπροστά σε νέες προκλήσεις στις οποίες η Ευρωπαϊκή Επιτροπή και κατ' επέκταση η Ευρωπαϊκή Ένωση καλείται να αντιμετωπίσει με την δημοσίευση του νέου Γενικού Κανονισμού Προστασίας των προσωπικών δεδομένων.

Την 27η Απριλίου 2016 ψηφίστηκε ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΕΕ) 2016/679 που αποτελεί το κύριο νομοθέτημα της νέας δέσμης κανόνων. Την 24η Μαΐου 2016 τέθηκε σε ισχύ. Η διαδικασία ενσωμάτωσης του Κανονισμού στο εθνικό δίκαιο του κάθε κράτους μέλους πρέπει να έχει ολοκληρωθεί μέχρι την 6η Μαΐου 2018, με σκοπό η καθολική εφαρμογή της να ισχύσει από την 25η Μαΐου 2018.

Ο Γενικός Κανονισμός για την προστασία των προσωπικών δεδομένων αντικαθιστά την Οδηγία 46 του 1995 που ενσωματώθηκε στην ελληνική νομοθεσία με το ν. 2472/1997. Ο Γενικός Κανονισμός για την Προστασία των Δεδομένων δεν αποτελεί απλή επικαιροποίηση της Οδηγίας, αλλά ένα νέο κατ' ουσία νομοθέτημα προς την κατεύθυνση της διαμόρφωσης ενός ισχυρότερου και πιο συνεκτικού νομικού πλαισίου που θα έχει ομοιόμορφη εφαρμογή σε όλη την επικράτεια της Ευρωπαϊκής

Ένωσης. Περιγράφει τα δικαιώματα του ατόμου και καθορίζει τις υποχρεώσεις των υπευθύνων για την επεξεργασία των δεδομένων. Παράλληλα, θωρακίζει τα δικαιώματα των πολιτών, επιβάλλοντας ωστόσο καινοτόμες υποχρεώσεις στους φορείς που επεξεργάζονται προσωπικά δεδομένα. Καθορίζει τις μεθόδους για τη διασφάλιση της συμμόρφωσης καθώς και το πεδίο εφαρμογής των κυρώσεων για τους παραβάτες των κανόνων. Επιπλέον, το προβλεπόμενο ύψος των προστίμων είναι υψηλό ώστε να συνιστά την κύρωση αποτελεσματική. Επιπροσθέτως, θα φέρει αρκετές βελτιώσεις στην επεξεργασία των προσωπικών δεδομένων από τις αστυνομικές και δικαστικές αρχές σε ποινικές υποθέσεις.

Ο Γενικός Κανονισμός για την προστασία των προσωπικών δεδομένων έχει ως σκοπό να καλυφθούν οι ανάγκες και να αντιμετωπιστούν οι κίνδυνοι που προκύπτουν στο τεχνολογικό περιβάλλον του 21ου αιώνα από την ανταλλαγή προσωπικών δεδομένων στο δεύτερο πλαίσιο της παγκοσμιοποίησης, τη ραγδαία εξέλιξη των μέσων κοινωνικής δικτύωσης και των τεχνολογιών των Μεγάλων Δεδομένων (Big Data) και του Διαδικτύου των Πραγμάτων (Internet of things IoT).

Σε γενικές γραμμές, ο Γενικός Κανονισμός διευρύνει τα δικαιώματα των υποκειμένων των προσωπικών δεδομένων, δηλαδή των φυσικών προσώπων, και αυξάνει τις υποχρεώσεις των υπευθύνων επεξεργασίας των δεδομένων. Με λίγα λόγια, δημιουργεί ένα νέο νομικό πλαίσιο.

1.4. Προσωπικά δεδομένα και διαδίκτυο

1.4.1. Προστασία της ιδιωτικής ζωής στην Κοινωνία της Πληροφορίας

Καθώς οι Τεχνολογίες Πληροφορικής και Επικοινωνιών καθίστανται πανταχού παρούσες, διεισδύοντας σε κάθε πτυχή της επαγγελματικής και προσωπικής ζωής του ατόμου, άνθρωποι και επιχειρήσεις καθίστανται ολοένα και πιο ευάλωτοι σε παραβιάσεις των προσωπικών τους δεδομένων. Η ιδιωτικότητα αναδεικνύεται ως ένας από τους σημαντικότερους κινδύνους που αντιμετωπίζει η συνεχώς αναπτυσσόμενη «κοινωνία της πληροφορίας».

Ως «κοινωνία της πληροφορίας» θα μπορούσε να ορισθεί η κοινωνία εκείνη, όπου οι τεχνολογίες πληροφορικής και επικοινωνιών επηρεάζουν το σύνολο των ανθρώπινων δραστηριοτήτων[5]. Με άλλα λόγια, είναι η κοινωνία εκείνη όπου η παραγωγή, διανομή, χρήση, ενσωμάτωση και διαχείριση πληροφοριών αποτελεί σημαντική οικονομική, πολιτική και πολιτιστική δραστηριότητα. Δια μέσου της χρήσης της πληροφορικής (IT) η κοινωνία της πληροφορίας έχει ως σκοπό να κερδίσει ανταγωνιστικό πλεονέκτημα διεθνώς, με δημιουργικό και παραγωγικό τρόπο. Οι άνθρωποι που έχουν τα μέσα να συμμετέχουν σε αυτή τη μορφή κοινωνίας ορισμένες φορές ονομάζονται «ψηφιακοί πολίτες». Σύμφωνα με την οικονομία της γνώσης, ο πλούτος δημιουργείται μέσα από την οικονομική εκμετάλλευση της κατανόησης. Αυτή αποτελεί και μια από τις δωδεκάδες ετικέτες που υποδηλώνουν ότι οι σύγχρονοι άνθρωποι μπαίνουν σε μία νέα μορφή κοινωνίας[6].

Η ψηφιακή πληροφορία αποτελεί από τη φύση της μια τεχνολογική καινοτομία, η οποία αμφισβητεί τις κρατούσες αντιλήψεις σχετικά με την ιδιοκτησία και την ιδιωτικότητα και ανατρέπει παραδοσιακές συνήθειες[7].

Από τη μια, όλο και περισσότερες ενέργειες στην καθημερινότητα του ατόμου προϋποθέτουν τη χρήση του διαδικτύου, από την άλλη, όλο και περισσότερες από τις ψηφιακές συσκευές που χρησιμοποιεί συνδέονται σε αυτό. Το «Internet of Things – IoT - Διαδίκτυο των Πραγμάτων» υπόσχεται ότι θα συνδέσει στο διαδίκτυο όχι μόνο τα κινητά τηλέφωνα, τις ταμπλέτες και τις κάμερες, αλλά ακόμη και τα αυτοκίνητα, τους «έξυπνους μετρητές» ηλεκτρικής ενέργειας, τα ψυγεία, τα ηχεία ή και το σύστημα

ασφαλείας του σπιτιού. Ενδεικτικά αναφέρεται πρόσφατη μελέτη της εταιρείας ερευνών Gartner, Inc. (εταιρεία έρευνας και συμβουλευτικής) σύμφωνα με την οποία υπολογίζεται ότι ο αριθμός των συνδεδεμένων συσκευών θα φτάσει τον αριθμό των 26 δισεκατομμυρίων μέχρι το έτος 2020. Αυτό σημαίνει ότι κάθε άνθρωπος στον πλανήτη θα διαθέτει κατά μέσο όρο τρεις συσκευές που μπορούν να υποστηρίξουν το IoT. Παράλληλα, προβλέπει ότι το IoT θα επιφέρει μία συνολική οικονομική πρόσθετη αξία της τάξης των 1,9 τρισεκατομμυρίων δολαρίων, ενώ οι πληροφορίες που θα διαχειρίζονται οι επιχειρήσεις θα αυξηθεί έως και 14 φορές.

Στον πιο απλουστευμένο ορισμό του, το Διαδίκτυο των Πραγμάτων είναι η εφαρμογή διατάξεων αισθητήρων, τεχνολογίας πληροφοριών και δικτυακών τεχνολογιών για τη σύνδεση δισεκατομμυρίων συσκευών μικρών ή μεγάλων σε όλο τον κόσμο τόσο μεταξύ τους όσο και με τον κατασκευαστή, για να λαμβάνουν και να μεταδίδουν σχετικά δεδομένα με στόχο να προσφέρουν περισσότερες προσωποποιημένες υπηρεσίες. Αυτή η διασύνδεση επιτρέπει την ανάπτυξη νέων «έξυπνων» εφαρμογών, την εξαγωγή στατιστικών δεδομένων και την ανάπτυξη νέων

επιχειρηματικών μοντέλων που θα έχουν ως αποτέλεσμα έναν καθαρότερο και πιο βιώσιμο τρόπο ζωής. Το Διαδίκτυο των Πραγμάτων έχει τη δυναμική να εξελίξει την ανθρωπότητα, όπως και τα δισεκατομμύρια των υπαρχόντων διασυνδεδεμένων υπολογιστικών συσκευών (ηλεκτρονικοί υπολογιστές, κινητά τηλέφωνα, κλπ) που έχουν δημιουργήσει νέες εφαρμογές και επιχειρηματικά μοντέλα, όπως μηχανές αναζήτησης, ηλεκτρονικό ταχυδρομείο (email), ηλεκτρονικό εμπόριο και δίκτυα κοινωνικής δικτύωσης.

Με απλά λόγια το Διαδίκτυο των Πραγμάτων είναι το τεχνολογικό μέλλον που έρχεται για να κάνει τη ζωή του ατόμου πιο εύκολη. Η ποσότητα της ψηφιακής

πληροφορίας πλέον αποκτά εκρηκτικές διαστάσεις. Η ραγδαία αυτή ανάπτυξη του «ψηφιακού κόσμου» οφείλεται κυρίως στην έκρηξη της κοινωνικής δικτύωσης, της ψηφιακής φωτογραφίας και του ψηφιακού βίντεο. Περίπου το 70 τοις εκατό των ψηφιακών δεδομένων παράγονται μεμονωμένα από ιδιώτες. Τα περισσότερα από αυτά βρίσκονται αποθηκευμένα σε ιστοσελίδες μεγάλων ιδιωτικών εταιρειών, όπως το YouTube[7].

Η διαφύλαξη αυτού του τόσο μεγάλου πληροφοριακού όγκου (Μεγάλα Δεδομένα – Big Data και Ανοικτά Δεδομένα – Open Data) και η διασφάλιση του δικαιώματος των πολίτων να έχουν τον έλεγχο των ψηφιακών δεδομένων τους, αποτελούν προϋπόθεση για τη χρήση των καινοτομιών των Τεχνολογιών Πληροφορικής και Επικοινωνιών προς όφελος της ανθρωπότητας. Και οι δύο τύποι δεδομένων μπορούν να μεταμορφώσουν τον κόσμο.

Η έννοια των Μεγάλων Δεδομένων – Big Data εμπεριέχει τρία βασικά χαρακτηριστικά: είναι υψηλού όγκου, υψηλής ποικιλίας στοιχεία και υψηλής ταχύτητας ανάλυσης που απαιτούν αποδοτικές και καινοτόμες μορφές επεξεργασίας πληροφοριών. Τα Big Data δημιουργούνται ουσιαστικά από όλα όσα περικλείουν το άτομο ανά πάσα στιγμή. Κάθε ψηφιακή αλληλεπίδραση με μέσα μαζικής δικτύωσης παράγει δεδομένα, από την πλοήγηση στον υπολογιστή και το online λιανεμπόριο μέχρι τις αγορές στο iTunes και τα likes στο Facebook. Τα δεδομένα αυτά αλιεύονται από πολλαπλές πηγές, με τρομακτική ταχύτητα, όγκο και ποικιλία.

Τα Μεγάλα Δεδομένα και το νέο φαινόμενο των Ανοικτών Δεδομένων (Open Data) είναι στενά συνδεδεμένα, αλλά δεν είναι το ίδιο. Ενώ τα Big Data καθορίζονται από το μέγεθος τους, τα Ανοιχτά Δεδομένα ορίζονται από τη χρήση τους. Είναι δημόσια προσβάσιμα δεδομένα που οι άνθρωποι, οι επιχειρήσεις και οι οργανισμοί μπορούν να χρησιμοποιούν για την έναρξη νέων επιχειρήσεων, την ανάλυση προτύπων και τάσεων, να λαμβάνουν αποφάσεις που βασίζονται σε αυτά, και να επιλύουν

σύνθετα προβλήματα. Τα ανοιχτά δεδομένα εμπεριέχουν δύο βασικά χαρακτηριστικά: τα δεδομένα πρέπει να είναι διαθέσιμα στο κοινό για οποιονδήποτε θελήσει να τα χρησιμοποιήσει και πρέπει να διαθέτουν άδεια κατά τέτοιο τρόπο που να επιτρέπει την επαναχρησιμοποίησή τους**.** Επιπλέον, θα πρέπει να είναι σχετικά εύκολα στη χρήση τους και να διατίθενται δωρεάν ή με ελάχιστο κόστος.

Το νέο ψηφιακό περιβάλλον των Μεγάλων και Ανοικτών Δεδομένων επιδρά στην ιδιωτικότητα του ατόμου. Αρκεί κάποιος να σκεφτεί την πολύ μεγαλύτερη κλίμακα έκθεσης των προσωπικών δεδομένων, βάσει των νέων δυνατοτήτων αναζήτησης, ανάλυσης και διασύνδεσής τους, που μπορεί να οδηγήσει ακόμα και στη λήψη αυτοματοποιημένων αποφάσεων, χωρίς δυνατότητα ελέγχου από το ίδιο το άτομο. Οι παραπάνω κίνδυνοι γεννούν καινούργιες απαιτήσεις για την προστασία της ιδιωτικότητας, με επίκεντρο κυρίως την ενδυνάμωση των χρηστών του διαδικτύου μέσω νέων μηχανισμών ενημέρωσης και συγκατάθεσης.

Η ποσότητα της ψηφιακής πληροφορίας είναι κατακλυσμική. Εκτιμάται ότι η ψηφιακή παραγωγή της ανθρωπότητας αγγίζει τα 800 δισεκατομμύρια Gigabytes και αναμένεται να ξεπεράσει τα 1,2 Zettabytes (1,2 τρισεκατομμύρια Gigabytes) ως το τέλος του έτους. Αυτό αντιστοιχεί σε περίπου 200 Gigabytes ψηφιακών δεδομένων ανά κάτοικο του πλανήτη. Το 2020 σε κάθε παιδί, γυναίκα και άντρα στον πλανήτη θα αντιστοιχούν 5,2 Terabytes ψηφιακής πληροφορίας. Δεδομένα που θα είναι αποθηκευμένα είτε σε τοπικά μαγνητικά και οπτικά μέσα είτε στο λεγόμενο cloud, δηλαδή σε απομακρυσμένους αποθηκευτικούς χώρους στο διαδίκτυο[7].

Μόνο η προσπάθεια αποθήκευσης αυτής της ποσότητας ψηφιακών δεδομένων αποτελεί από μόνη της μια δύσκολη πρόκληση για την τεχνολογία και την επιστήμη. Ακόμη δυσκολότερη κρίνεται η ανάλυση και η εξαγωγή χρήσιμης πληροφορίας και νοήματος από τα πρωτογενή δεδομένα. Σε κάθε περίπτωση, όλα αυτά τα δεδομένα μετασχηματίζουν τον τρόπο με τον οποίο ασκείται η πολιτική, η επιχειρηματικότητα, η επιστήμη.

Στην πραγματικότητα, ιδιώτες που πρόθυμα μοιράζονται τα προσωπικά τους δεδομένα είναι οι βασικοί υποστηρικτές των περισσότερων από τις καινοτόμες επιχειρήσεις του διαδικτύου. Οι χρήστες δεν φαίνεται να ενοχλούνται από την

εκμετάλλευση των προσωπικών τους δεδομένων. Αυτό είναι το τίμημα που πληρώνουν για τις τρομακτικές και ασύλληπτες ψηφιακές εμπειρίες που το διαδίκτυο τους προσφέρει.

Η μετάβαση, όμως, στον κυβερνοχώρο επιφέρει πρόσθετη πολυπλοκότητα. Οι ψηφιακές κοινότητες δεν διαφέρουν πολύ από τις παραδοσιακές. Αντιμετωπίζουν παρόμοιους κινδύνους, γι' αυτό το λόγο πρέπει να λαμβάνουν ανάλογες προφυλάξεις και να συμμορφώνονται με τις ίδιες αρχές. Τα ψηφιακά προσωπικά δεδομένα συλλέγονται με τρόπους που συχνά αδυνατεί ο ανθρώπινος νους να αντιληφθεί.

Ενδεικτικά, αναφέρεται η χρήση των Google Glass, των φορητών γυαλιών που έχουν την δυνατότητα να καταγράφουν ό,τι βλέπει, ακούει (και σε λίγο καιρό ό,τι νιώθει) ο χρήστης τους. Αυτό έχει ως αποτέλεσμα να μπορεί έτσι να προσδιοριστεί με μεγάλη ακρίβεια η πολιτιστική, πολιτική, και συναισθηματική ταυτότητα, του χρήστη.

Ο όγκος όμως αυτής της πληροφορίας είναι απειροελάχιστος αν συνυπολογίσει κανείς και τα βιομετρικά δεδομένα που παράγονται από ένα άτομο καθώς εργάζεται, ψυχαγωγείται, αγοράζει, ταξιδεύει, σκέφτεται. Δεδομένα, που σε όλο και περισσότερες περιπτώσεις πλέον, αποθηκεύονται.

Το διακύβευμα πλέον δεν είναι μόνο η ιδιωτικότητα, αλλά ακόμη και η ίδια η έννοια της ατομικότητας, του προνομίου να είναι ο κάθε άνθρωπος μοναδικός.

Οι τεχνολογίες του σήμερα είναι σε θέση να υλοποιήσουν όλα όσα ο Orwell έχει προβλέψει στο έργο του «1984»: υπάρχει πλέον η τεχνική δυνατότητα δημιουργίας «πανοπτικών» κοινωνιών, όπου σε πραγματικό χρόνο η παγκόσμια επιτήρηση θα είναι γεγονός[7].

Στη Μεγάλη Βρετανία, σύμφωνα με μια τελευταία καταμέτρηση υπάρχουν 4,2 εκατομμύρια κάμερες παρακολούθησης (αντιστοιχεί μία σε κάθε 14 κατοίκους αυτής της χώρας). Υπολογίζεται ότι σε ακτίνα 200 μέτρων γύρω από την κατοικία του George Orwell στο βόρειο Λονδίνο, είναι εγκατεστημένες 32 κάμερες παρακολούθησης[7].

Είναι πλέον προφανές ότι τα δεδομένα (προσωπικά και μη) αποτελούν πολύτιμο οικονομικό πόρο, ο οποίος φορολογείται, υποκλέπτεται, πωλείται, αγοράζεται, κ.ο.κ.

Η προστασίας της ιδιωτικής ζωής λοιπόν, είναι μια χαμένη υπόθεση; Η άσκηση ελέγχου επί των προσωπικών ψηφιακών δεδομένων έχει χαθεί; Είναι υποχρεωμένη η κοινωνία να θυσιάσει την ιδιωτικότητά της για να είναι ασφαλής;

Υπάρχει μια λεπτή και εύθραυστη ισορροπία μεταξύ της προστασίας της ιδιωτικής ζωής και της ασφάλειας. Μια ισορροπία που συνεχώς διαταράσσεται από την τεχνολογική καινοτομία, η οποία όμως μοιάζει να είναι και ο μοναδικός μηχανισμός που μπορεί να την αποκαταστήσει. Η προστασία της ιδιωτικής ζωής είναι μια συνεχής προσπάθεια εξοπλισμών μεταξύ αυτών που την επιβουλεύονται και αυτών που την προστατεύουν. Είναι τεράστιο το οικονομικό όφελος, από όποια πλευρά της γραμμής κι αν βρίσκεται κανείς. Η προστασία της ιδιωτικότητας είναι ο «ψυχρός πόλεμος» του 21ου αιώνα.

Αδιαμφισβήτητα, οι Τεχνολογίες Πληροφορικής και Επικοινωνιών προσφέρουν τεράστιο πεδίο εφαρμογών καινοτομίας. Είναι ωστόσο σημαντικό να προσεγγιστεί με ορθή εκτίμηση των γεγονότων το θέμα της προστασίας της ιδιωτικής ζωής. Είναι ευρέως γνωστό ότι για κάθε σύστημα ισχύος, δημόσιο ή ιδιωτικό, ο συγκεντρωτικός έλεγχος, ο προστατευτισμός και ο έλεγχος των πληροφοριακών ροών αποτελούν ελκυστικές πρακτικές.

Η προστασία της ιδιωτικής ζωής, τόσο στον ψηφιακό όσο και στον φυσικό κόσμο είναι θέματα πανομοιότυπα: οι πολίτες ή οι καταναλωτές έχουν δικαίωμα στην προστασία της ιδιωτικότητάς τους και στην ορθή χρήση των προσωπικών τους δεδομένων. Εύλογα λοιπόν περιμένουν ότι οι εταιρείες και οι διάφοροι οργανισμοί που συλλέγουν αναλύουν, διαμοιράζονται και αποθηκεύουν τα ψηφιακά τους δεδομένα, το κάνουν με την κατάλληλη προσοχή.

Επιπροσθέτως, στον ψηφιακό κόσμο ενισχύεται η αποσύνδεση μεταξύ αιτίου και αποτελέσματος. Όλες οι ενέργειες ενός ψηφιακού πολίτη είναι άυλες, μη αναγνωρίσιμες και σε πολλές περιπτώσεις και μη ανιχνεύσιμες.

Στο πλαίσιο αυτό, τα κέντρα παραγωγής πολιτικής δείχνουν ανίκανα να διαχειριστούν τη μετάβαση στην ψηφιακή εποχή. Οι εκπαιδευτικοί, κοινωνικοί και πολιτικοί, θεσμοί δεν διαθέτουν την απαραίτητη ευκινησία ώστε να προσαρμοστούν στους καταιγιστικούς ρυθμούς της κοινωνίας της πληροφορίας.

Ο εκπληκτικός ρυθμός της τεχνολογικής ανάπτυξης ξεπερνά κατά πολύ την ικανότητα των νομοθετών να αντιμετωπίσουν τα ζητήματα που τίθενται και να θεσπίσουν μέτρα για τη διασφάλιση των πολιτών. Στις περισσότερες περιπτώσεις, οι τεχνολογίες σχεδιάζονται ως μέσα για την εξεύρεση λύσεων σε προβλήματα ποσότητας (περισσότερα, φθηνότερα, ταχύτερα) και όχι ποιότητας.

Η μόνη βιώσιμη άμυνα έναντι των κινδύνων της προστασίας της ιδιωτικής ζωής είναι η ενίσχυση και η τόνωση των «ψηφιακών πολιτών». Αυτό επιτυγχάνεται μέσω της ενημέρωσης και της εκπαίδευσής τους για τους ψηφιακούς κινδύνους, τα δικαιώματα και τις υποχρεώσεις τους. Οι εκπαιδευτικοί, οι πολίτες, οι μελλοντικοί προγραμματιστές και επιστήμονες, οι δημόσιοι υπάλληλοι και φυσικά, οι νομοθέτες και οι πολιτικοί θα πρέπει να είναι ενημερωμένοι για την προστασία της ιδιωτικής τους ζωής και τις επιπτώσεις των διαδικτυακών συμπεριφορών τους. Η δημιουργία δηλαδή «ανοιχτών», συμμετοχικών κοινωνιών, οι οποίες να είναι ενήμερες για τους κινδύνους και εξοπλισμένες για να τους αντιμετωπίσουν, τόσο τεχνολογικά όσο και μέσα από ενσυνείδητες συμπεριφορές.

1.4.2. Πώς χρησιμοποιούνται τα προσωπικά δεδομένα στο διαδίκτυο

Σχεδόν το μεγαλύτερο μέρος από το πλήθος των καθημερινών δραστηριοτήτων ενός ατόμου στο διαδίκτυο συνεπάγεται επεξεργασία των προσωπικών δεδομένων του. Χαρακτηριστικά παραδείγματα αποτελούν τα εξής:

Κατά την διάρκεια ανάγνωσης της ηλεκτρονικής αλληλογραφίας (emails). Ο πάροχος ηλεκτρονικών επικοινωνιών δατηρεί αρχείο καταγραφής για κάθε μήνυμα ηλεκτρονικού ταχυδρομείου, με πληροφορίες όπως την ώρα εισόδου στο λογαριασμό, τον αποστολέα και τον παραλήπτη του μηνύματος, το θέμα του ηλεκτρονικού μηνύματος καθώς και την ημερομηνία και ώρα αποστολής του. Επιπροσθέτως, τηρεί – ακόμη και αν δεν επιτρέπεται να τα διαβάζει – όλο το πλήθος των emails, γεγονός που αποτελεί επιμέρους επεξεργασία προσωπικών δεδομένων.

Κατά την διάρκεια σύνδεσης στο διαδίκτυο μέσω προγραμμάτων πλοήγησης. Τα εκάστοτε προγράμματα πλοήγησης (browsers) καταγράφουν τις σελίδες που επισκέπτεται κάποιος. Μεγάλο πλήθος ιστοσελίδων εγκαθιστούν στον

υπολογιστή ή στην «έξυπνη συσκευή» μικρά αρχεία κειμένου (cookies). Πρόκειται για αρχεία κειμένου, τα οποία αποθηκεύει ένας ιστότοπος στη συσκευή κατά την επίσκεψη του χρήστη σε αυτή την ιστοσελίδα. Χρησιμοποιούνται ευρέως για την αποτελεσματικότερη λειτουργία των ιστοτόπων που επιτυγχάνεται μέσω της αποθήκευσης των προτιμήσεων του εκάστοτε επισκέπτη.

Μεταξύ των άλλων, χρησιμοποιούνται και «cookies παρακολούθησης» με σκοπό να παρακολουθούν την περιήγηση στο διαδίκτυο, να δημιουργούν προφίλ χρηστών και στη συνέχεια να παρέχουν στοχευμένη διαφήμιση με βάση τις προτιμήσεις των χρηστών. Για παράδειγμα, κάνοντας «click» πάνω σε μια διαφήμιση, η διαφημιστική εταιρεία μπορεί να καταγράφει τις προτιμήσεις μέσω των αρχείων αυτών, ώστε να μπορεί να στέλνει προσφορές στο μέλλον για αντίστοιχα προϊόντα που κρίνει ότι θα ενδιαφέρουν τον χρήστη.

Με βάση τους κανόνες της Ευρωπαϊκής Ένωσης, κάθε ιστότοπος που χρησιμοποιεί cookies έχει την υποχρέωση να ενημερώνει γι’ αυτό, και να ζητεί τη συγκατάθεσή του ατόμου. Το άτομο θα πρέπει πάντα να έχει το δικαίωμα να απενεργοποιεί ή να μη δέχεται cookies στη συσκευή του, καθώς και να γνωρίζει πώς θα χρησιμοποιηθούν οι πληροφορίες των cookies.

Κατά την αναζήτηση πληροφοριών μέσω των μηχανών αναζήτησης. Οι αναζητήσεις πληροφορίων, για θέματα ενδιαφέροντος του ατόμου, μέσω μιας μηχανής αναζήτησης, καταγράφονται. Στοιχεία που διατηρούνται στα πληροφοριακά συστήματα πρόσβασης στο διαδίκτυο είναι η διεύθυνση πρωτοκόλλου διαδικτύου (IP), με την οποία ο υπολογιστής ή η «έξυπνη συσκευή» του χρήστη συνδέεται στο διαδίκτυο, το πλήθος των αναζητήσεων που πραγματοποιήθηκαν, η χρονική στιγμή της κάθε αναζήτησης και το αποτέλεσμα των αναζητήσεων που αφορά τον χρήστη.

Κατά την συμπλήρωση ηλεκτρονικών φορμών. Αρκετά συχνά πλέον, όλο και περισσότεροι χρήστες καλούνται να συμπληρώσουν φόρμες με προσωπικά τους στοιχεία όπως, όνομα, τηλέφωνο, διεύθυνση και ηλικία, για την παροχή μιας διαδικτυακής υπηρεσίας. Παραδείγματα πολλά. Ενδεικτικά μόνο αναφέρονται η ηλεκτρονική κάρτα γενεθλίων για την αποστολή της σε φίλο και η δήλωση συμμετοχής σε έναν διαγωνισμό.

Κατά το «ανέβασμα» προσωπικών πληροφοριών σε υπηρεσίες κοινωνικής δικτύωσης (Facebook, Twitter, Instagram κ.τ.λ.). Μέσω αυτής της διαδικασίας ουσιαστικά ο χρήστης δημοσιεύει τα προσωπικά του δεδομένα στο διαδίκτυο. Δεδομένα όπως συνήθειες, μέρη που έχει επισκεφθεί, φωτογραφίες, ηλικία, οικογενειακή κατάσταση, είναι άμεσα διαθέσιμα στους «φίλους» του στο Facebook, στους «φίλους» των «φίλων» του, ενώ ορισμένα είναι διαθέσιμα σε όλους τους χρήστες του Facebook. Στην περίπτωση δε, που ο χρήστης αποφασίσει να ανεβάσει πληροφορίες ή φωτογραφίες άλλων, τότε δημοσιεύει τα προσωπικά δεδομένα των ατόμων αυτών στο διαδίκτυο.

Όλα τα προαναφερθέντα αποτελούν χαρακτηριστικά παραδείγματα και αποτυπώνουν το μέγεθος της επεξεργασίας των προσωπικών δεδομένων που λαμβάνει χώρα στο διαδίκτυο[1].

Αυτό που είναι άκρως σημαντικό και επιβάλλεται να συνειδητοποιήσει ο χρήσης του διαδικτύου είναι ότι, αν τα προσωπικά του δεδομένα πέσουν σε λάθος χέρια, ενδεχομένως να βρεθεί σε εξαιρετικά δυσμενή θέση στο μέλλον. Πώς όμως είναι δυνατόν τα προσωπικά δεδομένα να χρησιμοποιηθούν εναντίον του ατόμου που τα δημοσιοποιεί με σκοπό να το βλάψουν; Στο διαδίκτυο, δεν είναι δυνατόν να προβλέψει ή να φανταστεί κανείς το πώς και το πότε θα χρησιμοποιηθούν τα προσωπικά του δεδομένα. Οι προτιμήσεις ή οι απόψεις που δηλώνει κάποιος σήμερα, π.χ. σε ένα ιστολόγιο ή στο προφίλ του σε μία υπηρεσία κοινωνικής δικτύωσης, ενδεχομένως να επηρεάσουν αρνητικά τη μελλοντική του επαγγελματική πορεία ή τις προσωπικές του σχέσεις. Στο μέλλον, για παράδειγμα, δεν μπορεί να αποκλειστεί το γεγονός ότι πιθανοί εργοδότες θα αναζητούν πληροφορίες για υποψήφιους υπαλλήλους τους στο διαδίκτυο. «Τα γραπτά μένουν», γι' αυτό θα πρέπει, οι δημοσιεύσεις και οι αναρτήσεις πληροφοριών στο διαδίκτυο να είναι αρκετά προσεκτικές γιατί είναι πολύ δύσκολο να διαγραφούν πλήρως[1]. Ελλοχεύει επίσης και ο κίνδυνος, να δημοσιεύονται και σε ιστοσελίδες που δεν θα περίμενε ποτέ κανείς. Επίσης, σε ακραίες περιπτώσεις μπορεί κανείς να πέσει θύμα υποκλοπής ταυτότητας (δηλαδή κάποιος κακόβουλος που γνωρίζει πολλά από τα προσωπικά δεδομένα ενός ατόμου, που ίσως αυτοβούλως να του τα έχει δώσει, π.χ. κατά τη συνομιλία μαζί του σε ένα ηλεκτρονικό χώρο

συζητήσεων) ή θύμα παρενόχλησης και εξαπάτησης τόσο ο ίδιος όσο και οι φίλοι του. Δυστυχώς, τέτοια περιστατικά είναι πλέον πολύ σύνηθη[1].

Κάποια συχνά παραδείγματα υποκλοπής δεδομένων είναι:

Οι συναλλαγές με κάποιες μη αξιόπιστες σελίδες που σκοπό έχουν να κλέψουν κάποιες πληροφορίες του χρήστη που στη συνέχεια θα τις χρησιμοποιήσουν για να του πάρουν ένα χρηματικό ποσό.

Η διαρροή των διαπιστευτηρίων, όνομα χρήστη (username) και κωδικός πρόσβασης (password), για μια ιστοσελίδα ή ένα διαδικτυακό παιχνίδι (online game) σε άλλους.

Ένα άλλο παράδειγμα υποκλοπής προσωπικών δεδομένων που τα τελευταία χρόνια έχει αυξηθεί ο αριθμός των θυμάτων του, είναι η δημοσίευση των προσωπικών δεδομένων ενός ατόμου χωρίς την έγκριση ή την θέληση του. Αυτό το φαινόμενο παρουσιάστηκε και πήρε μεγάλες διαστάσεις με τον ερχομό των υπηρεσιών κοινωνικής δικτύωσης στο διαδίκτυο.

Ένας από τους βασικούς κανόνες που θέτουν οι νόμοι για την προστασία των προσωπικών δεδομένων είναι ο εξής: για να χρησιμοποιήσει κάποιος τα προσωπικά δεδομένα άλλου για έναν συγκεκριμένο σκοπό πρέπει να έχει εξασφαλίσει τη συγκατάθεσή του. Αυτό αποτελεί και τη συνήθη περίπτωση κατά την επεξεργασία προσωπικών δεδομένων στο Διαδίκτυο. Σημαίνει πρακτικά ότι πρέπει το άτομο να έχει δηλώσει άμεσα ή έμμεσα ότι συναινεί στην επεξεργασία, αφού προηγουμένως έχει ενημερωθεί ακριβώς για το ποιος είναι αυτός που θέλει να χρησιμοποιήσει τα δεδομένα του (ή αλλιώς ο «υπεύθυνος επεξεργασίας»), για ποιον λόγο θέλει να τα χρησιμοποιήσει, ποια στοιχεία του θέλει να αποκτήσει και σε ποιους θα τα διαβιβάσει. Υπάρχουν βέβαια και εξαιρέσεις (π.χ. η επεξεργασία των δεδομένων κάποιες φορές επιβάλλεται από νόμο ή αποτελεί έννομο συμφέρον του υπεύθυνου επεξεργασίας, οπότε και επιτρέπεται να γίνεται χωρίς τη συγκατάθεσή του ατόμου). Οι εξαιρέσεις αυτές ορίζονται ρητά στους νόμους για την προστασία των προσωπικών δεδομένων.

1.4.3. Συμβουλές για την προστασία των προσωπικών δεδομένων στο διαδίκτυο

Απαιτείται ιδιαίτερη προσοχή πριν κανείς δώσει στο διαδίκτυο οποιοδήποτε προσωπικό του δεδομένο. Προληπτικά μέτρα προστασίας πρέπει πάντα να λαμβάνονται από το σύνολο των χρηστών διαδικτύου, διότι οι κίνδυνοι από ιούς, παράνομες εισβολές, υποκλοπές και άλλες απάτες είναι πολύ συχνοί και πολλές φορές αποδεικνύονται μοιραίοι, αφού μεταξύ άλλων μπορούν να επηρεάσουν ψυχολογικά και οικονομικά το άτομο. Από τις πιο γνωστές μορφές κυβερνοεγκλήματος είναι οι απάτες μέσω διαδικτύου, το cracking και hacking (εισβολή - διάρρηξη σε υπολογιστικά συστήματα), η διακίνηση - πειρατεία λογισμικού και εγκλήματα στα chat rooms (διαδικτυακές τοποθεσίες συνομιλίας). Γεννιέται λοιπόν εύλογα το ερώτημα πώς μπορεί να χρησιμοποιεί ο χρήστης το διαδίκτυο χωρίς να κινδυνεύει από παραβίαση των προσωπικών του δεδομένων, από απάτες, απειλές ή άλλες εγκληματικές ενέργειες;

Ο χρήστης θα πρέπει να είναι ενημερωμένος και υποψιασμένος για τους κινδύνους που ελλοχεύουν. Συνήθως, ο κακόβουλος χρήστης – εγκληματίας χρησιμοποιεί κάποιους συγκεκριμένους τρόπους προκειμένου να πείσει τα υποψήφια θύματά του να του δώσουν τις προσωπικές πληροφορίες που αναζητά. Έχοντας αυτό κατά νου, ο χρήστης οφείλει να ακολουθεί πάντα τους ασφαλέστερους δρόμους για το ταξίδι του στον κόσμο του διαδικτύου.

Ζητούνται δεδομένα; Πρέπει πάντα να είναι κανείς αρκετά επιφυλακτικός όταν του ζητούνται προσωπικά δεδομένα. Πρώτα από όλα ο χρήστης θα πρέπει να σκεφτεί αν τα στοιχεία που του ζητούνται να γνωστοποιήσει είναι απαραίτητα για την πραγματοποίηση της συγκεκριμένης επικοινωνίας (π.χ. όταν κάποιος ζητά στοιχεία όπως τη διεύθυνση κατοικίας ή την ηλεκτρονική διεύθυνση κατά τη συμπλήρωση μιας φόρμας δεν σημαίνει ότι νομιμοποιείται πάντα να την έχει). Από την άλλη όμως, κατά την διαδικασία καταχώρησης μιας ηλεκτρονικής παραγγελίας για την αγορά ενός προϊόντος θεωρείται εύλογο να απαιτείται η συμπλήρωση μιας ηλεκτρονικής φόρμας με προσωπικά στοιχεία όπως ονοματεπώνυμο, διεύθυνση ή ακόμη και αριθμός πιστωτικής κάρτας, ανάλογα με τον τρόπο πληρωμής.

Ποιος είναι από την «άλλη πλευρά»; Ο χρήστης θα πρέπει να έχει πάντα στο μυαλό του και να μην ξεχνά ποτέ ότι στην πραγματικότητα δεν μπορεί να είναι σίγουρος ποιος είναι από την «άλλη πλευρά». Προκειμένου να διασφαλίσει την ταυτότητα του «απέναντι», θα πρέπει να αναζητήσει κάποια βασικά, αναγραφόμενα στοιχεία, από τα οποία να μπορεί να επιβεβαιώσει την ταυτότητα της άλλης πλευράς (π.χ. όταν πρόκειται για εταιρεία θα πρέπει να αναγράφονται, εκτός από την επωνυμία της, κάποια βασικά στοιχεία, όπως τρόποι επικοινωνίας, αριθμός φορολογικού μητρώου, αριθμός μητρώου στο εμπορικό επιμελητήριο που ανήκει).

Αυξημένη πρέπει πάντα να είναι και η προσοχή του χρήστη όταν απευθύνεται σε άτομα που δεν γνωρίζει και δεν είναι απόλυτα σίγουρος σε ποιόν απευθύνεται Μία αναρτημένη φωτογραφία ενός προσώπου, που δεν έχει δει ποτέ από κοντά, σε ένα forum ή σε μία υπηρεσία κοινωνικής δικτύωσης δεν πιστοποιεί την ταυτότητά του και δεν σημαίνει ουσιαστικά τίποτα για το ποιος πραγματικά αυτός είναι[1].

Ανάρτηση δεδομένων. Ο χρήστης θα πρέπει να έχει πάντα στο μυαλό του πως οτιδήποτε αναρτά στο διαδίκτυο, αυτό παραμένει. Ακόμα και στην περίπτωση που ο ίδιος αποφασίσει να «κατεβάσει» μια ανάρτησή του, υπάρχει μεγάλη πιθανότητα αυτή η ανάρτηση να έχει ήδη διαβαστεί, διαδοθεί και πιθανότατα τροποποιηθεί από πολλούς άλλους χρήστες. Λόγω της φύσης του διαδικτύου και της εξάπλωσής του, ο χρήστης δεν πρέπει να λησμονεί ότι τα προσωπικά του δεδομένα και οτιδήποτε αναρτά δεν θα έχουν ως αποδέκτες μόνο τους προσωπικούς του φίλους. Εδώ θα πρέπει να επισημανθεί ότι, ακόμα και στην περίπτωση «διαδικτυακών» φίλων, όταν κάποιος επεξεργάζεται προσωπικά δεδομένα τους, θα πρέπει να υπάρχει προηγούμενη, σαφής συγκατάθεση τους για αυτή την ενέργεια. Για παράδειγμα, αν κάποιος προτίθεται να αναρτήσει μια φωτογραφία στο Facebook από μια κοινωνική εκδήλωση, αυτό προϋποθέτει ότι θα έχει εξασφαλίσει προηγουμένως τη συγκατάθεση όλων των εικονιζόμενων για τη δημοσίευσή της[1].

Εκτός όμως από τις παραπάνω περιπτώσεις, για τις οποίες ο κάθε χρήστης θα πρέπει να είναι ενήμερος για τον τρόπο προφύλαξής του, οι δύο πιο σημαντικές μέθοδοι εξαπάτησης και υποκλοπής προσωπικών δεδομένων είναι η περίπτωση του «ψαρέματος» (Phishing) και της αζήτητης – ανεπιθύμητης αλληλογραφίας (Spam),

περιπτώσεις που λίγο πολύ όλοι οι χρήστες θα έρθουν αντιμέτωποι κατά τη χρήση του διαδικτύου.

1.4.3.1. Phishing

Η διαρκώς αυξανόμενη χρήση του μηνύματος ηλεκτρονικού ταχυδρομείου και του διαδικτύου, αλλά και η εμπιστοσύνη που δείχνει να έχει το άτομο προς αυτά, φέρνουν ευπάθειες που πρέπει να αναγνωρίζονται και να αντιμετωπίζονται εγκαίρως και με τα κατάλληλα μέσα.

Στις περιπτώσεις λήψης μηνυμάτων ηλεκτρονικού ταχυδρομείου από τράπεζες θα πρέπει ο χρήστης να είναι αρκετά καχύποπτος. Μια τράπεζα δε θα έστελνε ποτέ ένα μήνυμα ηλεκτρονικού ταχυδρομείου προς τους πελάτες της, προσκαλώντας τους να συμπληρώσουν τα στοιχεία τους σε μια ιστοσελίδα ή να τα αποστείλουν μέσω ενός μηνύματος ηλεκτρονικού ταχυδρομείου. Μια τέτοια περίπτωση αποτελεί χαρακτηριστικό παράδειγμα εξαπάτησης μέσω «Phishing» και απαιτείται ιδιαίτερη προσοχή από την πλευρά του παραλήπτη, ώστε να την αποφύγει. Οι κοινότητες ασφαλείας στο διαδίκτυο έχουν εκτιμήσει ότι αυτός ο τρόπος εξαπάτησης είναι μια εξαιρετικά αποτελεσματική τεχνική επίθεσης στον κυβερνοχώρο και η χρήση του είναι απίθανο να μειωθεί στο εγγύς μέλλον.

Ο όρος «Phishing» είναι παραλλαγή της αγγλικής λέξης «fishing» (ψάρεμα) και σχετίζεται με την προσπάθεια απόσπασης προσωπικών στοιχείων, οικονομικού συνήθως χαρακτήρα, που αφορούν τραπεζικούς λογαριασμούς και πιστωτικές κάρτες, χρησιμοποιώντας πάντα ως «δόλωμα» κάποιο ψεύτικο πρόσχημα.

Οι περιπτώσεις εξαπάτησης «Phishing» έχουν ως αφετηρία την αποστολή ενός

μηνύματος ηλεκτρονικού ταχυδρομείου (email). Συνήθως, στο μήνυμα αυτό προβάλλεται ο ψευδής κάθε φορά ισχυρισμός ότι αποστέλλεται από κάποια υπαρκτή και νόμιμη πηγή (δημόσια υπηρεσία, υπηρεσία ηλεκτρονικών πληρωμών, τράπεζα, ηλεκτρονικό κατάστημα κλπ.), με απώτερο

σκοπό να παραπλανήσει τον παραλήπτη - χρήστη και να του αποσπάσει απόρρητα οικονομικά και προσωπικά δεδομένα. Τα δεδομένα αυτά στη συνέχεια συλλέγονται προκειμένου να χρησιμοποιηθούν για την πραγματοποίηση μη εξουσιοδοτημένων, παράνομων, οικονομικών συναλλαγών. Ο πιο σημαντικός παράγοντας για να είναι επιτυχημένη μία επίθεση Phishing είναι η οπτική εξαπάτηση. Στόχος του εκάστοτε απατεώνα είναι να πείσει το θύμα για την αυθεντικότητα και την αξιοπιστία του. Αυτό θα το επιτύχει χρησιμοποιώντας παραπλανητικό κείμενο, παραπλανητικές εικόνες και παραπλανητική σχεδίαση. Εάν ο κακόβουλος αποστολέας καταφέρει να συνδυάσει τα παραπάνω, οι «επιθέσεις» του θα είναι επιτυχημένες σε ποσοστό 90%.

Στις περισσότερες των περιπτώσεων, τα μηνύματα ηλεκτρονικού ταχυδρομείου τύπου «Phishing» ζητούν από τον παραλήπτη επιτακτικά και υποχρεωτικά να ακολουθήσει κάποιο σύνδεσμο, που συνήθως επισυνάπτεται στο μήνυμα, ώστε αυτός να ενημερώσει ή να επαληθεύσει άμεσα κάποια προσωπικά στοιχεία του για λόγους ασφαλείας. Οι σύνδεσμοι (links) αυτοί ανακατευθύνουν τον εκάστοτε παραλήπτη – χρήστη σε επιτηδευμένες – κακόβουλες ιστοσελίδες (web sites), οι οποίες αντιγράφουν πολύ πειστικά τους επίσημους διαδικτυακούς τόπους υπαρκτών και αξιόπιστων οργανισμών - εταιρειών. Η αντιγραφή των επίσημων διαδικτυακών τόπων είναι τόσο αληθοφανής (δημιουργούνται με αντιγραφή του HTML κώδικά τους), που ακόμα και η ανίχνευσή της από την εφαρμογή πλοήγησης στο διαδίκτυο (browser) να είναι σχεδόν αδύνατη, αφού στην γραμμή θέματος εμφανίζεται η αναμενόμενη διεύθυνση (συνήθως με κάποιες επιπλέον καταλήξεις που ο κοινός χρήστης είναι αδύνατον να γνωρίζει αν δεν είναι κατάλληλα ενημερωμένος και υποψιασμένος) και όχι η πραγματική διεύθυνση της πλαστής διαδικτυακής τοποθεσίας.

Βασικό μέλημα των αποστολέων όλων αυτών των κακόβουλων μηνυμάτων είναι, εκτός από την απόκτηση των επιθυμητών για αυτούς πληροφοριών, να μειώσουν και τον χρόνο αντίδρασης του ανυποψίαστου παραλήπτη - θύματος. Για τον σκοπό αυτό, στα μηνύματα που αποστέλλουν καθορίζεται πάντα ένα σύντομο χρονικό διάστημα μέσα στο οποίο ο παραλήπτης οφείλει να ολοκληρώσει την αποστολή των ζητούμενων πληροφοριών (ενημέρωση, επαλήθευση και αποστολή στοιχείων). Σε διαφορετική περίπτωση, οι κακόβουλοι αποστολείς απειλούν να απενεργοποιήσουν

τους λογαριασμούς του θύματος, με αποτέλεσμα αυτό να μην έχει τη δυνατότητα πραγματοποίησης περαιτέρω νέων συναλλαγών. Με τον τρόπο αυτό, ωθούν τον χρήστη - παραλήπτη του μηνύματος να αποκαλύψει τις πληροφορίες που του ζητούν, χωρίς να έχει τον απαιτούμενο χρόνο στην διάθεση του για να εξετάσει την γνησιότητα του μηνύματος.

Αυτή η προσπάθεια απόσπασης απόρρητων οικονομικών και προσωπικών δεδομένων, που χρησιμοποιεί πάντα ως «δόλωμα» κάποιο ψεύτικο πρόσχημα, έχει πάρει τρομακτικές διαστάσεις, με αποτέλεσμα να έχουν αναπτυχθεί νέες, εναλλακτικές μορφές, όπως είναι το Vishing, το Spear Phishing και το Social Networking Phishing.

Το Vishing είναι η πρακτική της αξιοποίησης των τεχνολογιών φωνητικών μηνυμάτων που βασίζονται στην IP (Voice over Internet Protocol ή VoIP ή τηλεφωνία μέσω διαδικτύου ή σωστότερα «φωνή επί διαδικτυακού πρωτοκόλλου») για την εξεύρεση του ζητούμενου θύματος στην παροχή προσωπικών, οικονομικών ή άλλων εμπιστευτικών πληροφοριών με σκοπό την οικονομική ανταμοιβή. Ο όρος Vishing προέρχεται από τον συνδυασμό «φωνής (Voice) και Phishing».

Από την εποχή ακόμα που εφευρέθηκε το τηλέφωνο, τα συστήματα σταθερής τηλεφωνίας αποδείχτηκαν πολύ αποτελεσματικά εργαλεία εκτέλεσης ακούσιων πράξεων από την πλευρά των συνδρομητών. Οι τηλεφωνικές κλήσεις θεωρούνται ακόμα και σήμερα ως μια από τις πιο ασφαλής μορφές επικοινωνίας. Οι κακόβουλοι χρήστες - εγκληματίες, εκμεταλλευόμενοι την εμπιστοσύνη του παραλήπτη – θύματος, του δίνουν έναν τηλεφωνικό αριθμό εξυπηρέτησης ή του ζητούν να τους γνωστοποιήσει τον δικό του τηλεφωνικό αριθμό, με τη δικαιολογία της εύκολης επικοινωνίας των εκπροσώπων μιας υποτιθέμενης εταιρίας[8].

Με την αλματώδη ανάπτυξη της τεχνολογίας στον τομέα της IP τηλεφωνίας, υπάρχει πλέον η δυνατότητα σε υπηρεσίες τηλεφωνικής εξυπηρέτησης να ξεκινούν ή να τερματίζουν σε έναν υπολογιστή που μπορεί να βρίσκεται οπουδήποτε στον κόσμο. Οι κλήσεις αυτού του είδους γίνονται με τη χρήση πρωτοκόλλων διαδικτύου και είναι σχεδόν ανιχνεύσιμες. Το γεγονός αυτό οδήγησε τους απατεώνες του Vishing να αναπτύξουν μια νέα τεχνική εξαπάτησης, την τεχνική «spoofing». Πρόκειται για μια τεχνική πλαστογράφησης πληροφοριών αναγνώρισης του καλούντος και ως

αποτέλεσμα έχει η ανίχνευση της κλήσης να είναι πολύ δύσκολη έως και αδύνατη. Το κόστος αυτού του είδους κλήσεων είναι σχετικά φθηνό, οπότε ακόμη και ένα μικρό ποσοστό θυμάτων να ανταποκριθεί είναι αρκετό για να καταστήσει την απάτη πολύ κερδοφόρα.

Το Spear Phishing σχετίζεται με την αποστολή «στοχευμένων» μηνυμάτων ηλεκτρονικού ταχυδρομείου (emails) προς ομάδες ανθρώπων, οι οποίοι διαθέτουν ένα κοινό χαρακτηριστικό. Για παράδειγμα, οι παραλήπτες τέτοιων «στοχευμένων» μηνυμάτων ηλεκτρονικού ταχυδρομείου μπορεί να εργάζονται στην ίδια εταιρεία, να ανήκουν στο ίδιο χρηματοπιστωτικό ίδρυμα, να φοιτούν στο ίδιο κολέγιο, να παραγγέλλουν προϊόντα και εμπορεύματα από τον ίδιο ιστότοπο. Σκοπό των αποστολέων είναι να συγκεντρώσουν συγκεκριμένες πληροφορίες για τα μέλη της «στοχευμένης» ομάδας ή ακόμα χειρότερα να μολύνουν τις ηλεκτρονικές διευθύνσεις τους με κακόβουλο λογισμικό. Τα μηνύματα αυτά απευθύνονται προσωπικά σε κάθε μέλος – χρήστη της ομάδας – στόχος και ως αποστολέας εμφανίζεται κάποιο υπαρκτό και νόμιμο φυσικό πρόσωπο ή μια νόμιμη εταιρεία – υπηρεσία. Ο τρόπος σχεδίασής τους βασίζεται στο να πείσουν τους παραλήπτες να ανοίξουν ένα συνημμένο αρχείο ή να ακολουθήσουν έναν επισυναπτόμενο σύνδεσμο και να πληκτρολογήσουν τα προσωπικά τους διαπιστευτήρια (όνομα χρήστη και κωδικό πρόσβασης). Στην περίπτωση που κάποιο από τα μέλη της ομάδας - στόχου ανταποκριθεί στο αίτημα του μηνύματος Spear Phishing αμέσως θέτει προσωπικές και συχνά απόρρητες πληροφορίες της ομάδας στη διάθεση των απατεώνων. Οι επιτυχείς επιθέσεις μπορούν να οδηγήσουν σε εκμετάλλευση ή συμβιβασμό μεμονωμένων συσκευών ή και ολόκληρων πληροφοριακών συστημάτων και δικτύων. Κατ’ επέκταση, οι συνέπειες μιας τέτοιας κακόβουλης ενέργειας για τη φήμη και την οικονομική υπόσταση ενός οργανισμού ή μιας επιχείρησης μπορεί να είναι καταστροφικές.

Οι επιθέσεις αυτού του είδους είναι επίμονες και έχουν αρκετά υψηλό ποσοστό επιτυχίας. Είναι σε θέση να παρακάμπτουν τις παραδοσιακές άμυνες ασφαλείας και να εκμεταλλεύονται τα ευάλωτα λογισμικά, που ενδεχομένως είναι εγκατεστημένα σε συσκευές πρόσβασης στο διαδίκτυο. Προκειμένου να θεωρηθεί επιτυχής μια επίθεση τύπου Spear Phishing ακολουθούνται τρία βασικά στάδια:

Η αναγνώριση: Στη φάση αναγνώρισης, ο κακόβουλος αποστολέας περιηγείται σε ιστοσελίδες και μεταφορτώνει αρχεία, με σκοπό να συλλέξει πληροφορίες που αφορούν στην αρχιτεκτονική του δικτύου της ομάδας – στόχου. Οι πληροφορίες αυτές περιλαμβάνουν κυρίως διευθύνσεις IP, ονόματα διακομιστών, εκδόσεις εγκατεστημένων προγραμμάτων λογισμικού, domain names και οτιδήποτε άλλο θα βοηθήσει τον κακόβουλο αποστολέα να έχει μια πλήρη εικόνα του εσωτερικού δικτύου. Επίσης, αναζητά στοιχεία επικοινωνίας με το προσωπικό, οργανωτικά διαγράμματα και περιγραφές θέσεων εργασίας. Με τον τρόπο αυτό, ανιχνεύει πιθανά ευάλωτα σημεία του εσωτερικού δικτύου.

Η οπτικοποίηση: Έχοντας πλέον μια εικόνα της αρχιτεκτονικής του εσωτερικού δικτύου, ο κακόβουλος αποστολέας τοποθετεί τον κακόβουλο κώδικα σε ένα «όχημα» παράδοσης, όπως ένα συνημμένο αρχείο ή μια ιστοσελίδα. Τα συνημμένα αρχεία που περιέχονται στα μηνύματα ηλεκτρονικού ταχυδρομείου τύπου Spear Phishing εμφανίζονται ως ένας κοινός τύπος αρχείου, όπως (*.rtf) ή (*.pdf) ή (*.xls, *.xlsx) ή (*.rar) ή (*.zip) ή (*.dox , *.docx) ή (*.exe) ή (*.jpg) και το όνομα τους (*) παρουσιάζει ενδιαφέρον για τα μέλη της επιθυμητής ομάδας - στόχου, όπως για παράδειγμα «Αποδοχή πληρωμής.pdf».

Η διανομή: Η τελευταία φάση αποτελεί τη φάση της διανομής, δηλαδή της παράδοσης του ηλεκτρονικού μηνύματος στα μέλη της ομάδας – στόχου, η οποία θα συνεπάγεται τη μεταφορά του κακόβουλου κώδικα στο εσωτερικό δίκτυο. Μετά τη διεξαγωγή της διαδικτυακής αναγνώρισης, ο απατεώνας έχει συλλέξει αρκετές πληροφορίες και είναι πλέον σε θέση να δημιουργήσει ένα ηλεκτρονικό μήνυμα τύπου Spear Phishing. Σκοπός του είναι να «αλλάξει», να παραποιήσει το μήνυμα ηλεκτρονικού ταχυδρομείου ώστε αυτό να εμφανίζεται ότι στάλθηκε από μια αξιόπιστη επαφή, αναγνωρίσιμη από το σύνολο των μελών της ομάδας - στόχου. Ένα μήνυμα ηλεκτρονικού ταχυδρομείου που φαίνεται να προέρχεται από μια αξιόπιστη επαφή αυξάνει την πιθανότητα επιτυχούς συμβιβασμού.

Αυτή είναι η πιο επιτυχημένη μορφή απόκτησης εμπιστευτικών πληροφοριών στο διαδίκτυο, που αντιπροσωπεύει το μεγαλύτερο μέρος των επιθέσεων[9].

Το Social Networking Phishing σχετίζεται με τα δίκτυα κοινωνικής δικτύωσης, τα οποία αποδεικνύονται ότι είναι η πιο δημοφιλής πηγή πληροφοριών για τους επίδοξους απατεώνες. Στην περίπτωση αυτή, η αποστολή προσωποποιημένων μηνυμάτων γίνεται ακόμα πιο εύκολη για τους απατεώνες, αφού η άντληση πληροφοριών και πολλών προσωπικών δεδομένων που αφορούν το χρήστη – θύμα βρίσκονται αναρτημένα στο προφίλ που διατηρεί στις ιστοσελίδες κοινωνικής δικτύωσης.

Τα τελευταία χρόνια, το Phishing μέσω των υπηρεσιών κοινωνικής δικτύωσης έχει αποδειχτεί ένα πολύ αποτελεσματικό εργαλείο στα χέρια των απατεώνων. Αυτό οφείλεται κυρίως στην διαρκώς αυξανόμενη χρήση αυτού του είδους των υπηρεσιών από εκατομμύρια χρήστες, οι οποίοι το θεωρούν ένα αξιόπιστο μέσο επικοινωνίας, τόσο για προσωπική όσο και για επαγγελματική επικοινωνία. Παράλληλα, η πλειοψηφία των χρηστών των υπηρεσιών κοινωνικής δικτύωσης αισθάνονται ασφαλείς με τη χρήση των λογαριασμών που διατηρούν, επειδή θεωρούν ότι μόνο οι διαδικτυακοί τους φίλοι έχουν πρόσβαση σε προσωπικές τους πληροφορίες. Το γεγονός αυτό πολλές φορές τους κάνει απρόσεκτους όταν εισάγουν ή διαθέτουν προσωπικά τους στοιχεία σε ιστότοπους κοινωνικής δικτύωσης. Οι επιτιθέμενοι το γνωρίζουν αυτό πολύ καλά και εκμεταλλεύονται αρκετά συχνά την εμπιστοσύνη του χρήστη των κοινωνικών δικτύων για προσωπικό τους όφελος[10].

Σύμφωνα με έρευνα της Kaspersky Lab (παγκόσμια εταιρεία ασφάλειας στον κυβερνοχώρο), το 22% της εξαπάτησης Phishing στο διαδίκτυο έχουν ως στόχο το Facebook. Οι σύνδεσμοι (links) που ανακατευθύνουν το χρήστη σε επιτηδευμένες – κακόβουλες ιστοσελίδες (web sites) που μιμούνται ιστοσελίδες υπηρεσιών κοινωνικής δικτύωσης αποτελούν το 35% όλων των περιπτώσεων στις οποίες ενεργοποιήθηκαν τα προϊόντα ασφαλείας της Kaspersky Lab. Επίσης, έχουν καταγραφεί περισσότερες από 600 εκατομμύρια περιπτώσεις χρηστών προϊόντων ασφαλείας Kaspersky, οι οποίοι επιχείρησαν πρόσβαση σε ιστότοπους ηλεκτρονικού "ψαρέματος" - και κάθε μέρα υπάρχουν πάνω από 20.000 περιστατικά κατά τα οποία οι χρήστες των προϊόντων ασφαλείας της Kaspersky αποπειράθηκαν να ακολουθήσουν συνδέσμους που τους ανακατευθύνουν σε ψεύτικες σελίδες στο Facebook[11].

Λόγω της αυξανόμενης εξάρτησης των οργανισμών, των ατόμων αλλά και της κοινωνίας από τη χρήση του μηνύματος ηλεκτρονικού ταχυδρομείου και του διαδικτύου, δεν υπάρχει εγγυημένος τρόπος να σταματήσει κανείς έναν εισβολέα από το να έχει πρόσβαση σε ένα επιχειρηματικό δίκτυο ή σε προσωπικά δεδομένα ατόμων. Η καλύτερη μέθοδος προστασίας δεν είναι άλλη από την ενημέρωση και παράλληλα την ορθή εκπαίδευση του χρήστη στο τι είναι το Phishing και πως να το διακρίνει. Αρκεί απλά να είναι λίγο προσεκτικός και επιφυλακτικός.

Κακόβουλοι σύνδεσμοι. Σε κάθε περίπτωση, αυτό που οφείλει να κάνει πρωτίστως ο χρήστης – παραλήπτης τέτοιων κακόβουλων μηνυμάτων είναι να μην ακολουθεί τους συνδέσμους που επισυνάπτονται. Ακολούθως, προτείνεται να πληκτρολογήσει τις διευθύνσεις Ενιαίου Εντοπιστή Πόρων (Uniform Resource Locators, URLs) που του ζητούνε να επισκεφθεί σε καινούργια καρτέλα στον επιθυμητό για τον ίδιο πλοηγό ιστοσελίδων (browser), όπως Internet Explorer, Microsoft Edge, Mozilla, Chrome, Opera, Safari κλπ. Με τον τρόπο αυτό, ο browser είναι δυνατόν να ανιχνεύσει την κακόβουλη διεύθυνση URL, αναγνωρίζοντας τις απαγορευμένες καταλήξεις σε αυτή.

Ταυτότητα αποστολέα. Σαν γενική αρχή, ο χρήστης θα πρέπει να αποφεύγει να συμπληρώνει ηλεκτρονικές φόρμες με προσωπικά του στοιχεία, οι οποίες βρίσκονται ενσωματωμένες σε μηνύματα email. Αν υπάρχει η οποιαδήποτε αμφιβολία για την ταυτότητα του αποστολέα, το προτιμότερο θα ήταν πριν ο παραλήπτης απαντήσει, να έρθει πρώτα σε επικοινωνία με την εταιρεία, την υπηρεσία ή το άτομο που φαίνεται ως αποστολέας του μηνύματος ηλεκτρονικού ταχυδρομείου για να εξακριβώσει ότι δεν πρόκειται για περίπτωση εικονικού μηνύματος απάτης «Phishing».

Πρωτόκολλο https. Οι περιπτώσεις όπου ο χρήστης καλείται να εισάγει ευαίσθητες προσωπικές πληροφορίες στο πλαίσιο συμπλήρωσης κάποιας ηλεκτρονικής φόρμας ή πριν από κάθε ηλεκτρονική του συναλλαγή, θα πρέπει να τον κάνουν ιδιαίτερα προσεκτικό. Απαιτείται έλεγχος για το κατά πόσο είναι ασφαλής ο τρόπος επικοινωνίας με την ιστοσελίδα που επισκέπτεται, προσέχοντας η ηλεκτρονική διεύθυνσή της να αρχίζει με «https://» και όχι με το απλό «http://». Το Hypertext Transfer Protocol Secure (https) είναι ένα πρωτόκολλο επικοινωνιών για ασφαλή

επικοινωνία μέσω ενός δικτύου υπολογιστών που χρησιμοποιείται ευρέως στο διαδίκτυο. Πρόκειται ουσιαστικά για επικοινωνία με τη χρήση του πρωτοκόλλου Hypertext Transfer Protocol (http) μέσω μιας σύνδεσης κρυπτογραφημένης με τη χρήση των πρωτοκόλλων κρυπτογράφησης Transfer Layer Secure (TLS) ή του προκατόχου του Secure Sockets Layer (SSL). Ένας σύνδεσμος (URL) που αρχίζει με το πρόθεμα https υποδηλώνει ότι θα χρησιμοποιηθεί κανονικά το πρωτόκολλο http, αλλά η σύνδεση θα γίνει σε διαφορετική πόρτα (443 αντί 80) και τα δεδομένα θα ανταλλάσσονται κρυπτογραφημένα. Το πρωτόκολλο https χρησιμοποιείται σε ιστότοπους όπου απαιτείται αυθεντικοποίηση χρηστών και κρυπτογραφημένη επικοινωνία. Σήμερα χρησιμοποιείται ευρέως στο διαδίκτυο όπου χρειάζεται αυξημένη ασφάλεια διότι διακινούνται ευαίσθητες πληροφορίες (π.χ. αριθμοί πιστωτικών καρτών, ονόματα χρηστών, κωδικοί πρόσβασης, κ.λπ.).

Μέτρα ασφάλειας στις συσκευές σύνδεσης. Κρίνεται απαραίτητη η εγκατάσταση ενός λογισμικού φίλτρου και ενός λογισμικού προστασίας από ιούς (antivirus) στον υπολογιστή του χρήστη ή στις έξυπνες συσκευές που χρησιμοποιεί για την διασύνδεση του με το διαδίκτυο. Τα λογισμικά αυτά είναι από τις ελάχιστες εφαρμογές, αν όχι οι μόνες, που είναι απαραίτητο να ξεκινάνε αυτόματα μαζί με το λειτουργικό σύστημα κάθε συσκευής, και να παραμένουν ενεργές για όση ώρα είναι ενεργές, ανοιχτές οι συσκευές αυτές.

Το λογισμικό προστασίας (antivirus) δύναται να προστατεύσει τον εκάστοτε χρήστη τόσο από ιούς όσο και από κακόβουλα λογισμικά υποκλοπής (spyware ή Trojan horse ή Backdoor). Είναι αρκετά σύνηθες τα μηνύματα τύπου Phishing να παραπέμπουν σε ιστοσελίδες που εγκαθιστούν στον υπολογιστή λογισμικά υποκλοπής, ικανά να καταγράφουν όλες τις πληροφορίες που αφορούν σε αριθμούς λογαριασμών και πιστωτικών καρτών, μέχρι και κωδικών πρόσβασης που εισάγει κάθε φορά ο χρήστης, ακόμα και μετά την έξοδο του από την ιστοσελίδα. Εκ παραλλήλου, το λογισμικό φίλτρο είναι λογισμικό το οποίο μπορεί να επιτρέψει ή να αποκλείσει, διακόψει την πρόσβαση σε ιστότοπους με παράνομο ή ακατάλληλο ή επιβλαβές περιεχόμενο ανάλογα με τις «ρυθμίσεις» που έχει επιλέξει ο χρήστης.

Για να λειτουργήσουν και να προστατέψουν τον χρήστη οι εφαρμογές αυτές δεν είναι απαραίτητο να τις «τρέξει». Τέτοιου είδους λογισμικά έχουν μια λειτουργία προστασίας σε πραγματικό χρόνο (real time protection), ελέγχοντας άμεσα οποιοδήποτε ενέργεια ή αρχείο χρησιμοποιήσει ο χρήστης. Ο έλεγχος αυτός γίνεται σε κάθε αλληλεπίδραση που έχει ο χρήστης με ένα αρχείο, είτε αν το κατεβάζει από το διαδίκτυο, είτε όταν το μετακινεί, ή το αντιγράφει.

Το πόσο αποτελεσματικό μπορεί να είναι ένα φίλτρο ή ένα anivirus εξαρτάται από το πόσο «έξυπνο» είναι καθώς και από το πόσο «ενημερωμένες» και έγκυρες είναι οι βάσεις δεδομένων του (λίστες με απαγορευμένους ιστότοπους και χαρακτηριστικά του κώδικά εκατομμυρίων ιών, worms, trojans, και άλλων τύπων malware, αντίστοιχα). Επομένως, είναι πολύ σημαντικό τα λογισμικά αυτά να είναι συνδεδεμένα με το διαδίκτυο, για να «κατεβάζουν» τις νεότερες ενημερώσεις όσον αφορά τις βάσεις δεδομένων τους. Αν δεν είναι ενημερωμένα, είναι θέμα χρόνου να βρεθεί ο «ψηφιακός» πολίτης εκτεθειμένος και να πέσει θύμα απάτης.

Πολλοί από τους παρόχους υπηρεσιών διαδικτύου έχουν ήδη εγκατεστημένα λογισμικά φίλτρων και λογισμικά προστασίας από ιούς στα δικά τους συστήματα και υπηρεσίες. Σε αυτή την περίπτωση δεν είναι αναγκαία η εγκατάσταση στον εξοπλισμό του χρήστη τέτοιου είδους λογισμικών.

1.4.3.2. Αζήτητη – Ανεπιθύμητη ηλεκτρονική επικοινωνία (Spam)

Στη διεθνή βιβλιογραφία, με τον όρο αζήτητη – ανεπιθύμητη αλληλογραφία (spam) νοείται κάθε ηλεκτρονικό μήνυμα που αποστέλλεται με σκοπό την εμπορική προώθηση προϊόντων, υπηρεσιών, ιδεών ή και κάθε άλλο διαφημιστικό σκοπό, χωρίς ο παραλήπτης να έχει δώσει τη συγκατάθεσή του για αυτό. Συνήθως, ένα ή και περισσότερα μηνύματα ηλεκτρονικού ταχυδρομείου στέλνονται ανώνυμα προς πολλαπλούς αποδέκτες. Στα ανώνυμα spam μηνύματα η πραγματική ταυτότητα του αποστολέα δεν είναι έγκυρη ή είναι πλαστογραφημένη ή μεταμφιεσμένη σε κάποια άλλη πραγματική διεύθυνση. Ο σκοπός του ανώνυμου spam είναι η απόκρυψη των πραγματικών στοιχείων του αποστολέα.

Ο λόγος για τον οποίο χρησιμοποιούνται αυτού του είδους τα μηνύματα ηλεκτρονικού ταχυδρομείου είναι η αποκομιδή κέρδους. Κύριος σκοπός τους είναι η προώθηση διαφημιστικού περιεχομένου, όπως για παράδειγμα νέα προϊόντα ή και υπηρεσίες, δράσεις και ενημερώσεις πολιτικών κομμάτων (όπως για παράδειγμα μηνύματα από υποψήφιους βουλευτές, τα οποία ως επί το πλείστων βομβαρδίζουν τα κινητά τηλέφωνα κυρίως λίγες ημέρες πριν τις εκάστοτε εκλογές) ή και φιλανθρωπικών ιδρυμάτων.

Ενδέχεται όμως, όταν χρησιμοποιούνται υπηρεσίες επικοινωνίας, πολλά μηνύματα spam να μην έχουν διαφημιστικό ή εμπορικό σκοπό, αλλά ο σκοπός τους να είναι η παραπλάνηση του χρήστη – παραλήπτη. Πρόκειται, ή για μηνύματα που προτρέπουν την προώθηση τους σε τρίτους (μηνύματα αλυσίδα) ή για κακόβουλα μηνύματα εξαπάτησης με στόχο την υφαρπαγή προσωπικών δεομένων (Phishing), όπως ονόματα χρήστη (usernames) και κωδικοί πρόσβασης (passwords), αριθμοί πιστωτικών καρτών ή λογαριασμών κ.λπ., ή για κακόβουλα μηνύματα με στόχο την οικονομική εξαπάτηση ή ακόμα και για φαινομενικά εμπορικά μηνύματα που παραπέμπουν σε ιστοσελίδες που χρησιμοποιούνται για τη διάδοση κακόβουλου λογισμικού (malware). Σε αυτές τις περιπτώσεις χρειάζεται ο χρήστης να έχει αυξημένη την προσοχή του. Να μην «ανοίγει» συνημμένα αρχεία και συνδέσμους που περιέχονται σε μηνύματα ηλεκτρονικού ταχυδρομείου, όταν δεν γνωρίζει από πού προέρχονται.

Τα αζήτητα διαφημιστικά μηνύματα μπορεί να «ενοχλήσουν» σε πολλά σημεία επαφής της ιδιωτικής ζωής του ατόμου (ηλεκτρονικό ταχυδρομείο, ιστοσελίδα κοινωνικής δικτύωσης, κινητό τηλέφωνο). Για την αποστολή λοιπόν ενός μηνύματος spam, πρακτική γνωστή και ως «spamming», οι αποστολείς αυτών, γνωστοί και ως «spammers», είναι δυνατόν να χρησιμοποιήσουν όλες τις γνωστές, διαθέσιμες περιπτώσεις ηλεκτρονικής επικοινωνίας, όπως: τα κλασσικά μηνύματα ηλεκτρονικού ταχυδρομείου (emails), τις υπηρεσίες μηνυμάτων μέσω των συστημάτων κινητής τηλεφωνίας (SMS, MMS), τις υπηρεσίες φαξ, τις υπηρεσίες στιγμιαίων μηνυμάτων (instant messaging), όπως MSN, Yahoo Messenger, Google Chat, κ.ά., τις υπηρεσίες

ηλεκτρονικής ανταλλαγής μηνυμάτων, όπως σελίδες κοινωνικής δικτύωσης (Facebook, Twitter, Myspace)[12].

Η δημοσιοποίηση της διεύθυνσης ηλεκτρονικού ταχυδρομείου σε ηλεκτρονικές λίστες, καταλόγους, μηχανές αναζήτησης, διαδικτυακούς τόπους ή και σε διαδικτυακές τοποθεσίες συνομιλίας (chat rooms) θα πρέπει να αποφεύγεται. Η χρήση μηχανισμών αυτόματης συλλογής διευθύνσεων από τα ανωτέρω σημεία διαδικτύου είναι από τις συνηθέστερες μεθόδους των spammers και είναι γνωστή ως συγκομιδή (harvesting).

Το spam των κινητών τηλεφώνων είναι μια μορφή αζήτητης - ανεπιθύμητης αλληλογραφίας (ειδικά μηνύματα διαφημίσεων), που απευθύνεται σε μηνύματα κειμένου ή σε άλλες υπηρεσίες επικοινωνίας κινητών τηλεφώνων (SMS, MMS spamming). Δεδομένου ότι η δημοτικότητα των κινητών τηλεφώνων αυξήθηκε στις αρχές της δεκαετίας του 2000, λόγω της εξέλιξης των κινητών τηλεφώνων και της εμφάνισης των έξυπνων συσκευών κινητής τηλεφωνίας (smartphones), οι χρήστες μηνυμάτων κειμένου άρχισαν να βλέπουν την αύξηση του αριθμού των ανεπιθύμητων και ιδιαίτερα των εμπορικών και διαφημιστικών μηνυμάτων που αποστέλλονται στα smartphones τους μέσω μηνυμάτων κειμένου. Αυτό μπορεί να είναι ιδιαίτερα ενοχλητικό για τον παραλήπτη, διότι, σε αντίθεση με το ηλεκτρονικό ταχυδρομείο, ορισμένοι παραλήπτες ενδέχεται να χρεώνονται ένα «τέλος» για κάθε μήνυμα που λαμβάνουν, συμπεριλαμβανομένων και των ανεπιθύμητων μηνυμάτων.

Το spam των κινητών τηλεφώνων είναι γενικά λιγότερο διαδεδομένο από το spam μέσω ηλεκτρονικού ταχυδρομείου. Αυτό οφείλεται κυρίως στο υψηλότερο κόστος που έχει για τους spammers και στα τεχνολογικά εμπόδια στην αποστολή κινητών μηνυμάτων σε ορισμένους τομείς.

Μη αποστολή απάντησης. Γενικώς, ως η πιο ενδεδειγμένη λύση για να αποφύγει ο παραλήπτης την λήψη αζήτητης – ανεπιθύμητης ηλεκτρονικής αλληλογραφίας, είναι να μην απαντάει στον αποστολέα ηλεκτρονικά και να μην ακολουθεί προτεινομένους συνδέσμους (links), που ενδεχομένως αναφέρονται στο μήνυμα, ακόμα και αν πρόκειται για συνδέσμους διαγραφής της ηλεκτρονικής διεύθυνσης του από την λίστα του αποστολέα (unsubscribe links). Στην περίπτωση που απαντήσει σε μηνύματα spam ουσιαστικά επαληθεύει και συνάμα επικυρώνει την

διεύθυνση του ηλεκτρονικού του ταχυδρομείου. Αυτό έχει σαν αποτέλεσμα να ενθαρρύνει τους επίδοξους «spammers» να στείλουν περισσότερα μηνύματα[12].

Υποβολή καταγγελίας. Αν κάποιος χρήστης δεχθεί ένα μήνυμα ηλεκτρονικού ταχυδρομείου με οποιονδήποτε τρόπο από άγνωστο αποστολέα, οφείλει αρχικά να ελέγξει αν υπήρχε προηγούμενη συναλλαγή με την επιχείρηση/οργανισμό/υπηρεσία του αποστολέα (πχ. αγορά προϊόντων/ υπηρεσιών). Στην περίπτωση που υπήρχε προηγούμενη συναλλαγή, ο χρήστης θα πρέπει να ελέγξει αν ο ίδιος έχει δώσει τη συγκατάθεσή του για ενδεχόμενη αποστολή διαφημιστικών μηνυμάτων από τον αποστολέα. Όταν και οι δύο προαναφερόμενοι έλεγχοι αποβούν αρνητικοί, τότε πρόκειται για μήνυμα αζήτητης - ανεπιθύμητης επικοινωνίας. Ο χρήστης έχει το δικαίωμα να καταγγείλει τον υπεύθυνο για την αποστολή μηνύματος αζήτητης – ανεπιθύμητης αλληλογραφίας στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα είτε μέσω της υπηρεσίας ηλεκτρονικής υποβολής καταγγελιών (ιστοσελίδα της Αρχής) είτε μέσω ηλεκτρονικού ταχυδρομείου με τη χρήση της σχετικής φόρμας καταγγελίας, επισυνάπτοντας σε κάθε περίπτωση το μήνυμα[12]. Η Αρχή είναι το αρμόδιο όργανο να ελέγξει αποστολείς, οι οποίοι έχουν την έδρα τους στην Ελλάδα.

Φραγή ηλεκτρονικών διευθύνσεων. Η περαιτέρω μείωση της λήψης αζήτητης - ανεπιθύμητης ηλεκτρονικής επικοινωνίας μπορεί να επιτευχθεί με την χρήση και άλλων μέσων αναφοράς. Ενδεικτικά, για επιπλέον προστασία, ο χρήστης – παραλήπτης έχει δικαίωμα να αναφέρει στον πάροχο υπηρεσιών διαδικτύου ότι γίνεται δέκτης μηνυμάτων spam και να ζητήσει τη φραγή συγκεκριμένων ηλεκτρονικών διευθύνσεων από τις οποίες του αποστέλλονται αυτά. Επιπλέον, ο πάροχος υπηρεσιών διαδικτύου του χρήστη μπορεί να βοηθήσει σχετικά με τη χρήση ειδικού λογισμικού φιλτραρίσματος ή και να παρέχει ανάλογα προϊόντα που χρησιμοποιούν πλήθος εναλλακτικών δυνατοτήτων και υπηρεσιών. Συγκεκριμένα, δυνατότητα φραγής μηνυμάτων που προέρχονται από συγκεκριμένες διευθύνσεις ή ονόματα χώρου (IP/reverse, DNS name blacklist), εξειδικευμένες λίστες «Spamhaus» και έλεγχος της ηλεκτρονικής αλληλογραφίας μέσω αυτών, αναγνώριση μη υπαρκτών ονομάτων χώρου ή μη επιλυόμενων ηλεκτρονικών διευθύνσεων (bad sender/non-resolving IP

addresses), τεχνικές αποτροπής ανίχνευσης λογαριασμών χρηστών (anti-harvest) και έλεγχο για αποστολή σε μη υπαρκτούς χρήστες (spam trap)[12].

Προστασία της διεύθυνση ηλεκτρονικού ταχυδρομείου. Προκειμένου ο χρήστης – παραλήπτης να αποφύγει την πιθανότητα συλλογής της του από «spammers», οπότε και την λήψη αμέτρητων μηνυμάτων spam καθημερινώς, κρίνεται απαραίτητο να λαμβάνει επιπλέον μέτρα προστασίας.

Συστήνεται, ο χρήστης να είναι ιδιαίτερα προσεκτικός σε ποιον γνωστοποιεί κάθε φορά την διεύθυνση ηλεκτρονικού ταχυδρομείου του. Οφείλει να την γνωρίζουν άτομα ή υπηρεσίες και οργανισμοί που γνωρίζει και εμπιστεύεται πλήρως. Για παράδειγμα, όταν κατά την εγγραφή του σε κάποιο ηλεκτρονικό περιοδικό ή στο πλαίσιο χρήσης ηλεκτρονικών υπηρεσιών, του ζητείται να δώσει τη διεύθυνσή του θα πρέπει να ελέγξει αν έχει την δυνατότητα να δηλώσει εκ των προτέρων ότι δεν επιθυμεί την λήψη μηνυμάτων με διαφημιστικό περιεχόμενο ή άλλες πληροφορίες. Επίσης, θα πρέπει να ελέγχει την Πολιτική Ιδιωτικότητας (Privacy Policy) που οφείλει να εφαρμόζει η κάθε εταιρεία ή οργανισμός, προτού δώσει τα προσωπικά του δεδομένα στο διαδίκτυο, ούτως ώστε να ενημερωθεί για τον τρόπο επεξεργασίας τους και να βεβαιωθεί ότι αυτά δεν διαβιβάζονται σε τρίτους.

Στην περίπτωση που ο χρήστης χρειάζεται να αναρτήσει σε κάποιο διαδικτυακό τόπο τα στοιχεία του, καλό θα είναι να γράψει τη διεύθυνση ηλεκτρονικού ταχυδρομείου του με τέτοιο τρόπο ώστε να μην είναι δυνατή η αυτόματη συλλογή της και η αναγνώρισή της από τους μηχανισμούς των «spammers». Δυο από τους πιο ενδεδειγμένους τρόπους είναι η ανάρτησή της ως εικόνα αντί για κείμενο ή η αναγραφή της χωρίς το σύμβολο «@», που χαρακτηρίζει όλες τις διευθύνσεις ηλεκτρονικού ταχυδρομείου. Για παράδειγμα, αντί για «my_name@mycompany.com» να επιλεγεί ο τρόπος γραφής «my_name At mycompany dot com».

Χρήση λογισμικού φιλτραρίσματος. Η χρήση ενός τέτοιου λογισμικού δίνει την δυνατότητα και την ευελιξία στον χρήστη να μπορεί ο ίδιος να εντοπίσει και να διαχειριστή ανάλογα την αζήτητη – ανεπιθύμητη ηλεκτρονική αλληλογραφία που λαμβάνει μεταξύ των εισερχόμενων μηνυμάτων ηλεκτρονικού ταχυδρομείου. Ανάλογα με τις ρυθμίσεις που επιλέγει να κάνει κάθε φορά ο χρήστης μπορεί είτε να

«μπλοκάρει» τα ανεπιθύμητα μηνύματα, είτε να τα τοποθετήσει σε ειδικό φάκελο τον γνωστό σε όλους φάκελο «Ανεπιθύμητης αλληλογραφίας».

Παρά το γεγονός ότι η χρησιμότητα του λογισμικού φιλτραρίσματος είναι αδιαμφησβήτητη, η αποτελεσματικότητα του αρκετές φορές δεν είναι η αναμενόμενη. Υπάρχουν περιπτώσεις που τα φίλτρα αποτυγχάνουν να εντοπίσουν τα μηνύματα spam, ενώ άλλες φορές να χαρακτηρίσουν ως spam μηνύματα που είναι χρήσιμα.

Υπάρχει μια σειρά από εξελιγμένα ελεύθερα και εμπορικά προγράμματα spam φίλτρων τα οποία διατίθενται και στο διαδίκτυο. Με την εγκατάσταση του «antispam» λογισμικού στον υπολογιστή ή στις έξυπνες συσκευές που χρησιμοποίει ο χρήστης, προκειμένου να διαχειριστή την ηλεκτρονική του αλληλογραφία, μπορεί να εφαρμόσει έλεγχο στον πελάτη (client) του ηλεκτρονικού ταχυδρομείου που χρησιμοποιεί. Ο έλεγχος επιτυγχάνεται μέσω της αναζήτησης συγκεκριμένων ύποπτων χαρακτηριστικών (heuristics), για υπογραφές (signatures), θεματικών λέξεων-κλειδιών, επισυναπτόμενων αρχείων, εξακριβωμένων προγραμμάτων αποστολής κ.ά.

Χρήση λογισμικού προστασίας από ιους (antivirus). Πάντα ελλοχεύει ο κίνδυνος οι spammers να αποκτήσουν τον έλεγχο των συσκευών που χρησιμοποιεί ο χρήστης για την διασύνδεση του με το διαδίκτυο και να τις χρησιμοποιήσουν για να στέλνουν μηνύματα spam εν αγνοία του. Γι’ αυτό κρίνεται απαραίτητη η εγκατάσταση λογισμικού προστασίας από ιούς (antivirus) στον υπολογιστή του χρήστη ή στις έξυπνες συσκευές που χρησιμοποιεί. Το λογισμικό προστασίας (antivirus) δύναται να προστατεύσει τον εκάστοτε χρήστη σε πραγματικό χρόνο (real time protection), ελέγχοντας άμεσα οποιοδήποτε ενέργεια ή αρχείο χρησιμοποιήσει ο χρήστης.

Αριθμός κινητού τηλεφώνου. Για την ελαχιστοποιήσει των spam μηνυμάτων σε κινητά τηλέφωνα, συστήνεται, ο χρήστης να είναι ιδιαίτερα προσεκτικός και να μην αποκαλύπτει τον αριθμό του κινητού τηλεφώνου του σε άτομα ή υπηρεσίες και οργανισμούς που δεν γνωρίζει και εμπιστεύεται πλήρως.

Επιπροσθέτως, προτείνεται η αποφυγή προώθησης και απάντησης με οποιοδήποτε τρόπο (sms, mms ή και φωνητική κλήση), μηνυμάτων που προέρχονται από άγνωστους αριθμούς, καθώς ενδέχεται να υπάρχουν ανεπιθύμητες ή και υψηλές χρεώσεις.

1.4.3.3. Ασφαλής χρήση του διαδικτύου: Συμβουλές για παιδιά

Το διαδίκτυο προσφέρει απεριόριστες ευκαιρίες διασκέδασης και μεγάλες δυνατότητες επιμόρφωσης και εκπαίδευσης στα παιδιά. Στη νέα εποχή που διέρχονται οι Τεχνολογίες Πληροφορικής και Επικοινωνιών, τα παιδιά έρχονται σε «επαφή» με το διαδίκτυο μέσω υπολογιστών και έξυπνων συσκευών σε όλο και μικρότερες ηλικίες.

Το γεγονός αυτό έρχεται να το επιβεβαιώσει και η έρευνα που υλοποιήθηκε από τη Δίωξη Ηλεκτρονικού Εγκλήματος σε συνεργασία με το Υπουργείο Παιδείας στα πλαίσια του 4ο Συνεδρίου Ασφαλούς Πλοήγησης. Στην έρευνα συμμετείχαν 524 παιδιά, στην πλειοψηφία τους κορίτσια, ηλικίας 10-14 ετών και τα αποτελέσματά της είναι πολλά και ενδιαφέροντα. Σύμφωνα με τα αποτελέσματα της έρευνας, το 50% των παιδιών έχει την πρώτη του «επαφή» με το διαδίκτυο σε ηλικία μικρότερη των 8 ετών, ενώ το 84,5% διατηρεί λογαριασμό σε κάποιο δίκτυο κοινωνικής δικτύωσης. Η ίδια έρευνα αποκάλυψε ότι το σύνολο των παιδιών χρησιμοποιούν το διαδίκτυο καθημερινά για τουλάχιστον μία με δύο ώρες, αλλά και ότι η διαδικτυακή περιήγηση κρύβει παγίδες. Συγκεκριμένα, το 18% των παιδιών που συμμετείχαν στην έρευνα απάντησαν ότι έχουν νιώσει απειλή ή κίνδυνο ή φόβο και το 31,9% ότι έχουν δεχτεί ύβρεις ή απειλές. Αναμφισβήτητα, η χρήση του διαδικτύου αποτελεί αναπόσπαστο κομμάτι της καθημερινότητας στην σημερινή εποχή[13].

Γίνεται ολοφάνερο πως προτού αφήσουν οι γονείς ελεύθερα τα παιδιά τους να πλοηγηθούν στα «μονοπάτια του διαδικτύου» και να έρθουν αντιμέτωπα με την «κοινωνία της πληροφορίας», χρειάζεται να κατέχουν οι ίδιοι σχετική παιδεία, σωστή ενημέρωση αλλά και ορθή εκπαίδευση, ώστε να είναι σε θέση να την μεταδόσουν με την σειρά τους στα παιδιά. Κάποιες χρήσιμες και απλές συμβουλές ασφαλούς πλοήγησης στο διαδίκτυο τόσο για τα παιδιά όσο και για τους γονείς τους, περιγράφονται περιεκτικά παρακάτω:

Παιδιά ως 10 ετών. Σε αυτή την μικρή ηλικία είναι άκρως σημαντική η ενεργή συμμετοχή των γονιών κατά τη διάρκεια χρήσης του διαδικτύου από τα παιδιά. Απαιτείται έλεγχος και εποπτεία από την πλευρά των ενηλίκων, ώστε θα εμποδίσουν τα παιδιά τους να εκτεθούν σε ακατάλληλο και επικίνδυνο για την ηλικία τους υλικό. Η εφαρμογή κατάλληλων φίλτρων και λογισμικών προστασίας στις συσκευές

πρόσβασης στο διαδίκτυο θα δώσουν την δυνατότητα στους γονείς να απαγορεύσουν την πλοήγηση σε ιστοσελίδες με ακατάλληλο περιεχόμενο και δραστηριότητες[14].

Παιδιά 11-14 ετών. Σε αυτή την ηλικία η χρήση του διαδικτύου είναι πλέον γνωστή. Τα παιδιά, έχοντας αποκτήσει περισσότερες γνώσεις για τη χρήση και την πλοήγηση στο διαδίκτυο, αφιερώνουν περισσότερο χρόνο συνήθως παίζοντας παιχνίδια και συνομιλώντας με τους διαδικτυακούς τους φίλους. Παρόλα αυτά, ο κίνδυνος έκθεσής τους σε ακατάλληλο υλικό παραμένει και ακόμα και σε αυτή την ηλικία απαιτείται επιτήρηση και έλεγχος από την πλευρά των γονιών. Εκτός από την προστασία που προσφέρουν τα κατάλληλα φίλτρα και λογισμικά προστασίας, υπάρχει και η δυνατότητα αναφοράς και ενημέρωσης των γονιών σχετικά με τη «διαδικτυακή συμπεριφορά» των παιδιών τους. Σε αυτή την ηλικία, οι γονείς θα πρέπει να εξηγήσουν λεπτομερειακώς τις επιπτώσεις που μπορεί να έχουν οι ενέργειες των παιδιών στο διαδίκτυο και κυρίως να τα εκπαιδεύσουν να μην γνωστοποιούν προσωπικές τους πληροφορίες στο διαδίκτυο ανεξέλεγκτα[14].

Έφηβοι 15-18 ετών. Πλέον, οι περιορισμοί στο περιεχόμενο, στις ιστοσελίδες και στις δραστηριότητες αίρονται. Οι έφηβοι γνωρίζουν πλέον καλά τις δυνατότητες που τους δίνονται μέσω διαδικτύου. Αυτό όμως δεν σημαίνει ότι δεν χρειάζονται την καθοδήγηση των γονιών τους, ώστε να τους ορίζουν κατάλληλες οδηγίες ασφαλείας, να τους βοηθήσουν να αποφύγουν επικίνδυνες καταστάσεις και να τους υπενθυμίζουν πως δεν πρέπει να γνωστοποιούν προσωπικές πληροφορίες στο διαδίκτυο[14].

Συστάσεις. Ένα από τα βασικότερα μέτρα που πρέπει να λάβουν οι γονείς είναι να μην επιτρέπεται η χρήση των συσκευών πρόσβασης στο διαδίκτυο σε υπνοδωμάτια και γενικά σε χώρους όπου το παιδί μπορεί εύκολα να απομονωθεί και να λειτουργεί χωρίς επίβλεψη. Η χρήση των συσκευών αυτών θα πρέπει να επιτρέπεται σε χώρους όπως είναι το σαλόνι ή η κουζίνα, δηλαδή σε χώρους όπου η γονική επίβλεψη είναι εφικτή, χωρίς ταυτόχρονα να δίνεται η εντύπωση στο παιδί ότι ελέγχεται από τους γονείς του.

Ένα μέτρο που θα πρέπει να επιβάλουν οι γονείς είναι ο αυστηρός χρονικός περιορισμός που σπαταλάει ένα παιδί μπροστά στην οθόνη. Οι σχολικές δραστηριότητες, τα προσωπικά ενδιαφέροντα και οι φίλοι (όχι οι «διαδικτυακοί» φίλοι)

του παιδιού δεν πρέπει να παραμεληθούν εξαιτίας της ενασχόλησής του με το διαδίκτυο.

Επιπλέον, απαιτείται έλεγχος του οπτικοακουστικού υλικού που κατέχει το παιδί. Κάτι τέτοιο μπορεί εύκολα να επιτευχθεί, αν οι γονείς αφιερώσουν χρόνο και πλοηγηθούν στο διαδίκτυο μαζί με το παιδί. Με τον τρόπο αυτό, οι γονείς πετυχαίνουν δύο βασικά πράγματα. Από τη μία, επιτρέπουν τη βελτίωση του ψηφιακού αλφαβητισμού και την ανάπτυξη δεξιοτήτων ασφαλούς πλοήγησης στο διαδίκτυο του παιδιού και από την άλλη πετυχαίνουν έναν έμμεσο έλεγχο του υλικού που διαχειρίζεται το ίδιο. Επιπροσθέτως, τα παιδιά θα πρέπει να αισθάνονται άνετα και να μην ντρέπονται να συζητούν με τους γονείς τους για όλα όσα βλέπουν και «ζουν» κατά την πλοήγησή τους στο διαδίκτυο. Θα πρέπει να γνωρίζουν ότι σε περίπτωση που αισθανθούν οποιαδήποτε μορφή απειλής στο διαδίκτυο (επικοινωνία με επικίνδυνα άτομα, πρόσβαση σε ιστότοπους με βλαβερό περιεχόμενο), θα πρέπει να ενημερώσουν άμεσα τους γονείς τους, χωρίς να φοβούνται ότι θα τιμωρηθούν για αυτό. Αυτό θα βοηθήσει το παιδί να αναπτύξει την κριτική του διάθεση σε ό,τι διαβάζει στο διαδίκτυο και να μην εμπιστεύεσαι αμέσως ό,τι δει σε αυτό.

Εκτός από την πολύ στενή σχέση με το παιδί, οι γονείς θα πρέπει να μην αμελούν την καθημερινή, αυτόματη ανανέωση του λογισμικού προστασίας απέναντι σε ιούς και άλλους κινδύνους κατά την πλοήγηση στο διαδίκτυο. Επίσης, ο έλεγχος πρόσβασης σε ιστοσελίδες μέσω ειδικού λογισμικού (parental control) θα πρέπει και αυτός να γίνεται σε καθημερινή βάση. Τέλος, για την προστασία από πιθανή εισβολή κακόβουλων προγραμμάτων και «τρίτων» στις συσκευές πρόσβασης στο διαδίκτυο χρειάζεται η ενεργοποίηση του τείχους προστασίας (personal firewall). Η διαχείριση και ο έλεγχος των προγραμμάτων ασφαλείας θα πρέπει να επιτρέπεται μόνο από τους γονείς και όχι από τα παιδιά.

Ένα ακόμα μέτρο ασφαλείας που θα πρέπει να επιβληθεί είναι η χρήση διαφορετικών κωδικών πρόσβασης για την είσοδο σε διαφορετικούς ιστότοπους και υπηρεσίες. Οι κωδικοί αυτοί θα πρέπει να είναι αυστηρά προσωπικοί, να αλλάζουν υποχρεωτικά και τακτικά και να είναι αρκετά ισχυροί (χρήση συγκεκριμένου αριθμού – τουλάχιστον 8 – αλφαριθμητικών), ενώ καλή πρακτική είναι και η αποφυγή χρήσης

τους για πρόσβαση μέσω δημόσιων και ανοιχτών ασύρματων δικτύων (free-WiFi, internet cafe, ξενοδοχεία, κ.λπ).

Τα παιδιά θα πρέπει να είναι ενημερωμένα για όλους τους κινδύνους που κρύβει η πλοήγηση στο διαδίκτυο. Πρέπει να γνωρίζουν και να δίνουν μεγάλη προσοχή όταν τους ζητούνται να γνωστοποιήσουν προσωπικά στοιχεία όπως ονοματεπώνυμο, διεύθυνση, τηλέφωνο, σχολείο, επάγγελμα γονιών, οικογενειακή κατάσταση, αριθμός πιστωτικής κάρτας, ονόματα φίλων από άγνωστα άτομα. Το ίδιο ισχύει και για τις «διαδικτυακές» συνομιλίες (chatrooms). Επίσης, θα πρέπει να αποφεύγουν συναντήσεις με άγνωστους του διαδικτύου. Σε περίπτωση συνάντησης, αυτή πρέπει να γίνεται πάντα σε δημόσιο χώρο και με την συνοδεία του γονέα ή ενός έμπιστου ενήλικα. Επίσης, πρέπει τα παιδιά να μάθουν να αρνούνται από μόνα τους τις προσωπικές συναντήσεις με άτομα που έχουν γνωρίσει στο διαδίκτυο. Πρέπει να γίνει κατανοητό ότι οι άγνωστοι με τους οποίους θέλουν να συναντηθούν μπορεί να είναι επικίνδυνοι.

Τα παιδιά θα πρέπει να εκπαιδευτούν σχετικά με τις ειδοποιήσεις που αφορούν σε ιστοσελίδες με την χαρακτηριστική ένδειξη «άνω των 18 ετών». Οι ενδείξεις αυτού του είδους είναι για να προστατεύσουν τα παιδιά. Η πλοήγηση σε ιστοσελίδες με επιμορφωτικό, ψυχαγωγικό και ενημερωτικό περιεχόμενο, ανάλογα με την ηλικία και τα ενδιαφέροντά τους, είναι προτιμότερη, ακίνδυνη και πιο εποικοδομητική.

Είναι σημαντικό τα παιδιά να μάθουν ότι δεν ανοίγονται συνημμένα αρχεία και περιεχόμενοι σύνδεσμοι που βρίσκονται σε μηνύματα ηλεκτρονικού ταχυδρομείου άγνωστου προς αυτά αποστολέα. Στην περίπτωση λήψης μηνυμάτων με προσβλητικό περιεχόμενο θα πρέπει να αποφεύγεται η απάντηση και απαιτείται η άμεση ενημέρωση των γονιών ή άλλου έμπιστου ατόμου. Η εγκατάσταση ενός συστήματος φιλτραρίσματος της ηλεκτρονικής αλληλογραφίας αποτελεί μια πολύ αποτελεσματική πρακτική, ώστε κάθε φορά να γίνεται λήψη μόνο της επιθυμητής αλληλογραφίας[15].

Μεγάλη πληγή της σύγχρονης εποχής αποτελούν οι υπηρεσίες κοινωνικής δικτύωσης. Τα παιδιά θα πρέπει να γνωρίζουν τους κινδύνους που κρύβονται εκεί και να μάθουν να προστατεύονται. Και σε αυτή την περίπτωση, οι κωδικοί πρόσβασης στους λογαριασμούς (προφίλ) που διατηρούν στις υπηρεσίες κοινωνικής δικτύωσης δε θα πρέπει να αποκαλύπτονται σε κανέναν, ενώ οι κανόνες δημιουργίας τους θα πρέπει

να είναι το ίδιο αυστηροί, όπως αναφέρθηκε και παραπάνω. Πρέπει τα παιδιά να κατανοήσουν ότι σε περίπτωση που κάποιος τρίτος καταφέρει να μάθει τους προσωπικούς τους κωδικούς για τους λογαριασμούς αυτούς, τότε αυτομάτως μπορεί να διαχειριστεί όλα τα προσωπικά δεδομένα που έχουν αναρτήσει. Μια πολύ καλή πρακτική είναι, αμέσως μετά τη δημιουργία του προφίλ, να γίνει και αλλαγή των προεπιλεγμένων ρυθμίσεων, και κυρίως των ρυθμίσεων για την διαχείριση των προσωπικών δεδομένων.

Επίσης, είναι σωστό τα παιδιά να επιλέξουν τα δεδομένα που φαίνονται στο προφίλ τους να είναι προσβάσιμα μόνο στους «δικτυακούς τους φίλους» και όχι δημόσια προσβάσιμα σε όλους. Από τη στιγμή που κάποιο άτομο προστίθεται στη λίστα των φίλων (αποδοχή friend request), το άτομο αυτό αποκτά πρόσβαση στα προσωπικά δεδομένα που εμφανίζονται στο προφίλ του ατόμου που αποδέχτηκε το αίτημα φιλίας. Τέλος, προκειμένου να αποφευχθεί η δυνατότητα φυσικού εντοπισμού, θα πρέπει τα παιδιά να μην αναρτούν πληροφορίες ή φωτογραφίες όπου φαίνεται καθαρά η τοποθεσία στην οποία βρίσκονται.

Τέλος, είναι απαραίτητο τα παιδιά να καταλάβουν ότι οι πληροφορίες και οι φωτογραφίες που αναρτούν στις υπηρεσίες κοινωνικής δικτύωσης είναι ευρέως προσπελάσιμες. Συνεπώς, καλό θα ήταν να μην παρέχουν κάτι που πιθανών θα τα φέρει σε δύσκολη θέση. Ακόμα και στην περίπτωση διαγραφής του λογαριασμού (προφίλ) ή διαγραφής σχολίων ή φωτογραφιών, πολλές πληροφορίες δεν αφαιρούνται και ελλοχεύει ο κίνδυνος να χρησιμοποιηθούν για κακόβουλο σκοπό στο μέλλον[15].

Συνεχής επίβλεψη και προστασία θα πρέπει να γίνεται και στο κινητό. Καλό θα είναι να αποφεύγεται ο δανεισμός του σε τρίτους, εκτός αν είναι κάτι απολύτως αναγκαίο. Επιπροσθέτως, ιδιαίτερη προσοχή απαιτείται και κατά την γνωστοποίηση του αριθμού κινητού τηλεφώνου. Ποτέ σε αγνώστους, γιατί υπάρχει ο κίνδυνος λήψης ανεπιθύμητων κλήσεων και μηνυμάτων (SMS, MMS). Τέτοιου είδους μηνύματα δεν απαντώνται και διαγράφονται.

1.4.3.4. Δικαιώματα και αρχές κατά την πρόσβαση σε διαδικτυακές υπηρεσίες

Ένα από τα βασικότερα και θεμελιώδη δικαιώματα του ατόμου είναι η προστασία των προσωπικών του δεδομένων, δικαίωμα το οποίο κατοχυρώνεται στη Συνθήκη της Λισαβόνας. Στον Χάρτη των Θεμελιωδών Δικαιωμάτων, μεταξύ άλλων, ορίζονται τα εξής:

- *«Κάθε πρόσωπο έχει δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν. Η επεξεργασία αυτών των δεδομένων πρέπει να γίνεται νομίμως, για καθορισμένους σκοπούς και με βάση τη συγκατάθεση του ενδιαφερόμενου ή για άλλους θεμιτούς λόγους που προβλέπονται από το νόμο. Κάθε πρόσωπο δικαιούται να έχει πρόσβαση στα συλλεγέντα δεδομένα που το αφορούν και να επιτυγχάνει τη διόρθωσή τους».*
- *«Κάθε φυσικό πρόσωπο έχει δικαίωμα στην επαρκή προστασία των προσωπικών δεδομένων που το αφορούν».*
- *«Η επεξεργασία των προσωπικών δεδομένων πρέπει να είναι απαραίτητη, δίκαιη, νόμιμη και αναλογική. Τα δεδομένα που παρέχονται άμεσα ή έμμεσα από φυσικά πρόσωπα δεν πρέπει να χρησιμοποιούνται για σκοπούς άλλους από αυτούς που προβλέπονταν αρχικά. Δεν δύναται επίσης τα δεδομένα αυτά να περιέλθουν αδιακρίτως σε νομικά πρόσωπα με τα οποία το φυσικό πρόσωπο δεν έχει επιλέξει να εμπλακεί. Τα εν λόγω δικαιώματα ισχύουν για όλους, ανεξαρτήτως εθνικότητας ή τόπου κατοικίας. Δεδομένα προσωπικού χαρακτήρα που δηλώνουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, τη συμμετοχή σε συνδικαλιστικές οργανώσεις, καθώς και η επεξεργασία δεδομένων που αναφέρονται στην υγεία και τη σεξουαλική ζωή επιτρέπονται μόνο με τη ρητή συγκατάθεση του φυσικού προσώπου, εφόσον αυτό επιτρέπεται από την εθνική νομοθεσία»**[16]**.*

Το άτομο έχει το δικαίωμα να λαμβάνει πληροφορίες από άλλα φυσικά πρόσωπα ή και εταιρείες που διατηρούν ορισμένα από τα προσωπικά δεδομένα του στο αρχείο τους, όπως δικτυακοί τόποι, βάσεις δεδομένων, πάροχοι υπηρεσιών κ.λπ.

(«υπεύθυνοι επεξεργασίας δεδομένων»). Το άτομο έχει το δικαίωμα να διορθώσει ή να διαγράψει τα δεδομένα αυτά, αν είναι ελλιπή ή ανακριβή:

- *Οι υπεύθυνοι επεξεργασίας δεδομένων οφείλουν να ενημερώνουν το άτομο για τη συλλογή προσωπικών δεδομένων που το αφορούν.*
- *Το άτομο πρέπει και είναι δικαίωμά του να γνωρίζει το όνομα του υπεύθυνου επεξεργασίας, τον προβλεπόμενο τρόπο χρήσης και επεξεργασίας των δεδομένων του, καθώς και τα τρίτα πρόσωπα τα οποία ενδεχομένως να λάβουν γνώση των δεδομένων του.*
- *Το άτομο δικαιούται να ρωτήσει τον υπεύθυνο επεξεργασίας δεδομένων εάν επεξεργάζεται προσωπικά δεδομένα που το αφορούν.*
- *Το άτομο δικαιούται να λάβει αντίγραφο των δεδομένων που το αφορούν σε όσο το δυνατόν πιο κατανοητή για το ίδιο μορφή.*
- *Η διαγραφή, ο αποκλεισμός και η απαλοιφή των δεδομένων, αν αυτά είναι ελλιπή, ανακριβή ή έχουν ληφθεί παράνομα, είναι δικαίωμα του ατόμου που αφορούν τα δεδομένα αυτά.*
- *Η εναντίωση του ατόμου στην επεξεργασία των προσωπικών δεδομένων που το αφορούν είναι δικαίωμά του*[16].

Το άτομο δικαιούται να μη συμμορφωθεί με απόφαση που παράγει νομικά αποτελέσματα έναντι αυτού ή το θίγει σημαντικά, στην περίπτωση που η εν λόγω απόφαση βασίζεται αποκλειστικά και μόνο σε αυτοματοποιημένη επεξεργασία των δεδομένων του που αξιολογεί ορισμένες πτυχές της προσωπικότητάς του, όπως η απόδοσή του στην εργασία, η φερεγγυότητα, η αξιοπιστία, η διαγωγή του κ.λπ..

Τα δικαιώματα αυτά ισχύουν και στο επιγραμμικό (on-line) περιβάλλον, όπου το άτομο δικαιούται επιπλέον:

- *Να έχει πλήρη ενημέρωση και τη δυνατότητα παροχής της συγκατάθεσή του, όταν ένας δικτυακός τόπος αποθηκεύει και συλλέγει πληροφορίες από τον τερματικό εξοπλισμό του ή επιθυμεί να τον παρακολουθεί κατά την πλοήγηση στο διαδίκτυο·*
- *Όλες οι επιγραμμικές επικοινωνίες του, όπως μηνύματα ηλεκτρονικού ταχυδρομείου, πρέπει να είναι διέπονται από όρους εμπιστευτικότητας.*

- *Να λαμβάνει πλήρη ενημέρωση, σε περίπτωση παραβίασης των προσωπικών δεδομένων του που διατηρούνται στα συστήματα του παρόχου υπηρεσιών διαδικτύου του (χαθούν, κλαπούν ή που ενδέχεται να επηρεαστεί αρνητικά η ιδιωτικότητά τους).*
- *Να λαμβάνει αυτόκλητες εμπορικές ανακοινώσεις, γνωστές ως «spam», μόνο εφόσον υπάρχει ρητά προηγούμενη συγκατάθεσή του για αυτή την ενέργεια*[16].

1.4.3.5. Αρμόδιες υπηρεσίες

Όλες αυτές οι απειλές που αναλύθηκαν στις προηγούμενες ενότητες καθιστούν την ανάγκη προστασίας των προσωπικών δεδομένων του ατόμου επιτακτική και αναγκαία. Οι χρήστες, προκειμένου να είναι σε θέση να απολαμβάνουν, να επωφελούνται και να ευεργετούνται από το σύνολο των υπηρεσιών που τους προσφέρει η συνεχώς αναπτυσσόμενη και ραγδαία εξελισσόμενη κοινωνία της πληροφορίας, θα πρέπει να αισθάνονται ασφαλής και σίγουροι για αυτές. Δεδομένου ότι οι χρήστες του διαδικτύου δεν διαθέτουν όλοι το ίδιο εκπαιδευτικό και μορφωτικό επίπεδο, ώστε να είναι σε θέση να προφυλάσσουν τους εαυτούς τους από τις αμέτρητες απειλές του διαδικτύου, γίνεται αμέσως αντιληπτό ότι δεν αρκεί μόνο η ενημέρωση και η διαρκής επαγρύπνησή τους. Μέχρι ένα βαθμό, αυτό βοηθάει και έχει πολύ καλά αποτελέσματα. Όμως, η τεράστια πρόοδος στον τομέα της πληροφορικής, η ανάπτυξη νέων τεχνολογιών, οι νέες μορφές διαφήμισης και ηλεκτρονικών συναλλαγών και η ανάγκη της ηλεκτρονικής οργάνωσης του κράτους έχουν σαν συνέπεια την αυξημένη ζήτηση, αποθήκευση και επεξεργασία προσωπικών πληροφοριών από τον ιδιωτικό και δημόσιο τομέα. Και εδώ γεννιέται η αμφιβολία και ο φόβος των χρηστών: Ποιος έχει τα προσωπικά τους δεδομένα; Πώς αυτά χρησιμοποιούνται; Πόσο σίγουροι είναι ότι τα δεδομένα αυτά προφυλάσσονται και δεν κινδυνεύουν να πέσουν σε χέρια κακόβουλων;

Στην εποχή λοιπόν της «ψηφιοποίησης», η κοινωνία καλείται να προστατεύσει και να θωρακίσει τους πολίτες και τις δομές της. Για τον σκοπό αυτό, στην Ελλάδα ιδρύθηκε με τον Νόμο 2472/1997 η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα ως ανεξάρτητος διοικητικός φορέας, ενώ το 2014 ιδρύθηκε η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος. Αντίστοιχα, σε ευρωπαϊκό επίπεδο το 2004

ιδρύθηκε ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων, ρόλος του οποίου είναι να διασφαλίζει ότι κατά την επεξεργασία προσωπικών δεδομένων, τα όργανα και οι οργανισμοί της Ευρωπαϊκής Ένωσης σέβονται το δικαίωμα των πολιτών για προστασία της ιδιωτικής ζωής.

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα είναι συνταγματικά κατοχυρωμένη ανεξάρτητη Αρχή και έχει ως αποστολή της την εποπτεία της εφαρμογής του ν. 2472/1997 και άλλων ρυθμίσεων που αφορούν στην προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και την ενάσκηση των αρμοδιοτήτων που της ανατίθενται κάθε φορά. Εξυπηρετείται από δική της Γραμματεία που λειτουργεί σε επίπεδο Διεύθυνσης και έχει δικό της προϋπολογισμό.

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, σύμφωνα με το άρθρο 19 του ν. 2472/1997, ασκεί μια σειρά αρμοδιοτήτων, οι οποίες μπορούν να διακριθούν σε δύο μεγάλες κατηγορίες, τις ρυθμιστικές εν ευρεία έννοια και τις ελεγκτικές.

Η Αρχή, σύμφωνα με την παρ. 1 του άρθρου 20 του ιδρυτικού της νόμου 2472/1997, εξυπηρετείται από Γραμματεία, η οποία λειτουργεί σε επίπεδο Διεύθυνσης, και αποτελείται από τρία τμήματα: το Τμήμα Ελεγκτών, το Τμήμα Επικοινωνίας και το Τμήμα Διοικητικών και Οικονομικών Υποθέσεων[17].

Από την ίδρυσή της, η Αρχή έχει επεξεργαστεί και αναπτύξει σπουδαίο ενημερωτικό και συμβουλευτικό υλικό σχετικά με θέματα προστασίας προσωπικών δεδομένων στο διαδίκτυο, τα οποία βρίσκονται αναρτημένα στην ιστοσελίδα της. Μεγάλο κομμάτι αυτού του υλικού απευθύνεται κυρίως σε ανήλικους μαθητές Γυμνασίου και Λυκείου και στους καθηγητές τους. Το υλικό αυτό είναι δομημένο σε τέσσερις εκπαιδευτικές ενότητες, οι οποίες αναλύονται ως εξής: α) «Μαθαίνω για τα προσωπικά μου δεδομένα». Η πρώτη ενότητα περιλαμβάνει γενική ενημέρωση για την προστασία της ιδιωτικότητας και τα δικαιώματα των πολιτών, δίνοντας ιδιαίτερη έμφαση στα ψηφιακά ίχνη και την παρακολούθηση στο Διαδίκτυο.

β) «Σκέφτομαι πριν δημοσιεύσω». Η δεύτερη ενότητα στοχεύει στην ευαισθητοποίηση των μαθητών σχετικά με τη δημοσίευση προσωπικών δεδομένων

δικών τους ή άλλων (π.χ. φωτογραφιών ή βίντεο) στο διαδίκτυο, ιδίως κατά τη χρήση ηλεκτρονικών fora, ιστολογίων (blogs), ηλεκτρονικών χώρων συζητήσεων (chat), κλπ.

γ) «Γνωρίζω με ποιον μιλώ». Η τρίτη ενότητα προβάλλει ιδιαίτερα το ζήτημα της πλαστοπροσωπίας στο Διαδίκτυο, όπως π.χ. κατά τη συμμετοχή σε ηλεκτρονικές ομάδες συζητήσεων ή διαδικτυακά παιχνίδια.

δ) «Δικτυώνομαι» με ασφάλεια». Η τέταρτη ενότητα εστιάζει στην προστασία προσωπικών δεδομένων κατά τη χρήση υπηρεσιών κοινωνικής δικτύωσης. Επιπλέον, σε όλες τις ενότητες, εκτός του ενημερωτικού κειμένου, υπάρχουν διαθέσιμα τεστ γνώσεων και σχετικά βίντεο που αποσκοπούν στην περαιτέρω ευαισθητοποίηση γύρω από τα διάφορα θέματα προστασίας προσωπικών δεδομένων. Τέλος, στο διαδικτυακό τόπο της Αρχής έχει αναρτηθεί ένα τεστ αυτο-αξιολόγησης και ενημέρωσης σχετικά με την υποκλοπή ταυτότητας, το οποίο απευθύνεται σε όλες τις ηλικιακές ομάδες. Το τεστ αυτό υποδεικνύει τρόπους με τους οποίους μπορεί κάποιος να μειώσει τους κινδύνους υποκλοπής της ταυτότητάς του[1]. Περισσότερες πληροφορίες για την προστασία των προσωπικών δεδομένων μπορεί να αναζητήσει κανείς στο διαδικτυακό τόπο της Αρχής: http://www.dpa.gr[17].

Αναφορικά με την αζήτητη – ανεπιθύμητη αλληλογραφία (spam), η Αρχή έχει υιοθετήσει από το 2010 συγκεκριμένη πολιτική αντιμετώπισης των καταγγελιών που αφορούν σε αυτού του είδους τα μηνύματα ηλεκτρονικού ταχυδρομείου. Σύμφωνα με την πολιτική αυτή, αρχικά αποστέλλεται σύσταση στον υπεύθυνο επεξεργασίας προσωπικών δεδομένων για τον οποίο υπάρχει καταγγελία ότι αποστέλει αζήτητη ηλεκτρονική επικοινωνία. Η σύσταση συνοδεύεται από το ενημερωτικό έντυπο για τη νόμιμη προώθηση προϊόντων και υπηρεσιών και το spam, το οποίο αφορά, στην τρέχουσα μορφή του, κυρίως την πραγματοποίηση διαφημιστικών ενεργειών μέσω ηλ. ταχυδρομείου. Σε περίπτωση μη συμμόρφωσης του υπεύθυνου επεξεργασίας (π.χ. σε περίπτωση νέας καταγγελίας για τον ίδιο υπεύθυνο επεξεργασίας μετά την πάροδο ενός ευλόγου χρονικού διαστήματος), η Αρχή προχωρά σε αναλυτικότερη εξέταση. Επισημαίνουμε ότι, σύμφωνα με τη διάταξη του άρθρου 19 παρ. 1 ιγ' του ν. 2472/97, η προτεραιότητα εξέτασης των καταγγελιών εκτιμάται από την Αρχή με κριτήριο τη σπουδαιότητα και το γενικότερο ενδιαφέρον του θέματος[12].

Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος. Με το Π.Δ. 178/2014 προβλέφθηκε η ίδρυση και η διάρθρωση της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος με έδρα την Αθήνα και η ίδρυση και διάρθρωση Υποδιεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος με έδρα τη Θεσσαλονίκη.

Αποστολή της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος είναι η πρόληψη, η έρευνα και η καταστολή εγκλημάτων ή αντικοινωνικών συμπεριφορών, που διαπράττονται μέσω του διαδικτύου ή άλλων μέσων ηλεκτρονικής επικοινωνίας. Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος είναι αυτοτελής κεντρική Υπηρεσία και υπάγεται απευθείας στον κ. Αρχηγό της Ελληνικής Αστυνομίας.

Στην εσωτερική της δομή αποτελείται από πέντε τμήματα που συμπληρώνουν όλο το φάσμα προστασίας του χρήστη και ασφάλειας του Κυβερνοχώρου. Αποτελείται από το Τμήμα Διοικητικής Υποστήριξης και Διαχείρισης Πληροφοριών, το Τμήμα Καινοτόμων Δράσεων και Στρατηγικής, το Τμήμα Ασφάλειας Ηλεκτρονικών και Τηλεφωνικών Επικοινωνιών και Προστασίας Λογισμικού και Πνευματικών Δικαιωμάτων, το Τμήμα Διαδικτυακής Προστασίας Ανηλίκων και Ψηφιακής Διερεύνησης και το Τμήμα Ειδικών Υποθέσεων και Δίωξης Διαδικτυακών Οικονομικών Εγκλημάτων. Η δράση της περιλαμβάνει μόνο εκείνες τις συμπεριφορές που έχουν αξιόποινο χαρακτήρα και εξετάζονται από τις Δικαστικές Αρχές, ενώ κατά τη διάρκεια προκαταρκτικής εξέτασης ή προανάκρισης παύει να ισχύει το φορολογικό, τραπεζικό, χρηματιστηριακό ή επιχειρηματικό απόρρητο[18].

Η Διεύθυνση έχει πρόσβαση στα αρχεία οποιασδήποτε αστυνομικής υπηρεσίας, καθώς και σε αρχεία άλλων υπηρεσιών, αρχών, οργανισμών και φορέων, ενώ ανταλλάσσει πληροφοριακά και άλλα στοιχεία με υπηρεσίες του Υπουργείου Οικονομικών, τα οποία είναι αναγκαία για την εφαρμογή της φορολογικής και τελωνειακής νομοθεσίας. Επίσης, προκειμένου να φέρει εις πέρας την εκτέλεση του καθήκοντος και της αποστολής της, συνεργάζεται με όλες τις αρμόδιες υπηρεσίες και φορείς. Τέλος, χρησιμοποιεί ειδικό λογισμικό για την ανάλυση εγκληματολογικών πληροφοριών, τη λεπτομερή μελέτη και υποστήριξη της διερεύνησης σοβαρών υποθέσεων, καθώς και την στρατηγική ανάλυση για την εξέλιξη του οικονομικού και ηλεκτρονικού εγκλήματος στην Ελλάδα.

Ευρωπαίος Επόπτης Προστασίας Δεδομένων (ΕΕΠΔ). Πρόκειται για την ανεξάρτητη, Ευρωπαϊκή Αρχή Προστασίας Δεδομένων[19] (European Independent Data Protection Authority) και έχει την έδρα του στην πρωτεύουσα του Βελγίου, στις Βρυξέλλες. Ο ρόλος της Αρχής είναι να εποπτεύει την επεξεργασία προσωπικών δεδομένων που πραγματοποιούν οι υπηρεσίες της Ευρωπαϊκής Ένωσης, ώστε να διασφαλίζει τη συμμόρφωση με τους κανόνες περί προστασίας της ιδιωτικής ζωής, να συμβουλεύει τα όργανα και τους οργανισμούς της Ένωσης για όλα τα θέματα επεξεργασίας προσωπικών δεδομένων, των συναφών πολιτικών και της νομοθεσίας, να διεκπεραιώνει καταγγελίες και να διενεργεί ελέγχους, να συνεργάζεται με τις εθνικές αρχές των χωρών της Ένωσης με στόχο τη συνεπή προστασία των δεδομένων και να παρακολουθεί νέες τεχνολογίες που θα μπορούσαν να έχουν επιπτώσεις στην προστασία των δεδομένων.

Ο Ευρωπαίος Επόπτης διοικείται από τον Επόπτη και τον βοηθό Επόπτη, οι οποίοι διορίζονται για πέντε χρόνια, με δικαίωμα ανανέωσης θητείας. Απαρτίζεται από δύο κύρια τμήματα: το Τμήμα Εποπτείας και Επιβολής, το οποίο αξιολογεί την εφαρμογή των κανόνων προστασίας δεδομένων από τα όργανα και τους οργανισμούς της Ευρωπαϊκής Ένωσης και το Τμήμα Πολιτικής και Διαβούλευσης, το οποίο συμβουλεύει τους νομοθέτες της Ευρωπαϊκής Ένωσης για θέματα προστασίας δεδομένων, που άπτονται τομέων πολιτικής και νέων νομοθετικών προτάσεων[20].

Ο Ευρωπαίος πολίτης, που θεωρεί ότι το δικαίωμα της ιδιωτικής του ζωή έχει παραβιαστεί από όργανο ή οργανισμό της Ευρωπαϊκής Ένωσης, οφείλει πρώτα να ενημερώσει τα μέλη του προσωπικού της Ευρωπαϊκής Ένωσης (μέσω της υπηρεσίας του επίσημου καταλόγου της Ένωσης EU Whoiswho)[21], που είναι αρμόδια για την επεξεργασία των δεδομένων του στο όργανο ή τον οργανισμό όπου θεωρεί ότι διαπράχθηκε η παραβίαση. Αν το αποτέλεσμα για τον πολίτη δεν είναι ικανοποιητικό, αυτό που μπορεί να κάνει είναι να επικοινωνήσει με τον υπεύθυνο προστασίας δεδομένων του οργάνου της Ένωσης που κατά τη γνώμη του έχει διαπράξει την παραβίαση. Στην περίπτωση που και πάλι η ενέργεια αυτή δεν αποδώσει, τότε ο πολίτης έχει το δικαίωμα να υποβάλει καταγγελία στον ΕΕΔΠ, συμπληρώνοντας και αποστέλλοντας ηλεκτρονικά την αντίστοιχη φόρμα[22]. Ακολούθως, ο ΕΕΔΠ, αφού

ερευνήσει τα στοιχεία που αναφέρονται στην καταγγελία, γνωστοποιεί στον πολίτη την απόφασή του σχετικά με αυτή και για το πώς μπορεί να διορθωθεί η κατάσταση. Σε κάθε περίπτωση, αν και πάλι ο πολίτης έχει αντίρρηση ως προς την απόφαση του ΕΕΔΠ, μπορεί να παραπέμψει την υπόθεσή του στο Δικαστήριο της Ευρωπαϊκής Ένωσης.

2. ΕΠΙΣΤΗΜΟΝΙΚΗ ΕΡΕΥΝΑ ΚΑΙ ΤΡΟΠΟΙ ΔΙΕΞΑΓΩΓΗΣ ΕΡΕΥΝΩΝ

Εισαγωγή

Στο κεφάλαιο αυτό γίνεται μια σύντομη παρουσίαση των ειδών της επιστημονικής έρευνας. Καθορίζονται οι σκοποί της επιστημονικής έρευνας, διευκρινίζονται απλές στατιστικές έννοιες όπως ο πληθυσμός, το δείγμα, η μεταβλητή κ.α., τα τεχνικά θέματα της δειγματοληψίας και ο τρόπος καθορισμού μεγέθους δείγματος. Εκτενέστερα, εξετάζεται τόσο ο τρόπος διεξαγωγής της έρευνας, όσο και τα πλεονεκτήματα και μειονεκτήματα της δειγματοληπτικής έρευνας, της έρευνας πεδίου, των πειραματικών σχεδιασμών και των μη αντιδραστικών ερευνών.

Η χρήση της επιστημονικής έρευνας γενικά, αλλά και ειδικότερα στη στατιστική γίνεται πιο εύκολη και αποτελεσματική, εάν κάποιος ξέρει τα αίτια δημιουργίας του φαινομένου που εξετάζει, τι ανάγκες καλύπτει και πως αυτό λειτουργεί σε βάθος. Οι γνώσεις αυτές θα τον οδηγήσουν να προσδιορίσει ακριβέστερα τι θέλει να ανακαλύψει, αλλά και να σχεδιάσει ορθότερα την έρευνα που καλείται να διενεργήσει. Η επιστημονική έρευνα δεν είναι τίποτα παραπάνω από παρατήρηση και ερμηνεία των ορθών στοιχείων και πληροφοριών που απαιτούνται για να υλοποιηθεί ένα οποιοδήποτε σχέδιο. Για αυτό θα πρέπει κάθε φορά να συγκεκριμενοποιείται ακριβώς, τι πρόκειται να παρατηρηθεί και να αναλυθεί, το γιατί και το πώς.

Ο σχεδιασμός μιας έρευνας περιλαμβάνει τέσσερις βασικές παραμέτρους, αυτές είναι: οι βασικοί σκοποί της έρευνας, η λογική της έρευνας, οι μονάδες ανάλυσης τι ή ποιος θα μελετηθεί και οι εναλλακτικοί τρόποι διαχείρισης του χρόνου στην έρευνα (συγχρονικές και διαχρονικές μελέτες).

2.1. Επιστημονική έρευνα

Στην εποχή την οποία διανύουμε είναι γενικά αποδεκτό, ότι σε κάθε τομέα η επιστημονική έρευνα είναι αποτέλεσμα παρατηρήσεων.

Η εφαρμογή της επιστημονικής έρευνας στηρίζεται στο πείραμα, ή τον έλεγχο των όποιων παρατηρήσεων των ερευνητών, με αποτέλεσμα την δημιουργία μιας σειράς κριτηρίων για την επαλήθευση των υποθέσεών της. Οι συνηθέστεροι και χρησιμότεροι

σκοποί της επιστημονικής έρευνας, κατά τον Earl Babbie (2012), είναι οι εξής τρεις: η διερεύνηση, η περιγραφή και η ερμηνεία[23].

Διερεύνηση. Συνήθως, οι διερευνητικές εμπειρικές μελέτες διεξάγονται κάθε φορά που ένας ερευνητής έρχεται αντιμέτωπος με ένα καινούργιο θέμα. Οι τεχνικές που χρησιμοποιούνται για την διεξαγωγή των σχετικών ερευνών είναι οι συνεντεύξεις, οι συζητήσεις, ή οι καθοδηγούμενες συζητήσεις σε μικρές ομάδες κ.λπ.. Τεχνικές που συχνά χρησιμοποιούνται σε έρευνες αγοράς. Οι κύριοι λόγοι διεξαγωγής μιας τέτοιας έρευνας είναι η επιθυμία του ερευνητή για την καλύτερη κατανόηση ενός αντικειμένου ή θέματος και ο εντοπισμός της ορθής μεθόδου με σκοπό τη συγκέντρωση των κατάλληλων πληροφοριών για έρευνα. Μπορεί να πραγματοποιηθεί η διερευνητική έρευνα για να ελεγχθεί για παράδειγμα η δυνατότητα διεξαγωγής μιας εκτενέστερης μελέτης ή για να διαμορφωθούν οι κατάλληλες μέθοδοι που θα χρησιμοποιηθούν σε επόμενη μελέτη (π.χ. ένας ερευνητής, πάει σε μία περιοχή που μόλις έγινε μια φυσική καταστροφή για να εξετάσει τις συνθήκες διαβίωσης, τη σύνθεση πληθυσμού, κ.λπ.).

Το βασικό μειονέκτημα των διερευνητικών μελετών είναι ότι σε σπάνιες περιπτώσεις προσφέρουν έγκυρες και αξιόπιστες απαντήσεις σε ερευνητικά ερωτήματα και αυτό γιατί η δειγματοληψία που χρησιμοποιούν συνήθως είναι περιστασιακή. Μπορούν όμως να χρησιμοποιηθούν με σκοπό να επιλεγούν οι κατάλληλες ερευνητικές μέθοδοι που θα ήταν σε θέση να προσφέρουν οριστικές απαντήσεις καθώς επίσης και να υποδείξουν πιθανές απαντήσεις.

Περιγραφή. Στην περίπτωση αυτή σκοπός του ερευνητή είναι η περιγραφή και η καταγραφή όλων όσων παρατηρεί βασιζόμενος σε ακριβή δεδομένα, χωρίς όμως να εντοπίζει και χωρίς να αναλύει αιτιακές σχέσεις, γεγονός που αποτελεί και το κύριο μειονέκτημα των περιγραφικών μελετών. Συνήθως, είναι από τις πιο ακριβείς και έγκυρες έρευνες από όλα τα άλλα είδη ερευνών.

Ένα παράδειγμα περιγραφικής μελέτης είναι η απογραφή του πληθυσμού αλλά και των κτιρίων της Ελλάδας, που διενεργήθηκε από την Ελληνική Στατιστική Αρχή (ΕΛΣΤΑΤ) το 2011. Η μελέτη ξεκίνησε τον Φεβρουάριο και ολοκληρώθηκε τον Μάιο. Σκοπός της απογραφής ήταν η καταγραφή του «μόνιμου» πληθυσμού της Ελλάδας και

όχι του «πραγματικού», δηλαδή όλων όσων ζούσαν μόνιμα στην περιοχή τους το τελευταίο δωδεκάμηνο.

Ερμηνεία και αναζήτηση αιτιότητας. Σε αντίθεση με τα προηγούμενα είδη μελετών οι ερμηνευτικές μελέτες δεν καταγράφουν απλώς τα γεγονότα αλλά προχωρούν σε μια πιο έγκυρη και τεκμηριωμένη ερμηνεία αυτών. Για να γίνει κατανοητή η αντίθεση αυτή ενδεικτικά αναφέρεται ότι το ποσοστό πωλήσεων δύο προϊόντων είναι περιγραφική έρευνα, ενώ το γιατί υπερτερούν οι πωλήσεις του Α σε σχέση με αυτές του Β είναι ερμηνευτική.

Σκοπός των ερμηνευτικών μελετών είναι να αναζητηθούν τα αίτια των αποτελεσμάτων, των οποίων η αιτιατή σχέση εξηγείται είτε με τη νομοθετική εξήγηση (nomothetic explanation) είτε με την ιδιογραφική (idiographic explanation).

Με τη νομοθετική εξήγηση γίνεται μια προσπάθεια καταγραφής των ανεξάρτητων μεταβλητών που ερμηνεύουν ορισμένες αιτίες ενός φαινομένου. Αντίθετα με την ιδιογραφική εξήγηση εξετάζεται η πλήρη ερμηνεία των αιτίων ενός φαινομένου.

Η αιτιότητα στη νομοθετική εξήγηση δεν είναι ούτε πλήρης, ούτε αποκλειστική. Ως παράδειγμα, αναφέρεται η περίπτωση που εξετάζεται η αιτία πρόκλησης μιας αρρώστιας σε έναν ασθενή, π.χ. είναι ευρέως γνωστό ότι το κάπνισμα έχει σχέση με τον καρκίνο του πνεύμονα, αυτό όμως δεν συνεπάγεται, ότι το κάπνισμα είναι η αποκλειστική αιτία της εμφάνισης αυτής της ασθένειας σε έναν άνθρωπο ή ότι όποιος καπνίζει θα εμφανίσει καρκίνο στους πνεύμονες κάποια στιγμή στη ζωή του.

Ένα παράδειγμα ιδιογραφικής προσέγγισης είναι η οπαδική προτίμηση των παιδιών. Είναι γνωστό πως τα παιδιά επηρεάζονται άμεσα από την προτίμηση του πατέρα για το ποια ομάδα θα επιλέξουν να υποστηρίζουν. Μπορεί να παρατηρήσει κανείς πως το αίτιο (οπαδική προτίμηση πατέρα) προηγείται του αποτελέσματος (οπαδική προτίμηση παιδιού). Η σχέση αυτή μεταξύ αιτίας και αποτελέσματος είναι γνωστή ως αιτιολογική.

Στις αιτιολογικές σχέσεις είτε υπάρχει ανάλογη ή αντιστρόφως ανάλογη συσχέτιση μεταξύ των μεταβλητών είτε η συσχέτιση είναι απλά στατιστική και όχι αιτιολογική. Για να γίνει κατανοητό αναφέρεται σαν παράδειγμα το κάπνισμα. Το

κάπνισμα εκτός από τον καρκίνο του πνεύμονα συνδέεται και με τον κιτρινισμό των δοντιών από τη νικοτίνη. Γίνεται εύκολα αντιληπτή σε κάποιον η στατιστική συσχέτιση μεταξύ του κιτρινισμού των δοντιών με τον καρκίνο του πνεύμονα. Μια τέτοιου είδους συσχέτιση όμως δεν είναι αιτιολογική με αποτέλεσμα να παραλείπεται γιατί δεν έχει επιστημονικό ενδιαφέρον. Σε αρκετές περιπτώσεις λόγω λανθασμένης ερμηνείας της αιτιότητας προκύπτουν σφάλματα. Για παράδειγμα κάποιος οδηγός που απέκτησε τώρα το δίπλωμα του είναι πιθανότερο να προκαλέσει ατύχημα παραβιάζοντας τον κώδικα οδικής κυκλοφορίας (Κ.Ο.Κ.) π.χ. σε χρονικό διάστημα ενός έτους, από έναν πιο έμπειρο. Αυτό όμως δεν συνεπάγεται ότι η πλειοψηφία των νέων οδηγών υποπίπτει σε ανάλογες παραβάσεις.

Για την εξαγωγή αποτελεσμάτων υπάρχουν δυο ειδών συνθήκες που πρέπει να ισχύουν, η αναγκαία και η ικανή. Αναγκαία συνθήκη ονομάζεται η συνθήκη που απαιτείται για να προκύψει ένα συγκεκριμένο αποτέλεσμα ενώ ικανή καλείται η συνθήκη που υποχρεωτικά οδηγεί στο επιθυμητό αποτέλεσμα, π.χ. για να στεφθεί πρωταθλήτρια μια ομάδα στο μπάσκετ πρέπει να συμμετέχει στο σχετικό πρωτάθλημα (αναγκαία συνθήκη) αλλά και να έχει συγκεντρώσει τους περισσότερους βαθμούς στο τέλος του πρωταθλήματος από όλες τις υπόλοιπες ομάδες που συμμετέχουν σε αυτό (ικανή συνθήκη). Στην περίπτωση που μια συνθήκη θεωρείται ταυτόχρονα αναγκαία και ικανή είναι πολύ σημαντικό στοιχείο σε μια έρευνα. Το στοιχείο αυτό συνήθως συναντάται στα μαθηματικά και γενικότερα στις θετικές επιστήμες ενώ σπάνια παρουσιάζεται σε κοινωνικές έρευνες.

2.1.1. Λογική της έρευνας

Ο ερευνητής μέσω του παραγωγικού ή του επαγωγικού τρόπου προσέγγισης καλείται να προβάλει τη λογική μιας μελέτης.

Συγκεκριμένα, η παραγωγική προσέγγιση μιας μελέτης δίνει την δυνατότητα στον ερευνητή για μετάβαση από το «γενικό» στο «ειδικό» ενώ αντίθετα η επαγωγική προσέγγιση από το «ειδικό» προς το «γενικό». Πρακτικά αυτό σημαίνει ότι μελέτες στις οποίες εφαρμόζεται παραγωγική λογική εξετάζεται αρχικά η υπάρχουσα θεωρία πάνω στην οποία θα αναπτυχθούν οι προς έλεγχο ερευνητικές υποθέσεις, ενώ στις

μελέτες που εφαρμόζεται επαγωγική λογική η προσπάθεια επικεντρώνεται στην ένταξη εμπειρικών στοιχείων σε πλαίσια κάποιας θεωρίας.

Για παράδειγμα στην έρευνα για το κατά πόσο ένα φροντιστήριο είναι καλό για την προετοιμασία μαθητών σε εξετάσεις θα χρησιμοποιηθεί ο επαγωγικός τρόπος προσέγγισης. Δηλαδή, θα γίνει προσπάθεια να εξετασθεί αν λειτουργούν ολιγομελή τμήματα, αν υπάρχουν έμπειροι καθηγητές, αν διεξάγονται διαγωνίσματα κ.λπ., για να γίνει στο τέλος μια πρόβλεψη για το επίπεδο εκπαίδευσης που προσφέρει. Ενώ επαγωγική προσέγγιση θα ακολουθηθεί στην περίπτωση που ο σκοπός της έρευνας θα είναι να εξετάσει τις επιδόσεις των μαθητών από διάφορα φροντιστήρια και με βάση τα στοιχεία αυτά να συμπεράνει πιο φροντιστήριο είναι το καλύτερο από τα άλλα αφού σε αυτό υπήρχαν οι περισσότεροι επιτυχόντες μαθητές.

2.1.2. Μονάδες Ανάλυσης

Ως μονάδα ανάλυσης χαρακτηρίζεται κάθε μέλος – οντότητα μιας έρευνας. Οι μονάδες μπορεί να είναι άτομα, ομάδες (νοικοκυριά, κόμματα), οργανώσεις (επιχειρήσεις, νοσοκομεία), ανθρώπινα δημιουργήματα (βιβλία, πίνακες ζωγραφικής, τραγούδια κ.λπ.), ζώα, μέτρησες που επαναλαμβάνονται, (π.χ. θερμομετρική, σφυγμομετρική κ.λπ.), αλλά και σε ευρύτερη έρευνα γεωγραφικοί χώροι (π.χ. νησιά, λιμάνια, αεροδρόμια κ.ά.), επαγγελματικές δραστηριότητες.

Συνήθως, η αναγνώριση της μονάδας ανάλυσης γίνεται εύκολα. Υπάρχουν όμως περιπτώσεις όπου η μονάδα που δίνει την πληροφορία δεν είναι εύκολο να αναγνωριστεί με αποτέλεσμα κάποιες φορές να προκύπτουν λανθασμένα συμπεράσματα λόγω εσφαλμένης μονάδας. Έχει αποδειχθεί πως στην έρευνα για το επίπεδο της φτώχειας ενός πληθυσμού καλύτερη μονάδα ανάλυσης θεωρείται «ένα νοικοκυριό» από ότι τα «μεμονωμένα άτομα». Η λανθασμένη επιλογή μονάδων ανάλυσης ονομάζεται οικολογικό σφάλμα (ecological fallacy). Σφάλμα λόγω της χρησιμοποίησης λανθασμένων μονάδων ανάλυσης μπορεί επίσης να προκύψει και στον αναγωγισμό (reductionism) και καλείται αναγωγικό σφάλμα. Αναγωγισμός είναι η μέθοδος που προσεγγίζει ένα θέμα έρευνας μέσω της κατανόησης των επιμέρους μερών που το απαρτίζουν. Σε αυτή την περίπτωση η προσπάθεια άντλησης

συμπερασμάτων λαμβάνοντας υπόψη ένα μόνο παράγοντα, αυτόν που θεωρείται πιο σημαντικός, χωρίς να υπολογιστεί η πολυπλοκότητα του φαινομένου χρήζει ιδιαίτερης προσοχής και απαιτεί άλλο τρόπο προσέγγισης. Παράδειγμα αναγωγικού σφάλματος είναι αν προβλέψουμε ότι στο ποδόσφαιρο η Ρεάλ Μαδρίτης θα κατακτήσει το Champions League την επόμενη χρονιά απλά και μόνο επειδή είναι η ομάδα με το μεγαλύτερο προϋπολογισμό από όλες τις υπόλοιπες ομάδες που συμμετέχουν στο θεσμό.

2.1.3. Χρονική διάσταση των ερευνών

Από τους σημαντικότερους παράγοντες στη διεξαγωγή μια έρευνας είναι ο χρόνος. Επισημάνθηκε, στις ερμηνευτικές έρευνες, η σχέση μεταξύ αιτίας και αποτελέσματος. Η χρονική αλληλουχία των γεγονότων και των καταστάσεων είναι αυτή που καθορίζει τις αιτίες και τα αποτελέσματα. Όσον αφορά τον παράγοντα χρόνο οι έρευνες διαχωρίζονται σε συγχρονικές και διαχρονικές.

Όταν μια έρευνα βασίζεται σε παρατηρήσεις σε συγκεκριμένο πεδίο στο χρόνο και για συγκεκριμένη κατηγορία πληθυσμού τότε καλείται συγχρονική. Ως παραδείγματα θα μπορούσαν να αναφερθούν όλες οι δημοσκοπήσεις που αφορούν την πρόθεση ψήφου των κατοίκων μιας χώρας.

Στην περίπτωση που η έρευνα βασίζεται σε δεδομένα που αντλούνται σε διαφορετικά χρονικά διαστήματα τότε ονομάζεται διαχρονική. Οι διαχρονικές έρευνες ταξινομούνται στις ακόλουθες τρείς κατηγορίες: στις έρευνες τάσης (trend study), στις έρευνες κοόρτης (cohort study) και στις έρευνες πάνελ (panel study).

Έρευνα τάσης (trend study). Το συγκεκριμένο είδος έρευνας καταγράφει ένα χαρακτηριστικό δεδομένο μιας μονάδας ανάλυσης σε διάφορες χρονικές περιόδους. Παραδείγματα τέτοιας έρευνας είναι η έρευνες που διεξήχθησαν για την εξεύρεση του ποσοστού των αναλφάβητων στην Ελλάδα το 1920, 1940, 1960 και 1980.

Έρευνα κοόρτης (cohort study). Στην περίπτωση των ερευνών κοόρτης παρατηρούνται οι μεταβολές των μονάδων ανάλυσης (π.χ. αντιλήψεις, συνήθειες κ.λπ.) σε ένα συγκεκριμένο υπό-πληθυσμό σε διαφορετικές χρονικές στιγμές. Ένα

παράδειγμα είναι η έρευνα για την γνώμη των γεννηθέντων το 1975 ως προς το πολιτικό σύστημα της χώρας τους (π.χ. η αλλαγή του προσανατολισμού τους, (αριστερός, δεξιός κ.λπ.) ανάλογα με την ηλικία). Έτσι επιτυγχάνεται η καταγραφή του πολιτικού προσανατολισμού των γεννηθέντων το 1975 (π.χ. ανά δεκαετία) μετά το 1985.

Έρευνα πάνελ (panel study). Η έρευνα πάνελ εξάγει τα δεδομένα της από ένα συγκριμένο σύνολο μονάδων ανάλυσης ανά τακτά χρονικά διαστήματα. Ως παράδειγμα αναφέρεται η έρευνα για τις θρησκευτικές πεποιθήσεις των ίδιων ατόμων ανά πέντε χρόνια. Τα πιο τεκμηριωμένα και έγκυρα αποτελέσματα εξάγονται από έρευνες πάνελ. Η συγκεκριμένη κατηγορία διαχρονικής έρευνας μειονεκτεί όμως στο γεγονός ότι είναι δύσκολη η διατήρηση του ίδιου «πάνελ» (π.χ. ίδιο σύνολο ερωτηθέντων) με το πέρας του χρόνου. Οι συνηθέστερες απώλειες οφείλονται στην άρνηση των συμμετεχόντων να συνεχίσουν την έρευνα, στη φυσική φθορά – απώλεια των μονάδων ανάλυσης κ.λπ..

Επίσης, οι ερευνητές έχουν την δυνατότητα να μπορούν να οδηγηθούν σε αποτελέσματα κατά προσέγγιση για διαχρονικές διαδικασίες, ακόμα και στην περίπτωση που τα δεδομένα έχουν στην διάθεση τους είναι μόνο συγχρονικά. Συγκεκριμένα, θεωρούν διεργασίες που μεταβάλλονται με τη πάροδο του χρόνου, καταλήγουν σε λογικά συμπεράσματα και ζητούν από τις μονάδες ανάλυσης (π.χ. άτομα) να ανακαλέσουν παλαιότερες συμπεριφορές. Αυτές οι έρευνες χαρακτηρίζονται ως «κατά προσέγγιση διαχρονικές».

2.2. Δειγματοληψία

Δειγματοληψία στην έρευνα είναι η τεχνική της επιλογής ενός μέρους του πληθυσμού το οποίο ονομάζεται δείγμα.

Αν όλα τα μέλη ενός πληθυσμού ήταν, από όλες τις απόψεις, πανομοιότυπα δεν θα υπήρχε καμία ανάγκη για προσεκτικές δειγματοληπτικές διαδικασίες. Αυτό, βέβαια, συμβαίνει σπάνια.

Ένα δείγμα ατόμων από έναν πληθυσμό πρέπει να περιέχει ουσιαστικά τις ίδιες παραλλαγές που υπάρχουν στον πληθυσμό[23].

2.2.1. Βασικές έννοιες

Στις σύγχρονες έρευνες αρκετά συχνά γίνονται μετρήσεις σε ένα αντιπροσωπευτικό μόνο δείγμα του συνόλου. Συγκεκριμένα, όπου οι μονάδες ανάλυσης είναι άτομα, οι μετρήσεις σχετικών παραμέτρων για όλα τα άτομα του ερωτηθέντος συνόλου που συμμετέχει στην έρευνα αν αυτό είναι μεγάλο είναι αδύνατες ή πολύ δαπανηρές. Αυτό έχει σαν αποτέλεσμα να οδηγείται ο ερευνητής στη χρησιμοποίηση ενός αντιπροσωπευτικού δείγματος από το σύνολο του πληθυσμού. Δείγμα που στην περίπτωση που επιλεγεί σωστά, σύμφωνα με τους κανόνες που ισχύουν για την δειγματοληψία, μπορεί να χρησιμοποιηθεί για να γίνουν αναφορές στο σύνολο του πληθυσμού.

Χρήζει ιδιαίτερης αναφοράς η δημοσκόπηση για την πρόθεση ψήφου σε εκλογές που έγινε στις Ηνωμένες Πολιτείες Αμερικής (ΗΠΑ) το 1936 και κατέληξε σε λάθος συμπεράσματα. Ήταν μια από τις πρώτες δημοσκοπήσεις που πραγματοποιήθηκαν και το μέγεθος του δείγματος που χρησιμοποιήθηκε ήταν δυο εκατομμύρια τετρακόσιες χιλιάδες (2.400.000) ψηφοφόροι. Τα αποτελέσματα της έρευνας έδειξαν να προηγείται με μεγάλη διαφορά ο ρεπουμπλικάνος υποψήφιος Alf Landon. Μετά την ολοκλήρωση της εκλογικής διαδικασίας όμως, πρόεδρος των ΗΠΑ, με πολύ υψηλά ποσοστά ήταν ο δημοκρατικός υποψήφιος Franklin Roosevelt (τα ποσοστά ήταν 60,7% έναντι 39,3%). Η αποτυχία της δημοσκόπησης αυτής οφείλεται στο μέσω που χρησιμοποιήθηκε για να πραγματοποιηθεί. Έγινε μέσω του τηλεφώνου, μέσο επικοινωνίας που δεν ήταν ευρέως διαδεδομένο εκείνη την εποχή λόγω του υψηλού κόστους. Απόρροια της χρήσης του τηλεφώνου ήταν ότι το μεγαλύτερο μέρος του δείγματος ψηφοφόρων που έλαβαν μέρος στη δημοσκόπηση να είναι σχετικά ευκατάστατοι ψηφοφόροι και υποστήριζαν τον ρεπουμπλικάνο υποψήφιο. Όμως η μεγάλη πλειοψηφία των πολίτων των ΗΠΑ που είχε χαμηλά εισοδήματα και δεν μπορούσε να κάνει χρήση του τηλεφώνου, ψήφισε τον Roosevelt, τον υποψήφιο των δημοκρατικών.

Με την πάροδο του χρόνου στην στατιστική ανάλυση δεδομένων άρχισαν να χρησιμοποιούνται οι ηλεκτρονικοί υπολογιστές. Η ραγδαία εξέλιξη, όμως, που έχει

σημειωθεί στον χώρο των ηλεκτρονικών υπολογιστών, καθιέρωσε τη δειγματοληψία ως το απαραίτητο εργαλείο όλων των επιστημών.

Το σύνολο των μονάδων ανάλυσης που μελετώνται κατά την πραγματοποίηση της έρευνας ονομάζεται στατικός πληθυσμός. Θα μπορούσε να πει κανείς πως είναι το σύνολο των ατόμων ή αντικειμένων για τα οποία ενδιαφέρεται ο ερευνητής να βγάλει συμπεράσματα σε σχέση με κάποιες ιδιότητες που αφορούν τα στοιχεία του. Τα στοιχεία του πληθυσμού αναφέρονται πολλές φορές και ως υποκείμενα. Με «N» συμβολίζεται το πλήθος των παρατηρήσεων ή των μετρήσεων ή των μονάδων ανάλυσης (στοιχείων) του πληθυσμού και ονομάζεται μέγεθος του πληθυσμού. Ο πληθυσμός πρέπει να είναι καλά ορισμένος, έτσι ώστε κάθε στοιχείο να μπορεί να αποφασιστεί μονοσήμαντα αν είναι μέλος του.

Ανάλογα με τη φύση της έρευνας ο πληθυσμός διακρίνεται σε άπειρο και πεπερασμένο. Κατά την διεξαγωγή μιας έρευνας ο καθορισμός του πληθυσμού δεν είναι πάντοτε σαφής. Όταν ένας πληθυσμός είναι πρακτικά άπειρος ή μεταβάλλεται κατά την διάρκεια πραγματοποίησης της έρευνας, τότε μελετάτε κάποιο υποσύνολο του πληθυσμού, το οποίο ονομάζεται δείγμα. Με «n» συμβολίζεται το πλήθος των παρατηρήσεων ή των μετρήσεων ή των μονάδων ανάλυσης (στοιχείων) του δείγματος και ονομάζεται μέγεθος του δείγματος. Ανάλογα, λοιπόν, με το σκοπό της έρευνας επιλέγονται κάθε φορά οι κατάλληλες προς μελέτη μονάδες ανάλυσης του πληθυσμού, μέσω του δείγματος,. Η όλη διαδικασία ονομάζεται δειγματοληψία. Δειγματοληψία δηλαδή ονομάζουμε την τεχνική με την οποία γίνεται η επιλογή του δείγματος. Για την ορθή επιλογή των μονάδων ανάλυσης του δείγματος είναι απαραίτητο να κατανοηθεί η έννοια της μεταβλητής.

Με τον όρο μεταβλητή εννοούνται τα χαρακτηριστικά ή οι ιδιότητες των μονάδων ανάλυσης (πρόσωπο, αντικείμενο, κατάσταση κ.λπ.) τις οποίες σκοπεύει να καταμετρήσει ο ερευνητής για την έρευνα του. Εύκολα καταλαβαίνει κανείς πως υπάρχουν διαφορετικά είδη μεταβλητών ανάλογα με το δειγματοχώρο. Τα είδη των μεταβλητών διακρίνονται σε δύο βασικές κατηγορίες ανάλογα με τις τιμές που παίρνουν τις «Ποσοτικές μεταβλητές» και τις «Ποιοτικές μεταβλητές».

Ποσοτικές (quantitative). Στην κατηγορία αυτή ανήκουν οι μεταβλητές που μπορούν να μετρηθούν, που μπορούν να πάρουν δηλαδή αριθμητικές τιμές και εκφράζονται με μια μονάδα μέτρησης. Σ΄ αυτή την περίπτωση αντιστοιχούν δύο είδη μεταβλητών. Οι μεταβλητές που παίρνουν οποιαδήποτε τιμή σε ένα διάστημα πραγματικών τιμών, δηλαδή για κάθε δυο τιμές του διαστήματος υπάρχει άλλη μια τιμή ανάμεσά τους, και καλούνται συνεχείς (continuous) (π.χ. ύψος, ηλικία, βάρος, εισόδημα, κ.λπ.) και οι μεταβλητές που παίρνουν συγκεκριμένες τιμές, συνήθως ακέραιες, δηλαδή για κάθε δυο τιμές δεν υπάρχει πάντα μια τιμή της μεταβλητής ανάμεσά τους, και ονομάζονται διακριτές (discrete) (π.χ. αριθμός παιδιών οικογένειας, κ.λπ.).

Ποιοτικές (qualitative, categorical). Στην κατηγορία αυτή ανήκουν οι μεταβλητές που δεν μπορούν να μετρηθούν. Στην κατηγορία των μεταβλητών αυτών η αντιστοίχιση τιμών του δειγματικού χώρου με πραγματικούς αριθμούς είναι θέμα ορισμού και παραδοχής και δεν έχει καμία αριθμητική υπόσταση, παίρνουν δηλαδή τιμές που δεν έχουν αριθμητικές ιδιότητες. Για παράδειγμα στα δημογραφικά στοιχεία μιας δημοσκόπησης στο φύλο ενός ατόμου, μπορεί να γίνει η αντιστοίχιση «0» στον άντρα και «1» στη γυναίκα ή το ανάποδο. Σ΄ αυτή την περίπτωση αντιστοιχούν πάλι δύο είδη μεταβλητών. Στις μεταβλητές διάταξης (ordinal) και στις μη διατάξιμες που καλούνται και μεταβλητές κατηγορίας (nominal).

Διάταξης. Μεταβλητές που εμπεριέχουν την έννοια της διάταξης στις τιμές που παίρνουν, δηλαδή οι μεταβλητές που για το σύνολο τιμών τους μπορεί να οριστεί μια διάταξη, π.χ. σειρά κατάταξης σε ένα αγώνισμα, επίπεδο εκπαίδευσης, κλίμακα σεισμών RICHTER, η εξέλιξη μιας νόσου, κ.λπ..

Κατηγορίας. Ονομάζονται οι μεταβλητές που το σύνολο τιμών τους δεν έχει καμία ιδιότητα, π.χ. χρώμα ματιών, φύλο, τόπος γέννησης, πάσχοντες ή μη από μια νόσο, κ.λπ..

Γενικά θα μπορούσε να πει κανείς πως η επιλογή των στατιστικών τεχνικών εξαρτάται κατά κύριο λόγο από τον τύπο των μεταβλητών που εξετάζονται.

2.2.2. Καθορισμός μεγέθους δείγματος

Από την μελέτη του δείγματος εξάγονται τα συμπεράσματα για τον πληθυσμό. Το πλήθος των παρατηρήσεων που πρέπει να έχει ένα δείγμα αποτελεί έναν από τους σημαντικότερους παράγοντες σε μια δειγματοληπτική έρευνα. Είναι αυτονόητο ότι όσο μεγαλύτερο είναι το πλήθος του δείγματος τόσο μεγαλώνει και ο βαθμός εγκυρότητάς του με αποτέλεσμα τα συμπεράσματα της δειγματοληπτικής έρευνας να έχουν αυξημένο βαθμό αξιοπιστίας. Το κυριότερο μέτρο, όμως, της εγκυρότητας ενός δείγματος δεν είναι ωστόσο το μέγεθος του αλλά η αντιπροσωπευτικότητά του που πηγάζει από την σωστή επιλογή της μεθόδου. Το δείγμα που επιλέγεται πρέπει να είναι αντιπροσωπευτικό, δηλαδή πρέπει να είναι τυχαίο και να μην υπάρχει μεροληψία στην επιλογή των υποκειμένων του πληθυσμού.

Η διασπορά των παρατηρήσεων του πληθυσμού είναι αυτή που παίζει τον πρωτεύοντα ρόλο για τον καθορισμό μεγέθους του δείγματος. Για παράδειγμα στην περίπτωση μιας έρευνας που θέλει να κάνει εκτίμηση του μέσου μισθού των καθηγητών της δευτεροβάθμιας εκπαίδευσης στην Ελλάδα, θα πρέπει να θεωρηθεί ως πληθυσμός το σύνολο των καθηγητών της δευτεροβάθμιας εκπαίδευσης στα δημόσια σχολεία. Η μισθολογική διακύμανση των καθηγητών ανάλογα με τα χρόνια προϋπηρεσίας τους δεν είναι πολύ μεγάλη, κατά συνέπεια η διασπορά δεν είναι εξίσου πολύ μεγάλη και γι' αυτό και το μέγεθος του δείγματος μπορεί να είναι σχετικά μικρό. Αν όμως το ζητούμενο της έρευνας είναι να εκτιμήσει τον μέσο μισθό των πτυχιούχων μηχανικών στην Ελλάδα, η μισθολογική διακύμανση είναι πολύ μεγαλύτερη από πριν και κατά συνέπεια η διασπορά είναι μεγαλύτερη οπότε και το μέγεθος πρέπει να είναι πολύ μεγαλύτερο. Στην ακραία περίπτωση που η διασπορά είναι μηδέν αρκεί μία μόνο παρατήρηση (μια μόνο μονάδα ανάλυσης), προκειμένου να εκτιμηθεί ο μέσος μισθός π.χ. των πρωτοετών αστυνομικής σχολής.

2.2.3. Τα είδη δειγματοληψίας

2.2.3.1. Μη πιθανοτική δειγματοληψία

Μη πιθανοτική δειγματοληψία ονομάζεται η διαδικασία που ακολουθείται για την εξαγωγή δείγματος χωρίς να βασίζεται σε τεχνικές που χρησιμοποιούν οι νόμοι των πιθανοτήτων. Αυτό το είδος δειγματοληψίας συνήθως, χρησιμοποιείται σε πιλοτικές έρευνες και όχι σε έρευνες επιστημονικού κύρους. Κατά κανόνα στις μη πιθανοτικές δειγματοληψίες εφαρμόζονται τέσσερις διαφορετικές μέθοδοι δειγματοληψίας: η «Δειγματοληψία ευκαιρίας», η «Δειγματοληψία κρίσεως ή σκόπιμη δειγματοληψία», η «Δειγματοληψία της χιονοστιβάδας» και η «Ποσοτική δειγματοληψία».

Δειγματοληψία ευκαιρίας (convenience sampling). Με την εφαρμογή της μεθόδου αυτής γίνεται προσπάθεια συλλογής όσο το δυνατό μεγαλύτερου δείγματος. Ο ερευνητής στην περίπτωση αυτή συγκεντρώνει όλες τις παρατηρήσεις στις οποίες έχει εύκολη πρόσβαση. Ένα παράδειγμα ευκαιριακής δειγματοληψίας είναι όταν ένας ερευνητής διεξάγει ερεύνα για να καταγράψει την ικανοποίηση των πελατών ενός καταστήματος μοιράζοντας ερωτηματολόγια στους πελάτες που βρίσκονται στο κατάστημα μια μόνο συγκεκριμένη ημέρα. Ένα άλλο παράδειγμα είναι τα ρεπορτάζ των τηλεοπτικών καναλιών που διερευνούν την άποψη του κόσμου για τις τιμές των προϊόντων σε ένα μεγάλο εμπορικό κέντρο, π.χ. στην οδό Ερμού. Είναι προφανές ότι ο τρόπος αυτός συλλογής δείγματος δεν έχει επιστημονική εγκυρότητα γιατί δεν αντιπροσωπεύει επαρκώς τον πληθυσμό. Γίνεται κατανοητό ότι η χρήση της ευκαιριακής δειγματοληψίας γίνεται κυρίως για πιλοτικές έρευνες και όχι για την εξαγωγή συμπερασμάτων.

Δειγματοληψία κρίσεως ή σκόπιμη δειγματοληψία (judgement sampling). Η μέθοδός αυτή έχει πολλά κοινά με την δειγματοληψία ευκαιρίας. Η μόνη διαφορά τους είναι ότι ο ερευνητής κάνει επιλεκτική συλλογή των μονάδων ανάλυσης με σκοπό να κάνει πιο αντιπροσωπευτικό το δείγμα του. Αν στο προηγούμενο παράδειγμα της ευκαιριακής δειγματοληψίας για την ικανοποίηση των πελατών ο ερευνητής μοιράσει επιλεκτικά το ερωτηματολόγιο της έρευνας του (π.χ. έχοντας δώσει τα τρία πρώτα ερωτηματολόγια σε γυναίκες, δίνει το τέταρτο σε άνδρα, γιατί έτσι πιστεύει ότι κάνει

το δείγμα του πιο αντιπροσωπευτικό), τότε η μέθοδος πλέον καλείται δειγματοληψία κρίσεως. Όπως σε όλες τις μεθόδους μη πιθανοτικής δειγματοληψίας έτσι και η δειγματοληψία κρίσεως στερείται επιστημονικής εγκυρότητας και δεν χρησιμοποιείται για επιστημονικές δημοσιεύσεις παρά μόνο για πιλοτικές έρευνες.

Δειγματοληψία χιονοστιβάδας (snowball sampling). Είναι η μέθοδος μη πιθανοτικής δειγματοληψίας κατά την οποία ο ερωτώμενος που συμμετέχει στην έρευνα καλείται να βρει και να υποδείξει άλλους συμμετέχοντες σε αυτήν. Παρά το γεγονός ότι η όλη διαδικασία φαντάζει αρκετά ιδιότροπη, η μέθοδος αυτή δειγματοληψίας χρησιμοποιείται και σε επιστημονικές έρευνες. Οι λόγοι που επιλέγεται η χρήση της συγκεκριμένης μεθόδου είναι γιατί σε πολλές περιπτώσεις είναι δύσκολο να βρεθούν οι μονάδες ανάλυσης, ενώ άλλες φορές είναι δύσκολο να καταγραφεί ο πληθυσμός ώστε να υπάρχει δειγματοληπτικό πλαίσιο και να μπορεί να πραγματοποιηθεί η επιθυμητή δειγματοληψία. Παράδειγμα δειγματοληψίας στοιβάδας θεωρείται η προσπάθεια ενός ερευνητή να διεξάγει έρευνα για θέματα που σχετίζονται με τους λαθρομετανάστες. Η δυνατότητα πρόσβασης του ερευνητή σε αυτούς τους ανθρώπους είναι αρκετά περιορισμένη. Μπορεί όμως να διευκολυνθεί σημαντικά από την ύπαρξη ενός λαθρομετανάστη, οποίος θα ενδιαφέρεται να βοηθήσει για την διεξαγωγή της έρευνας ερχόμενος σε επαφή με ανθρώπους που γνωρίζει (άλλους λαθρομετανάστες) και να τους παροτρύνει να συμμετέχουν στην συγκεκριμένη έρευνα.

Ποσοτική δειγματοληψία (quota sampling). Αρκετά συχνά γίνεται σύγχυση μεταξύ των μεθόδων της μη πιθανοτικής ποσοτικής δειγματοληψίας και των αντίστοιχων μεθόδων της πιθανοτικής δειγματοληψίας. Στην περίπτωση της μη πιθανοτικής ποσοτικής δειγματοληπτικής μεθόδου ο ερευνητής διαμορφώνει το ερευνητικό του δείγμα εξασφαλίζοντας συγκεκριμένα ποσοστά σε κάποιες παραμέτρους που κατά την κρίση είναι οι σημαντικότεροι. Έστω ότι ένας ερευνητής θέλει να βρει το δείγμα που θα στηριχθεί για την υλοποίηση έρευνας που σχετίζεται με τους φοιτητές του τμήματος Αυτοματισμού του ΑΤΕΙ Πειραιά. Από τα στοιχεία της γραμματείας της σχολής γνωρίζει ότι το ποσοστό των φοιτητριών είναι 35% και των φοιτητών 65%. Επίσης από τα στοιχεία της γραμματείας συνάγεται ότι το 18% είναι

πρωτοετείς, το 16% δευτεροετείς, το 15% τεταρτοετείς και το υπόλοιπο 36% είναι φοιτητές επί πτυχίο.

Φύλο			
Έτος	**Άνδρες**	**Γυναίκες**	**Σύνολο**
Πρωτοετείς	65%*18% = 11,7%	6,3%	18%
Δευτεροετείς	10,40%	5,6%	16%
Τριτοετείς	9,75%	5,25%	15%
Τεταρτοετείς	9,75%	5,25%	15%
Επί πτυχίο	23,4%	12,6%	36%
Σύνολο	65%	35%	100%

Πίνακας 1. Ποσοστά ανά κατηγορία

Έστω ότι το δείγμα θα το αποτελούν 1000 φοιτητές τότε προκύπτουν τα παρακάτω αποτελέσματα (Πίνακας 2.) ανά κατηγορία.

Φύλο			
Έτος	**Άνδρες**	**Γυναίκες**	**Σύνολο**
Πρωτοετείς	117	63	180
Δευτεροετείς	104	56	160
Τριτοετείς	97,5	52,5	150
Τεταρτοετείς	97,5	52,5	150
Επί πτυχίο	234	126	360
Σύνολο	650	350	1000

Πίνακας 2. Συχνότητες ανά κατηγορία

Η συγκεκριμένη μέθοδος δειγματοληψίας σε αρκετές περιπτώσεις μπορεί να δώσει αντιπροσωπευτικά δείγματα. Στερείται όμως εγκυρότητας, λόγω του γεγονότος ότι ο τρόπος εξεύρεσης του δείγματος από τον ερευνητή, στηρίζεται σε περιορισμένο αριθμό παραγόντων (ενός, δύο ή τριών) που εκείνος αυθαίρετα θεωρεί ότι είναι και οι πιο σημαντικοί. Στην πραγματικότητα όμως, ο ερευνητής δεν μπορεί να είναι απόλυτα σίγουρος για το κατά πόσο σημαντικοί είναι οι παράγοντες που χρησιμοποιεί. Στο προαναφερθέν παράδειγμα με τους φοιτητές αν ο σκοπός της έρευνας ήταν να κάνει εκτίμηση του εισοδήματος των φοιτητών οι παράγοντες φύλο και έτος μπορεί να μην είναι οι πιο σημαντικοί. Για την έρευνα αυτή μπορεί να χρειάζεται να χρησιμοποιηθούν άλλοι παράγοντες, όπως ο τόπος προέλευσης των φοιτητών, αν είναι από αστικό κέντρο ή από επαρχία, αν μπορούν να παρακολουθήσουν τα μαθήματα ή όχι γιατί π.χ. αναγκάζονται να εργαστούν, αν διαμένουν στην φοιτητική εστία ή όχι.

2.2.3.2. Πιθανοτική δειγματοληψία

Πιθανοτική δειγματοληψία είναι η επιλογή αντιπροσωπευτικών δειγμάτων από μεγάλους γνωστούς πληθυσμούς. Πρόκειται για τον γενικό όρο των δειγμάτων που επιλέγονται σύμφωνα με τη θεωρία των πιθανοτήτων. Χρησιμοποιείται συχνά σε έρευνες μεγάλης κλίμακας.

Στις πιθανοτικές δειγματοληψίες εφαρμόζονται πέντε διαφορετικές μέθοδοι δειγματοληψίας: η «Απλή τυχαία δειγματοληψία», η «Συστηματική δειγματοληψία», η «Στρωματοποιημένη δειγματοληψία», η «Δειγματοληψία κατά συστάδες» και η «Διπλή δειγματοληψία».

Απλή τυχαία δειγματοληψία (simple random sampling). Σε αυτή τη μέθοδο δειγματοληψίας εκλέγεται ένα τυχαίο δείγμα χωρίς επανάθεση από ένα πληθυσμό ορισμένου πλήθους μονάδων ανάλυσης. Ο ερευνητής στην τυχαία δειγματοληψία δεν επιλέγει στην τύχη όποιους εκείνος θέλει από τον πληθυσμό των μονάδων ανάλυσης. Στην περίπτωση αυτή η τυχαία επιλογή των ατόμων διασφαλίζεται είτε μέσω κάλπης είτε με χρήση τυχαίων αριθμών.

Ο όρος επανάθεση εξασφαλίζει την διαφορετικότητα μεταξύ των πειραματικών μονάδων του δείγματος. Σε ένα πληθυσμό «Ν» μελών, το πλήθος των δειγμάτων («n» στοιχείων το καθένα), υπολογίζεται με βάση την σχέση: $\frac{N}{n} = \frac{N!}{n!*(N-n)!}$

Συστηματική δειγματοληψία (systematic sampling). Στη συστηματική δειγματοληψία αριθμούνται όλα τα μέλη του πληθυσμού. Σε αυτή την περίπτωση, σε ένα πληθυσμό «Ν» μονάδων ανάλυσης το πλήθος του δείγματος «n» εξάγεται ως εξής:

Υπολογίζεται πρώτα το πηλίκο $k = \frac{N}{n}$

Από το πηλίκο k παίρνουμε το ακέραιο μέρος του οπότε έχουμε $\lambda = [k]$

Μετά τον υπολογισμό του λ επιλέγεται τυχαίος αριθμός ρ μεταξύ του 1 και του λ. Τα n μέλη του δείγματος θα έχουνε τους εξής αύξοντες αριθμούς στο πλαίσιό τους ρ, ρ+λ, ρ+2λ, …, ρ+(n-1)λ.

Πολύ εύκολά εφαρμόζεται η διαδικασία αυτή σε περιπτώσεις που οι πειραματικές μονάδες είναι είδη αριθμημένες π.χ. ιατρικοί φάκελοι νοσοκομείου. Στην διαδικασία αυτή αν η αρίθμηση εμπεριέχει και μια περιοδικότητα στα δεδομένα τότε μπορεί να προκύψει λάθος. Αν για παράδειγμα τα δεδομένα αναφέρονται σε φύλλα εφημερίδων και με το βήμα να είναι λ=30 τότε θα προκύπτουν φύλλα εφημερίδων με ίδιες ημερομηνίες κάθε μήνα (π.χ. 20/5 – 20/6 – 20/7 κ.λπ.).

Στρωματοποιημένη δειγματοληψία (stratified sampling). Με την χρήση της μεθόδου της στρωματοποιημένης δειγματοληψίας ο πληθυσμός διαιρείται σε «στρώματα (strata)» και στη συνέχεια εξάγονται δείγματα από κάθε ένα «στρώμα» κάνοντας χρήση της μεθόδου της απλής τυχαίας δειγματοληψίας. Σε περιπτώσεις ανομοιομορφίας των μονάδων ανάλυσης του πληθυσμού η διαδικασία που ακολουθείται στη μέθοδο αυτή έχει πολύ καλή εφαρμογή. Τα «στρώματα» καθορίζονται με βάση το μέγεθος της διασπορά στο εσωτερικό τους. Το επιθυμητό είναι μέσα στα «στρώματα» να υπάρχει όσο αυτό είναι εφικτό η μικρότερη διασπορά ενώ αντιθέτως, ανάμεσα στα «στρώματα» όσο γίνεται μεγαλύτερη. Τα δείγματα που προκύπτουν από την μέθοδο της στρωματοποιημένης δειγματοληψίας μπορεί να είναι είτε αναλογικά (ο αριθμός των μονάδων ανάλυσης που επιλέγονται να είναι ανάλογος του μεγέθους του δείγματος) είτε μη αναλογικά.

Δειγματοληψία κατά συστάδες (cluster sampling). Στη μέθοδο δειγματοληψίας κατά συστάδες η διαδικασία που ακολουθείται είναι πρώτα να διαιρείται ο πληθυσμός σε «συστάδες (clusters)», με την κάθε μια από αυτές να αντιπροσωπεύει ένα νέο πληθυσμό. Στην συνέχεια εφαρμόζοντας την μέθοδο της απλής τυχαίας δειγματοληψίας χωρίς επανάθεση εξάγεται δείγμα από τις «συστάδες» και τέλος πραγματοποιείται η απογραφή των «συστάδων». Με μια πρώτη ματιά θα μπορούσε να πει κανείς πως η μέθοδος δειγματοληψίας κατά συστάδες μοιάζει αρκετά με την στρωματοποιημένη δειγματοληψία. Παρόλα αυτά όμως, κατά την εφαρμογή τους οι διαφορές τους είναι αρκετά διακριτές. Πιο συγκεκριμένα για να έχει την μεγαλύτερη δυνατή αποτελεσματικότητα η δειγματοληψία συστάδων θα πρέπει η διασπορά μέσα στις «συστάδες» να είναι όσο το δυνατό μεγαλύτερη ενώ μεταξύ των «συστάδων» η διασπορά να είναι όσο το δυνατό μικρότερη, πράγμα που έρχεται σε πλήρη αντίθεση με ότι ισχύει στη στρωματοποιημένη δειγματοληψία.

Διπλή δειγματοληψία (double sampling). Στον τομέα κυρίως της βιομηχανικής παραγωγής είναι απαραίτητη η διαδικασία στατιστικού ελέγχου ποιότητας και αξιοπιστίας προϊόντων (quality control). Υπάρχει λοιπόν η δυνατότητα χρησιμοποίησης δύο δειγμάτων από τον ίδιο πληθυσμό, στην προκειμένη περίπτωση την ίδια παρτίδα, για να ληφθεί απόφαση για την αποδοχή ή τη μη αποδοχή της. Εδώ πρέπει να επισημανθεί πως πολλές φορές κατά την διαδικασία αυτή του ελέγχου ενός δείγματος επέρχεται και η καταστροφή του προϊόντος. Για παράδειγμα στην περίπτωση ελέγχου της παραγωγής σοκολάτας ως προς την γεύση το πρώτο δείγμα που παράγεται είναι και η πρώτη παρτίδα του προϊόντος. Συνεπώς ανάλογα με τα αποτελέσματα που θα προκύψουν, εξάγονται και τα συμπεράσματα για τα υπόλοιπα παραγόμενα προϊόντα[23].

2.3. Τα είδη ερευνών

2.3.1 Έρευνα πεδίου

Η έρευνα πεδίου αφορά στην άμεση παρατήρηση των κοινωνικών φαινομένων στο φυσικό τους περιβάλλον. Είναι το είδος έρευνας που παρέχει στον ερευνητή την

δυνατότητα να παρατηρεί το αντικείμενο έρευνας στο περιβάλλον που συντελείται. Συνήθως γίνεται καταγραφή των παρατηρήσεων και μια ολοκληρωμένη γνώμη για το προς μελέτη αντικείμενο χωρίς να περιλαμβάνεται ποσοτική ανάλυση. Έρευνες τέτοιου τύπου έχουν συνήθως διερευνητικό σκοπό, χωρίς να αποκλείεται ο σκοπός τους να είναι και περιγραφικός ή ερμηνευτικός.

Ζητήματα κατάλληλα για έρευνα πεδίου είναι κυρίως ζητήματα και διαδικασίες που δεν ποσοτικοποιούνται εύκολα, όπως έχει ήδη αναφερθεί, αλλάζουν με την πάροδο του χρόνου ή μπορούν να μελετηθούν καλύτερα στο φυσικό τους περιβάλλον. Στην συνέχεια ακολουθούν κάποια ενδεικτικά παραδείγματα ζητημάτων που θα μπορούσε να εφαρμοστεί η έρευνα πεδίου.

Μελέτη της απήχησης που έχει στον κόσμο η εμφάνιση ενός νέου πολιτικού προσώπου. Ο ερευνητής θα πρέπει να καταγράψει των παλμό, την απήχηση, τα συνθήματα και γενικά τα χαρακτηριστικά του κόσμου που θα συμμετέχει στις κεντρικές ομιλίες του πολιτικού.

Δημοσιογραφική κάλυψη των επιπτώσεων ενός συμβάντος, π.χ. ενός σεισμού. Εδώ ο ερευνητής καλείται να παρατηρήσει και να καταγράψει τις αντιδράσεις των πληγέντων πολίτων (σεισμόπληκτων) που κοιμούνται σε σκηνές, που περιμένουν να πάρουν φαγητό συσσίτια, κ.λπ..

Μελέτη των σχέσεων μεταξύ συνεργαζόμενων ατόμων, π.χ. των υπαλλήλων μιας εταιρείας. Για να υλοποιηθεί μια τέτοιου είδους έρευνα κρίνεται απαραίτητη η ύπαρξη παρατηρητή από μέσα. Θα πρέπει δηλαδή ο ερευνητής, να μπει στην εταιρεία, να ζήσει την ατμόσφαιρα στους χώρους εργασίας και να καταγράψει το κλίμα συνεργασίας μεταξύ των υπαλλήλων. Στην περίπτωση αυτή θα μπορούσε η έρευνα να αφορά και την διερεύνηση των συνθηκών εργασίας που επικρατούν στην εταιρεία. Πληροφορίες για αυτό τον σκοπό της έρευνας θα μπορούσαν να εξαχθούν μέσω της χρήσης στοχευμένων ερωτηματολογίων που θα μοιράζονταν στους εργαζόμενους. Είναι προτιμότερο όμως ο ερευνητής να βρεθεί ο ίδιος κοντά στους εργαζόμενους για να παρακολουθήσει τις συνθήκες εργασίας αλλά και τις πρακτικές της εταιρείας από κοντά.

Μελέτη της ζωής ανθρώπων πετυχημένων στον επαγγελματικό τους χώρο, οι οποίοι κατέχουν μια καλή θέση στην κοινωνία και έχουν ξεκινήσει από χαμηλά. Σε ορισμένους από αυτούς η ανέλιξη τους ήταν δύσκολη και έγινε με πολύ κόπο ενώ σε κάποιους άλλους ήταν όλα πιο εύκολα γιατί ήταν απλά πολύ τυχεροί. Ο σκοπός της μελέτης θα μπορούσε να ήταν ο εντοπισμός τυχόν αλλαγών στον χαρακτήρα τους και στη συμπεριφορά τους. Για να επιτευχθεί όμως αυτή η έρευνα πρέπει ο ερευνητής να βρεθεί κοντά όχι μόνο σε αυτούς τους ανθρώπους αλλά και σε έναν μικρό κύκλο ανθρώπων που τους γνωρίζουν καλά από παλιά για να μπορέσει να αντλήσει πληροφορίες και να βγάλει συμπεράσματα.

2.3.1.1. Οι ρόλοι του ερευνητή

Στην έρευνα πεδίου εξ' ορισμού απαιτείται η άμεση παρατήρηση των αντικειμένων έρευνας στο φυσικό τους περιβάλλον, γεγονός που επιβάλει στον εκάστοτε ερευνητή να βρίσκεται κοντά στα προς παρατήρηση αντικείμενα έρευνας υποδυόμενος πάντα έναν «ρόλο». Οι τρεις «ρόλοι» που καλείται να υποδυθεί ο ερευνητής είναι του «Συμμετέχων», του «Παρατηρητή» και του «Συμμετέχων – Παρατηρητή».

Συμμετέχων. Ως συμμετέχων ο ερευνητής δρα ο ίδιος στο πεδίο που ερευνά, προσπαθώντας πάντα να μην γίνει αντιληπτός από τα υποκείμενα της έρευνάς του. Φυσικά, εξυπακούεται πως στην περίπτωση αυτή ο ερευνητής πρέπει να έχει ένα υπόβαθρο γνώσεων σχετικά με το αντικείμενο που καλείται να μελετήσει, γιατί σε διαφορετική περίπτωση κινδυνεύει να γίνει αντιληπτός. Το βασικότερο μειονέκτημα του «ρόλου» αυτού είναι ότι ο ερευνητής συμμετέχει στο πεδίο που ερευνά με αποτέλεσμα να μπορεί να το επηρεάσει. Επιρροή πάνω στο πεδίο έρευνας μπορεί να ασκηθεί από τον ερευνητή όχι μόνο από την απλή παρουσία του, αλλά και από το γεγονός ότι θα εκφράσει την γνώμη του πάνω σε διάφορα θέματα, αλλά και από τις αποφάσεις που θα κληθεί να πάρει για τις επόμενες δράσεις των ατόμων που συμμετέχουν στο πεδίο της έρευνας, επηρεαζόμενος από το υπόλοιπο περιβάλλον. Επίσης μειονέκτημα αποτελεί και το γεγονός ότι μπορεί να επηρεαστεί και ο ίδιος από

τα γεγονότα που παρακολουθεί και έρχεται σε επαφή χάνοντας έτσι την αντικειμενικότητά του.

Σε κάθε περίπτωση γεννάται και σημαντικό θέμα δεοντολογίας. Για να εξασφαλιστεί η εγκυρότητα και για να έχει ο ερευνητής την σωστή απεικόνιση των πραγμάτων δε θα πρέπει να αποκαλυφθεί η ιδιότητα του στο περιβάλλον που καλείται να δράσει.

Παρατηρητής. Είναι ο ρόλος του ερευνητή που παρακολουθεί απλά χωρίς να παίρνει μέρος σε καμία δραστηριότητα. Κίνδυνοι πολύ υπάρχουν και εδώ, και θα γίνουν πιο εύκολα κατανοητοί μέσα από ένα παράδειγμα έρευνας που διεξάγεται για διαδήλωση με έντονα επεισόδια. Ο ερευνητής στην προκειμένη περίπτωση δεν δύναται να βρίσκεται μέσα στο πλήθος των διαδηλωτών (στην συγκεκριμένη περίπτωση αποτελούν τα υποκείμενα της έρευνας του) και απλά να κάθεται σε μία γωνία και να παρατηρεί την συμπεριφορά τους, γιατί σε ενδεχόμενες φασαρίες και επεισόδια μεταξύ διαδηλωτών και αστυνομικών μπορεί να γίνει αντιληπτός από τους διαδηλωτές και να διατρέξει κάποιο κίνδυνο η ατομική του ακεραιότητα. Επιπροσθέτως, αν περιοριστεί στην απλή μόνο παρατήρηση δεν θα αποκτήσει ολοκληρωμένη άποψη για το αντικείμενο μελέτης του.

Συμμετέχων – Παρατηρητής. Ρόλος που δίνει την δυνατότητα στον ερευνητή να ενεργεί ταυτόχρονα σαν συμμετέχων και παρατηρητής και είναι ο πιο ορθός για μια έρευνα πεδίου. Ο ερευνητής στην περίπτωση αυτή έχει την ευχέρεια να κατευθύνει τη μελέτη του κατά την κρίση του, αλλά και να λάβει υπόψη του γεγονότα που πιθανόν να οδηγούν σε απρόβλεπτες καταστάσεις που με την σειρά τους να τον οδηγήσουν σε διαφοροποίηση της αρχικής του προσέγγισης.

Όπως έχει ήδη αναφερθεί πρέπει να δοθεί η δέουσα προσοχή στην σχέση του ερευνητή με το αντικείμενο μελέτης. Είναι πάντα υπαρκτός ο κίνδυνος να χάσει ο ερευνητής την αντικειμενικότητά του κατά την συμμετοχή του σε μια έρευνα πεδίου. Για παράδειγμα μπορεί να υπάρχει μια συμπάθεια είτε προς τα φυσικά πρόσωπα της έρευνας (π.χ. συμμετέχοντες σε μια οργάνωση), είτε προς το αντικείμενο της έρευνας (π.χ. την ιδεολογία της οργάνωσης). Η προσέγγιση των γεγονότων από τον ερευνητή αποστασιοποιημένα και με αντικειμενικότητα ονομάζεται «ημικτή οπτική γωνία».

Θα πρέπει να επισημανθεί πως η αντικειμενική οπτική γωνία (ημικτή) δεν είναι πάντα και ο πιο ενδεδειγμένος τρόπος προσέγγισης των γεγονότων. Ως παράδειγμα θα αναφερθεί η περίπτωση έρευνας για τα αισθήματα των κατοίκων ενός απολυταρχικού καθεστώτος σε χώρα της Αφρικής, που ο ηγέτης θεωρείται ότι έχει και θρησκευτικές υπερεξουσίες. Σε μια τέτοια έρευνα η επιλογή αντικειμενικού ερευνητή με βάση τα δυτικά πρότυπα διαβίωσης ίσως να μην είναι και αυτή που ενδείκνυται. Αντιθέτως η επιλογή ως ερευνητή ενός θρησκευόμενου πολίτη από αυτή την χώρα θα είχε ως αποτέλεσμα την καλύτερη προσέγγιση του αντικειμένου της έρευνας και συνεπώς θα οδηγούσε σε ορθότερα συμπεράσματα. Η οπτική γωνία που έχει ο ερευνητής που υιοθετεί τις απόψεις του αντικειμένου της έρευνας του λέγεται «ητική οπτική γωνία»[24].

2.3.1.2. Συνεντεύξεις

Η συνέντευξη είναι η πιο προσφιλή μέθοδος για να αντληθούν οι απαραίτητες πληροφορίες π.χ. που σχετίζονται με την γνώση της σκέψης, των κινήτρων, των συναισθημάτων, κ.λπ. των ερωτώμενων, προκειμένου να επιτευχθεί η βαθύτερη κατανόηση και ανάλυση κάποιου θέματος. Πάντα υπάρχει κάποιος σχεδιασμός για το πώς θα κυλήσει μια συνέντευξη αλλά ο βασικότερος στόχος είναι να διεξαχθεί η συζήτηση όσον το δυνατό πιο αβίαστα. Μια συνέντευξη χαρακτηρίζεται επιτυχής όταν βασίζεται στην αλληλεπίδραση μεταξύ του συνεντευκτή και του συνεντευξιαζόμενου. Σε αρκετές περιπτώσεις μάλιστα όταν κρίνεται σκόπιμο ένα μέρος της συνέντευξης μπορεί να αφιερωθεί σε συζήτηση πάνω σε γεγονότα που είναι εκτός σχεδιασμού προκειμένου να δοθούν απαντήσεις σε στάσεις συμπεριφορών, κινήτρων, σκέψεων, κ.λπ.. Εύλογο είναι σε μια συνέντευξη ο συνολικός χρόνος ομιλίας να διαμοιράζεται μεταξύ του συνεντευκτή και του συνεντευξιαζόμενου. Ένα λογικό μέτρο είναι οι απαντήσεις του συνεντευξιαζόμενου να καλύπτουν το 95% του συνολικού χρόνου της συνέντευξης και οι ερωτήσεις – τοποθετήσεις του συνεντευκτή να καλύπτον το υπόλοιπο 5% του συνολικού χρόνου.

Τα βασικά στάδια της διαδικασίας μιας συνέντευξης είναι η Θεματοποίηση, ο Σχεδιασμός, η Ανάλυση, η Επαλήθευση και η Έκθεση.

Θεματοποίηση. Είναι ο καθορισμός του σκοπού και των στόχων της συνέντευξης.

Σχεδιασμός. Καλείται η διατύπωση της διαδικασίας της συνέντευξης (συνέντευξη, απομαγνητοφώνηση, δηλαδή μεταφορά σε κείμενο της συνέντευξης).

Ανάλυση. Είναι η μελέτη των συλλεχθέντων πληροφοριών σύμφωνα με το σκοπό της έρευνας.

Επαλήθευση. Καλείται η διαδικασία ελέγχου της αξιοπιστίας και της εγκυρότητας των συμπερασμάτων.

Έκθεση. Ονομάζεται η διαδικασία δημοσίευσης των συμπερασμάτων της έρευνας.

Εν κατακλείδι, κατά την διάρκεια μιας συνέντευξης ο ερευνητής θα πρέπει να δώσει ιδιαίτερη προσοχή στα εξής:

- Στον τρόπο διατύπωσης της ερώτησης γιατί καθορίζει την απάντηση που θα αποσπάσει, ενώ με την σειρά τους οι απαντήσεις αυτές διαμορφώνουν ένα μέρος των επόμενων ερωτήσεων.
- Επιπλέον, κατά την διάρκεια μιας συνέντευξης θα πρέπει ο ερευνητής να έχει την ικανότητα να μπορεί να ακούει, να σκέφτεται και να μιλά σχεδόν ταυτόχρονα. Θα πρέπει να είναι καλός ακροατής, δηλαδή να ακούει και να κοιτάει με ενδιαφέρον τον ερωτώμενο και να του επιτρέπει την πρωτοβουλία σε στιγμές μικρών παύσεων. Από την άλλη δεν πρέπει να είναι παθητικός και να μην μιλά, αλλά να είναι ικανός να διαχειριστεί τον χρόνο ακολουθώντας τον κανόνα που αναφέρθηκε, δηλαδή ο συνολικός χρόνος ομιλίας του να μην ξεπερνά σε διάρκεια το 5% της διάρκειας της συνέντευξης.
- Επιπροσθέτως, ένας ερευνητής θα πρέπει να καθοδηγεί έμμεσα την συζήτηση προς την κατεύθυνση που εκείνος επιθυμεί. Η διακοπή του ερωτώμενου ερμηνεύεται ως έλλειψη ενδιαφέροντος. Αντιθέτως, θα πρέπει συνεχώς να ενθαρρύνει τον συνεντευξιαζόμενο για μεγαλύτερη ανάπτυξη του θέματος, κίνηση που δηλώνει το πραγματικό ενδιαφέρον του.
- Τα βασικά θέματα της συνέντευξης θα πρέπει να είναι από πριν προκαθορισμένα ούτως ώστε να καταφέρει ο ερευνητής να επιτύχει λογικές και

ομαλές μεταβάσεις από το ένα θέμα στο άλλο (Rubin, H. & Rubin, R., 1995). Η συζήτηση μεταξύ του ερευνητή και του ερωτώμενου δεν έχει την έννοια της αυθόρμητης συζήτησης, αλλά είναι επίσημη. Αυτό συνεπάγεται ότι οποιαδήποτε προσπάθεια από την πλευρά του ερευνητή να εμφανιστεί ο ίδιος ενδιαφέρον ως άτομο είναι εντελώς αντιπαραγωγική. Σκοπός του ερευνητή είναι να κάνει τον συνεντευξιαζόμενο να νιώθει αυτός ως ένα ενδιαφέρον άτομο. Αυτό θα το επιτύχει αν καταφέρει να εφαρμόσει τον προαναφερθέν κανόνα του 5% δηλαδή, περισσότερο να τον ακούει παρά να μιλάει ο ίδιος[24].

2.3.1.3. Ομάδες εστίασης (focus group)

Οι έρευνες με ομάδες εστίασης είναι έρευνες με συχνή εφαρμογή στις επιστήμες Διοίκησης και Οικονομίας. Ο ερευνητής σε τέτοιου είδους έρευνες είναι ο συντονιστής της συζήτησης που πραγματοποιείται με μια ομάδα εστίασης. Διαδικασία όμοια με αυτή που ακολουθείται από έναν δημοσιογράφο όταν καλείται να συντονίσει ένα πάνελ με πολλούς καλεσμένους, σε μια πολιτική εκπομπή στην τηλεόραση. Οι έρευνες με ομάδες εστίασης χρησιμοποιούνται ευρέως σε έρευνες που σχετίζονται με την αγορά για την αξιολόγηση προϊόντων και ειδών εμπορευμάτων και βασίζονται σε δομημένες, ημιδομημένες ή μη δομημένες συνεντεύξεις.

Για την συζήτηση ενός συγκεκριμένου θέματος συγκεντρώνονται σε ιδιωτικό χώρο και σε ένα άνετο περιβάλλον συνήθως 5 έως 12 άτομα. Η επιλογή των ατόμων αυτών γίνεται μέσω δειγματοληψίας που σπάνια είναι πιθανοτική λόγω του περιορισμένου αριθμού του δείγματος γεγονός που κάνει το δείγμα να μην είναι αντιπροσωπευτικό. Το δείγμα συνήθως το αποτελούν άτομα που λογίζονται ως κατάλληλα για την έρευνα π.χ. μπορεί να είναι εν δυνάμει πελάτες ενός φορητού υπολογιστή που αναμένεται να βγει σε λίγο στην αγορά.

Ο ερευνητής έχει την συνολική ευθύνη για να διεξαχθεί μια συζήτηση εποικοδομητικά και πολιτισμένα. Οφείλει να δίνει το λόγο σε όλα τα μέλη της ομάδας για το ίδιο ερώτημα και να μοιράζει τον χρόνο εξίσου, ούτως ώστε να μην μονοπωλούν τη συζήτηση μόνο κάποια από τα μέλη της ομάδας.

Σύμφωνα με τον Krueger (1988), οι έρευνες με ομάδες εστίασης έχουν τα μειονεκτήματα και τα πλεονεκτήματα τους.

Πλεονεκτήματα. Στις έρευνες με ομάδες εστίασης η ερευνητική μέθοδος είναι κοινωνικά προσανατολισμένη με στόχο να συγκεντρώνει δεδομένα της πραγματικής ζωής στο κοινωνικό περιβάλλον. Είναι ευέλικτη με μικρό κόστος και προσφέρει άμεσα αποτελέσματα υψηλής εγκυρότητας.

Μειονεκτήματα. Σε αντίθεση με ότι ισχύει στις ατομικές συνεντεύξεις, στις έρευνες με ομάδες εστίασης ο ερευνητής δεν έχει τον απόλυτο έλεγχο και επιπλέον απαιτείται να έχει ειδικές δεξιότητες όσον αφορά τον συντονισμό της συζήτησης. Η συζήτηση πρέπει να διεξάγεται σε πρόσφορο περιβάλλον, κάτι το οποίο δεν είναι πάντα εφικτό. Υπάρχουν αρκετές περιπτώσεις όπου η αντιπαράθεση μεταξύ των ερωτώμενων που ανήκουν στην ομάδα εστίασης μπορεί να προκαλέσει προβλήματα. Δυσκολίες εμφανίζονται ενίοτε και κατά την συγκέντρωση των ομάδων. Η ανάλυση των δεδομένων είναι δυσκολότερη.

Μεγάλο ενδιαφέρον έχει η άποψη του Krueger που λέει ότι η έρευνα σε ομάδες εστίασης μπορεί να είναι ο κατάλληλος τρόπος για να γίνει μία σωστή και πλήρης σύνταξη ερωτηματολογίου δειγματοληπτικής έρευνας.

2.3.1.4. Ποιοτική έρευνα πεδίου και δεοντολογία

Για να εξασφαλιστεί η εγκυρότητα μιας έρευνας πεδίου δεν πρέπει η παρουσία του ερευνητή να γίνει αντιληπτή. Αυτό συνεπάγεται όμως ανυποψίαστοι άνθρωποι να γίνονται αντικείμενα μελέτης ερευνών, ή ακόμα να δημιουργούνται ανθρώπινες σχέσεις επιτηδευμένα σχεδιασμένες, και πάντα να υφέρπει ο κίνδυνος, όπως και σε άλλες έρευνες, προσωπικές πληροφορίες των ατόμων που συμμετέχουν στην έρευνα να διαρρεύσουν

2.3.2. Δειγματοληπτική έρευνα

Οι δειγματοληπτικές έρευνες συνήθως διενεργούνται από ερευνητές για τη συγκέντρωση πληροφοριών και δεδομένων με στόχο είτε την περιγραφή, είτε τη

διερεύνηση, είτε την ερμηνεία διαφόρων θεμάτων. Το κύριο «εργαλείο» διεξαγωγής μιας τέτοιου είδους έρευνας είναι το ερωτηματολόγιο. Η εξαγωγή, συλλογή των δεδομένων μπορεί να επιτευχθεί είτε με προσωπικές συνεντεύξεις μέσω ερωτηματολογίων και τηλεφώνου, είτε με την ατομική συμπλήρωση ερωτηματολογίων που διανέμονται ταχυδρομικά ή διαδικτυακά στους εκάστοτε συμμετέχοντες στην έρευνα. Στις δειγματοληπτικές έρευνες υπάρχει η δυνατότητα της δευτερογενούς ανάλυσης των συλλεγμένων δεομένων, δηλαδή δεδομένα που συλλέχθηκαν για μια έρευνα να χρησιμοποιούνται ξανά σε κάποια άλλη μεταγενέστερη

2.3.2.1. Ερωτηματολόγια

Τα ζητήματα που εστιάζουν την προσοχή τους οι ερευνητές ώστε να προβούν στη διενέργεια δειγματοληπτικών ερευνών, στη μεγαλύτερη πλειοψηφία τους έχουν ως επίκεντρο τον άνθρωπο και τα προβλήματα που τον απασχολούν. Συνεπώς, σε αυτές τις περιπτώσεις των δειγματοληπτικών ερευνών ως μονάδες ανάλυσης είναι είτε μεμονωμένα άτομα, είτε διάφορες ομάδες ατόμων.

Η ενδεικνυόμενη μέθοδος για την συγκέντρωση πληροφοριών και δεδομένων από ένα μεγάλο σύνολο ατόμων είναι η δειγματοληπτική έρευνα. Μέσω αυτού του είδους ερευνών υπάρχει η δυνατότητα της μέτρησης της αντίληψης, των απόψεων και των κατευθύνσεων ενός μεγάλου μέρους του πληθυσμού. Οι δημοσκοπήσεις είναι από τα πλέον χαρακτηριστικά παραδείγματα τέτοιων ερευνών.

2.3.2.2. Πλεονεκτήματα και μειονεκτήματα δειγματοληπτικών ερευνών

Οι δειγματοληπτικές έρευνες, όπως και όλα τα είδη ερευνών, έχουν πλεονεκτήματα και μειονεκτήματα.

Πλεονεκτήματα. Οι δειγματοληπτικές έρευνες εφαρμόζονται σε ζητήματα μεγάλων πληθυσμών, τα οποία με μεγάλη δυσκολία μπορούν να ερευνηθούν με άλλες μεθόδους ερευνών. Επίσης, οι απαντήσεις δίνονται σε κλειστού τύπου ερωτήσεις γεγονός που κάνει πιο εύκολες τις διαδικασίες της επεξεργασία και της συμπερασματολογίας.

Μειονεκτήματα. Σε τέτοιου είδους έρευνες υπάρχει πιθανότητα απώλειας πληροφορίας η οποία οφείλεται στο «στρίμωγμα» δεδομένων σε γενικευμένες κατηγορίες. Γι' αυτό πολλές φορές οι δειγματοληπτικές έρευνες χαρακτηρίζονται και «άκαμπτες». Επίσης, υπάρχουν περιπτώσεις όπου το θέμα που ερευνάται να μην είναι εφικτό να «μετρηθεί» μέσω ερωτηματολογίων. Μάλιστα, στην περίπτωση λάθους στον αρχικό σχεδιασμό, π.χ. στη σύνταξη των ερωτήσεων του ερωτηματολογίου, είναι αδύνατον να διορθωθεί.

Επιπροσθέτως, η επιτυχείς διεξαγωγή τέτοιων ερευνών χρειάζεται πολύ χρόνο και χρήμα.

2.3.2.3. Δευτερογενής έρευνα

Η συνεχής συγκέντρωση πληροφοριών, δεδομένων και συμπερασμάτων δίνει συχνά την δυνατότητα σε πολλούς επιστήμονες και ερευνητές να εξαγάγουν από αυτά κατάλληλα στοιχεία που άπτονται του δικού τους ενδιαφέροντος. Πιο συγκεκριμένα, υπάρχουν αρκετές περιπτώσεις όπου δεδομένα ή πληροφορίες μιας έρευνας να επαναχρησιμοποιούνται από ερευνητές σε μια άλλη έρευνα με τελείως διαφορετικό προσανατολισμό, σκοπό και στόχο. Ως παραδείγματα χρησιμοποίησης εκ νέου καταγεγραμμένης γνώσης θα μπορούσαν να αναφερθούν τα απογραφικά στοιχεία και οι μετρήσεις πειραμάτων, οι απαντήσεις σε ερωτηματολόγια, κ.λπ.. Αρκετές δεκαετίες πριν η συλλογή δεδομένων γίνονταν σε έντυπη μορφή και διαφυλάσσονταν σε βιβλιοθήκες. Με την ραγδαία εξέλιξη του διαδικτύου και την ανάπτυξη των ηλεκτρονικών υπολογιστών και γενικά των έξυπνων συσκευών τα δεδομένα πλέον φυλάσσονται σε ηλεκτρονικές διευθύνσεις.

Υπάρχει μεγάλος αριθμός ερευνητικών κέντρων όπου μπορεί κανείς να ανατρέξει προκειμένου να βρει καταγεγραμμένα δεδομένα για την έρευνα του. Τέτοια κέντρα είναι η Ελληνική Τράπεζα Κοινωνικών Δεδομένων (ΕΤΚΔ), η Ειδική Τράπεζα Πληροφοριών (ΕΤΠ), το Αρχείο Κοινωνικών Δεδομένων και Δεικτών (ΑΚΔΔ), το Περιβάλλον Διαχείρισης Κοινωνικών Δεδομένων (ΠΔΚΔ), και ο Κόμβος Δευτερογενούς Επεξεργασίας (ΚΔΕ).

Όπως σε όλα τα είδη ερευνών, έτσι και οι δευτερογενής έρευνες έχουν πλεονεκτήματα και μειονεκτήματα.

Πλεονεκτήματα. Το κύριο πλεονέκτημα των δευτερογενών ερευνών είναι η οικονομία. Επιπλέον μια τέτοιου είδους έρευνα δίνει τη δυνατότητα της μετά-ανάλυσης στον ερευνητή. Δηλαδή ο ερευνητής μπορεί να συγκεντρώσει πληροφορίες και δεδομένα από άλλες παλαιότερες έρευνες για ένα συγκεκριμένο θέμα.

Μειονεκτήματα. Το βασικότερο μειονέκτημα τους είναι η εγκυρότητα. Αυτό γιατί οι πληροφορίες και τα δεδομένα που συλλέγουν οι ερευνητές εξυπηρετούν κάποιον συγκεκριμένο σκοπό με αποτέλεσμα η καταγεγραμμένη αυτή γνώση να μην είναι κατάλληλη για άλλους ερευνητικούς σκοπούς.

2.3.2.4. Δεοντολογία δειγματοληπτικής έρευνας

Σημαντικά ζητήματα δεοντολογίας δεν παρουσιάζονται στις δειγματοληπτικές έρευνες. Ο ρόλος που έχει ο ερευνητής είναι σαφής, ξεκάθαρος και πλήρως αντιληπτός στον ερωτώμενο. Δεοντολογικά ζητήματα μπορούν να ανακύψουν μόνο κατά τη διαχείριση των προσωπικών δεδομένων και πληροφοριών. Χαρακτηριστική είναι η περίπτωση των δημοσκοπήσεων όπου χρησιμοποιούνται κάλπες προκειμένου ο ερωτώμενος να παραμείνει ανεπηρέαστος για την απόφαση που καλείται να πάρει. Στην συνέχεια όμως ο εκάστοτε ερευνητής συνδέει την «ψήφο» με τις υπόλοιπες ερωτήσεις εν αγνοία του ερωτώμενου[23].

2.3.3. Πειραματικοί σχεδιασμοί

Για την πλειοψηφία των ανθρώπων ο όρος πείραμα ταυτίζεται άμεσα με τις επιστήμες της χημείας, της φυσικής, της ιατρικής, κ.λπ. (Κίτσος, 1994). Πειράματα όμως, μπορούν να διενεργηθούν, πραγματοποιηθούν εκτός από τις ελεγχόμενες συνθήκες ενός εργαστηρίου και στην κοινωνία.

2.3.3.1. Κατάλληλα θέματα για πειράματα

Ο σκοπός της έρευνας στις περιπτώσεις των πειραματικών σχεδιασμών, είναι τις περισσότερες φορές ερμηνευτικός και όχι περιγραφικός. Στόχος αυτών των ερευνών είναι η άσκηση κάποιας επιρροής, επενέργειας σε μια δεδομένη κατάσταση και στην συνέχεια η εξέταση των αποτελεσμάτων αυτής. Ουσιαστικά εξετάζεται αν σημειώθηκαν αλλαγές στην αρχική κατάσταση μετά την άσκηση της όποιας επιρροής.

Στις περισσότερες των περιπτώσεων τα πειράματα διενεργούνται σε μελετητικά προγράμματα που σχετίζονται με περιορισμένες και σαφής έννοιες και προτάσεις. Για παράδειγμα, έστω ότι σκοπός μιας έρευνας πειραματικής σχεδίασης είναι να μειώσει τον μεγάλο βαθμό προκατάληψης που υπάρχει έναντι των επιτυχημένων γυναικών, γυναικών που κατέχουν μια διευθυντική θέση μέσα σε μια επιχείρηση. Από πολλούς θεωρείται ότι οι γυναίκες δεν έχουν τις απαραίτητες ικανότητες και προσόντα για να αναλάβουν μια θέση με τόσες ευθύνες και απαιτήσεις. Στην περίπτωση αυτή όμως αν γίνει προσπάθεια να αναδειχθεί η συμβολή των γυναικών στην ανάπτυξη πολλών και μεγάλων επιχειρήσεων σε βάθος χρόνου, τότε ίσως η επίδραση αυτού του στοιχείου να επιφέρει μια κάποια μείωση της σχετικής προκατάληψης. Τα βήματα που θα πρέπει να ακολουθηθούν για να ελεγχθεί το συγκεκριμένο ζήτημα με την πειραματική μέθοδο είναι τα ακόλουθα:

- Πρώτα από όλα θα πρέπει να ελεγχθεί μια ομάδα υποκειμένων ούτως ώστε να καθοριστεί το επίπεδο της συγκεκριμένης προκατάληψης (για το σκοπό αυτό θα μπορούσε να χρησιμοποιηθεί ένα ερωτηματολόγιο).
- Με την ολοκλήρωση της συμπλήρωσης του ερωτηματολογίου θα πρέπει στην συνέχεια να γνωστοποιηθούν (π.χ. μέσω ενός ντοκιμαντέρ ή ενός ενημερωτικού φυλλαδίου) όλες εκείνες οι πληροφορίες που αποδεικνύουν την επιτυχημένη πορεία των γυναικών στον επιχειρηματικό κόσμο.
- Μετά την ενημέρωση της ομάδας των υποκειμένων θα πρέπει να μετρηθεί εκ νέου το επίπεδο της σχετικής προκατάληψης τους με στόχο να διαπιστωθεί αν η ενημέρωση που τους έγινε συνέβαλε ή όχι και σε ποιο βαθμό για την μείωση του βαθμού προκατάληψης.

2.3.3.2. Το πείραμα

Όπως έγινε αντιληπτό και από το προαναφερθέν παράδειγμα η πειραματική διαδικασία διενεργείται σε δυο στάδια, το στάδιο του προ-ελέγχου και το στάδιο του μετά-ελέγχου (δηλαδή μέτρηση των αποτελεσμάτων πριν και μετά την επενέργεια, επίδραση).

Στην διαδικασία αυτή λαμβάνουν μέρους οι «πειραματικές ομάδες» και οι «ομάδες ελέγχου». Με τον όρο «πειραματική ομάδα» εννοείται η ομάδα των μονάδων ανάλυσης πάνω στην οποία θα διεξαχθεί το πείραμα, η δράση. Ενώ με τον όρο «ομάδα ελέγχου» εννοείται η ομάδα μονάδων ανάλυσης πάνω στην οποία δεν ασκείται κάποια δράση αλλά καταμετρείται κανονικά προκειμένου να χρησιμοποιηθεί ως μέτρο σύγκρισης με την πειραματική ομάδα.

Επιπροσθέτως για το πείραμα χρησιμοποιούνται δυο ειδών μεταβλητές, η εξαρτημένη και η ανεξάρτητη. Η εξαρτημένη είναι το αποτέλεσμα του πειράματος και μπορεί να πάρει το σύνολο των ποσοτικών μεταβλητών, ενώ η ανεξάρτητη είναι μια ποιοτική μεταβλητή δύο τιμών:

- «η μονάδα ανάλυσης έχει δεχθεί την επίδραση»,
- «η μονάδα ανάλυσης δεν έχει δεχθεί την επίδραση».

Στο προαναφερθέν παράδειγμα ως εξαρτημένη μεταβλητή θεωρείται «η προκατάληψη κατά τις αποτελεσματικότητας των γυναικών σε θέσεις ευθύνης» και η μέτρηση της οποίας μπορεί να επιτευχθεί είτε μέσω συνέντευξης είτε μέσω της συμπλήρωσης ερωτηματολογίου. Ενώ ως ανεξάρτητη μεταβλητή θεωρείται η μεταβλητή με τις τιμές «η μονάδα ανάλυσης έχει διαβάσει το ενημερωτικό φυλλάδιο ή έχει δει το ντοκιμαντέρ» και «η μονάδα ανάλυσης δεν έχει διαβάσει το ενημερωτικό φυλλάδιο ή δεν έχει δει το ντοκιμαντέρ». Καλό είναι εδώ να επισημανθεί πως μια ανεξάρτητη μεταβλητή σε ένα πείραμα μπορεί να θεωρηθεί ως εξαρτημένη μεταβλητή σε ένα άλλο πείραμα. Στο παραπάνω παράδειγμα η προκατάληψη θεωρείτο ως η εξαρτημένη μεταβλητή, αλλά σε ένα άλλο πείραμα, που σκοπός του είναι να εξετάσει το αποτέλεσμα της προκατάληψης π.χ. στην εκλογική συμπεριφορά, θα μπορούσε να θεωρηθεί ως η ανεξάρτητη μεταβλητή.

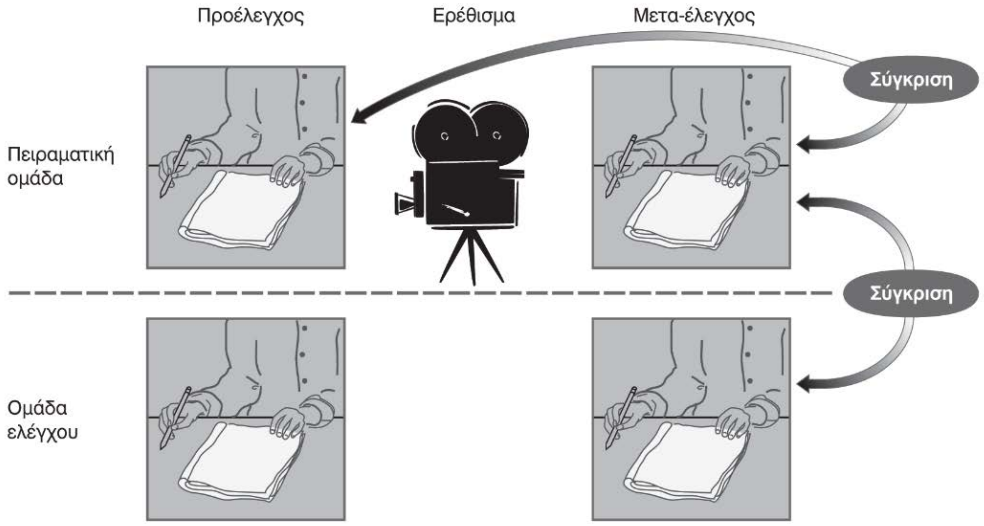
2.3.3.3. Στάδια προ-ελέγχου και μετά-ελέγχου

Σε όλα τα είδη ερευνών πάντα ανακύπτει το θέμα της εγκυρότητας. Στις περιπτώσεις ερευνών που βασίζονται σε πειραματικούς σχεδιασμούς θέμα εγκυρότητας προκύπτει κυρίως στο στάδιο του μετά-ελέγχου.

Στο προαναφερόμενο παράδειγμα, στο πρώτο στάδιο του προ-ελέγχου, δηλαδή κατά την πρώτη διεξαγωγή του ερωτηματολογίου, οι συμμετέχοντες ερωτώμενοι αγνοούν το σκοπό του. Αντιθέτως στο δεύτερο στάδιο της έρευνας, δηλαδή κατά τη δεύτερη διεξαγωγή του ερωτηματολογίου, οι ερωτώμενοι είναι σχεδόν βέβαιο ότι θα καταλάβουν το λόγο για τον οποίο διεξάγεται η έρευνα. Αυτό έχει σαν αποτέλεσμα να υπάρχει μεγάλη πιθανότητα να επηρεαστούν και να απαντήσουν εντελώς διαφορετικά από ότι θα απαντούσαν αν παρέμεναν ανεπηρέαστοι. Έτσι κάποιος που θα αντιληφθεί πως η έρευνα που συμμετέχει έχει σαν σκοπό την καταμέτρηση της προκατάληψης κατά των γυναικών, είναι πολύ πιθανόν να απαντήσει με τέτοιο τρόπο που να μην προδίδεται η προκατάληψή του. Οι μεροληπτικές απαντήσεις λοιπόν, είναι το κύριο ζητούμενο που έχουν να ξεπεράσουν οι ερευνητές σε έρευνες με πειραματικούς σχεδιασμούς οικονομικών και κοινωνικών επιστημών. Αξιοσημείωτο είναι το γεγονός πως η μεροληψία προκύπτει ακόμα και σε θετικές επιστήμες (ιατρική, κ.λπ.).

2.3.3.4. Το κλασσικό πείραμα

Για να αντιμετωπίσουν οι ερευνητές το ζήτημα της μεροληψίας που εμφανίζεται στις έρευνες που βασίζονται σε πειραματικούς σχεδιασμούς χρησιμοποιούν στην όλη διαδικασία δυο ομάδες μονάδων ανάλυσης (όπως έχει είδη προαναφερθεί την «πειραματική ομάδα» και την «ομάδα ελέγχου»)[25]. Τα αποτελέσματα της επίδρασης δεν θα προκύπτουν μόνο από τα αποτελέσματα της «πειραματικής ομάδας» πριν και μετά την επιρροή, όπως θα ήταν και το αναμενόμενο, αλλά θα προκύπτουν από τη σύγκριση μεταξύ των μονάδων ανάλυσης που έχουν δεχτεί την επίδραση («πειραματική ομάδα») και μονάδων ανάλυσης που δεν την έχουν δεχτεί («ομάδα ελέγχου»). Το κλασσικό πείραμα παρουσιάζεται στο σχήμα που ακολουθεί.



Εικόνα 1. Το κλασσικό πείραμα

Με βάση τα κριτήρια πιθανοτικής δειγματοληψίας οι δυο ομάδες ελέγχου θα πρέπει να μοιάζουν μεταξύ τους. Στο στάδιο του προ-ελέγχου γίνεται η καταμέτρηση της εξαρτημένης μεταβλητής (π.χ. την προκατάληψη κατά της ικανότητας των γυναικών για την ανάληψη θέσεων ευθύνης) στις μονάδες ανάλυσης που απαρτίζουν την «πειραματική ομάδα» αλλά και στις μονάδες ανάλυσης που απαρτίζουν την «ομάδα ελέγχου». Στην συνέχεια ασκείται το ερέθισμα, η επίδραση στην «πειραματική ομάδα» και γίνεται εκ νέου καταμέτρηση της εξαρτημένης μεταβλητής (στάδιο μετά-ελέγχου). Το στάδιο μετά-ελέγχου διεξάγεται και στην «ομάδα ελέγχου» παρόλο που δεν της έχει ασκηθεί το ανάλογο ερέθισμα ή δράση. Το τελικό συμπέρασμα για το κατά πόσο η επίδραση που ασκήθηκε είχε αποτέλεσμα πηγάζει από την σύγκριση των σταδίων μετά-ελέγχων των δυο ομάδων. Έτσι επιτυγχάνεται η μέτρηση της μεροληπτικότητας που προέρχεται από τον τρόπο που απαντά κάποιος όταν αντιλαμβάνεται ότι είναι το «υποκείμενο πειράματος» μιας έρευνας.

Εάν κάποιος δηλαδή από αυτούς που ανήκουν στην «πειραματική ομάδα» αντιληφθεί ότι η άποψή του για την καταλληλόλητα των γυναικών στελεχών γίνει αντικείμενο μελέτης, είναι αναμενόμενο να απαντήσει μεροληπτικά στο μετά-έλεγχο στάδιο για να αποκρύψει την προκατάληψή του. Με την ύπαρξη όμως της «ομάδας

ελέγχου» μπορεί να εκτιμηθεί ο βαθμός της προκατάληψης και τα όποια αποτελέσματα να συγκριθούν με εκείνα του μετά-ελέγχου σταδίου της «πειραματικής ομάδας».

Στο παράδειγμα τα αποτελέσματα που αναμένονται είναι δυο. Το πρώτο αποτέλεσμα είναι ότι το ενημερωτικό φυλλάδιο ή το ντοκιμαντέρ δεν είχε καμία επίδραση επομένως ο μετά-έλεγχος και για τις δυο ομάδες απεικονίζει τον ίδιο βαθμό προκατάληψης. Αντιθέτως, το δεύτερο αποτέλεσμα θα είναι ότι το ενημερωτικό φυλλάδιο ή το ντοκιμαντέρ είχε κάποια θετική επίδραση πάνω στις μονάδες ανάλυσης και συνεπώς ο βαθμός προκατάληψης της «πειραματικής ομάδας» είναι μικρότερος από αυτόν της «ομάδας ελέγχου».

Το πόσο μεγάλη είναι η σημασία του βαθμού προκατάληψης φαίνεται από το «φαινόμενο Χόθορν». Σύμφωνα με αυτό σε μια έρευνα που διενεργήθηκε στις αρχές του αιώνα σκοπός των ερευνητών ήταν να μάθουν πως θα μπορούσε να αυξηθεί η παραγωγικότητα των εργαζομένων. Για να πετύχουν τον σκοπό τους αυτό μελέτησαν τις συνθήκες εργασίας των εργαζομένων στο τηλεφωνικό κέντρο της εταιρείας Χόθορν στο Σικάγο[23].

Τα αποτελέσματα της έρευνα ανέδειξαν ότι όσο βελτιώνονταν οι συνθήκες φωτισμού τόσο αυξάνονταν και η παραγωγικότητα των εργαζομένων. Έτσι η έρευνα κατέληξε στο συμπέρασμα ότι η παραγωγικότητα βελτιωνόταν από τις συνθήκες φωτισμού. Για να αποδειχθεί όμως ότι το συμπέρασμα ήταν σωστό και ασφαλές έγινε επαναφορά των αρχικών συνθηκών φωτισμού και αυτό που διαπιστώθηκε ήταν ότι η παραγωγικότητα συνέχισε να αυξάνεται. Συνεπώς το τελικό συμπέρασμα είναι ότι η παραγωγικότητα άρχισε να βελτιώνεται όχι όμως λόγω του φωτισμού αλλά επειδή οι εργαζόμενοι διαισθάνονταν την παρακολούθηση των ερευνητών.

Ένα ακόμα ενδιαφέρον φαινόμενο είναι και η προκατάληψη του ερευνητή. Σε αρκετές περιπτώσεις και ειδικότερα σε υποκειμενικές μετρήσεις υπάρχει η πιθανότητα ο ερευνητής να επηρεαστεί γνωρίζοντας ότι το υποκείμενο (μονάδα ανάλυσης) ανήκει στην «πειραματική ομάδα». Για παράδειγμα ένας γιατρός ερευνητής είναι πολύ πιθανόν να βλέπει ότι βελτιώνεται ο ασθενής του, όταν πιστεύει ότι έχει πάρει την κατάλληλη φαρμακευτική αγωγή. Στις περιπτώσεις αυτές εφαρμόζεται η διαδικασία της ύπαρξης δυο «πειραματικών ομάδων». Η μια να λαμβάνει ένα ψευτοφάρμακο και

η άλλη να λαμβάνει το πειραματικό φάρμακο με τους υπευθύνους ερευνητές να μην γνωρίζουν τι είδους φάρμακο έχει χορηγηθεί σε κάθε μια από τις δυο ομάδες. Το τι είδους φάρμακο έχει χορηγηθεί σε κάθε ομάδα δεν πρέπει να το γνωρίζουν όμως, ούτε οι συμμετέχοντες σε αυτές, ώστε να εξασφαλιστεί ότι τα αποτελέσματα θα είναι έγκυρα και χωρίς μεροληψία. Αυτή η διαδικασία ονομάζεται «διπλό τυφλό πείραμα».

2.3.3.5. «Ταίριασμα» και «Τυχαιοποίηση»

Σύμφωνα με όσα αναφέρθηκαν και πιο πάνω για να είναι εφαρμόσιμος ο κλασσικός σχεδιασμός θα πρέπει τόσο η «ομάδα ελέγχου» όσο και η «πειραματική ομάδα» να μοιάζουν σε όσο το δυνατό περισσότερα σημεία, να έχουν δηλαδή κάποια κοινά χαρακτηριστικά. Αυτό είναι εφικτό να επιτευχθεί είτε με πιθανοτική δειγματοληψία είτε με «ταίριασμα». Ένα από τα συνηθέστερα παραδείγματα πιθανοτικής δειγματοληψίας είναι στην περίπτωση που και οι δυο ομάδες συλλέγονται με την διαδικασία της απλής δειγματοληψίας από τον πληθυσμό. Σε τέτοιες καταστάσεις θα πρέπει να ληφθεί υπόψη και το μέγεθος του δείγματος ούτως ώστε να είναι ικανοποιητικό.

Σε περιπτώσεις που ο πληθυσμός είναι μικρός και δεν είναι εφικτό να ακολουθηθεί η διαδικασία της πιθανοτικής δειγματοληψίας για την σύσταση των ομάδων τότε επιλέγεται συνήθως η διαδικασία της «τυχαιοποίησης». Συνήθως, με τυχαίο τρόπο, κάποια κλήρωση, χωρίζεται ο πληθυσμός σε «πειραματική ομάδα» και «ομάδα ελέγχου». Η μέθοδος της «τυχαιοποίησης» είναι γενικά καλύτερη από το «ταίριασμα», δηλαδή, σε περιπτώσεις όπου για κάθε παρατήρηση από τη μια ομάδα, επιλέγεται και μια από την άλλη που της «ταιριάζει». Το βασικότερο κριτήριο για την μέθοδο του «ταιριάσματος» είναι η ομοιότητα των σημαντικότερων, σύμφωνα με τον ερευνητή, παραγόντων, (π.χ. ηλικία, φύλο, οικογενειακή κατάσταση, εκπαίδευση, κ.λπ.), σε περιορισμένο πλήθος. Το μειονέκτημα της διαδικασίας αυτής είναι το ίδιο με της ποσοστικής δειγματοληψίας. Οι παράγοντες δηλαδή, που μπορεί να λαμβάνονται υπόψη να είναι λίγοι με αποτέλεσμα να είναι πολύ πιθανόν ο ερευνητής να κάνει λάθος εκτίμηση για τους παράγοντες που επηρεάζουν την εξαρτημένη μεταβλητή που εξετάζεται. Η μέθοδος του «ταιριάσματος» πλεονεκτεί έναντι των μεθόδων της

«τυχαιοποίησης» και της πιθανοτικής δειγματοληψίας, μόνο όταν το πλήθος των μονάδων ανάλυσης ενός πληθυσμού είναι μικρό.

2.3.3.6. Εγκυρότητα

Η εγκυρότητα στην πειραματική έρευνα επηρεάζεται αρνητικά από δύο ειδών παράγοντες, τους παράγοντες που αποτελούν πηγή έλλειψης εσωτερικής εγκυρότητας και τους παράγοντες που αποτελούν πηγή έλλειψης εξωτερικής εγκυρότητας.

Έλλειψη εσωτερικής εγκυρότητας. Είναι οι περιπτώσεις κατά τις οποίες υπάρχει η πιθανότητα τα συμπεράσματα που προκύπτουν από πειραματικά αποτελέσματα να μην αντανακλούν τι ακριβώς συνέβη κατά τη διάρκεια του πειράματος αυτού.

Οι Campbell και Stanley (1963) και οι Cook και Campbell (1979) εξέτασαν πηγές που επηρεάζουν την εσωτερική εγκυρότητα μιας έρευνας. Τέτοιες είναι το ιστορικό της έρευνας, η ωρίμανση, η επίδραση του ελέγχου, η επίδραση των εργαλείων μέτρησης, η στατιστική παλινδρόμηση, τα σφάλματα μεροληπτικής επιλογής, η «πειραματική θνησιμότητα», η αποζημίωση και η αποθάρρυνση συμμετοχής στην έρευνα[23].

Μια κατάσταση, ένα γεγονός που γνωστοποιείται κατά την εξέλιξη ενός πειράματος υπάρχει πιθανότητα να ασκήσει κάποια επιρροή πάνω στο πείραμα. Ως παράδειγμα, θα μπορούσε να θεωρηθεί μια έρευνα που θα μετρούσε την εμπιστοσύνη των πολιτών στην κυβέρνηση μιας χώρας, π.χ. την αμερικανική κυβέρνηση. Στην περίπτωση αυτή η αποκάλυψη Snowden ότι οι αμερικανικές και βρετανικές κυβερνήσεις εφαρμόζουν προγράμματα μαζικής παρακολούθησης θα μπορούσε να επηρεάσει το πείραμα.

Κατά την διάρκεια ενός πειράματος, ένα υποκείμενο υπάρχει η πιθανότητα να επηρεαστεί από τον ψυχολογικό-ανθρώπινο παράγοντα, ανεξαρτήτως αν το πείραμα είναι μακροχρόνιο ή όχι. Αυτό πρακτικά σημαίνει ότι το υποκείμενο μπορεί να πεινάσει, να διψάσει, να βαρεθεί, να κουραστεί, ή στην περίπτωση μακροχρόνιου

πειράματος να κρατήσει διαφορετική στάση απέναντι στο ζήτημα λόγω αλλαγής π.χ. των αντιλήψεων του ή των απόψεών του.

Κατά την εξέλιξη μιας πειραματικής έρευνας το υποκείμενο μπορεί να αντιληφθεί ότι αποτελεί μέρος ενός πειράματος με αποτέλεσμα είτε να δώσει απαντήσεις τις οποίες νομίζει ότι θέλει να ακούσει ο ερευνητής είτε οι απαντήσεις του να είναι τέτοιες που θα το κάνουν να φαίνεται καλύτερο και πιο αρεστό.

Σε περιπτώσεις πειραμάτων όπου χρησιμοποιούνται ομάδες που έχουν ακραίες συμπεριφορές, παρατηρείται το φαινόμενο της στατικής παλινδρόμησης. Αρκετές φορές διεξάγονται πειράματα με υποκείμενα των οποίων η εξαρτημένη μεταβλητή έχει ως εκκίνηση ακραίες τιμές. Σε τέτοιες καταστάσεις ελλοχεύει ο κίνδυνος οι αλλαγές που θα σημειωθούν να οφείλονται στο γεγονός της εκκίνησης (δηλαδή ότι οι μονάδες ανάλυσης εκκινούν από ακραία θέση) και όχι λόγω της επιρροής του πειράματος. Για παράδειγμα σε μια ομάδα ποδοσφαίρου η οποία κατέχει την τελευταία θέση στον βαθμολογικό πίνακα του πρωταθλήματος που συμμετέχει δοκιμάζεται μια νέα μέθοδος προπόνησης. Τότε η οποιαδήποτε βαθμολογική βελτιώσει της ομάδας δεν μπορεί να συνδεθεί με τη νέα μέθοδο προπόνησης (πείραμα) γιατί ακόμα και χωρίς αυτό το πειραματικό ερέθισμα (νέα μέθοδο προπόνησης) η βαθμολογική βελτίωση θα ήταν η μόνη αλλαγή που θα μπορούσε να γίνει. Υπάρχουν περιπτώσεις όπου κατά την διάρκεια του πειράματος οι μονάδες ανάλυσης, τα υποκείμενα δηλαδή, λέγεται ότι μπορεί να «πεθάνουν». Προφανώς δεν πρόκειται για βιολογικό θάνατο, αλλά για θάνατο σε επίπεδο έρευνας, δηλαδή αν για οποιοσδήποτε λόγο το υποκείμενο υποχρεωθεί να αποσυρθεί από το πείραμα μετά το στάδιο του προ-ελέγχου τότε εντάσσεται πλέον στην κατηγορία της «πειραματικής θνησιμότητας» αφού επηρεάζει τα τελικά αποτελέσματα.

Έλλειψη εξωτερικής εγκυρότητας. Είναι οι περιπτώσεις εκείνες κατά τις οποίες υπάρχει η πιθανότητα τα συμπεράσματα που προκύπτουν από πειραματικά αποτελέσματα να είναι αδύνατο να γενικευτούν και να εφαρμοστούν στον «πραγματικό» κόσμο[25].

2.3.3.7. Πλεονεκτήματα και μειονεκτήματα

Όπως σε όλα τα είδη ερευνών, έτσι και η διεξαγωγή έρευνας με πειραματικούς σχεδιασμούς έχει πλεονεκτήματα και μειονεκτήματα.

Πλεονεκτήματα. Η απομόνωση της επιρροής της ανεξάρτητης μεταβλητής ενός ελεγχόμενου πειράματος αποτελεί και το βασικότερο πλεονέκτημα αυτού του είδους ερευνών. Πρακτικά αυτό σημαίνει ότι η μεταβολή των στοιχείων από το στάδιο του προ-ελέγχου στο στάδιο του μετά-ελέγχου βασίζεται στην επιρροή του πειράματος στην περίπτωση που τα υποκείμενα δεν έχουν υποπέσει σε μεταβολή με κάποιον άλλο τρόπο. Επιπροσθέτως με την εφαρμογή των πειραματικών σχεδιασμών σε μια έρευνα δίνεται η δυνατότητα της επανάληψης κάτι που είναι πιο εύκολο από την επανάληψη σε δειγματοληπτική έρευνα.

Μειονεκτήματα. Το μειονέκτημα των ερευνών που βασίζονται στους πειραματικούς σχεδιασμούς είναι ότι στην πραγματικότητα είναι αδύνατο να απομονωθούν πλήρως οι συνθήκες διεξαγωγής του πειράματος και να εξαλειφθεί η προκατάληψη των υποκειμένων του πειράματος, π.χ. στις απαντήσεις που δίνουν κάθε φορά τα υποκείμενα.

2.3.3.8. Δεοντολογία και πειράματα

Από την διεξαγωγή ενός πειράματος προκύπτουν διάφορα ζητήματα όπως και στην έρευνα πεδίου. Κρίνεται σκόπιμο λοιπόν, τα υποκείμενα που συμμετέχουν στο πείραμα να μην γνωρίζουν ότι μελετώνται, γιατί έτσι υπάρχει κίνδυνος να δημιουργηθούν συνθήκες μεροληπτικότητας στη συμπεριφορά και στις απαντήσεις τους. Επιπλέον, στις μονάδες ανάλυσης από τη συμμετοχή τους σε ένα πείραμα μπορεί να δημιουργηθούν προβλήματα υγείας (αν πρόκειται για ιατρικό πείραμα) ή ψυχικά και σωματικά τραύματα[23].

2.3.4. Μη αντιδραστικές μέθοδοι ανάλυσης

Τα είδη ερευνών που έχουν παρουσιαστεί μέχρι τώρα προϋποθέτουν λίγο ή πολύ κάποια αλληλεπίδραση με τις μονάδες ανάλυσης που συμμετέχουν στην έρευνα.

Κατά κανόνα οι μονάδες ανάλυσης είναι οι άνθρωποι που καλούνται να δώσουν την απαραίτητη πληροφορία και γι' αυτό χρειάζεται να υπάρχει αλληλεπίδραση μεταξύ αυτών και του εκάστοτε ερευνητή.

Υπάρχουν όμως και μέθοδοι έρευνας που δεν προϋποθέτουν την αλληλεπίδραση του ερευνητή με τις μονάδες ανάλυσης. Αυτού του είδους οι έρευνες καλούνται και μη αντιδραστικές μέθοδοι.

Παραδείγματα μη αντιδραστικών ερευνών παρουσιάζει ο Eugene Webb στο βιβλίο του Unobtrusive Research (1966). Ο Webb κάνει έναν παραλληλισμό της δουλειάς που πρέπει να γίνει από τον ερευνητή με αυτή που κάνει ένας ντετέκτιβ προκειμένου να εξιχνιάσει ένα έγκλημα, μια υπόθεση. Ένα από τα παραδείγματα του που προκαλούν αίσθηση και εντυπωσιασμό, είναι αυτό, όπου ο ερευνητής προκειμένου να εξάγει συμπεράσματα για το πιο είναι το πιο ενδιαφέρον έκθεμα ενός μουσείου, παρατηρεί τη φθορά του ξύλινου πατώματος μπροστά από κάθε έκθεμα.

Οι μη αντιδραστικές μέθοδοι ερευνών διακρίνονται σε δυο τύπους, τις έρευνες περιεχομένου και τις έρευνες καταγεγραμμένων στατιστικών.

Έρευνες περιεχομένου. Πρόκειται για το είδος ερευνών οπού οι μονάδες ανάλυσης είναι καταγεγραμμένα αποτελέσματα ανθρώπινων δραστηριοτήτων και επικοινωνιών (π.χ. ιστοσελίδες, βιβλία, κ.λπ.).

Για παράδειγμα για μια έρευνα που ασχολείται με τις συνθήκες των εργαζομένων στο χρηματιστήριο της Νέας Υόρκης τη δεκαετία του 1970, ο ερευνητής θα μπορεί να χρησιμοποιήσει υλικό όπως συλλογή άρθρων από τις εφημερίδες της εποχής, φωτογραφίες, αγγελίες εφημερίδων για εργασία, δεδομένα με τις χρηματιστηριακές τιμές των μετοχών της εποχής, πολιτικό καθεστώς εκείνης της εποχής, κ.λπ..

Άλλη μια περίπτωση εφαρμογής της έρευνας περιεχομένου είναι η συσχέτιση των τηλεοπτικών διαφημίσεων με το περιεχόμενο των ταινιών ή εκπομπών που προβάλλονται. Για παράδειγμα η σύνδεση αντρικών κα γυναικείων προϊόντων με δημοσιογραφικές εκπομπές πολιτικού περιεχομένου (talk show). Αυτό το αποτέλεσμα θα επιβεβαιωθεί ή θα απορριφθεί με μια απλή και μόνο καταγραφή των διαφημίσεων που προβλήθηκαν στο επιθυμητό χρονικό διάστημα σε όλες τις εκπομπές πολιτικού

περιεχομένου της τηλεόρασης. Ακόμα μεγαλύτερο ενδιαφέρον παρουσιάζει η περίπτωση κατά την οποία αλλάζει ο προσανατολισμός των διαφημίσεων σε μια συγκεκριμένη πολιτική εκπομπή, δηλαδή, αν διαφοροποιείται το αποτέλεσμα της έρευνας όταν ο δημοσιογράφος της εκπομπής καλεί για συνέντευξη κάθε φορά ένα πολιτικό με διαφορετικό πολιτικό προσανατολισμό (π.χ. αριστερός, δεξιός, κ.λπ.).

Έρευνες καταγεγραμμένων στατιστικών. Τέτοιου είδους έρευνες είναι οι έρευνες στις οποίες χρησιμοποιούνται καταγεγραμμένα στατιστικά είτε πρωτογενών είτε επεξεργασμένων δεδομένων. Τα δεδομένα αυτά συνήθως παρέχονται από την Ελληνική Στατιστική Αρχή (ΕΛΣΤΑΤ), τη Eurostat (στατιστική υπηρεσία της Ευρωπαϊκής Ένωσης), διαφόρους άλλους επιστημονικούς οργανισμούς, όπως το Εθνικό Κέντρο Κοινωνικών Ερευνών (ΕΚΚΕ), τον Παγκόσμιο Οργανισμό Υγείας (ΠΟΥ) γνωστός με το διεθνές αρκτικόλεξο (WHO) World Health Organization, συνδικαλιστικούς φορείς, όπως την Ανώτατη Διοίκηση Ενώσεων Δημοσίων Υπαλλήλων (ΑΔΕΔΥ), τη Γενική Συνομοσπονδία Εργατών Ελλάδος (ΓΕΣΕΕ), κ.λπ..

Ως παράδειγμα θα μπορούσε να αναφερθεί έρευνα που θέλει να συσχετίσει την εκλογική απήχηση των δυο ή τριών κορυφαίων κόμματων σε μια χώρα με την οικονομική κατάσταση των πολίτων και κατ' επέκταση των ψηφοφόρων. Η συγκεκριμένη έρευνα θα μπορούσε να απαντήσει τεκμηριωμένα στο προς μελέτη ζήτημα αν είχε στην διάθεση της τα ποσοστά των κομμάτων και τα κατά κεφαλήν εισοδήματα των ψηφοφόρων.

2.3.4.1. Πλεονεκτήματα και μειονεκτήματα

Θα μπορούσε να πει κανείς πως οι έρευνες των μη αντιδραστικών μεθόδων έχουν μόνο πλεονεκτήματα. Πρώτα από όλα είναι από πιο τις οικονομικές μεθόδους και αυτό γιατί ως επί το πλείστων διεξάγονται από έναν ερευνητή που πρέπει να συλλέξει δεδομένα με μικρό ή μηδενικό κόστος. Επίσης η διόρθωση των σφαλμάτων στις μεθόδους αυτές μπορεί να γίνει στον σχεδιασμό ή στην καταγραφή. Γεγονός που έρχεται σε πλήρη αντίθεση με την διόρθωση σφαλμάτων στις δειγματοληπτικές έρευνες στις οποίες αν προκύψει πρόβλημα θα πρέπει να συλλεχθούν επιπλέον ομάδες ανάλυσης ή να μελετηθούν άλλα άτομα. Επιπροσθέτως σε σύγκριση με τους

πειραματικούς σχεδιασμούς και τις δειγματοληπτικές μεθόδους, οι μονάδες ανάλυσης σε τέτοιου είδους έρευνες δεν είναι άνθρωποι, συνεπώς, κατά την διεξαγωγή της έρευνας δεν δημιουργούνται ψυχικές και σωματικές βλάβες σε ανθρώπους (ή πειραματόζωα). Ακόμα δεν είναι απαραίτητο να ειπωθούν ψέματα με σκοπό την απόκρυψη της ιδιότητας του ερευνητή, όπως χρειάζεται να γίνει στις έρευνες πεδίου.

2.3.4.2 Δεοντολογία μη αντιδραστικών ερευνών

Στις περιπτώσεις των μη αντιδραστικών ερευνών ο ρόλος του ερευνητή είναι ευδιάκριτος, συνεπώς τα δεοντολογικά θέματα είναι μικρά έως ανύπαρκτα. Πρόβλημα μπορεί να υπάρχει μόνο σε ζητήματα προσωπικών δεδομένων όπως για παράδειγμα η δημοσιοποιήσει προσωπικών πληροφοριών σε έρευνα που κάνει χρήση αλληλογραφίας μέσω emails[23].

3. ΣΤΑΤΙΣΤΙΚΗ ΕΠΕΞΕΡΓΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΜΕ ΤΟ SPSSS

Εισαγωγή

Η στατιστική είναι ο κλάδος της επιστήμης που βοηθάει στην μελέτη και κατανόηση φαινομένων ή ιδιοτήτων πολυπληθών ομάδων, πληθυσμών. Η εφαρμογή της εκτείνεται σε πολλούς κλάδους της ανθρώπινης δραστηριότητας, π.χ. πολιτική, οικονομία, κοινωνιολογία, ιατρική, βιολογία, ψυχολογία.

Η ανάγκη για άμεση εφαρμογή της στατιστικής σε ποικίλες επιστήμες οδήγησε στην δημιουργία στατιστικών πακέτων τα οποία έχουν την δυνατότητα εισαγωγής, επεξεργασίας, ανάλυσης και παρουσίασης δεδομένων σε σύντομο χρονικό διάστημα. Φυσικά χάρη στην ανάπτυξη της τεχνολογίας των υπολογιστών υπάρχουν απεριόριστες πλέον δυνατότητες όσον αφορά τον όγκο των δεδομένων αλλά και την επεξεργασία τους.

Το SPSS (Statistical Package for Social Sciences) είναι ένα στατιστικό πακέτο που έχει πολλές δυνατότητες όσον αφορά την επεξεργασία και παρουσίαση των δεδομένων μιας επιστημονικής έρευνας αλλά και μεγάλη αξιοπιστία. Οι τελευταίες εκδόσεις του SPSS έχουν γραφικό περιβάλλον, πράγμα που το καθιστά πολύ εύκολο στη χρήση του.

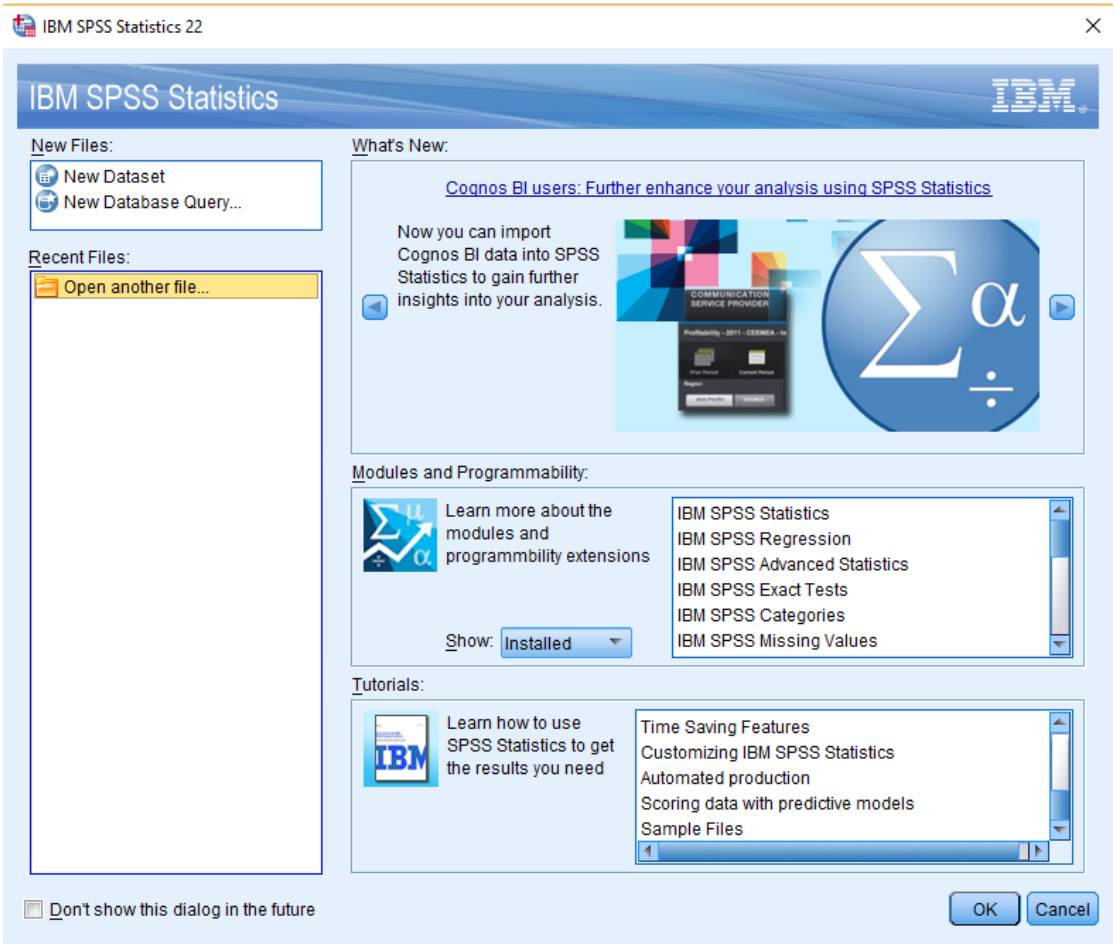
Στην συνέχεια ακολουθεί μία σύντομη εισαγωγή στο στατιστικό πακέτο SPSS22 που είναι το πιο διαδεδομένο στατιστικό πακέτο αυτήν τη στιγμή στην Ελλάδα. Γίνεται λόγος για την καταχώρηση δεδομένων στο SPSS καθώς και για τις βασικές εντολές διαχείρισης δεδομένων από το SPSS. Αρχικά γίνεται αναφορά στο περιβάλλον του και σε συγκεκριμένες επιλογές καθώς και στα φύλα Data View και Variable View. Επίσης, γίνεται αναφορά στον τρόπο καταχώρησης δεδομένων στο IBM SPSS, και στην κωδικοποίηση δεδομένων ερωτηματολογίων. Τέλος γίνεται μια μικρή αναφορά στα διαγράμματα μέσω του μενού Graphs.

3.1. Φύλλα εργασίας του SPSS

Με την ολοκλήρωση της εγκατάστασης του στατιστικού πακέτου SPSS22, μπορεί κανείς να προχωρήσει στη χρήση του για τη διεξαγωγή στατιστικών αναλύσεων

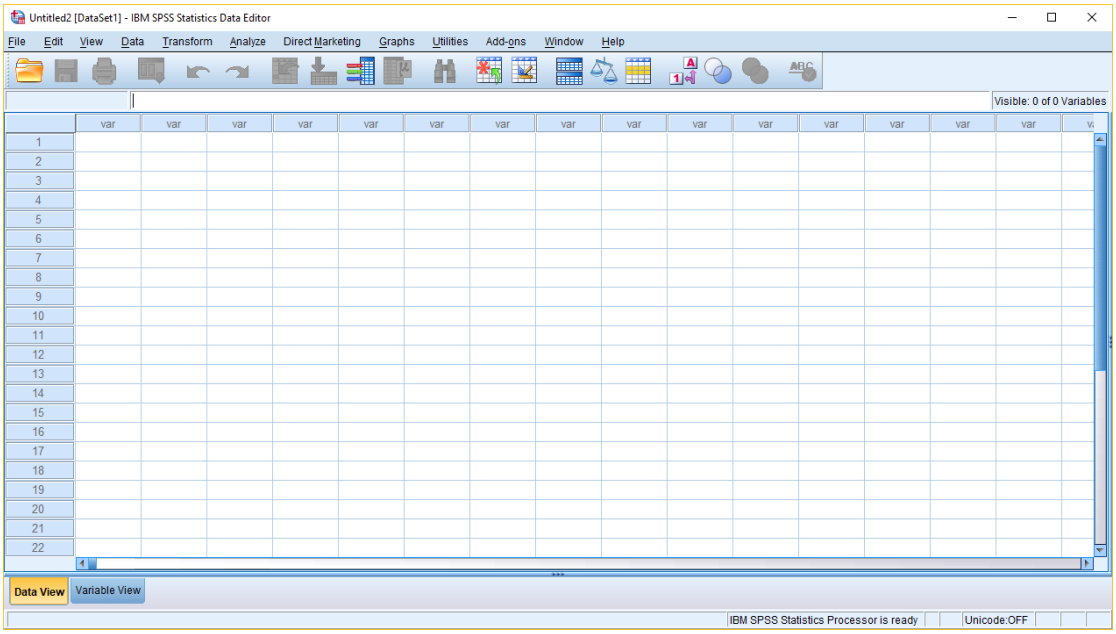
ή και μόνο στη συνοπτική παρουσίαση στατιστικών στοιχείων που πιθανόν να τον αφορούν. Για να ανοίξει το SPSS χρειάζεται διπλό κλικ πάνω στο εικονίδιο που βρίσκεται στην επιφάνεια εργασίας (αν υπάρχει) ειδάλλως από το μενού εργασιών των windows επιλέγοντας IBM Statistics SPSS22.

Μόλις η εφαρμογή φορτωθεί θα εμφανιστεί μία οθόνη γεμάτη κελιά, ένα κενό δηλαδή φύλο εργασίας του IBM SPSS Data Editor, όπως στην περίπτωση του Microsoft Office Excel, αλλά και το πλαίσιο διαλόγου της εικόνας 2. Στο παράθυρο που εμφανίζεται υπάρχει ένα ερώτημα σχετικά με το τι θέλει ο χρήστης με το SPSS να κάνει. Για την δημιουργία μιας νέας εργασίας επιλέγεται το New dataset επάνω δεξιά και μετά OK.

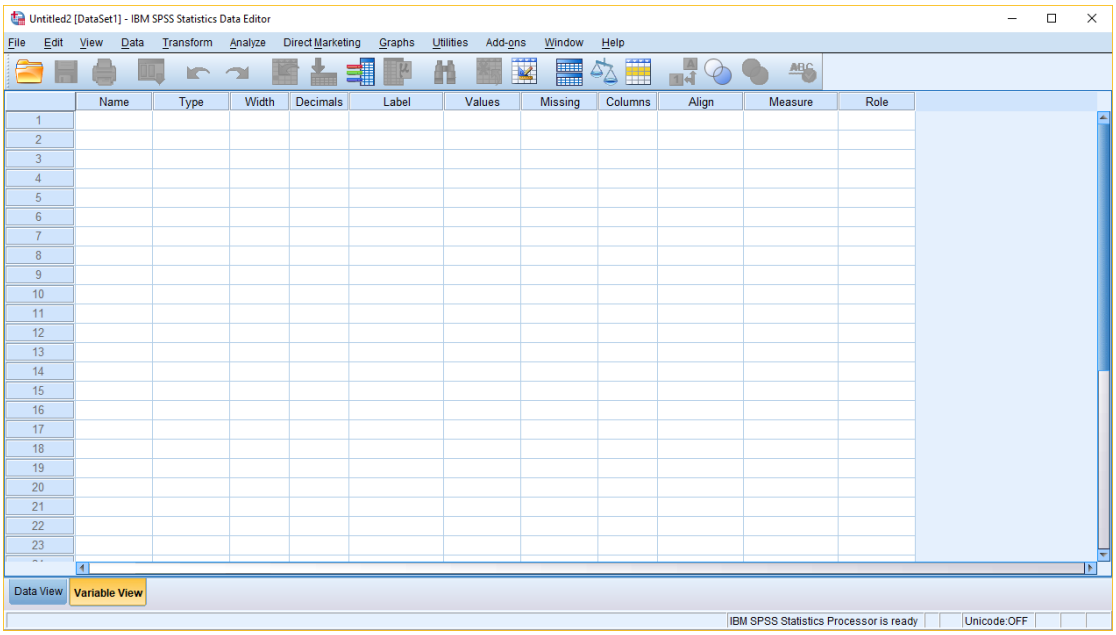


Εικόνα 2. Εισαγωγικό παράθυρο του SPSS

Στο SPSS υπάρχουν δύο βασικά αρχεία: το αρχείο δεδομένων (SPSS Data Editor), και το αρχείο αποτελεσμάτων (SPSS Viewer). Ο SPSS Data Editor είναι ένα φύλλο εργασίας, στο οποίο καταχωρούνται τα δεδομένα που πρόκειται να αναλυθούν. Ο SPSS Data Editor αποτελείται από δύο παράθυρα: Το Data View (Εικόνα 3) και το Variable View (Εικόνα 4). Στο πρώτο εισάγονται τα δεδομένα που θα αναλυθούν και στο δεύτερο ορίζονται τα δεδομένα αυτά, δηλαδή δίνονται επιμέρους στοιχεία για αυτά. Οι οριζόντιες γραμμές στο Data View ονομάζονται Cases (Περιπτώσεις) και είναι αριθμημένες με αύξουσα σειρά, ενώ οι στήλες αντιστοιχούν στις Variables (Στατιστικές Μεταβλητές).

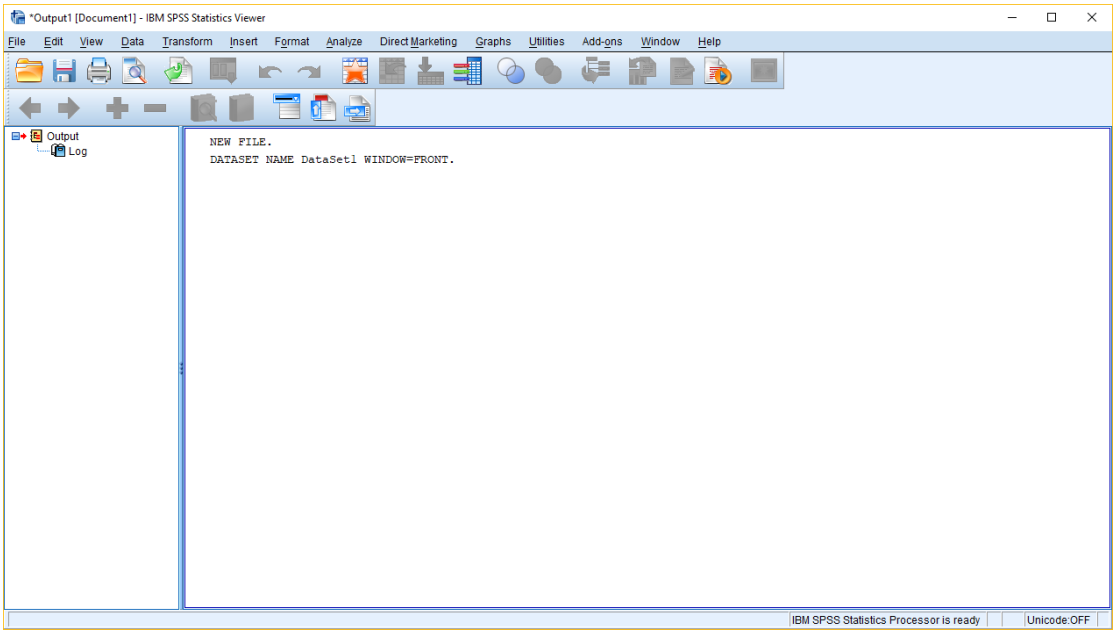


Εικόνα 3. Ο SPSS Data Editor στο Data View για εισαγωγή δεδομένων



Εικόνα 4. Ο SPSS Data Editor στο Variable View για μορφοποίηση δεδομένων

Ο SPSS Viewer είναι το αρχείο αποτελεσμάτων (Εικόνα 5). Στο αριστερό του παράθυρο, στο Output, εμφανίζονται οι στατιστικές πράξεις που έχουν γίνει και στο δεξιό τα στατιστικά αποτελέσματα.



Εικόνα 5. Ο SPSS Viewer για την παρουσίαση των αποτελεσμάτων

Η γραμμή τίτλου είναι η γραμμή που φαίνεται στο πάνω μέρος του παραθύρου. Το μενού επιλογών (menu bar) είναι παρόμοιο με αυτό που συναντάται στο Microsoft Office. Είναι η σειρά που φαίνεται κάτω από τη γραμμή τίτλου και περιλαμβάνει τις εξής επιλογές του παραθύρου: File, Edit, View, Data, Transform, Analyze, Direct Marketing, Graphs, Utilities, Add-ons, Window και Help. Οι ίδιες λέξεις υπάρχουν και στον SPSS Viewer, όπου όμως υπάρχουν επιπλέον και οι λέξεις Insert και Format. Οι ενέργειες που επιτρέπουν να γίνουν αυτές οι επιλογές είναι οι εξής:

- File: Άνοιγμα ενός νέου αρχείου (New), ή ενός παλιού (Open), αποθήκευση ενός αρχείου (Save), εκτύπωση (Print), κ.λπ..
- Edit: Τροποποίηση ή αντιγραφή τμημάτων του αρχείου δεδομένων.
- View: Προσαρμογή των διαφόρων στοιχείων του παραθύρου ανάλογα με τις επιλογές.
- Data: Πραγματοποίηση αλλαγών στα δεδομένα.
- Transform: Πραγματοποίηση αλλαγών στις μεταβλητές.
- Analyze: Πραγματοποίηση της στατιστικής ανάλυσης των δεδομένων.
- Direct Marketing: Περιέχει εφαρμογές για διαχείριση επιχειρησιακών δεδομένων.
- Graphs: Δημιουργία γραφικών παραστάσεων.
- Utilities: Πρόκειται για μια επιλογή γενικών χρήσεων. Για παράδειγμα, δίνονται πληροφορίες για μια μεταβλητή ή ένα αρχείο.
- Add-ons: Περιλαμβάνει πρόσθετες παροχές της IBM (εταιρείας-κατόχου του SPSS)
- Window: Δυνατότητες μετάβασης σε κάποιο άλλο ενεργό παράθυρο.
- Help: Προσφέρει διάφορα είδη βοήθειας.

Η γραμμή εργαλείων (toolbar) βρίσκεται κάτω από το μενού επιλογών και αποτελείται από εικονίδια χρήσιμα για λειτουργίες που χρησιμοποιούνται συχνά, όπως αποθήκευση, εκτύπωση, άνοιγμα κάποιου αρχείου. Οι γραμμές κύλισης βρίσκονται στα δεξιά και στο κάτω μέρος του παραθύρου και βοηθάνε την πάνω-κάτω και δεξιά-αριστερή μετακίνηση. Στο κάτω μέρος του παραθύρου (δεξιά) εμφανίζεται ένα μήνυμα

που λέει IBM SPSS Statistics Processor is ready. Η γραμμή αυτή στην οποία εμφανίζεται αυτό το μήνυμα είναι η γραμμή κατάστασης. Όταν το SPSS διεξάγει κάποιον υπολογισμό, ή έχει μία διεργασία σε εξέλιξη, ή τερματίσει μία οποιαδήποτε διεργασία θα εμφανίζεται το αντίστοιχο μήνυμα[26].

3.2. Καταχώριση δεδομένων στο SPSS

Ο απλούστερος τρόπος καταχώρησης δεδομένων σε ένα φύλλο εργασίας είναι με την απ' ευθείας πληκτρολόγηση των δεδομένων στο Data View. Ο βασικός κανόνας καταχώρισης δεδομένων στο Data View είναι ότι κάθε στήλη (column) στο Data View αντιστοιχεί σε μια μεταβλητή (variable) ή αλλιώς σε ένα χαρακτηριστικό της μελέτης, ενώ κάθε γραμμή (row) αντιστοιχεί στις απαντήσεις ενός ατόμου ή σε μια παρατήρηση (case) όπως συνηθίζεται να λέγεται στην στατιστική. Από τη διασταύρωση μίας στήλης και μίας γραμμής σχηματίζονται οι κυψέλες. Οι κυψέλες (cells) περιέχουν τιμές. Κάθε κυψέλη περιέχει μία μόνο τιμή μίας μεταβλητής για μία περίπτωση και περιέχουν αποκλειστικά δεδομένα (ενώ στα λογιστικά φύλλα οι κυψέλες περιέχουν και τύπους).

Με άλλα λόγια, σε κάθε στήλη καταχωρούνται οι απαντήσεις της ίδιας ερώτησης από το ερωτηματολόγιο μιας έρευνας, ενώ σε κάθε γραμμή καταχωρείται ένα διαφορετικό ερωτηματολόγιο (οι απαντήσεις ενός ατόμου). Έτσι αν για παράδειγμα διεξαχθεί έρευνα σε 50 άτομα χρησιμοποιώντας ένα ερωτηματολόγιο 8 ερωτήσεων, το Data View θα είναι ένας πίνακας δεδομένων με 8 στήλες και 50 γραμμές.

Επίσης είναι ευκόλως εννοούμενο ότι δεδομένα μπορούν να μεταφερθούν και από ένα φύλλο του Excel σε φύλλο του SPSS επιλέγοντας τα δεδομένα στο φύλλο του Excel, αντιγράφοντάς τα με Ctrl+C και επικολλώντας τα στο φύλλο του SPSS με Ctrl+V[27].

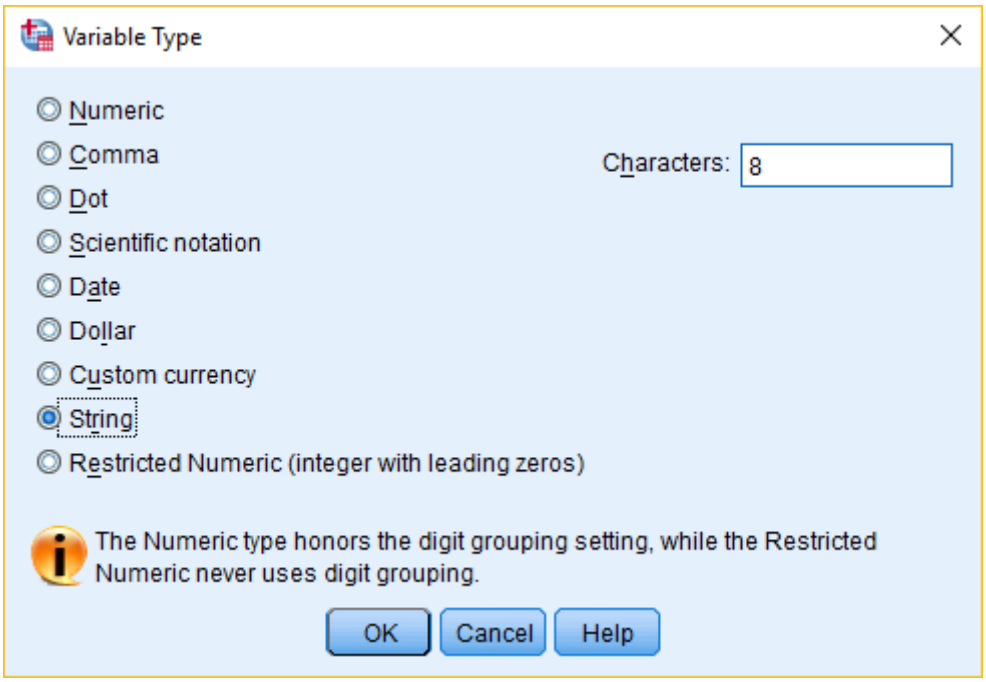
3.3. Μορφοποίηση δεδομένων

Στο SPSS κάθε μεταβλητή όπως έχει ήδη αναφερθεί εισάγεται σε μία ξεχωριστή στήλη στο παράθυρο Data View. Τα προς ανάλυση δεδομένα που εισάγονται για κάθε μεταβλητή μορφοποιούνται από το παράθυρο Variable View ως εξής:

- Στην πρώτη στήλη (Name) πληκτρολογεί κανείς τις επικεφαλίδες που θέλει να έχουν οι στήλες (Μεταβλητές) στο Data View (π.χ. sex, education, bday, height, bmass).
- Στη δεύτερη στήλη (Type) προσδιορίζεται ο τύπος των μεταβλητών. Κάνοντας κλικ σε ένα κελί αυτής της στήλης, στα δεξιά του κελιού εμφανίζεται ένα μικρό ορθογώνιο. Με κλικ στο ορθογώνιο αυτό εμφανίζεται ένα παράθυρο διαλόγου που επιτρέπει να επιλεγεί ο τύπος της μεταβλητής (Εικόνα 6). Εμφανίζονται οι ακόλουθες επιλογές: Numeric, Comma, Dot, Scientific notation, Date, Dollar, Custom currency και String. Η κάθε μία από τις 8 επιλογές αναλύεται πιο κάτω.

  Numeric (Αριθμητική). Χρησιμοποιείται εάν η απάντηση, που θα δοθεί σε μια μεταβλητή είναι κάποιος αριθμός. Αυτός ο αριθμός δεν εμφανίζει κάποιο κόμμα ή τελεία για τον προσδιορισμό των χιλιάδων, αλλά μόνο μια τελεία για τον προσδιορισμό των δεκαδικών ψηφίων. Για παράδειγμα ο τετραψήφιος αριθμός χίλια θα εμφανιστεί με τη μορφή 1000. Εάν όμως προστεθούν δύο δεκαδικά ψηφία ο αριθμός θα πάρει τη μορφή 1000.00. (Τα δεκαδικά εμφανίζονται με τελεία γιατί το πρόγραμμα είναι από τις Ηνωμένες Πολιτείες της Αμερικής όπου συνηθίζεται τα δεκαδικά να απεικονίζονται με τελεία, αντί με το κόμμα που χρησιμοποιείται στην Ελλάδα). Το μέγιστο μήκος είναι 60 ψηφία και το μέγιστο μήκος των δεκαδικών είναι 16 ψηφία.

  Comma (Κόμμα). Χρησιμοποιείται για τους μεγάλους αριθμούς και ο διαχωρισμός των χιλιάδων γίνεται με το κόμμα. Επομένως με την επιλογή Comma ορίζει κάποιος, ότι μια Numeric μεταβλητή θα εμφανίζει με κόμμα τις χιλιάδες και με τελεία το δεκαδικό κομμάτι. Δηλαδή ο αριθμός χίλια θα εμφανιστεί με τη μορφή 1,000 και αν προσθέσει κάποιος δύο δεκαδικά γίνεται 1,000.00.



Εικόνα 6. Παράθυρο για επιλογή τύπου δεδομένων - μεταβλητής

Dot (Τελεία). Είναι και αυτή μια Numeric μεταβλητή, που όμως διαφέρει από τις προηγούμενες αφού εμφανίζεται με τελεία για τον προσδιορισμό των χιλιάδων, ενώ τα δεκαδικά προσδιορίζονται με κόμμα. Δηλαδή στις μεταβλητές Dot ο αριθμός χίλια θα εμφανιστεί με τη μορφή 1.000 και αν προσθέσει κάποιος δεκαδικά γίνεται 1.000,00, ακριβώς όπως συνηθίζεται στην Ελλάδα.

Scientific notation (Επιστημονική σημείωση). Σ' αυτές τις μεταβλητές οι τιμές εμφανίζονται με τη μορφή επιστημονικής σημείωσης, π.χ. 8.35E2, 8.35D2, 8.35E+2 και 8.35+2.

Date (Ημερομηνία). Σε περίπτωση, που η μεταβλητή που καταχωρείται αναφέρεται σε κάποια ημερομηνία, με την επιλογή της μεταβλητής Date, εμφανίζεται πλαίσιο διαλόγου απ' όπου επιλέγει κάνείς τη μορφή με την οποία θέλει να εμφανίζεται η ημερομηνία.

Dollar (Δολάριο). Στην περίπτωση, που η μεταβλητή αναφέρεται σε νομίσματα δολαρίου ενεργοποιείται το αντίστοιχο είδος μεταβλητής. Από το πλαίσιο

διαλόγου που εμφανίζεται επιλέγει κάποιος τη μορφή και το δεκαδικό ψηφίο που θέλει να έχει η μεταβλητή.

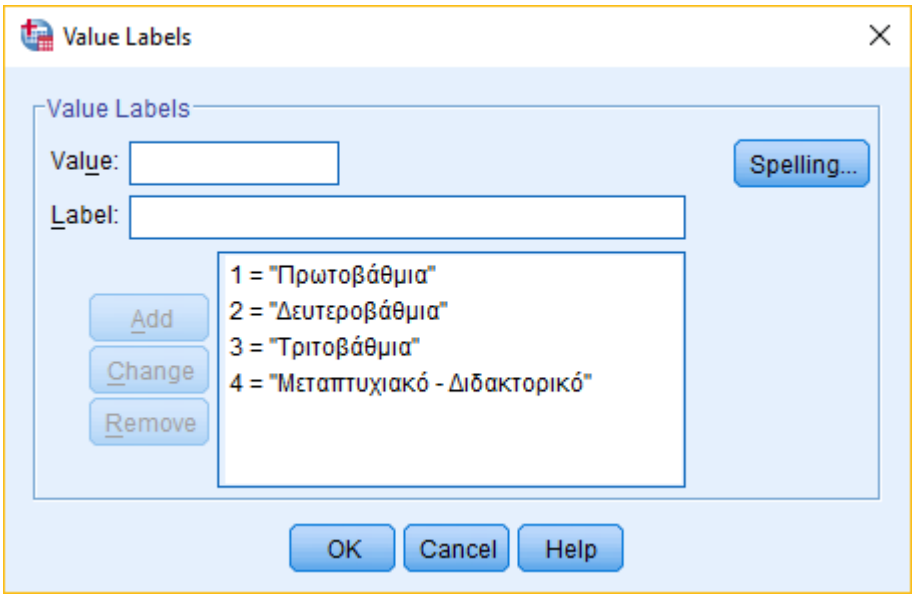
Custom currency (Συνηθισμένο νόμισμα). Στις περιπτώσεις που η μεταβλητή αναφέρεται σ' άλλο είδος νομίσματος εκτός δολαρίου τότε επιλέγεται το Custom currency και ακολουθείται η ίδια διαδικασία μ' αυτή της μεταβλητής Dollar.

String (Αλφαριθμητική σειρά χαρακτήρων). Οι μεταβλητές String αποτελούν μία σειρά από χαρακτήρες που συμπεριλαμβάνουν γράμματα, σύμβολα, αριθμούς και κενά. Για παράδειγμα εάν θέλει κάποιος να καταγράψει τα ονόματα όλων των ατόμων ή επιχειρήσεων που συμμετείχαν σε μια έρευνα, τότε αυτή η μεταβλητή πρέπει να είναι της μορφής String. Όμως για να γίνει κάτι τέτοιο πρέπει να ρυθμίσει κανείς το πρόγραμμα, ώστε να επιτρέψει να χρησιμοποιηθούν παραπάνω από οκτώ χαρακτήρες (Characters), αφού κάποιο ονοματεπώνυμο μπορεί για παράδειγμα να απαιτεί 30 χαρακτήρες. Για να γίνει αυτό αφού επιλέξει κανείς ότι η μεταβλητή του είναι String αυτόματα το πρόγραμμα εμφανίζει την επιλογή Characters, όπου μπορεί να αλλάξει κάποιος τον προεπιλεγμένο αριθμό από 8 σε 30. Κάτω από οκτώ χαρακτήρες λέγεται sort string και πάνω από οκτώ χαρακτήρες λέγεται long string[28].

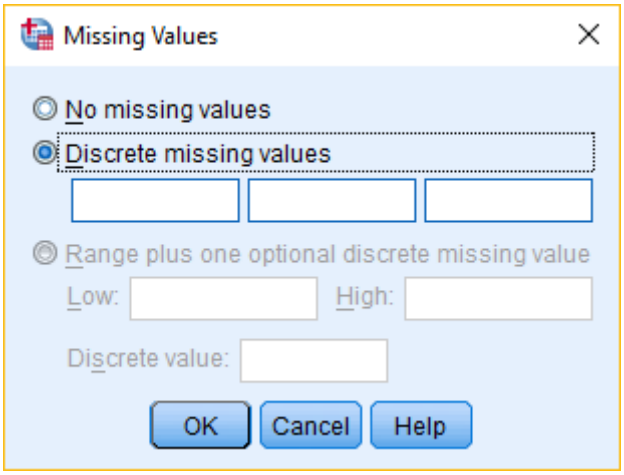
- Στη στήλη Width καθορίζετε το πόσα γράμματα μπορεί να έχει το όνομα της μεταβλητής.
- Στη στήλη Decimals καθορίζεται ο αριθμός των δεκαδικών ψηφίων των αριθμητικών μεταβλητών.
- Στη στήλη Label (Ετικέτες) δίνεται μια σύντομη περιγραφή της κάθε μεταβλητής.
- Στη στήλη Values εισάγονται πληροφορίες για τις τιμές της μεταβλητής όταν αυτή είναι κατηγορική. Η προεπιλογή είναι None και αφορά κυρίως τις ποσοτικές μεταβλητές. Έστω όμως για παράδειγμα μια μεταβλητή, η «Εκπαίδευση», η οποία παίρνει τις τιμές 1, 2, 3 και 4 ανάλογα με το επίπεδο μόρφωσης του καθενός. Σ' αυτή την περίπτωση, για καλύτερη πληροφόρηση του αναλυτή, με κλικ στο Values που αντιστοιχεί στη μεταβλητή «Εκπαίδευση»

και στην συνέχεια κλικ στο μικρό ορθογώνιο, ανοίγει το παράθυρο διαλόγου της Εικόνας 7. Στο πλαίσιο Value εισάγονται κάθε φορά οι τιμές 1, 2, 3 και 4, ενώ στο Label πληκτρολογούνται οι ετικέτες «Πρωτοβάθμια», «Δευτεροβάθμια», «Τριτοβάθμια» και «Μεταπτυχιακό – Διδακτορικό» σε πλήρη αντιστοιχία με τις τιμές του πλαισίου Value και κάθε φορά με κλικ στο Add προκύπτει η τελική μορφή της στήλης Value για την μεταβλητή «Εκπαίδευση» (Εικόνα 7).

- Στο κελί Missing ορίζονται οι χαμένες παρατηρήσεις (Εικόνα 8). Για παράδειγμα στην περίπτωση ενός ερωτηματολογίου όπου κάποιοι εκ των ερωτηθέντων δεν έχουν απαντήσει σε όλες τις ερωτήσεις. Πρέπει να δοθεί η απαιτούμενη προσοχή στον τρόπο ορισμού των χαμένων τιμών. Ενδεικτικά σε ένα ερωτηματολόγιο που οι απαντήσεις είναι σε κλίμακα Likert από 1 έως 5 τότε στις χαμένες τιμές θα δοθεί ένας αριθμός που δε βρίσκεται μεταξύ του 1 και του 5. Θα πρέπει να είναι δηλαδή ένας αριθμός που δε συναντάται στα δεδομένα της κάθε στήλης ξεχωριστά. Μπορεί κανείς να χρησιμοποιήσει μέχρι και τρεις διαφορετικές τιμές για να δηλώσει τις απούσες τιμές. Επίσης, μπορεί να ορίσει ένα εύρος απουσών τιμών, π.χ. όλες οι τιμές από 0 έως -10 να δηλώνουν πως τα κελιά είναι κενά, καθώς επίσης ένα εύρος τιμών και μία επιπλέον τιμή (π.χ. 0 έως -10, 333).



Εικόνα 7. Το παράθυρο διαλόγου Value Labels για τη μεταβλητή «Εκπαίδευση»



Εικόνα 8. Το παράθυρο διαλόγου Missing Values

- Στη στήλη Columns καθορίζεται το πλάτος που θα έχει η στήλη μιας μεταβλητής (πόσα ψηφία μπορεί να πάρει δηλαδή η μεταβλητή).
- Η στήλη Align καθορίζει τη στοίχιση των τιμών μιας μεταβλητής στη στήλη της με επιλογές Left (αριστερά), Right (δεξιά) και Center (κέντρο).

- Η στήλη Measure παρέχει ένα drop-down μενού που επιτρέπει σε κάποιον να διαλέξει τρεις επιλογές βασιζόμενος στη φύση των δεδομένων του: Nominal (ονομαστική κλίμακα), Ordinal (ιεραρχική κλίμακα), και Scale (ποσοτική κλίμακα) (περιλαμβάνονται οι γνωστές από τη στατιστική κλίμακες Interval (διαστήματος) και Ratio (Αναλογίας).

  Ονομαστικές Κλίμακες (Nominal). Αντιπροσωπεύουν το χαμηλότερο επίπεδο μέτρησης και απλά ταξινομούν τα δεδομένα σε κατηγορίες, δηλαδή κάθε τιμή προσδιορίζει απλά μία ξεχωριστή κατηγορία, αλλά δεν έχουν καμία εσωτερική διάταξη (λιγότερο σε περισσότερο). Τέτοιου είδους μεταβλητές που μετριόνται σε ονομαστική κλίμακα είναι ο τόπος γέννησης κάθε ανθρώπου, το φύλο, η εθνικότητα, η οικογενειακή κατάσταση, το χρώμα των ματιών κ.λπ.. Εάν έχει κάποιος numeric μεταβλητές, οι οποίες είναι nominal δεν μπορεί να εφαρμοσθούν πράξεις όπως άθροιση πολλαπλασιασμός κ.λπ. Για παράδειγμα, μια μεταβλητή που δηλώνει το φύλο και παίρνει τις τιμές f (γυναίκα) και m (άνδρας) είναι ονομαστική. Θα μπορούσε αντί για f και m να χρησιμοποιηθούν οι αριθμοί 1 και 2, αντίστοιχα. Και πάλι οι τιμές 1 και 2 θα ήταν ονομαστικές.

  Τακτικές Κλίμακες ή Ιεραρχικές Κλίμακες (Ordinal). Ταξινομούν τα δεδομένα, όπως και οι ονομαστικές κλίμακες αλλά επιπλέον καθορίζουν και μία σειρά (εσωτερική διάταξη) μεταξύ των κατηγοριών. Για παράδειγμα, όταν κάποιος κατηγοριοποιήσει ένα πληθυσμό με βάση το επίπεδο εκπαίδευσης ξέρει, ότι οι απόφοιτοι λυκείου είναι ανώτερο επίπεδο εκπαίδευσης από τους απόφοιτους δημοτικού, αλλά κατώτερο σε σχέση με τους απόφοιτους πανεπιστημίων.

  Σε μια κλίμακα επιθετικότητας από το 1 έως το 10 κάποιος που βρίσκεται υψηλότερα στην κλίμακα είναι πιο επιθετικός από κάποιον που βρίσκεται χαμηλότερα, αλλά κάποιος που είναι στο 4 δεν είναι δυο φορές πιο επιθετικός απ' αυτόν που είναι στο 2. Όπως και στην ονομαστική κλίμακα μέτρησης οι μαθηματικοί χειρισμοί συνήθως δεν σημαίνουν τίποτα

  Κλίμακες Διαστήματος ή Ισοδιαστημικές Κλίμακες και Κλίμακες Αναλογίας (Scale). Στις κλίμακες αυτής της κατηγορίας τα μέτρα κλίμακας

έχουν εσωτερική αριθμητική σημασία που επιτρέπει γενικούς μαθηματικούς χειρισμούς.

Οι κλίμακες διαστήματος (interval), όπως και οι τακτικές (ordinal) ταξινομούν και ιεραρχούν τις κατηγορίες αλλά επιπλέον ορίζουν και την απόσταση μεταξύ δύο κατηγοριών. Το πηλίκο ευφυίας, η θερμοκρασία (σε βαθμούς κελσίου) αποτελούν μεταβλητές ισοδιαστημικής κλίμακας. Οι κλίμακες αναλογίας (ratio) είναι ισοδιαστημικές κλίμακες με τη διαφορά ότι έχουν απόλυτο μηδέν. Απόλυτο μηδέν υπάρχει όταν η τιμή (0) σημαίνει τη παντελή έλλειψη ή απουσία αυτού που μετριέται. Ο χρόνος και το βάρος είναι αναλογικές μεταβλητές γιατί η τιμή (0) δείχνει τη παντελή έλλειψη του χρόνου ή του βάρους. Σε αντίθεση η τιμή μηδέν στο πηλίκο ευφυίας ή στη θερμοκρασία δεν σημαίνει την απουσία τους.

Η επιλογή Scale στο SPSS είναι η αρχικά καθορισμένη για τις αριθμητικές μεταβλητές.

Οι μεταβλητές που έχουν δύο μόνο κατηγορίες ή παίρνουν δύο τιμές, 0 και 1 ονομάζονται Δίτιμες ή Διχοτομικές ή μεταβλητές Binary και αποτελούν μία ιδιαίτερη κατηγορία όσον αφορά τη χρήση τους στη στατιστική. Έχουν την έννοια της κατάταξης και της απόστασης (πάντα σταθερή διαφορά), αλλά δεν είναι αναλογικές. Όλες οι ονομαστικές και τακτικές μεταβλητές μπορούν να μετατραπούν σε μία ή περισσότερες μεταβλητές δύο κατηγοριών (0,1).

Στο SPSS, ανεξάρτητα από το τι λέει η επιστήμη της στατιστικής, ισχύουν οι εξής κανόνες:

- Για τις διχοτομικές μεταβλητές ορίζει κάποιος πάντα κλίμακα μέτρησης Ordinal.
- Οι μεταβλητές String μετρούνται σε κλίμακα Nominal (χρησιμοποιούνται για κατηγοριοποίηση, αλλά δεν συμμετέχουν στις περισσότερες αναλύσεις).
- Οι μεταβλητές με προκαθορισμένες κατηγορίες τιμών μετρούνται σε Κλίμακα Ordinal. Αν υπάρχουν περισσότερες από 24 κατηγορίες (default), τότε η κλίμακα αλλάζει σε Scale.

- Οι μεταβλητές Numeric οι τιμές των οποίων είναι καθαροί αριθμοί μετρούνται σε κλίμακα Scale.

Μερικές φορές μπορεί να είναι δύσκολο να διαλέξει κάποιος μεταξύ κλίμακας και ιεράρχησης. Σε όλες τις αναλύσεις, το SPSS αντιμετωπίζει και τις δύο κατηγορίες μεταβλητών με τον ίδιο τρόπο. Εκείνο που διαφέρει είναι τα στατιστικά και οι αναλύσεις, που έχουν έννοια για κάθε περίπτωση.

Αξίζει να σημειωθεί, ότι τα στατιστικά μέτρα που εφαρμόζονται σε μεταβλητές ενός επιπέδου μετρησιμότητας μπορούν πάντα να χρησιμοποιηθούν για μεταβλητές υψηλότερου επιπέδου μετρησιμότητας, αλλά όχι για μεταβλητές χαμηλότερου επιπέδου μετρησιμότητας.

Ένας άλλος τρόπος υποδιαίρεσης των κλιμάκων μέτρησης των μεταβλητών είναι η κατηγοριοποίηση τους σε δύο επίπεδα: στις ασυνεχείς και στις συνεχείς. Στις ασυνεχείς ανήκουν οι ονομαστικές και διατεταγμένες κλίμακες, ενώ στις συνεχείς ανήκουν οι κλίμακες διαστήματος και οι αναλογικές[28].

3.4. Κωδικοποίηση δεδομένων

Στην περίπτωση που τα δεδομένα προέρχονται από ερωτηματολόγια, πρέπει να γίνει κατάλληλη προετοιμασία για την εισαγωγή των στοιχείων τους σε έναν υπολογιστή και την επεξεργασία τους με τη βοήθεια του προγράμματος SPSS.

Πρώτα από όλα θα πρέπει να γίνει μια κωδικοποίηση των ερωτηματολογίων, δηλώνοντας στο κάθε ερωτηματολόγιο έναν μοναδικό κωδικό, ώστε στο μέλλον να είναι κανείς σε θέση να γνωρίζει από ποιο ερωτηματολόγιο προέρχονται οι παρατηρήσεις των μεταβλητών του. Η συγκεκριμένη κωδικοποίηση καταγράφεται σχεδόν πάντα στην πρώτη στήλη του λογιστικού φύλλου.

Για τη στατιστική επεξεργασία των ερωτηματολογίων πρέπει να δημιουργηθεί και ένας πίνακας κωδικοποίησης. Ο πίνακας αυτός αντιστοιχίζει κάθε ερώτηση του ερωτηματολογίου σε μια μεταβλητή. Για παράδειγμα, η ερώτηση «Φύλο» αντιστοιχίζεται στη μεταβλητή «Φύλο». Οι μεταβλητές λαμβάνουν διάφορες τιμές. Η μεταβλητή «Φύλο» έχει δύο πιθανές τιμές: «Άνδρας», «Γυναίκα». Όταν τα δεδομένα,

οι παρατηρήσεις, οι τιμές των μεταβλητών, ή αλλιώς οι απαντήσεις των ερωτήσεων είναι περιγραφικές, όταν δηλαδή υπάρχουν ποιοτικές μεταβλητές, τότε κωδικοποιούνται οι απαντήσεις, και στο λογιστικό φύλλο καταγράφονται απευθείας οι κωδικοποιήσεις αυτών. Για παράδειγμα, για τη μεταβλητή «Φύλλο» μπορούμε να ορίσουμε «1 - Άνδρας» και «2 - Γυναίκα». Έτσι στην καταγραφή των δεδομένων θα γραφτούν απευθείας οι τιμές «1» και «2», αντίστοιχα. Η συγκεκριμένη προσέγγιση εκτός από το γεγονός ότι εξυπηρετεί την πιο γρήγορη καταγραφή των δεδομένων, ενισχύει τη βέλτιστη ποιότητα δεδομένων, καθώς εάν χρησιμοποιούνταν String / Text τιμές, υπάρχει κίνδυνος διαφορετικότητας μεταξύ ιδίων τιμών, αφού μια τιμή «άνδρας» (με μικρό άλφα) είναι διαφορετική από την τιμή «Άνδρας» (με κεφαλαίο άλφα).

Υπάρχουν επίσης περιπτώσεις ερωτηματολογίων όπου μπορεί να συναντήσει κανείς πολυπληθείς ομάδες ερωτήσεων, για τις οποίες για την πιο γρήγορη και άμεση καταγραφή τους ορίζετε μια σύντομη περιγραφή, όπως «Q001», «Q002» κ.ο.κ. Ωστόσο, η πλήρης περιγραφή καταγράφεται, όπως έχει προαναφερθεί, στο πεδίο Label της ενότητας Variable View.

Καλό θα είναι πριν από οποιαδήποτε καταγραφή των δεδομένων, να υπάρχει μια αρχική συνεννόηση του αναλυτή με τους καταχωρητές, προκειμένου να αποφεύγονται μελλοντικά προβλήματα, δυσκολίες και ταλαιπωρία του αναλυτή κατά τον «καθαρισμό» των δεδομένων[23].

3.5. Γραφική παρουσίαση των δεδομένων

Από τις κρισιμότερες ενέργειες - αποφάσεις του ερευνητή που ενδιαφέρεται να παρουσιάσει ευρήματα κατανομών (και όχι μόνο), είναι η περιεκτική και αντιπροσωπευτική (γραφιστική) απόδοσή τους με τη βοήθεια κατάλληλων (γραφικών) παραστάσεων. Μια γραφική παράσταση οφείλει να είναι: παραστατική, διευκολύνοντας την αναγνώριση και κατανόηση των βασικών χαρακτηριστικών της εξεταζόμενης μεταβλητής, σαφής, αποφεύγοντας τις συγχύσεις ανάμεσα στις τιμές των μεταβλητών και ακριβής, ώστε να αποφεύγονται οι (οπτικές συνήθως) πλάνες.

Στη γραμμή τίτλου του SPSS περιλαμβάνεται η επιλογή Graphs η οποία δίνει τη δυνατότητα γραφικής απεικόνισης των δεδομένων μέσω προκαθορισμένων τύπων

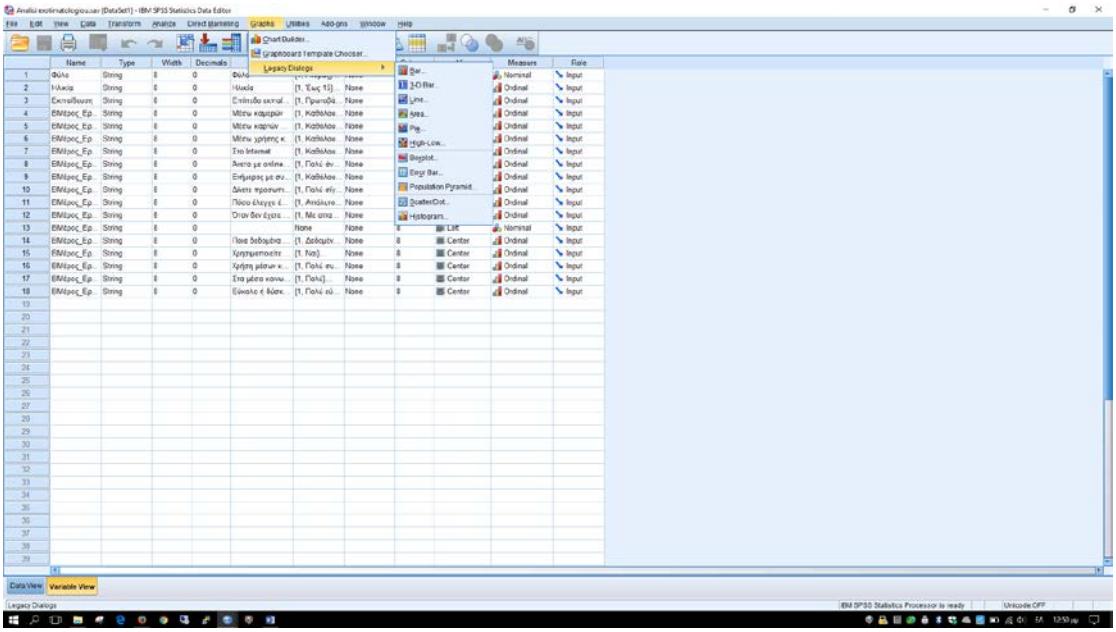
διαγραμμάτων. Γράφημα (plot) ονομάζεται μια γραφική αναπαράσταση μιας ή περισσότερων μεταβλητών. Τα γραφήματα είναι χρήσιμα διότι παρέχουν άμεση πληροφόρηση για το σχήμα και τη μορφή της κατανομής των μεταβλητών, ή την από κοινού σχέση τους.

Στο μενού της επιλογής Graphs υπάρχουν οι επιλογές Legacy Dialogs και Chart Builder. Η Legacy Dialogs διαφέρει από την επιλογή Chart Builder στο ότι επιτρέπει να δημιουργηθούν βασικά γραφήματα επιλέγοντας εκ των προτέρων το είδος του γραφήματος που θα δημιουργθεί.

Το Chart Builder, ωστόσο, είναι μια πραγματική μηχανή γραφικών που δημιουργήθηκε με την προσαρμογή του προγράμματος στην εξέλιξη της τεχνολογίας για να προσφέρει στους χρήστες μεγαλύτερη ευελιξία στη γραφική απεικόνιση, οδηγώντας τον χρήστη καθώς του παρέχει τη δυνατότητα να βλέπει πώς θα διαμορφωθεί το γράφημα με κάθε επιλογή του και μοιάζει πολύ με τον τρόπο δημιουργίας γραφημάτων του Excel.

Όμως μπορεί να παρατηρήσει κανείς ότι τα ραβδογράμματα και κυκλικά διαγράμματα γίνονται ιδιαίτερα εύκολα με το SPSS. Αυτό είναι αναμενόμενο δεδομένου ότι το SPSS έχει σχεδιαστεί για αυτή τη δουλειά, ενώ το Excel έχει δημιουργηθεί για πολύ ευρύτερες χρήσεις. Όλα τα διαγράμματα μπορούν να μεταφερθούν σε άλλο πρόγραμμα π.χ. Word, Powerpoint με τη διαδικασία αντιγραφής Copy, επικόλλησης Paste.

Οι τύποι των διαγραμμάτων που προσφέρονται από την επιλογή Legacy Dialogs (Εικόνα 9) είναι τα Ραβδογράμματα Bar Charts (Simple και Clustered), τα Γραμμικά Line (επιλογές Simple και Multiple) τα Γραφήματα Περιοχής Area, τα Κυκλικά Pie, τα Υψηλών - Χαμηλών τιμών High - Low (επιλογές Simple και Clustered) τα Θηκογράμματα ή Πλαισίου Απολήξεων BoxPlots (επιλογές Simple και Clustered), τα Διασποράς Scatter/ Dot (επιλογές Simple και Matrix και Scatter) και τα Ιστογράμματα, Histogram[23].



Εικόνα 9. Τύποι γραφημάτων που παρέχονται από την επιλογή Legacy Dialogs

4. ΤΟ ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ

Εισαγωγή

Ο πιο διαδεδομένος τρόπος συγκέντρωσης πρωτογενών πληροφοριών είναι αυτός που επιτυγχάνεται με τη χρησιμοποίηση ερωτηματολογίων, στα οποία καταχωρούνται από τους ερωτώμενους ή από τους ερευνητές οι σχετικές πληροφορίες.

Υπάρχουν πληθώρα είδη ερωτηματολογίων που έχουν ήδη εφαρμοστεί σε πολλές έρευνες. Οι διαφοροποιήσεις μεταξύ των ερωτηματολογίων υπάρχουν όχι μόνο αναφορικά με το αντικείμενο μελέτης τους αλλά και με την μορφή τους, καθώς κάποια ερωτηματολόγια βασίζονται μόνο σε εικόνες και δεν χρησιμοποιούν καθόλου τον γραπτό λόγο εν αντιθέσει με άλλα που χρησιμοποιούν μόνο τον γραπτό λόγο.

Το ερωτηματολόγιο αποτελεί το θεμελιώδες στοιχείο σε κάθε δειγματοληπτική έρευνα, αλλά και στα πειράματα, στις έρευνες πεδίου και σε άλλες δραστηριότητες όπου απαιτείται η συγκέντρωση πληροφοριών, στοιχείων και δεδομένων. Η κατασκευή λοιπόν ενός ερωτηματολογίου είναι πολύ σημαντική, επειδή αυτό παρέχει ουσιαστικά τα δεδομένα της έρευνας.

4.1. Η δημιουργία

Η διαδικασία ανάπτυξης και σύνταξης ενός ερωτηματολογίου αποτελεί ίσως το δυσκολότερο στάδιο μιας έρευνας, μιας και η επιτυχία της έρευνας εξαρτάται άμεσα από αυτό. Αν και δεν υπάρχει ένα σαφές και αναλυτικό μεθοδολογικό πλαίσιο για το σχεδιασμό του ερωτηματολογίου μιας οποιασδήποτε έρευνας, θα πρέπει σε γενικές γραμμές να τηρούνται κάποιοι βασικοί κανόνες για να είναι αξιοποιήσιμη η πληροφορία που προκύπτει.

Για τη φρασεολογία του ερωτηματολογίου θα πρέπει να λαμβάνεται υπόψη ο βαθμός εκπαίδευσης των ερωτώμενων και οι τυχόν ιδιωματισμοί των διαφόρων γεωγραφικών περιοχών. Το ερωτηματολόγιο θα πρέπει να είναι απλό, ώστε να γίνεται εύκολα κατανοητό από τους ερωτηθέντες. Ο ερωτώμενος πρέπει να αντιλαμβάνεται εύκολα τις ερωτήσεις, χωρίς να χρειάζεται ιδιαίτερη προσπάθεια και ιδιαίτερες οδηγίες.

Όσον αφορά στην εμφάνιση του ερωτηματολογίου θα πρέπει να υπάρχει στην αρχή της πρώτης σελίδας ο τίτλος έρευνας, ο φορέας που την πραγματοποιεί και η διεύθυνση του. Επίσης, αν υπάρχει, να αναφέρεται η νομική διάταξη που νομιμοποιεί την έρευνα, καθώς και η ρητή δήλωση ότι οι σχετικές ατομικές πληροφορίες είναι εμπιστευτικές και θα δημοσιευθούν μόνο με τη μορφή συγκεντρωτικών πινάκων. Αν το ερωτηματολόγιο αποστέλλεται ταχυδρομικά, θα πρέπει να αναγράφεται η ημερομηνία αποστολής και η ημερομηνία μέχρι την οποία αναμένεται η απάντηση.

Επιπροσθέτως, θα πρέπει οι ερωτήσεις να είναι διατεταγμένες με μια λογική τάξη. Η αλληλουχία που θα ακολουθείται στην δομή του ερωτηματολογίου θα πρέπει να διασφαλίζει την εύκολη συμπλήρωση του, ώστε αφενός να μεγιστοποιείται η ανταπόκριση των ερωτηθέντων και αφετέρου να διασφαλίζεται η εγκυρότητα της συλλεγόμενης πληροφορίας. Οι ερωτήσεις που αφορούν στα στοιχεία του ερωτώμενου (την ταυτότητα) όπως φύλο, ηλικία, επίπεδο μόρφωσης κ.λπ. πρέπει να είναι συγκεντρωμένες στην αρχή, και οι υπόλοιπες, αν είναι δυνατό, χωρισμένες σε ομοιογενείς ομάδες.

Το ερωτηματολόγιο πρέπει να καταρτίζεται κατά τέτοιο τρόπο ώστε ο ερωτώμενος να αντιλαμβάνεται εύκολα τις ερωτήσεις και να μπορεί να απαντά με ακρίβεια, σαφήνεια και ταχύτητα σε αυτές. Οι ερωτήσεις που θα περιλαμβάνει πρέπει να είναι συγκεκριμένες, ώστε να ελαχιστοποιείται η πιθανότητα δημιουργίας σύγχυσης. Οι προς συγκέντρωση επιθυμητές πληροφορίες, πρέπει να διατίθενται εύκολα από τον ερωτώμενο και να αποφεύγονται ερωτήσεις που αναφέρονται στο παρελθόν που χρειάζονται υπολογισμούς. Επίσης, οι ερωτήσεις πρέπει να είναι όσο το δυνατό λιγότερες, ώστε να αποφεύγεται η άρνηση, η καταπόνηση και η προχειρότητα στις απαντήσεις από τους ερωτώμενους.

Η διατύπωση των ερωτήσεων δεν πρέπει να επηρεάζει τις απαντήσεις των ερωτώμενων, αντίθετα μάλιστα, οφείλει να τους βοηθά ώστε να μπορούν να δώσουν τις ορθές γι' αυτούς απαντήσεις. Για αυτό το σκοπό πρέπει να επιδιώκεται η αφαίρεση από τον ερωτώμενο, της οποιαδήποτε πρωτοβουλίας ερμηνείας των ερωτημάτων. Όταν η ερώτηση αναφέρεται σε ποιοτικό χαρακτηριστικό, θα πρέπει να αναγράφονται όλες οι δυνατές κατηγορίες του, ώστε ο ερωτώμενος να μπορεί να δηλώσει αυτή στην οποία

ανήκει. Έχει παρατηρηθεί ότι υπάρχει η τάση των ερωτώμενων να στρογγυλοποιούν τα ποσοτικά χαρακτηριστικά. Αυτό μπορεί να αποφευχθεί με έμμεση ή τροποποιημένη ερώτηση, π.χ. δεν γίνεται ερώτηση για την ηλικία άλλα για την ημερομηνία γέννησης.

Σε ένα ερωτηματολόγιο οι ερωτήσεις μπορούν να είναι δύο ειδών: είτε κλειστού τύπου όπου ο ερωτώμενος καλείται να επιλέξει μεταξύ συγκεκριμένων απαντήσεων είτε ανοιχτού τύπου όπου ο ερωτώμενος απαντά στην ερώτηση συμπληρώνοντας το κενό περιθώριο που προβλέπεται για να καταχωρίσει την απάντησή του. Έτσι η επιλογή της μορφής των ερωτήσεων γίνεται με κριτήριο την αποτελεσματικότητα, την ευελιξία, το ενδιαφέρον, την ομοιογένεια και κυρίως την καταλληλόλητα στην επεξεργασία των δεδομένων.

Προφανώς οι κλειστές ερωτήσεις υπερτερούν στην ευκολία ανάλυσης των δεδομένων, ενώ οι ανοιχτές δίνουν επιπλέον δυνατότητα στον ερωτώμενο να ξεδιπλώσει τη σκέψη του. Σε γενικές γραμμές θα πρέπει να προηγούνται ανοιχτές ερωτήσεις με ανάλογο περιεχόμενο και κλειστές, που θα έπονται.

Η αποστολή των ερωτηματολογίων, για να συμπληρωθούν, μπορεί να γίνει ταχυδρομικά ή με ερευνητές. Η διακίνηση των ερωτηματολογίων με το ταχυδρομείο (αποστολή - επιστροφή) είναι η λιγότερο δαπανηρή μέθοδος, διότι απαλλάσσει από την δαπανηρή παρουσία των ερευνητών. Η διακίνηση των ερωτηματολογίων με τους ερευνητές, εξασφαλίζει τη συγκέντρωση των σωστών και με πληρότητα συμπληρωμένων ερωτηματολογίων. Επίσης ο τρόπος αυτός επιτρέπει να αποφεύγονται τα συστηματικά σφάλματα που οφείλονται στην ταχυδρομική διακίνηση. Δεν είναι δυνατό π.χ. να απαντήσει διαφορετικό πρόσωπο από αυτό που έχει επιλεγεί, με συνέπεια να αποφεύγεται η παραμόρφωση του δείγματος.

Για το σκοπό της συγκεκριμένης έρευνας συντάχθηκε ερωτηματολόγιο που εξυπηρετεί τον σκοπό αυτό λαμβάνοντας υπόψη όλους τους παραπάνω βασικούς κανόνες. Το ερωτηματολόγιο της παρούσας μελέτης αποτελείται από τρία μέρη:

Α. Μέρος. Το πρώτο μέρος περιλαμβάνει γενικές ερωτήσεις με σκοπό να αποτυπωθούν τα δημογραφικά χαρακτηριστικά του προς μελέτη πληθυσμού.

Β. Μέρος. Το δεύτερο μέρος εμπεριέχει ερωτήσεις στο κατά πόσο οι πολίτες γνωρίζουν τη νομοθεσία για την προστασία προσωπικών δεδομένων και στις γνώσεις

και δεξιότητες αναφορικά με τη πλοήγησή τους στο διαδίκτυο και τη χρήση συναφών υπηρεσιών και μέσων κοινωνικής δικτύωσης.

Γ. Μέρος. Το τρίτο μέρος επικεντρώνεται σε ερωτήσεις που αφορούν στην ιστοσελίδα (www.dpa.gr) και το ενημερωτικό δελτίο (newsletter) της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και στο κατά πόσο οι πολίτες γνωρίζουν την ύπαρξή τους. Για πρώτη φορά επιχειρείται η αξιολόγηση του περιεχόμενου, της σχεδίασης τους, της πλοήγηση στην ιστοσελίδα και της ανάγνωσης του newsletter.

4.2. Η κλίμακα

Με τη βοήθεια αυτού του απλού αλλά και συνάμα εξειδικευμένου ερωτηματολογίου δίνεται η δυνατότητα σε κάθε ερωτηθέντα να αξιολογήσει αφενός τις γνώσεις του σχετικά με τα προσωπικά δεδομένα και την πλοήγηση στο διαδίκτυο και αφετέρου τη συνολική αλλά και την επιμέρους ικανοποίηση του για την ιστοσελίδα (www.dpa.gr) και το ενημερωτικό δελτίο (newsletter) της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Οι συγκεκριμένες προτιμήσεις εκφράζονται με τη βοήθεια μιας προκαθορισμένης κλίμακας ικανοποίησης.

Ο καθορισμός των διαστάσεων ικανοποίησης αποτελεί ένα από τα σημαντικότερα βήματα ανάπτυξης του ερωτηματολογίου μιας έρευνας ικανοποίησης. Ο όρος «διάσταση ικανοποίησης» συχνά αναφέρεται ως χαρακτηριστικό μέτρο αποτελεσματικότητας, μέτρο απόδοσης ή κριτήριο.

Υπάρχουν διάφορες κλίμακες ικανοποίησης ανάλογα με τον τρόπο παρουσίασης όπως η ονομαστική κλίμακα (nominalscale), η βαθμιδωτή κλίμακα (ordinal scale), η κλίμακα διαστήματος (interval scale), η κλίμακα αναλογίας (ratio scale), οι λεκτικές κλίμακες (verbal scales), οι αριθμητικές κλίμακες (numeric scales) και οι γραφικές κλίμακες (pictorial scales).

Υπάρχουν όμως και οι κλίμακες που βασίζονται στο αντικείμενο μέτρησης και

είναι οι κλίμακες επιβεβαίωσης (confirmation), το αίσθημα ικανοποίησης (satisfaction feeling), τα αποτέλεσμα ικανοποίησης (satisfaction outcome) και απόδοσης (performance).

Οι κλίμακες ικανοποίησης που συνήθως χρησιμοποιούνται είναι οι λεκτικές των 4 ή 5 βαθμίδων και οι γραφικές με τα πρόσωπα, οι οποίες είναι πιο ευχάριστες και λιγότερο συνηθισμένες, προκαλώντας το ενδιαφέρον των ερωτηθέντων. Κάθε έρευνα χρησιμοποιεί την κλίμακα εκείνη που της επιτρέπει να βγάλει σωστά και ασφαλή αποτελέσματα ανάλογα με το μοντέλο επεξεργασίας των στοιχείων που χρησιμοποιεί (Σιάρδος, 2004).

Για το σκοπό της συγκεκριμένης έρευνας χρησιμοποιήθηκε η λεκτική κλίμακα των 4 ή 5 βαθμίδων. Το μέγεθος αυτό της (4-βάθμιας) ή της (5-βάθμιας) κλίμακας κρίθηκε κατάλληλο γιατί αφενός δεν είναι ιδιαίτερα μικρό και εξασφαλίζεται η ακρίβεια των αποτελεσμάτων και αφετέρου ούτε πολύ μεγάλο με αποτέλεσμα ο ερωτηθέντας να μην συναντήσει δυσκολία στην ερμηνεία και στη διάκριση των επιπέδων της κλίμακας. Αντιθέτως τοποθετώντας πολλά επίπεδα μπορεί κανείς να συναντήσει δυσκολία στην εκτίμηση της διαφοράς ανάμεσα στα επίπεδα της κλίμακας.

Στο ειδικό ερωτηματολόγιο της έρευνας εκτός από τις ερωτήσεις ικανοποίησης συμπεριλαμβάνονται επίσης και ερωτήσεις μονής επιλογής.

4.3. Το δείγμα, η εποχή, ο τόπος διεξαγωγής της έρευνας, αξιοπιστία και εγκυρότητα

Η Επιτροπή Υπουργών του Συμβουλίου της Ευρώπης έχει καθιερώσει, από το 2006, την 28η Ιανουαρίου ως Ευρωπαϊκή Ημέρα Προστασίας Προσωπικών Δεδομένων. Ο εορτασμός της ημέρας αυτής αποσκοπεί στην ευαισθητοποίηση των πολιτών σε θέματα προστασίας προσωπικών δεδομένων. Με αφορμή τον εορτασμό της 11ης Ευρωπαϊκής Ημέρας Προστασίας Προσωπικών Δεδομένων 2017, η Αρχή διοργάνωσε την Πέμπτη 26 Ιανουαρίου, την Πέμπτη 2 Φεβρουαρίου και την Πέμπτη 9 Φεβρουαρίου στην Αίθουσα Σεμιναρίων της, Λ. Κηφισίας 1-3, Αθήνα (1ος όροφος), ενημερωτικές ημερίδες.

Η έρευνα αυτή διεξήχθη στη διάρκεια των τριών ενημερωτικών ημερίδων για τον εορτασμού της 11ης Ευρωπαϊκής Ημέρας Προστασίας Προσωπικών Δεδομένων. Κρίθηκε σκόπιμο για την εξασφάλιση της αποτελεσματικότητας και εγκυρότητας, η διεξαγωγή της έρευνας να γίνει την συγκεκριμένη χρονική περίοδο. Η συμμετοχή των ερωτηθέντων στις τρεις αυτές ενημερωτικές ημερίδες πιστοποιούσε το γεγονός ότι έστω και μια φορά έχουν περιηγηθεί στην ιστοσελίδα της Αρχής με αποτέλεσμα η γνώμη τους για το περιεχόμενο, τη σχεδίαση και την πλοήγηση στην ιστοσελίδα, θα ήταν όσο το δυνατόν πιο έγκυρη με αποτέλεσμα να προκύψουν ασφαλέστερα συμπεράσματα.

Πρόκειται δηλαδή, για περίπτωση μη πιθανοτικής δειγματοληψίας διότι η εξαγωγή του δείγματος δε βασίστηκε σε τεχνικές που χρησιμοποιούν οι νόμοι των πιθανοτήτων. Αυτό το είδος δειγματοληψίας χρησιμοποιείται συνήθως σε πιλοτικές έρευνες. Η μέθοδος μη πιθανοτικής δειγματοληψίας που χρησιμοποιήθηκε είναι η «Δειγματοληψία ευκαιρίας». Έγινε δηλαδή προσπάθεια συλλογής όσο το δυνατό μεγαλύτερου δείγματος στο οποίο υπήρχε εύκολη πρόσβαση. Ένα αντίστοιχο παράδειγμα ευκαιριακής δειγματοληψίας είναι η διεξαγωγή έρευνας για την καταγραφή της ικανοποίησης των πελατών ενός καταστήματος μοιράζοντας ερωτηματολόγια στους πελάτες που βρίσκονται στο κατάστημα μια μόνο συγκεκριμένη ημέρα. Είναι προφανές ότι ο τρόπος αυτός συλλογής δείγματος δεν αντιπροσωπεύει επαρκώς τον πληθυσμό.

Για τους λόγους που προ αναφέρθηκαν, η συλλογή του δείγματος προέκυψε από το πλήθος των συμμετεχόντων και στις τρεις ενημερωτικές ημερίδες. Διανεμήθηκαν προς συμπλήρωση 200 ειδικά ερωτηματολόγια και σύμφωνα με την ερευνητική δεοντολογία, οι απαντήσεις των συμμετεχόντων στην έρευνα είναι εμπιστευτικές, ενώ τα στοιχεία που παρείχαν χρησιμοποιήθηκαν μόνο για τη στατιστική ανάλυση και την εξαγωγή συμπερασμάτων στην παρούσα έρευνα. Κατά την συλλογή των ερωτηματολογίων δόθηκαν και οι απαραίτητες διευκρινήσεις σε περιπτώσεις απορίων σχετικά με την συμπλήρωση του ερωτηματολογίου. Από τα 200 ερωτηματολόγια που διανεμήθηκαν συμπληρώθηκαν και ήταν έγκυρα τα 153.

4.4. Περιορισμοί ερωτηματολογίου

Το συγκεκριμένο ειδικό ερωτηματολόγιο εξετάζει μόνο τις γνώσεις και δεξιότητες αναφορικά με την πλοήγηση στο διαδίκτυο και τη χρήση συναφών υπηρεσιών και μέσων κοινωνικής δικτύωσης. Το φάσμα των ερωτήσεων που αφορούν τα προσωπικά δεδομένα και το διαδίκτυο είναι πολύ μεγάλο και δεν θα μπορούσαν να συμπεριληφθούν σε ένα και μοναδικό ερωτηματολόγιο. Αυτό είναι λογικό αν σκεφτεί κανείς ότι μόνο για τα προσωπικά δεδομένα υπάρχουν αντίστοιχες δημοσκοπήσεις του Ευρωβαρομέτρου. Πολλές ερωτήσεις της συγκεκριμένης έρευνας σχετικά με το διαδίκτυο και τα μέσα κοινωνικής δικτύωσης έχουν βασιστεί σε αντίστοιχες ερωτήσεις του Special Eurobarometer 431 Data Protection 2015. Γι' αυτό τα αποτελέσματα που θα προκύψουν αφορούν αποκλειστικά τις συγκεκριμένες ερωτήσεις.

Κατά την διεξαγωγή μιας έρευνας, υπάρχουν σημαντικοί παράμετροι που βοηθάνε στην αξιολόγηση και την επιστημονική αξία που η έρευνα αυτή διεκδικεί. Έτσι θα πρέπει να σταθεί κανείς σε κάποιες έννοιες προκειμένου, να αποφύγει τις παγίδες και τα συνήθη σφάλματα στα οποία ενδέχεται να υποπέσει κάθε ερευνητική απόπειρα. Κάθε έρευνα πρέπει να διέπετε από αξιοπιστία. Πρέπει να υπάρχει συνέπεια των αποτελεσμάτων σε περίπτωση επαναληπτικής διεξαγωγής της έρευνας ικανοποίησης. Κάθε έρευνα πρέπει να αναλύει τα κατάλληλα μεγέθη ώστε να γίνει σωστά η μέτρηση και να υπάρχει εγκυρότητα. Παράλληλα θα πρέπει να μπορεί να εντοπιστεί εάν υπάρξει αλλαγή στην στάση των ερωτηθέντων ώστε να εντοπιστεί το σφάλμα στα αποτελέσματα και να μην χαθεί η ακρίβεια της έρευνας.

Τέλος έχει μεγάλη σημασία να μην προκύψουν σφάλματα τα οποία θα οφείλονται σε ανειλικρινείς απαντήσεις, ή σε εσφαλμένο προσδιορισμό του προβλήματος ή σε καθοδήγηση των ερωτηθέντων.

Το εξειδικευμένο ερωτηματολόγιο πάνω στο οποίο βασίστηκε η συγκεκριμένη έρευνα επισυνάπτεται ως παράρτημα στην παρούσα έκθεση.

5. ΑΝΑΛΥΣΗ ΕΡΩΤΗΜΑΤΟΛΟΓΙΟΥ - ΣΥΜΠΕΡΑΣΜΑΤΑ

Εισαγωγή

Η έρευνα αρχικά εξετάζει το επίπεδο ελέγχου που θεωρούν ότι έχουν οι ερωτηθέντες πάνω στα ηλεκτρονικά προσωπικά τους δεδομένα, τις ανησυχίες τους για τυχόν αντιληπτή έλλειψη ελέγχου αυτών και το γεγονός της παρακολούθησης των δραστηριοτήτων τους.

Στη συνέχεια, η έρευνα αντιμετωπίζει το επίπεδο γνώσεων των ερωτηθέντων όσον αφορά τους όρους συλλογής δεδομένων και τη στάση τους στην παροχή προσωπικών πληροφοριών.

Οι προσδοκίες των πολιτών αξιολογούνται επίσης στο κατά πόσο εμπιστεύονται διάφορες αρχές και ιδιωτικούς ή δημόσιους φορείς για την προστασία των προσωπικών πληροφοριών τους και ποια προσωπικά τους δεδομένα αν χαθούν ή κλαπούν θα τους ανησυχούσαν περισσότερο.

Επιπροσθέτως μελετάει, το επίπεδο συνειδητοποίησης των ρυθμίσεων απορρήτου σε ιστό τόπους κοινωνικής δικτύωσης, με τους ερωτηθέντες να ρωτιούνται πόσο εύκολο είναι να το βρουν για να αλλάξουν τις ρυθμίσεις του.

Στο τελευταίο τμήμα της ασχολείται με το κατά πόσο οι ερωτηθέντες γνωρίζουν την εθνική δημόσια αρχή που είναι υπεύθυνη για την προστασία των προσωπικών δεδομένων και το επίπεδο ικανοποίησης τους όσον αφορά την ιστοσελίδα και το ενημερωτικό δελτίο της.

Στη συνέχεια θα ακολουθήσει η ανάλυση των ερωτήσεων του ερωτηματολογίου της έρευνας.

5.1. Περιγραφική ανάλυση

Σύμφωνα με το ερωτηματολόγιο (βλέπε Παράρτημα), οι μεταβλητές χωρίζονται σε τρία μέρη (Μέρος Α, Β και Γ).

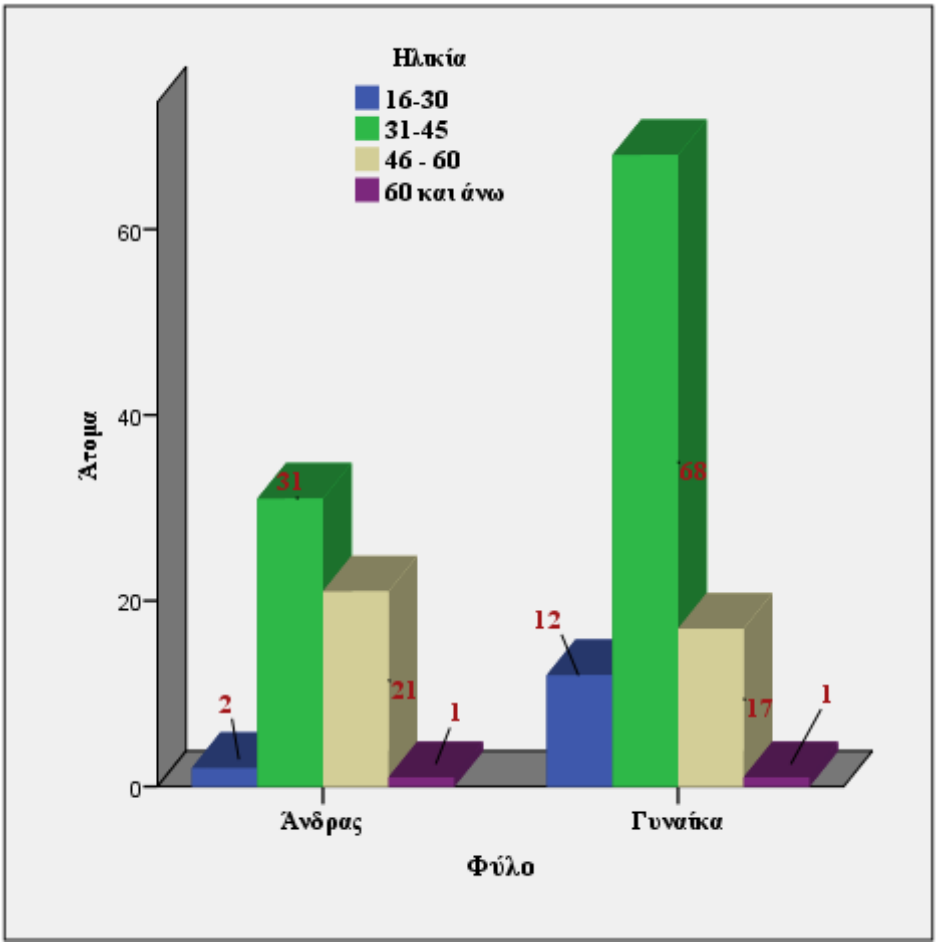
Α. Μέρος.

Το προφίλ των ατόμων που συμπλήρωσαν το ειδικό ερωτηματολόγιο με βάση το φύλο, την ηλικία και το μορφωτικό επίπεδο παρουσιάζεται στους Πίνακες 3 και 4

καθώς και στα ραβδογράμματα των Εικόνων 10 και 11.

			16-30	31-45	46 - 60	60 και άνω	Σύνολο
Φύλο	Άνδρας	Άτομα	2	31	21	1	55
		% του Συνόλου	1,3%	20,3%	13,7%	0,7%	35,9%
	Γυναίκα	Άτομα	12	68	17	1	98
		% του Συνόλου	7,8%	44,4%	11,1%	0,7%	64,1%
	Σύνολο	Άτομα	14	99	38	2	153
		% του Συνόλου	9,2%	64,7%	24,8%	1,3%	100,0%

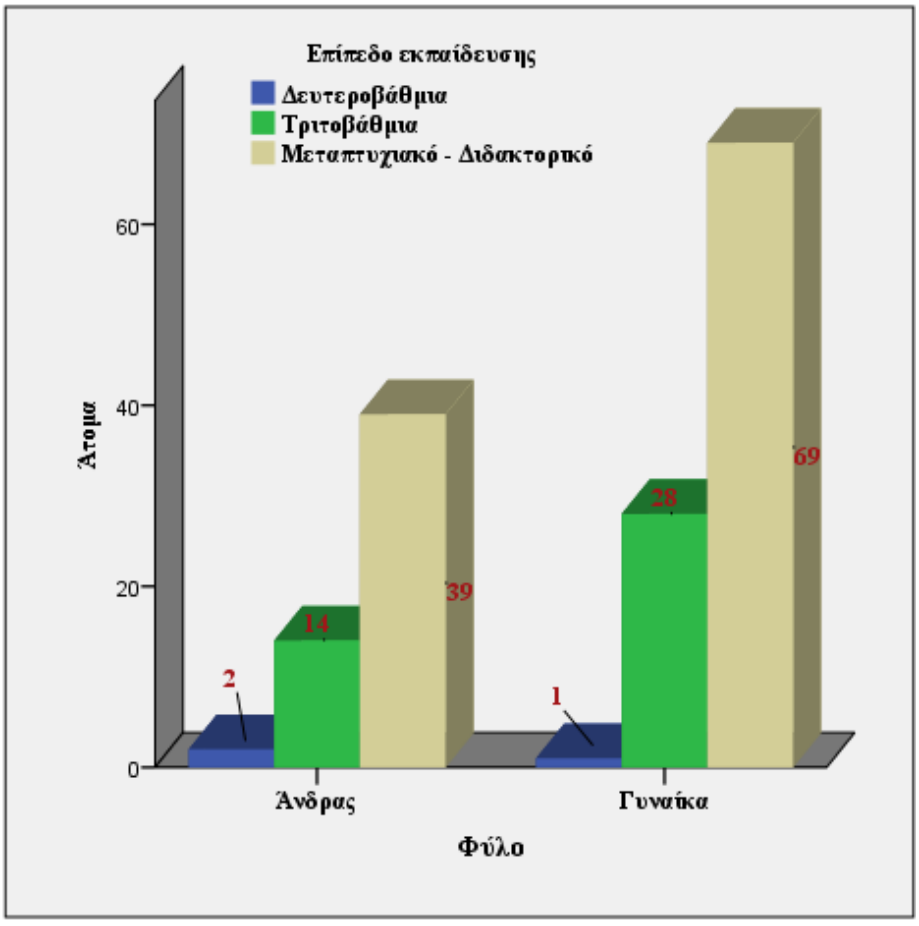
Πίνακας 3. Φύλο σε συνάρτηση με την ηλικία



Εικόνα 10. Ραβδόγραμμα φύλου - ηλικίας

			Δευτεροβάθμια	Τριτοβάθμια	Μεταπτυχιακό - Διδακτορικό	Σύνολο
Φύλο	Άνδρας	Άτομα	2	14	39	55
		% του Συνόλου	1,3%	9,2%	25,5%	35,9%
	Γυναίκα	Άτομα	1	28	69	98
		% του Συνόλου	0,7%	18,3%	45,1%	64,1%
Σύνολο		Άτομα	3	42	108	153
		% του Συνόλου	2,0%	27,5%	70,6%	100,0%

Πίνακας 4. Φύλο σε συνάρτηση με το επίπεδο εκπαίδευσης



Εικόνα 11. Ραβδόγραμμα φύλου – επιπέδου εκπαίδευσης

Παρατηρεί κανείς πως το (35.9%) των ερωτηθέντων είναι άνδρες ενώ το (64.1%) είναι γυναίκες.

Οι ηλικιακές ομάδες με τη μεγαλύτερη αντιπροσώπευση είναι μεταξύ 31 - 45 χρονών (64,7%) και μεταξύ 46 - 60 (24,8%). Μικρό είναι το ποσοστό όσων συμπλήρωσαν το ερωτηματολόγιο και είναι ηλικίας 16 - 30 χρονών (9,2%) και αντίστοιχα όσων είναι 60 χρονών και άνω (1,3%).

Το (27,5%) των ερωτηθέντων δήλωσαν ότι είναι κάτοχοι πτυχίου (τριτοβάθμια εκπαίδευση), (70,6%) είναι κάτοχοι μεταπτυχιακού – διδακτορικού και το (2%) απόφοιτοι δευτεροβάθμιας εκπαίδευση.

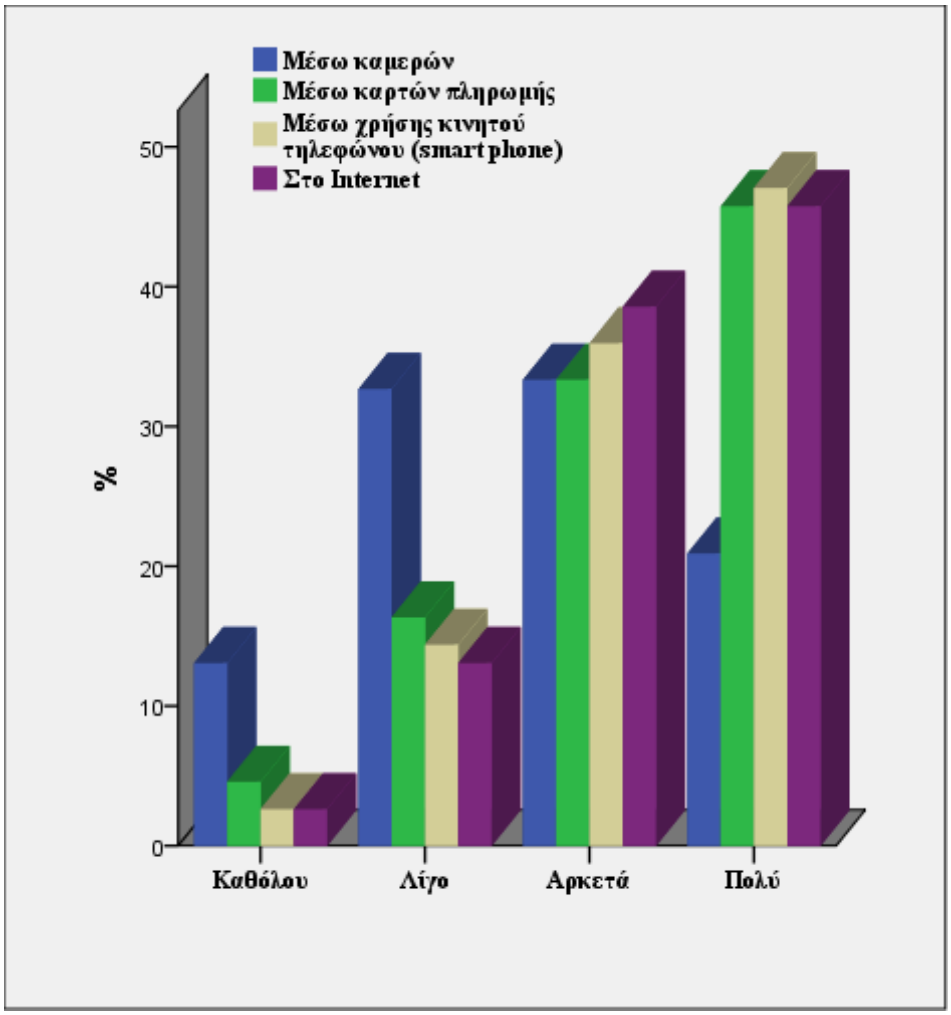
Β. Μέρος.

Ανησυχίες για την παρακολούθηση των καθημερινών δραστηριοτήτων.

Η συζήτηση τώρα κινείται στο θέμα της καταγραφής των καθημερινών δραστηριοτήτων των ανθρώπων. Οι ερωτηθέντες ανησυχούν περισσότερο για την καταγραφή των δραστηριοτήτων τους μέσω των κινητών τηλεφώνων, μέσω των καρτών πληρωμής και μέσω των ιστοσελίδων.

1. Σήμερα, πολλές από τις καθημερινές μας δραστηριότητες καταγράφονται με διάφορους τρόπους, όπως μέσω καμερών, καρτών πληρωμής, ιστοσελίδων, κλπ. Πόσο ανήσυχοι ή όχι είστε για αυτό;		**Καθόλου**	**Λίγο**	**Αρκετά**	**Πολύ**
Μέσω καμερών	Άτομα	20	50	51	32
	%	13,1%	32,7%	33,3%	20,9%
Μέσω καρτών πληρωμής	Άτομα	7	25	51	70
	%	4,6%	16,3%	33,3%	45,8%
Μέσω χρήσης κινητού τηλεφώνου (smart phone)	Άτομα	4	22	55	72
	%	2,6%	14,4%	35,9%	47,1%
Στο Internet	Άτομα	4	20	59	70
	%	2,6%	13,1%	38,6%	45,8%

Πίνακας 5. Παρακολούθηση καθημερινών δραστηριοτήτων



Εικόνα 12. Ραβδόγραμμα παρακολούθηση καθημερινών δραστηριοτήτων

Η πλειοψηφία των ερωτηθέντων (47,1%) ανησυχούν πολύ για την καταγραφή της συμπεριφοράς τους μέσω της χρήσης κινητών τηλεφώνων ή κινητών εφαρμογών, ενώ ένα παρόμοιο ποσοστό των ερωτηθέντων (45,8%) ανησυχούν πολύ για την καταγραφή των καθημερινών δραστηριοτήτων μέσω των καρτών πληρωμής και της χρήσης του διαδικτύου.

Αξιοσημείωτο είναι πως περισσότεροι από ένας στους τέσσερις ερωτηθέντες δηλώνουν ότι ανησυχούν αρκετά για τη καταγραφή των καθημερινών δραστηριοτήτων τόσο μέσω του διαδικτύου (38,6%) όσο και μέσω της χρήσης κινητών τηλεφώνων ή

κινητών εφαρμογών (35,9%) αλλά και μέσω καμερών και καρτών πληρωμής σε ποσοστό (33,3%).

Ενδιαφέρον παρουσιάζει επίσης το γεγονός πως πάνω από ένας στους δέκα, ποσοστό (13,1%), δεν ανησυχεί καθόλου για την καταγραφή των καθημερινών δραστηριοτήτων μέσω καμερών.

Η πλειοψηφία των ανθρώπων δεν αισθάνεται άνετα για τις εταιρείες του διαδικτύου που χρησιμοποιούν τις δικές τους προσωπικές πληροφορίες για την προσαρμογή των διαφημίσεων.

2. Όπως ίσως γνωρίζετε, μερικές online επιχειρήσεις είναι σε θέση να παρέχουν δωρεάν υπηρεσίες, όπως οι μηχανές αναζήτησης, δωρεάν λογαριασμούς e-mail, κ.λπ., χάρη στα έσοδα που λαμβάνουν από τους διαφημιστές που προσπαθούν να προσεγγίσουν τους χρήστες των ιστοσελίδων αυτών. Πόσο άνετα νιώθετε με το γεγονός ότι οι εν λόγω ιστοσελίδες χρησιμοποιούν πληροφορίες σχετικά με την online δραστηριότητά σας για να προσαρμόσουν διαφημίσεις ή περιεχόμενο σύμφωνα με τα χόμπι και τα ενδιαφέροντά σας;	**Άτομα**	**Ποσοστό %**
Πολύ άνετα	2	1,3%
Αρκετά άνετα	32	20,9%
Αρκετά άβολα	77	50,3%
Πολύ άβολα	42	27,5%
Σύνολο	153	100,0%

Πίνακας 6. Πόσο άνετα νιώθει κανείς με ιστοσελίδες που χρησιμοποιούν πληροφορίες σχετικά με online δραστηριότητά του

Η πλειονότητα των ερωτηθέντων (50,3%) δηλώνουν ότι είναι ανήσυχοι με το γεγονός ότι οι εταιρείες του διαδικτύου χρησιμοποιούν πληροφορίες σχετικά με την ηλεκτρονική τους δραστηριότητα και νιώθουν αρκετά άβολα.

Πάνω από 2 στους 10 ερωτηθέντες (22,2%) λένε ότι είναι άνετοι με το γεγονός ότι οι εταιρείες του διαδικτύου χρησιμοποιούν πληροφορίες σχετικά με την ηλεκτρονική τους δραστηριότητα για να προσαρμόσουν διαφημίσεις για τα χόμπι ή τα ενδιαφέροντά τους, αλλά μόλις το (1,3%) είναι πολύ άνετοι.

			Πολύ άνετα	Αρκετά άνετα	Αρκετά άβολα	Πολύ άβολα	Σύνολο
Φύλο	Άνδρας	Άτομα	1	5	33	16	55
		% του Συνόλου	0,7%	3,3%	21,6%	10,5%	35,9%
	Γυναίκα	Άτομα	1	27	44	26	98
		% του Συνόλου	0,7%	17,6%	28,8%	17,0%	64,1%
Σύνολο		Άτομα	2	32	77	42	153
		% του Συνόλου	1,3%	20,9%	50,3%	27,5%	100,0%

Πίνακας 7. Κοινωνικό δημογραφικά στοιχεία φύλου για χρήση πληροφοριών σχετικά με online δραστηριότητά

Σύμφωνα με τα κοινωνικό δημογραφικά στοιχεία, οι γυναίκες είναι πιο πιθανό από τους άνδρες (17,6% + 0,7% = 18,3% έναντι 3,3% + 0,7% = 4%) να αισθάνονται άνετα για τις εταιρείες του διαδικτύου που χρησιμοποιούν πληροφορίες σχετικά με online δραστηριότητα τους για την προσαρμογή των διαφημίσεων.

			Πολύ άνετα	Αρκετά άνετα	Αρκετά άβολα	Πολύ άβολα	Σύνολο
Ηλικία	16-30	Άτομα	0	6	5	3	14
		% του Συνόλου	0,0%	3,9%	3,3%	2,0%	9,2%
	31-45	Άτομα	2	20	54	23	99
		% του Συνόλου	1,3%	13,1%	35,3%	15,0%	64,7%
	46 - 60	Άτομα	0	6	16	16	38
		% του Συνόλου	0,0%	3,9%	10,5%	10,5%	24,8%
	60 και άνω	Άτομα	0	0	2	0	2
		% του Συνόλου	0,0%	0,0%	1,3%	0,0%	1,3%
Σύνολο		Άτομα	2	32	77	42	153
		% του Συνόλου	1,3%	20,9%	50,3%	27,5%	100,0%

Πίνακας 8. Κοινωνικό δημογραφικά στοιχεία ηλικίας για χρήση πληροφοριών σχετικά με online δραστηριότητά

Επίσης, πάνω από δύο στους δέκα ερωτηθέντες, (ποσοστό 13,1% + 1,3% = 14,4%) που ανήκουν στην ηλικιακή κατηγορία 31 – 45 αισθάνονται άνετα με το γεγονός ότι οι εταιρείες διαδικτύου χρησιμοποιούν προσωπικές πληροφορίες σχετικά με την ηλεκτρονική τους δραστηριότητα.

Οι ερωτηθέντες που χρησιμοποιούν το διαδίκτυο ρωτήθηκαν αν είναι συνήθως ενημερωμένοι σχετικά με τους όρους συλλογής δεδομένων και τις περαιτέρω χρήσεις των ηλεκτρονικών προσωπικών δεδομένων τους.

3. Θα λέγατε ότι είστε γενικά ενήμερος σχετικά με τις συνθήκες της συλλογής δεδομένων και με τις περαιτέρω χρήσεις των ηλεκτρονικών προσωπικών δεδομένων σας;	**Άτομα**	**Ποσοστό %**
Καθόλου	5	3,3
Λίγο	58	37,9
Αρκετά	73	47,7
Πολύ	17	11,1
Σύνολο	153	100,0

Πίνακας 9. Γνώση των συνθηκών συλλογής και χρήσης δεδομένων

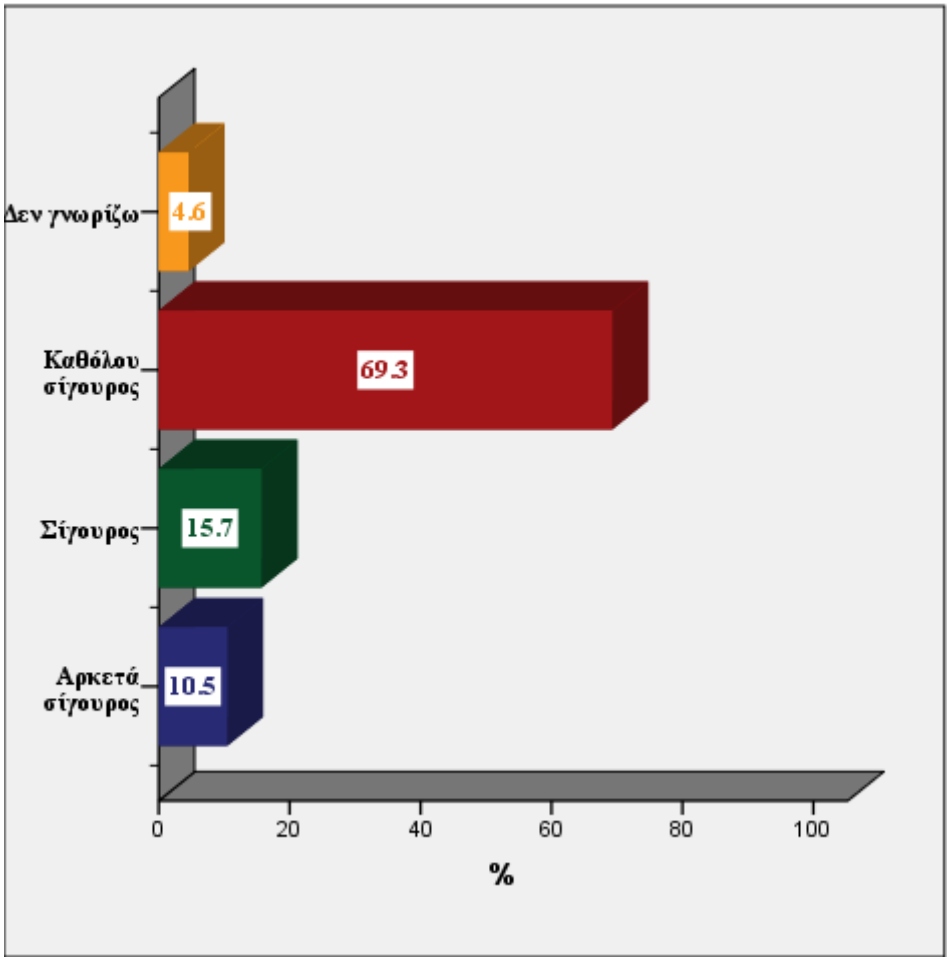
Για την γνώση των συνθηκών συλλογής και χρήσης δεδομένων οι έξι στους δέκα εκ των ερωτηθέντων (47,7% + 11,1% = 58,8%) δήλωσαν ότι είναι ενημερωμένοι για τις συνθήκες συλλογής δεδομένων και τις πιθανές χρήσεις τους όταν τους ζητείται να παρέχουν προσωπικές πληροφορίες στο διαδίκτυο. Το (11,1%) μάλιστα δήλωσαν ότι είναι πλήρως ενήμεροι σχετικά με τις συνθήκες και τις περαιτέρω χρήσεις της συλλογής δεδομένων σε αντίθεση με το (3,3%) αυτών που δεν ενημερώνονται ποτέ.

Η πλειοψηφία των ερωτηθέντων όμως εκφράζει μεγάλη δυσπιστία ως προς τα μέτρα που λαμβάνονται για την ασφαλή τήρηση των ηλεκτρονικών προσωπικών δεδομένων τους στο διαδίκτυο.

Οι εφτά στους δέκα ερωτηθέντες, ποσοστό (69,3%), θεωρούν πως η τήρηση των προσωπικών δεδομένων που παρέχουν στο διαδίκτυο για αγορές αγαθών καθώς και για υπηρεσίες ή συναλλαγές μέσου διαδικτύου δεν είναι καθόλου ασφαλής.

4. Πιστεύετε ότι όταν δίνετε προσωπικά σας δεδομένα στο διαδίκτυο (για αγορά αγαθών ή υπηρεσιών μέσω διαδικτύου ή λοιπές συναλλαγές), η τήρησή τους είναι ασφαλής;	**Άτομα**	**Ποσοστό %**
Αρκετά σίγουρος	16	10,5
Σίγουρος	24	15,7
Καθόλου σίγουρος	106	69,3
Δεν γνωρίζω	7	4,6
Σύνολο	153	100,0

Πίνακας 10. Ασφαλής τήρηση προσωπικών δεδομένων στο διαδίκτυο



Εικόνα 13. Ραβδόγραμμα ασφαλής τήρησης προσωπικών δεδομένων στο διαδίκτυο

Αρκετά μικρό φαίνεται να είναι το ποσοστό (4,6%) αυτών που παρόλο που κάνουν χρήση του διαδικτύου και δίνουν τα προσωπικά τους δεδομένα σε διάφορες διαδικτυακές συναλλαγές δεν ήταν σε θέση να μιλήσουν για την ασφαλή ή μη τήρηση τους.

Μπορεί να παρατηρήσει κανείς πως ενώ οι έξι στους δέκα εκ των ερωτηθέντων, ποσοστό (47,7% + 11,1% = 58,8%), δήλωσαν προηγουμένως ότι είναι ενημερωμένοι για τις συνθήκες συλλογής δεδομένων και τις πιθανές χρήσεις τους, όταν τους ζητείται να παρέχουν προσωπικές πληροφορίες στο διαδίκτυο, οι έφτα στους δέκα, ποσοστό (69,3%), εξέφρασαν την πλήρη δυσπιστία τους για το αν η τήρηση τους είναι ασφαλής.

			Αρκετά σίγουρος	Σίγουρος	Καθόλου σίγουρος	Δεν γνωρίζω	Σύνολο
Εκπαίδευση	**Δευτεροβάθμια**	Άτομα	0	0	3	0	3
		% του Συνόλου	0,0%	0,0%	2,0%	0,0%	2,0%
	Τριτοβάθμια	Άτομα	5	8	28	1	42
		% του Συνόλου	3,3%	5,2%	18,3%	0,7%	27,5%
	Μεταπτυχιακό - Διδακτορικό	Άτομα	11	16	75	6	108
		% του Συνόλου	7,2%	10,5%	49,0%	3,9%	70,6%
	Σύνολο	Άτομα	16	24	106	7	153
		% του Συνόλου	10,5%	15,7%	69,3%	4,6%	100,0%

Πίνακας 11. Επίπεδο εκπαίδευσης και ασφαλής τήρηση προσωπικών δεδομένων στο διαδίκτυο

Περίπου οι μισοί (49%) ερωτηθέντες κάτοχοι μεταπτυχιακού - διδακτορικού δεν είναι καθόλου σίγουροι, πολύ λιγότεροι είναι σίγουροι (10,5%) και αρκετά σίγουροι το (7,2%).

Επίσης, οι εφτά στους δέκα, ποσοστό (18,3%), των ατόμων τριτοβάθμιας εκπαίδευσης που συμμετείχαν στην έρευνα δεν είναι καθόλου σίγουροι, το (5,2%) είναι σίγουροι, το (3,3%) αρκετά σίγουροι, ενώ πολύ μικρό είναι το ποσοστό αυτών που δεν γνώριζαν για την ασφαλή τήρηση των προσωπικών τους δεδομένων.

Χρήζει αναφοράς πως το σύνολο των ερωτηθέντων δευτεροβάθμιας εκπαίδευσης (2%) δεν είναι καθόλου σίγουρο όταν δίνει προσωπικά δεδομένα στο διαδίκτυο.

Οι περισσότεροι από τους ερωτηθέντες πιστεύουν πως ο έλεγχος που μπορεί να έχουν στα προσωπικά δεδομένα που παρέχουν στο διαδίκτυο εξαρτάται από την ιστοσελίδα ή την εφαρμογή που τα διαχειρίζεται.

5. Πόσο έλεγχο αισθάνεστε ότι έχετε στις πληροφορίες που παρέχετε σε απευθείας σύνδεση (online), π.χ. η ικανότητα να διορθώσετε, να αλλάξετε ή να διαγράψετε αυτές τις πληροφορίες;	**Άτομα**	**Ποσοστό %**
Απόλυτο έλεγχο	1	0,7
Μερικό έλεγχο	58	37,9
Καθόλου έλεγχο	28	18,3
Εξαρτάται από την ιστοσελίδα ή την εφαρμογή	64	41,8
Δεν γνωρίζω	2	1,3
Σύνολο	153	100,0

Πίνακας 12. Έλεγχος προσωπικών δεδομένων του ατόμου στο διαδίκτυο

Η μεγάλη δυσπιστία που εξέφρασε προηγουμένως η πλειοψηφία των ερωτηθέντων ως προς την ασφαλή τήρηση των ηλεκτρονικών προσωπικών δεδομένων που παρέχουν στο διαδίκτυο, επιβεβαιώνεται από το γεγονός ότι μόλις το (0,7%) αισθάνεται να έχει τον απόλυτο έλεγχο πάνω στις πληροφορίες που παρέχει σε απευθείας σύνδεση (online).

Το (41,8%) των ανθρώπων αυτής της ομάδας θεωρούν πως ο έλεγχος που μπορεί να έχουν στα προσωπικά τους δεδομένα εξαρτάται από την ιστοσελίδα ή την εφαρμογή, το (37,9%) ότι έχουν μερικό έλεγχο, ενώ σχεδόν παραπάνω από το ένα

πέμπτο (18,3%) θεωρούν ότι δεν έχουν καθόλου έλεγχο των προσωπικών τους πληροφοριών στο διαδίκτυο.

			Απόλυτο έλεγχο	Μερικό έλεγχο	Καθόλου έλεγχο	Εξαρτάται από την ιστοσελίδα ή την εφαρμογή	Δεν γνωρίζω	Σύνολο
Εκπαίδευση	**Δευτεροβάθμια**	Άτομα	0	2	0	1	0	3
		% του Συνόλου	0,0%	1,3%	0,0%	0,7%	0,0%	2,0%
	Τριτοβάθμια	Άτομα	0	13	6	23	0	42
		% του Συνόλου	0,0%	8,5%	3,9%	15,0%	0,0%	27,5%
	Μεταπτυχιακό - Διδακτορικό	Άτομα	1	43	22	40	2	108
		% του Συνόλου	0,7%	28,1%	14,4%	26,1%	1,3%	70,6%
	Σύνολο	Άτομα	1	58	28	64	2	153
		% του Συνόλου	0,7%	37,9%	18,3%	41,8%	1,3%	100,0%

Πίνακας 13. Επίπεδο εκπαίδευσης και έλεγχος των προσωπικών δεδομένων του ατόμου στο διαδίκτυο

Τα άτομα με υψηλότερο επίπεδο εκπαίδευσης έχουν περισσότερες πιθανότητες να αισθάνονται τον έλεγχο των προσωπικών τους πληροφοριών στο διαδίκτυο. Πράγματι, μόλις το (14,4%) των ερωτηθέντων με μεταπτυχιακό – διδακτορικό τίτλο σπουδών δήλωσε ότι αισθάνεται να μην έχει καθόλου έλεγχο, σε σύγκριση με το υπόλοιπο (54,2%) της κατηγορίας αυτής το οποίο αισθάνεται είτε ότι έχει τον μερικό έλεγχο (28,1%), είτε ότι ο έλεγχος που μπορεί να έχει στα προσωπικά δεδομένα που παρέχει στο διαδίκτυο εξαρτάται από την ιστοσελίδα ή την εφαρμογή που τα διαχειρίζεται (26,1%).

Η αίσθηση ελέγχου των ηλεκτρονικών προσωπικών δεδομένων που έχουν οι κάτοχοι μεταπτυχιακού – διδακτορικού τίτλου σπουδών, παρατηρεί κανείς, πως

υπάρχει και στους κατόχους δευτεροβάθμιου και τριτοβάθμιου τίτλου σπουδών. Μερικό έλεγχο αισθάνονται να έχουν το (1,3%) και (8,5%) ενώ αν ο έλεγχος εξαρτάται από την ιστοσελίδα ή την εφαρμογή τα ποσοστά είναι (0,7%) και (15%) αντίστοιχα.

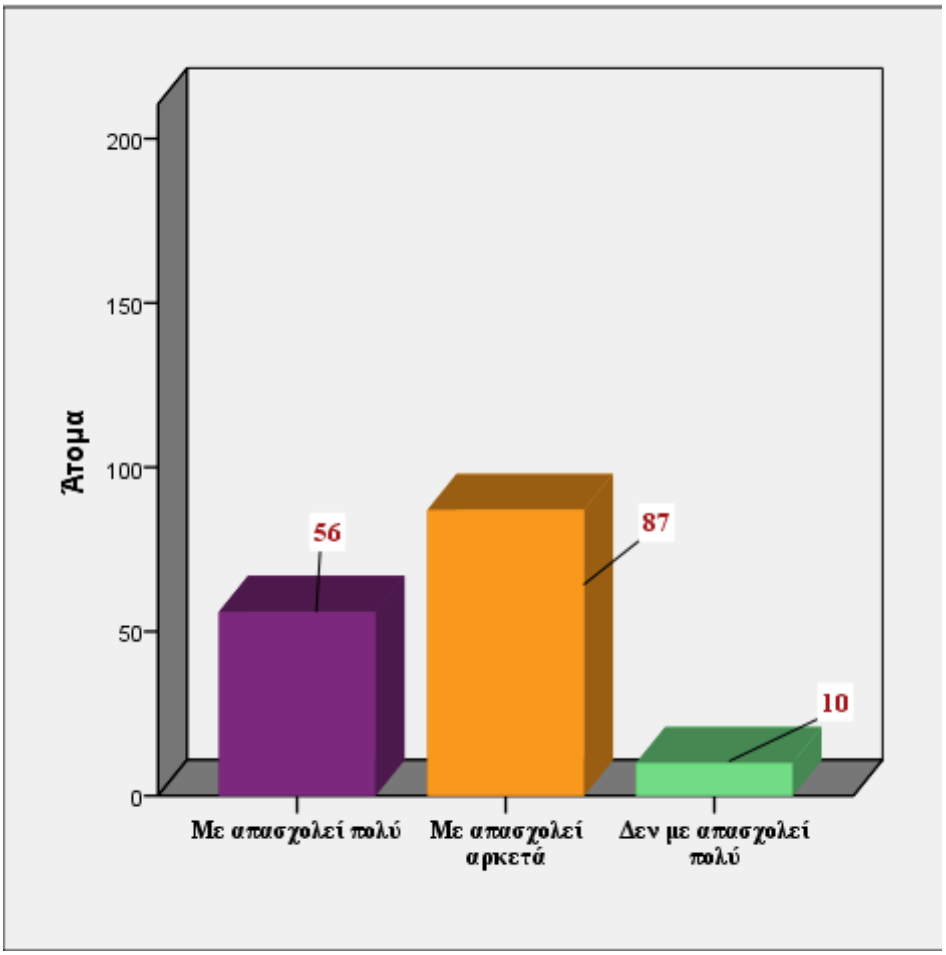
Οι εννέα στους δέκα εκ των ερωτηθέντων ανησυχούν ότι δεν έχουν πλήρη έλεγχο πάνω στις πληροφορίες που παρέχουν online.

6. Σε περίπτωση που δεν έχετε τον «*απόλυτο έλεγχο*» των πληροφοριών που παρέχετε στο διαδίκτυο, πόσο σας απασχολεί το γεγονός αυτό;	**Άτομα**	**Ποσοστό %**
Με απασχολεί πολύ	56	36,6
Με απασχολεί αρκετά	87	56,9
Δεν με απασχολεί πολύ	10	6,5
Σύνολο	153	100,0

Πίνακας 14. Ερωτηθέντες που τους απασχολεί ότι δεν έχουν πλήρη έλεγχο των πληροφοριών που παρέχουν online

Οι άνθρωποι που δήλωσαν στην προηγούμενη ενότητα ότι αισθάνονται ότι δεν έχουν πλήρη έλεγχο των προσωπικών τους πληροφοριών στο διαδίκτυο στη συνέχεια ρωτήθηκαν πόσο ανησυχούν ότι δεν έχουν πλήρη έλεγχο.

Παραπάνω από εννιά στους δέκα των ανθρώπων αυτής της ομάδας (93,5%) δηλώνουν ότι ανησυχούν και τους απασχολεί συνολικά το γεγονός ότι δεν έχουν τον πλήρη έλεγχο των πληροφοριών που παρέχουν στο διαδίκτυο, με το (36,6%) να δηλώνουν ότι τους απασχολεί πολύ και το (56,9%) ότι τους απασχολεί αρκετά. Αντιθέτως, λιγότεροι από ένας στους δέκα, ποσοστό (6,5%), δηλώνουν ότι δεν ανησυχούν και δεν τους απασχολεί πολύ.



Εικόνα 14. Ραβδόγραμμα ερωτηθέντων που τους απασχολεί ότι δεν έχουν πλήρη έλεγχο των πληροφοριών που παρέχουν online

Αποτελεί έκπληξη το γεγονός ότι ενώ οι εννιά στους δέκα (93,5%) δήλωσαν ότι ανησυχούν και τους απασχολεί ότι δεν έχουν τον πλήρη έλεγχο των πληροφοριών που παρέχουν στο διαδίκτυο, μόνο το ένα πέμπτο αυτών (18,3%) εξέφρασε την άποψη ότι αισθάνονται να μην έχουν καθόλου έλεγχο των προσωπικών πληροφοριών στο διαδίκτυο.

Η πλειοψηφία των ερωτηθέντων πιστεύει ότι οι εταιρείες στο διαδίκτυο, τα ίδια τα άτομα και όλες οι υπεύθυνες αρχές έχουν την ευθύνη να προστατεύουν τα ηλεκτρονικά προσωπικά τους δεδομένα.

7. Ποιος νομίζετε ότι θα πρέπει να σας διαβεβαιώσει ότι οι προσωπικές πληροφορίες που παρέχετε στο διαδίκτυο συλλέγονται, αποθηκεύονται και ανταλλάσσονται με ασφάλεια; (Μπορείτε να επιλέξετε παραπάνω από μια απαντήσεις)	Ποσοστό %
Online εταιρείες	38,2%
Εσύ	19,1%
Δημόσιες αρχές	40,6%
Άλλοι	0,3%
Δεν παρέχω προσωπικές πληροφορίες στο διαδίκτυο	1,0%
Δεν ξέρω	0,7%
Σύνολο	100,0%

Πίνακας 15. Ποιοι πρέπει να προστατεύουν τα ηλεκτρονικά προσωπικά δεδομένα

Οι ερωτηθέντες, οι οποίοι δήλωσαν ότι παρέχουν πληροφορίες στο διαδίκτυο (online), ερωτήθηκαν ποιον θεωρούν κατάλληλο για να διασφαλίσει ότι οι προσωπικές πληροφορίες που παρέχουν στο διαδίκτυο συλλέγονται, αποθηκεύονται και ανταλλάσσονται με ασφάλεια. Σε αυτήν την ερώτηση υπήρχε η δυνατότητα οι ερωτηθέντες να επιλέξουν παραπάνω από μια απάντηση. Στην περίπτωση αυτή για αποφυγή παρερμηνείας παρουσιάζεται τόσο στον Πίνακα 15 όσο και στον Πίνακα 16 μόνο το εκατοστιαίο ποσοστό κάθε απάντησης και όχι το πλήθος των ατόμων που επέλεξαν την κάθε απάντηση.

Περίπου στα δύο πέμπτα των ερωτηθέντων (38,2,6%) πιστεύουν ότι οι εταιρείες στο διαδίκτυο θα πρέπει να είναι υπεύθυνες, καθώς χρειάζονται για να εξασφαλίσουν την ασφαλή επεξεργασία των πληροφοριών.

Κοντά στα ένα πέμπτο των ερωτηθέντων (19,1%) πιστεύουν επίσης ότι πρέπει να είναι υπεύθυνοι για αυτό οι ίδιοι, δεδομένου ότι οι άνθρωποι πρέπει να φροντίζουν τις δικές τους πληροφορίες.

Τα δύο πέμπτα των ερωτηθέντων (40,6%) πιστεύουν ότι οι δημόσιες αρχές θα πρέπει να είναι υπεύθυνες γι' αυτό, δεδομένου ότι πρέπει να διασφαλίσουν την προστασία των δεδομένων των πολιτών.

Παρατηρεί κανείς πως ανεξαρτήτως του επιπέδου εκπαίδευσης των ατόμων που συμμετείχαν στην έρευνα, τείνει να υπάρχει μια απόλυτη ισορροπία μεταξύ των

απόψεων που θέλουν την ευθύνη για την διασφάλιση της προστασίας των ηλεκτρονικών προσωπικών δεδομένων να την έχουν οι υπεύθυνες δημόσιες αρχές, οι εταιρείες διαδικτύου και οι ίδιοι που παρέχουν τα προσωπικά τους δεδομένα.

		Online εταιρείες	Εσύ	Δημόσιες αρχές	Άλλοι	Δεν παρέχω προσωπικές πληροφορίες στο διαδίκτυο	Δεν ξέρω
Εκπαίδευση	Δευτερο/θμια	0,3%	0,0%	1,0%	0,0%	0,0%	0,0%
	Τριτοβάθμια	10,8%	4,5%	11,8%	0,0%	0,3%	0,7%
	Μεταπτυχιακό - Διδακτορικό	27,1%	14,6%	27,8%	0,3%	0,7%	0,0%
Σύνολο		38,2%	19,1%	40,6%	0,3%	1,0%	0,7%

Πίνακας 16. Επίπεδο εκπαίδευσης και ποιοι πρέπει να προστατεύουν τα ηλεκτρονικά προσωπικά δεδομένα

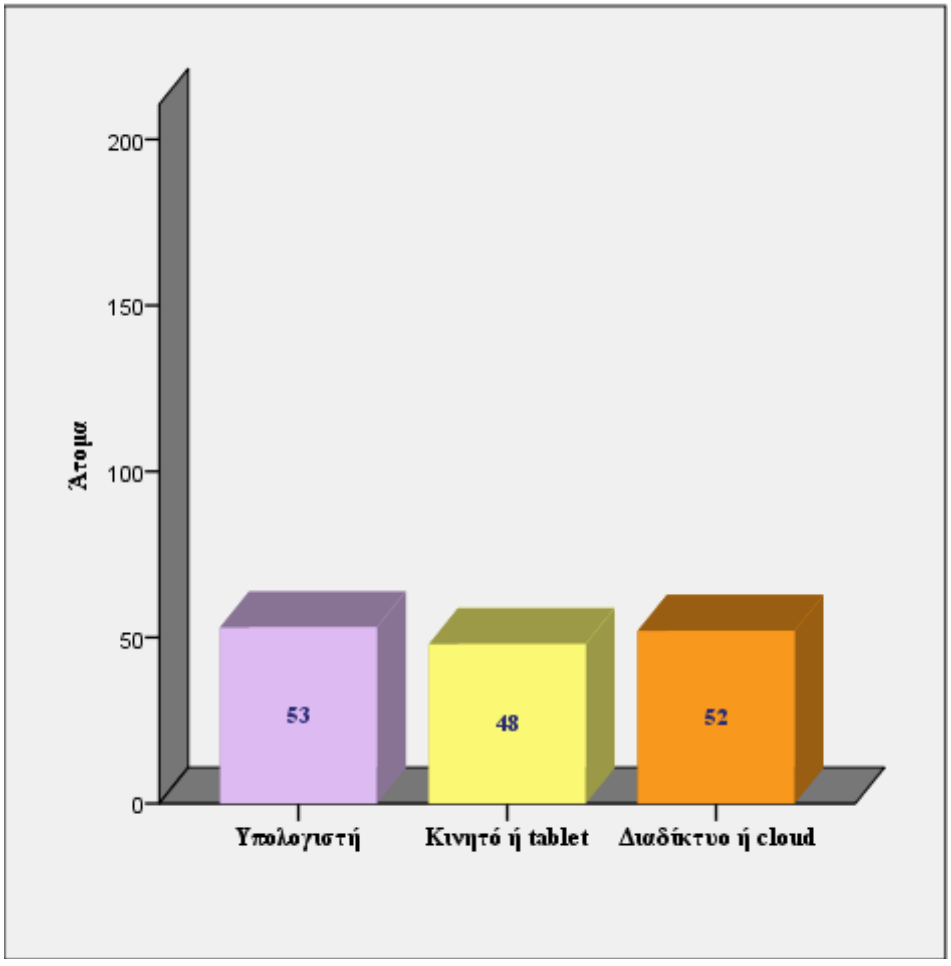
Στους κατόχους μεταπτυχιακού – διδακτορικού τίτλου σπουδών τα ποσοστά είναι για τις μεν δημόσιες αρχές (27,8%), για τις εταιρείες διαδικτύου (27,1%), και οι ίδιοι (14,6%). Για τους κάτοχους πτυχίου τριτοβάθμιας εκπαίδευσης τα ποσοστά είναι (11,8%), (10,8%) και (4,5%) αντίστοιχα.

Απόλυτη ισορροπία ανάμεσα στις απαντήσεις των ερωτηθέντων για το πότε θα ανησυχούσαν περισσότερο για τα δεδομένα που έχουν αποθηκευτεί στο δικό τους υπολογιστή ή στις κινητές συσκευές τους και στο διαδίκτυο ή στο σύννεφο σε περίπτωση κλοπής.

Τα δυο τρίτα των ερωτηθέντων δηλώσαν ότι θα ανησυχούσαν για τα δεδομένα που είναι αποθηκευμένα σε υπολογιστή (34,6%) ή δεδομένα αποθηκευμένα σε κινητό τηλέφωνο ή tablet (31,4%). Το υπόλοιπο ένα τρίτο, ποσοστό (34%), δήλωσε ότι θα ανησυχούσε περισσότερο για τα δεδομένα που είναι αποθηκευμένα στο διαδίκτυο ή στο σύννεφο.

8. Ποια δεδομένα σας αν χαθούν ή κλαπούν θα σας ανησυχούσαν περισσότερο;	Άτομα	Ποσοστό %
Δεδομένα που αποθηκεύονται στον υπολογιστή	53	34,6
Δεδομένα που αποθηκεύονται στο κινητό ή στο tablet	48	31,4
Δεδομένα που αποθηκεύονται στο διαδίκτυο ή στο cloud	52	34,0
Σύνολο	153	100,0

Πίνακας 17. Δεδομένα σε συσκευές που αν χαθούν ή κλαπούν ανησυχούν περισσότερο



Εικόνα 15. Ραβδόγραμμα δεδομένων σε συσκευές που αν χαθούν ή κλαπούν ανησυχούν περισσότερο

Η πλειοψηφία των ερωτηθέντων κάνει χρήση των ρυθμίσεων απορρήτου των φυλλομετρητών (browsers).

9. Χρησιμοποιείτε τις ρυθμίσεις απορρήτου του φυλλομετρητή σας (browser) αναφορικά με τη λήψη cookies κατά την είσοδό σας σε ιστοσελίδες;	**Άτομα**	**Ποσοστό %**
Όχι	39	25,5
Ναι	101	66,0
Δεν γνωρίζω	13	8,5
Σύνολο	153	100,0

Πίνακας 18. Χρήση των ρυθμίσεων απορρήτου των φυλλομετρητών (browsers)

Ο μεγαλύτερος αριθμός εκ των συμμετεχόντων στην έρευνα, ποσοστό (66%), έδειξαν να γνωρίζουν για την δυνατότητα των ρυθμίσεων απορρήτου που έχουν τα προγράμματα περιήγησης, φυλλομετρητές (browsers) και ειδικά όσον αφορά τις ρυθμίσεις για την λήψη cookies κατά την πλοήγηση τους σε ιστότοπους.

Στην ερώτηση που τέθηκε προηγουμένως σχετικά με το πόσο άνετα νιώθει κανείς με το γεγονός ότι ιστότοποι χρησιμοποιούν πληροφορίες με την online δραστηριότητά του για να προσαρμόσουν διαφημίσεις ή περιεχόμενο σύμφωνα με τα χόμπι και τα ενδιαφέροντά του, η πλειονότητα των ερωτηθέντων (50,3%) δήλωσαν ότι είναι ανήσυχοι με το γεγονός αυτό και νιώθουν αρκετά άβολα. Ένα μεγάλο ποσοστό (17,7%) όμως εξ αυτών, φαίνεται να μην γνωρίζει (4,6%) ή να μην κάνει χρήση (13,1%) των ρυθμίσεων απορρήτου των φυλλομετρητών όσον αφορά τα cookies. Η καταγραφή της online δραστηριότητας όμως ενός χρήστη επιτυγχάνεται μέσω των cookies.

Η χρήση των cookies σε ιστότοπους διευκολύνει τη διαχείριση των περιόδων σύνδεσης, την παροχή εξατομικευμένων ιστοσελίδων και την προσαρμογή διαφημιστικού και άλλου περιεχομένου ώστε να αντικατοπτρίζει τις ιδιαίτερες ανάγκες και τα ενδιαφέροντα των χρηστών. Επίσης τα cookies μπορούν να χρησιμοποιηθούν για να συνταχθούν ανώνυμες, αθροιστικές στατιστικές που επιτρέπουν σε κάθε

ιστότοπο να αντιληφθεί τα «θέλω» του κοινού και γενικότερα γιατί χρησιμοποιούν τον συγκεκριμένο ιστότοπο με αποτέλεσμα να βοηθούν έτσι ώστε να βελτιωθεί η δομή και το περιεχόμενό του.

			Όχι	Ναι	Δεν γνωρίζω	Σύνολο
Άνετα με online δρστηριότητα	**Πολύ άνετα**	Άτομα	1	1	0	2
		% του Συνόλου	0,7%	0,7%	0,0%	1,3%
	Αρκετά άνετα	Άτομα	9	20	3	32
		% του Συνόλου	5,9%	13,1%	2,0%	20,9%
	Αρκετά άβολα	Άτομα	20	50	7	77
		% του Συνόλου	13,1%	32,7%	4,6%	50,3%
	Πολύ άβολα	Άτομα	9	30	3	42
		% του Συνόλου	5,9%	19,6%	2,0%	27,5%
Σύνολο		Άτομα	39	101	13	153
		% του Συνόλου	25,5%	66,0%	8,5%	100,0%

Πίνακας 19. Χρήση των ρυθμίσεων απορρήτου των φυλλομετρητών και πόσο άνετα νιώθει κανείς με ιστοσελίδες που χρησιμοποιούν πληροφορίες σχετικά με online δραστηριότητά του

Τα cookies στοχευμένων διαφημίσεων χρησιμοποιούνται για την παροχή περιεχομένου, που ταιριάζει περισσότερο με τα ενδιαφέροντα των χρηστών. Μπορεί να χρησιμοποιηθούν για την αποστολή στοχευμένων διαφημίσεων και προσφορών, τον περιορισμό προβολών διαφήμισης ή την μέτρηση αποτελεσματικότητας μιας διαφημιστικής καμπάνιας. Μπορεί επίσης να χρησιμοποιηθούν για καταγραφή των ιστότοπων που έχει επισκεφθεί κάνεις ώστε να καθοριστούν ποια ηλεκτρονικά κανάλια μάρκετινγκ είναι πιο αποτελεσματικά για τον χρήστη και να επιτρέψουν στον ιστότοπο να επιβραβεύσει εξωτερικές ιστοσελίδες και συνεργάτες που προώθησαν τον χρήστη στον συγκεκριμένο ιστότοπο.

Οι χρήστες μπορούν να τροποποιούν τις ρυθμίσεις των προγραμμάτων περιήγησης για να απορρίψουν ορισμένα ή και όλα τα cookies, με σκοπό να μπορούν

να προστατέψουν έτσι την online δραστηριότητα τους. Ένας στους τέσσερις όμως, ποσοστό (25,5%) δεν χρησιμοποιεί τις ρυθμίσεις αυτές. Σημαντικό είναι και το ποσοστό (8,5%), των ερωτηθέντων που φαίνεται να μην γνωρίζουν τίποτα γενικά με τις ρυθμίσεις απορρήτου των προγραμμάτων περιήγησης.

Η πλειονότητα των συμμετεχόντων στην έρευνα κάνει χρήση των μέσων κοινωνικής δικτύωσης.

10. Κάνετε χρήση μέσων κοινωνικής δικτύωσης (Facebook, Twitter, Linkedin, Instagram, Snapchat κλπ.);	**Άτομα**	**Ποσοστό %**
Πολύ συχνά	42	27,5
Συχνά	62	40,5
Σχεδόν καθόλου	29	19,0
Καθόλου	20	13,1
Σύνολο	153	100,0

Πίνακας 20. Χρήση μέσων κοινωνικής δικτύωσης

Το (68%), δηλαδή περίπου εφτά στους δέκα χρησιμοποιούν τα μέσα κοινωνικής δικτύωσης, (Facebook, Twitter, Linkedin, Instagram, Snapchat κ.λπ.) με το (40,5%) να τα χρησιμοποιεί συχνά και το (27,5%) να κάνει πολύ συχνή χρήση.

Το ποσοστό του (19%) κάνει περιοδική χρήση έως σχεδόν καθόλου, ενώ το (13,1%) δεν διαθέτει κανέναν λογαριασμό κοινωνικής δικτύωσης και δεν ασχολείται καθόλου με αυτά.

Σύμφωνα με τα κοινωνικό δημογραφικά στοιχεία, το σύνολο των ερωτηθέντων που ανήκουν στην ηλικιακή κατηγορία των 16 – 30 χρησιμοποιούν είτε συχνά (3,9%) είτε πολύ συχνά (5,2%) τα μέσα κοινωνικής δικτύωσης. Αυτό γιατί αν αναλογιστεί κανείς ότι τα μέσα κοινωνικής δικτύωσης πρωτοεμφανίστηκαν πριν από δέκα πέντε περίπου χρόνια, θα μπορούσε να ισχυριστεί πως τα άτομα που ανήκουν στην ηλικιακή κατηγορία των 16 – 30 γεννήθηκαν παράλληλα με τα μέσα κοινωνικής δικτύωσης. Ενδεικτικά αναφέρεται ότι το LinkedIn ξεκίνησε το 2003, το Facebook δημιουργήθηκε το 2004, ενώ το Twitter το 2006.

			Πολύ συχνά	Συχνά	Σχεδόν καθόλου	Καθόλου	Σύνολο
Ηλικία	16-30	Άτομα	8	6	0	0	14
		% του Συνόλου	5,2%	3,9%	0,0%	0,0%	9,2%
	31-45	Άτομα	22	44	17	16	99
		% του Συνόλου	14,4%	28,8%	11,1%	10,5%	64,7%
	46 - 60	Άτομα	11	11	12	4	38
		% του Συνόλου	7,2%	7,2%	7,8%	2,6%	24,8%
	60 και άνω	Άτομα	1	1	0	0	2
		% του Συνόλου	0,7%	0,7%	0,0%	0,0%	1,3%
Σύνολο		Άτομα	42	62	29	20	153
		% του Συνόλου	27,5%	40,5%	19,0%	13,1%	100,0%

Πίνακας 21. Ηλικία και χρήση μέσων κοινωνικής δικτύωσης

Στις μεγαλύτερες ηλικιακές κατηγορίες (31 – 45, 46 – 60 και 60 και άνω) φαίνεται πως η πλειοψηφία των ατόμων χρησιμοποιεί τα μέσα κοινωνικής δικτύωσης.

Στις ηλικίες μεταξύ 31 – 45 το (43,2%) ασχολείται με τα μέσα κοινωνικής δικτύωσης, με το (28,8%) να κάνει συχνή χρήση, ενώ πολύ συχνή το (14,4%). Σε αντίθεση, σχεδόν καθόλου δεν ασχολείται το (11,1%) και καθόλου το (10,5%).

Το (14,4%) της ηλικιακής κατηγορίας των 46 – 60 ασχολείται με τα μέσα κοινωνικής δικτύωσης, με το (7,2%) να κάνει συχνή χρήση και πολύ συχνή το υπόλοιπο μισό (7,2%). Σε αντίθεση, σχεδόν καθόλου δεν ασχολείται το (7,8%) και καθόλου το (2,6%).

Για την ηλικιακή κατηγορία των 60 και άνω το δείγμα είναι πολύ μικρό και δεν χρήζει σχολιασμού.

Πάνω από εφτά στους δέκα από αυτούς που χρησιμοποιούν online κοινωνικά δίκτυα έχουν προσπαθήσει αλλαγή, προσαρμογή των ρυθμίσεων απορρήτου.

11. Όταν χρησιμοποιείτε μέσα κοινωνικής δικτύωσης (Facebook, Twitter, Linkedin, Instagram, Snapchat κλπ.), προσαρμόζετε τις αρχικές ρυθμίσεις απορρήτου;	**Άτομα**	**Ποσοστό % του συνόλου**	**Ποσοστό %**
Πολύ	47	30,7	35,3
Αρκετά	54	35,3	40,6
Ελάχιστα	23	15,0	17,3
Καθόλου	5	3,3	3,8
Δεν γνωρίζω	4	2,6	3,0
Σύνολο	133	86,9	100,0
Δεν απάντησαν γιατί δεν χρησιμοποιούν μέσα κοινωνικής δικτύωσης	20	13,1	
Σύνολο	153	100,0	

Πίνακας 22. Χρήση μέσων κοινωνικής δικτύωσης, ρυθμίσεις απορρήτου

Οι ερωτηθέντες που χρησιμοποιούν τα μέσα κοινωνικής δικτύωσης ρωτήθηκαν στη συνέχεια αν έχουν προσπαθήσει ποτέ να αλλάξουν τη ρύθμιση απορρήτου του προσωπικού τους προφίλ από τις προεπιλεγμένες ρυθμίσεις σε ένα κοινωνικό δίκτυο στο διαδίκτυο. Από το σύνολο των 153 συμπληρωμένων και έγκυρων ερωτηματολογίων, 20 εξ αυτών ποσοστό (13,1%), όπως διαπιστώθηκε και από την προηγούμενη ερώτηση, δήλωσαν ότι δεν έχουν ασχοληθεί και δεν χρησιμοποιούν καθόλου τα μέσα κοινωνικής δικτύωσης οπότε και δεν απάντησαν στην ερώτηση αυτή.

Από το πλήθος των 133 ερωτηθέντων, η πλειοψηφία αυτών ποσοστό (75,9%), έχουν προσαρμόσει τις αρχικές ρυθμίσεις απορρήτου των διαδικτυακών μέσων κοινωνικής δικτύωσης με το (40,6%) αρκετά και με το (35,5%) πολύ.

Το υπόλοιπο (24,1%), είτε έχει ασχοληθεί ελάχιστα (17,3%) με το να αλλάξει τις ρυθμίσεις απορρήτου των διαδικτυακών μέσων κοινωνικής δικτύωσης, είτε καθόλου (3,8%), είτε δεν γνωρίζει (3,0%) πώς να τις αλλάξει.

Οι περισσότεροι ερωτηθέντες που προσπάθησαν να αλλάξουν τις ρυθμίσεις απορρήτου δηλώνουν ότι η όλη διαδικασία ήταν εύκολη.

12. Πόσο εύκολο ή δύσκολο σας είναι να βρείτε και να χρησιμοποιήσετε τις ρυθμίσεις απορρήτου στα μέσα κοινωνικής δικτύωσης (Facebook, Twitter, Linkedin, Instagram, Snapchat κλπ.);	**Άτομα**	**Ποσοστό % του συνόλου**	**Ποσοστό %**
Πολύ εύκολο	15	9,8	11,3
Αρκετά εύκολο	39	25,5	29,3
Εύκολο	33	21,6	24,8
Δύσκολο	27	17,6	20,3
Αρκετά δύσκολο	13	8,5	9,8
Πολύ δύσκολο	2	1,3	1,5
Δεν γνωρίζω	4	2,6	3,0
Σύνολο	133	86,9	100,0
Δεν απάντησαν γιατί δεν χρησιμοποιούν μέσα κοινωνικής δικτύωσης	20	13,1	
Σύνολο	153	100,0	

Πίνακας 23. Χρήση μέσων κοινωνικής δικτύωσης και πόσο εύκολο ή δύσκολο είναι να βρεθούν και να χρησιμοποιηθούν οι ρυθμίσεις απορρήτου

Οι ερωτηθέντες που ανέφεραν στο προηγούμενο ερώτημα ότι χρησιμοποιούν τα διαδικτυακά μέσα κοινωνικής δικτύωσης και ότι έχουν προσπαθήσει να αλλάξουν τις ρυθμίσεις απορρήτου τους ερωτήθηκαν τότε πόσο εύκολο ή δύσκολο το βρήκαν αυτό. Όπως και προηγουμένως έτσι και εδώ από το σύνολο των 153 συμπληρωμένων και έγκυρων ερωτηματολογίων, 20 εξ αυτών ποσοστό (13,1%) είναι άτομα που δεν ασχολούνται με τα μέσα κοινωνικής δικτύωσης και δεν απάντησαν και σε αυτό το ερώτημα.

Από το πλήθος των 133 ερωτηθέντων, η πλειοψηφία αυτών περίπου πάνω από έξι στους δέκα ποσοστό (65,4%) λένε ότι ήταν εύκολο, με το (11,3%) να περιγράφει τη διαδικασία ως πολύ εύκολη, το (29,3%) να λέει ότι ήταν αρκετά εύκολη και το (24,8%) να δηλώνει ότι η όλη διαδικασία ήταν εύκολη.

Οι δυο στους δέκα ποσοστό (20,3%) δήλωσαν ότι ήταν δύσκολη η διαδικασία εύρεσης των ρυθμίσεων απορρήτου των διαδικτυακών μέσων κοινωνικής δικτύωσης. Το υπόλοιπο (14,3%), είτε βρήκε αρκετά δύσκολα (9,8%) τις ρυθμίσεις απορρήτου των διαδικτυακών μέσων κοινωνικής δικτύωσης, είτε πολύ δύσκολα (1,5%), είτε δεν γνωρίζει (3,0%) πώς να τις βρει.

Χρήζει ειδικής αναφοράς πως στο προηγούμενο ερώτημα το ποσοστό αυτών που δεν γνωρίζουν πως να αλλάξουν τις ρυθμίσεις απορρήτου (3,0%) είναι ίδιο με το ποσοστό αυτών (3,0%) που δεν γνωρίζουν πώς να τις βρουν.

	Πολύ εύκολο	**Αρκετά εύκολο**	**Εύκολο**	**Δύσκολο**	**Αρκετά δύσκολο**	**Πολύ δύσκολο**	**Δεν γνωρίζω**	**Σύνολο**
Απόλυτο έλεγχο	0,0%	0,0%	0,8%	0,0%	0,0%	0,0%	0,0%	0,8%
Μερικό έλεγχο	4,5%	15,0%	12,8%	4,5%	2,3%	0,0%	0,8%	39,8%
Καθόλου έλεγχο	2,3%	5,3%	2,3%	5,3%	0,8%	0,8%	1,5%	18,0%
Εξαρτάται από την ιστοσελίδα ή την εφαρμογή	4,5%	9,0%	9,0%	9,8%	6,8%	0,8%	0,8%	40,6%
Δεν γνωρίζω	0,0%	0,0%	0,0%	0,8%	0,0%	0,0%	0,0%	0,8%
Σύνολο	11,3%	29,3%	24,8%	20,3%	9,8%	1,5%	3,0%	100,0%

Πίνακας 24. Χρήση μέσων κοινωνικής δικτύωσης και πόσο εύκολο ή δύσκολο είναι να βρεθούν και να χρησιμοποιηθούν οι ρυθμίσεις απορρήτου παράλληλα με το πόσο έλεγχο αισθάνεται ότι έχει κανείς σε online πληροφορίες που παρέχει

Η πλειονότητα, ποσοστό (33,1%), των ερωτηθέντων που αισθάνονται ότι έχουν τον απόλυτο και μερικό έλεγχο (0,8% + 39,8% = 40,6%) των διαδικτυακών προσωπικών τους στοιχείων και πληροφοριών, βρίσκουν πιθανότερα ευκολά (0,8%) και (12,8%) αντίστοιχα, αρκετά εύκολα (15%) και πολύ εύκολα (4,5%) τον τρόπο να αλλάξουν τις ρυθμίσεις απορρήτου σε λογαριασμούς που διαθέτουν στα διαδικτυακά μέσα κοινωνικής δικτύωσης.

Οι ερωτηθέντες, ποσοστό (40,6%) που αισθάνονται ότι ο έλεγχος που έχουν στα διαδικτυακά προσωπικά τους στοιχεία και πληροφορίες εξαρτάται από τις ιστοσελίδες ή τις εφαρμογές που τα διαχειρίζονται, δηλώνουν, παραπάνω από τους μισούς (22,5%), ότι είναι γενικά εύκολο να μπορέσουν να αλλάξουν τις ρυθμίσεις απορρήτου των διαδικτυακών μέσων κοινωνικής δικτύωσης.

Γ. Μέρος.

Το σύνολο των πολιτών που παραβρέθηκαν στη διάρκεια των τριών ενημερωτικών ημερίδων για τον εορτασμού της 11ης Ευρωπαϊκής Ημέρας Προστασίας Προσωπικών Δεδομένων γνωρίζουν την ύπαρξη της ιστοσελίδας της Αρχής.

Η συζήτηση τώρα κινείται γύρω από ερωτήσεις που σκοπό έχουν να αξιολογήσουν την ιστοσελίδα (www.dpa.gr) της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

1. Έχετε ποτέ επισκεφθεί την ιστοσελίδα (*www.dpa.gr*) της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα;	**Άτομα**	**Ποσοστό %**
Ναι	153	100,0

Πίνακας 25. Με βάση την έρευνα οι επισκέπτες της ιστοσελίδας της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (www.dpa.gr)

Η συμμετοχή των ερωτηθέντων στις τρεις αυτές ενημερωτικές ημερίδες θα πιστοποιούσε το γεγονός ότι έστω και μια φορά θα έχουν περιηγηθεί στην ιστοσελίδα της Αρχής. Αυτό αποδείχθηκε και από τις απαντήσεις των ερωτηθέντων στο ερώτημα

εάν έχουν ποτέ επισκεφθεί την ιστοσελίδα της Αρχής. Το σύνολο των ατόμων που συμμετείχαν στην έρευνα, ποσοστό (100%), γνωρίζουν και έχουν επισκεφθεί την ιστοσελίδα (www.dpa.gr).

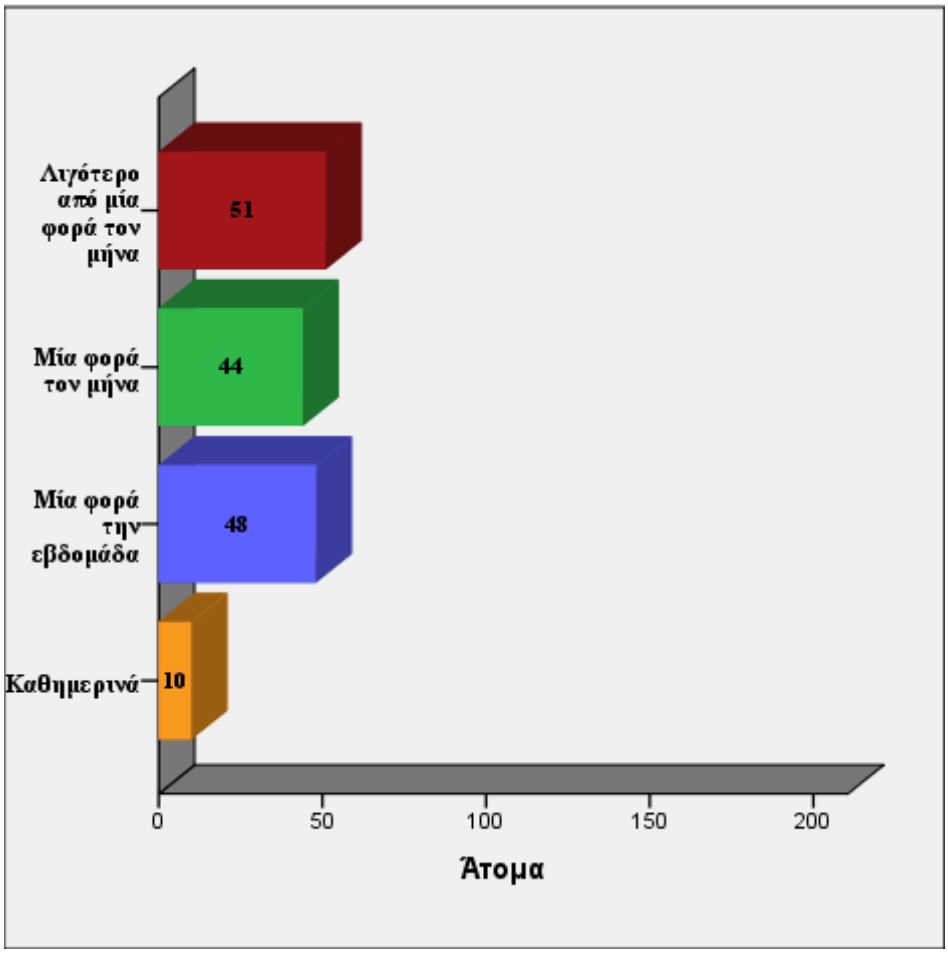
Το ένα τρίτο των ερωτηθέντων της έρευνας επισκέπτονται λιγότερο από μια φορά τον μήνα την ιστοσελίδα (www.dpa.gr).

2. Εάν επισκέπτεστε την ιστοσελίδα (*www.dpa.gr*) της Αρχής πόσο συχνά το κάνετε;	**Άτομα**	**Ποσοστό %**
Καθημερινά	10	6,5
Μία φορά την εβδομάδα	48	31,4
Μία φορά τον μήνα	44	28,8
Λιγότερο από μία φορά τον μήνα	51	33,3
Σύνολο	153	100,0

Πίνακας 26. Συχνότητα επισκεψιμότητας της ιστοσελίδας της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (www.dpa.gr)

Οι ερωτηθέντες που ανέφεραν στο προηγούμενο ερώτημα ότι γνωρίζουν και έχουν επισκεφθεί την ιστοσελίδα της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα ερωτήθηκαν τότε πόσο συχνά την επισκέπτονται. Ένας στους τρείς, ποσοστό (33,3%), δήλωσε ότι την επισκέπτεται λιγότερο από μια φορά τον μήνα, ενώ μια φορά τον μήνα δήλωσαν ότι την επισκέπτονται το (28,8%) των ερωτηθέντων.

Κάτι λιγότερο από ένας στους τρεις, ποσοστό (31,4%) δήλωσε ότι επισκέπτεται την ιστοσελίδα (www.dpa.gr) εβδομαδιαίως, ενώ το (6,5%) δήλωσαν πως επισκέπτονται την ιστοσελίδα της Αρχής σε καθημερινή βάση.



Εικόνα 16. Ραβδόγραμμα συχνότητας επισκεψιμότητας της ιστοσελίδας της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (www.dpa.gr)

Η πλειονότητα των ερωτηθέντων εξέφρασε την ικανοποίηση της για το περιεχόμενο της ιστοσελίδας (www.dpa.gr).

Οι ερωτηθέντες εξέφρασαν γενικά την ικανοποίηση τους για την επάρκεια και χρησιμότητα των πληροφοριών που παρέχει στους πολίτες, για την επικαιροποίηση των συνδέσμων και για την φιλική δυνατότητα επικοινωνίας που προσφέρει.

Η πλειοψηφία των ερωτηθέντων (48,4%) βαθμολόγησαν ως πολύ καλό, τόσο το περιεχόμενο της ιστοσελίδας όσον αφορά την επάρκεια, αλλά και όσον αφορά τη χρησιμότητα των πληροφοριών που παρέχει στο κοινό. Μάλιστα περίπου οι τρείς στους δέκα, ποσοστό (28,1%) θεωρούν ότι η χρησιμότητα των πληροφοριών που παρέχει

είναι άριστη, γεγονός που έρχεται σε αντίθεση με το (37,3%) των ερωτηθέντων που αξιολόγησε ως μέτρια την επάρκεια των πληροφοριών.

3. Σε κλίμακα από το 1 μέχρι το 5, με άριστα το 5, πώς θα βαθμολογούσατε την ιστοσελίδα της Αρχής σε σχέση με το περιεχόμενο;		**Καθόλου καλό**	**Λίγο καλό**	**Μέτριο**	**Πολύ καλό**	**Άριστο**	**Σύνολο**
Οι πληροφορίες είναι επαρκείς	Άτομα	0	6	57	74	16	153
	% του Συνόλου	0,0%	3,9%	37,3%	48,4%	10,5%	100,0%
Οι πληροφορίες είναι χρήσιμες	Άτομα	0	4	32	74	43	153
	% του Συνόλου	0,0%	2,6%	20,9%	48,4%	28,1%	100,0%
Οι σύνδεσμοι είναι ενημερωμένοι	Άτομα	0	17	46	72	18	153
	% του Συνόλου	0,0%	11,1%	30,1%	47,1%	11,8%	100,0%
Θεωρείτε φιλική τη δυνατότητα επικοινωνίας	Άτομα	4	25	38	66	20	153
	% του Συνόλου	2,6%	16,3%	24,8%	43,1%	13,1%	100,0%

Πίνακας 27. Αξιολόγηση της ιστοσελίδα (www.dpa.gr) σε σχέση με το περιεχόμενο

Το (47,1%) από τους συμμετέχοντες στην έρευνα πιστεύουν ότι είναι πολύ καλά ενημερωμένοι οι σύνδεσμοι της ιστοσελίδας, με το (30,1%) όμως εξ αυτών να κρίνουν πως η ενημέρωση των συνδέσμων είναι μέτρια.

Πολύ καλή θεωρούν την δυνατότητα επικοινωνίας το (43,1%), ενώ το (24,8%) την αξιολογούν ως μέτρια και το (16,3%) λίγο καλή. Αξιοσημείωτο είναι πως το (2,6%) εκ των ερωτηθέντων κρίνουν πως η δυνατότητα επικοινωνίας δεν είναι καθόλου καλή.

Ενδιαφέρον παρουσιάζει επίσης το γεγονός πως κανείς εκ των συμμετεχόντων δεν έκρινε ότι η επικαιροποίηση των συνδέσμων καθώς επίσης η επάρκεια και η χρησιμότητα των πληροφοριών που προσφέρει η ιστοσελίδα δεν είναι καθόλου καλή.

Η πλειοψηφία των ατόμων που συμμετείχαν στην έρευνα εξέφρασαν την ικανοποίηση τους για τη σχεδίαση και την πλοήγηση της ιστοσελίδας (www.dpa.gr).

Οι συμμετέχοντες στην έρευνα εξέφρασαν γενικά την ικανοποίηση τους για τη φιλικότητα στη χρήση, την αναγνωσιμότητα, την ταχύτητα και την οργάνωση της πληροφορίας της ιστοσελίδας.

4. Σε κλίμακα από το 1 μέχρι το 5, με άριστα το 5, πώς θα βαθμολογούσατε την ιστοσελίδα της Αρχής σε σχέση με την σχεδίαση και την πλοήγηση;		**Καθόλου καλή**	**Λίγο καλή**	**Μέτρια**	**Πολύ καλή**	**Άριστη**	**Σύνολο**
Φιλικότητα στη χρήση (Ο ιστότοπος έχει μια ομοιομορφία και μια συγκεκριμένη εμφάνιση σε όλες τις σελίδες του)	Άτομα	3	12	60	64	14	153
	% του Συνόλου	2,0%	7,8%	39,2%	41,8%	9,2%	100,0%
Αναγνωσιμότητα (Οι σελίδες έχουν ευκρινείς γραμματοσειρές και χρώματα)	Άτομα	1	10	37	77	28	153
	% του Συνόλου	0,7%	6,5%	24,2%	50,3%	18,3%	100,0%
Ταχύτητα (Οι σελίδες φορτώνουν γρήγορα)	Άτομα	4	8	35	82	24	153
	% του Συνόλου	2,6%	5,2%	22,9%	53,6%	15,7%	100,0%
Οργάνωση της πληροφορίας (Οργάνωση και παρουσίαση φιλική στην πλοήγησή. Βρίσκετε εύκολα αυτό που θέλετε)	Άτομα	1	26	44	67	15	153
	% του Συνόλου	0,7%	17,0%	28,8%	43,8%	9,8%	100,0%
Αισθητική - Σχεδιασμός (Ιστοσελίδας www.dpa.gr)	Άτομα	8	40	59	33	13	153
	% του Συνόλου	5,2%	26,1%	38,6%	21,6%	8,5%	100,0%

Πίνακας 28. Αξιολόγηση της ιστοσελίδα (www.dpa.gr) σε σχέση με τη σχεδίαση και την πλοήγηση

Η πλειονότητα των ερωτηθέντων (41,8%) βαθμολόγησαν ως πολύ καλή την φιλικότητα στη χρήση και την ομοιομορφία που έχει ο ιστότοπος σε όλες τις σελίδες του. Ωστόσο περίπου τέσσερις στους δέκα, ποσοστό (39,2%) την έκριναν ως μέτρια, ενώ λίγο καλή έως καθόλου καλή την αξιολόγησε το (9,8%) των συμμετεχόντων στην έρευνα.

Οι μισοί εκ των ερωτηθέντων (50,3%) αξιολόγησαν ως πολύ καλή την αναγνωσιμότητα, κυρίως όσον αφορά την ευκρίνεια στις γραμματοσειρές και τα χρώματα της ιστοσελίδας. Σημαντικό είναι επίσης το ποσοστό των ατόμων (18,3%) που έκριναν την ευκρίνεια της ιστοσελίδας ως άριστη. Ενδιαφέρον παρουσιάζει και το ποσοστό των ερωτηθέντων (24,2%) που βαθμολόγησαν την αναγνωσιμότητα ως μέτρια και αυτό γιατί είναι αρκετά μικρότερο σε σύγκριση με το ποσοστό (30,2%) αυτών που έκριναν ως μέτρια την φιλικότητα στη χρήση.

Παραπάνω από τους μίσους συμμετέχοντες (53,6%) αξιολόγησαν ως πολύ καλή την ταχύτητα με την οποία φορτώνουν οι σελίδες του ιστότοπου, ενώ ένα ποσοστό της τάξεως του (15,7%) την έκριναν ως άριστη. Στο κριτήριο αυτό αξιολόγησης όπως και στο προηγούμενο οι ερωτηθέντες που βαθμολόγησαν ως μέτρια (22,9%) την ταχύτητα είναι και εδώ συγκριτικά λιγότεροι σε σχέση με αυτούς που έκριναν ως μέτρια τη φιλικότητα στη χρήση.

Όσον αφορά τα κριτήρια αξιολόγησης για την οργάνωση των πληροφοριών που παρέχει ο ιστότοπος στο κοινό και την αισθητική – σχεδιασμό του, οι συμμετέχοντες στην έρευνα τα βαθμολόγησαν ως πολύ καλά με ποσοστά (43,8%) και (21,6%) αντίστοιχα.

Για τα δυο αυτά κριτήρια παρατηρείται μια σημαντική διαφοροποίηση στα ποσοστά της 5βάθμιας λεκτικής κλίμακας βαθμολόγησης σε σχέση με τα προηγούμενα κριτήρια του ερωτήματος. Για μεν την οργάνωση της πληροφορίας το ποσοστό που τη βαθμολόγησε ως μέτρια είναι (28,8%), ενώ για την αισθητική και το σχεδιασμό αγγίζει το (38,6%), το δεύτερο μεγαλύτερο στη βαθμίδα «Μέτρια» της κλίμακας. Η μεγάλη όμως διαφοροποίηση εμφανίζεται σε εκείνους που τα αξιολόγησαν ως λίγο καλά με ποσοστά (17,0%) και (26,1%) αντίστοιχα, όπου είναι και τα δυο υψηλότερα στην βαθμίδα «Λίγο καλή» της 5βάθμιας λεκτικής κλίμακας. Αξιοσημείωτο είναι επίσης το

γεγονός ότι το (5,2%) βαθμολόγησε την αισθητική και το σχεδιασμό της ιστοσελίδας ως καθόλου καλά, το υψηλότερο ποσοστό στην βαθμίδα «Καθόλου καλή» της κλίμακας.

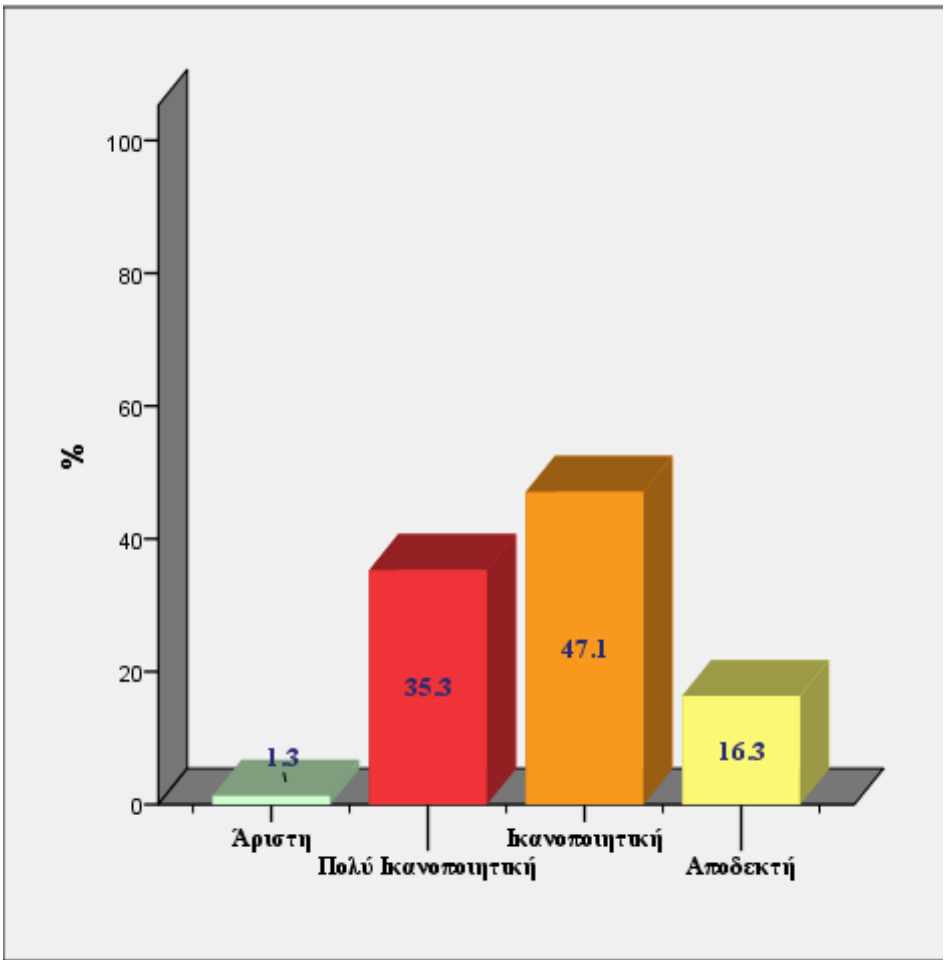
Πάνω από τέσσερις στους δέκα εξέφρασαν την ικανοποίηση τους για την συνολική εικόνα που παρουσιάζει η ιστοσελίδα (www.dpa.gr).

5. Αξιολογήστε συνολικά την ιστοσελίδα της Αρχής.	**Άτομα**	**Ποσοστό %**
Άριστη	2	1,3
Πολύ Ικανοποιητική	54	35,3
Ικανοποιητική	72	47,1
Αποδεκτή	25	16,3
Σύνολο	153	100,0

Πίνακας 29. Συνολική αξιολόγηση της ιστοσελίδας (www.dpa.gr)

Το (82,4%) των ερωτηθέντων αξιολόγησαν την συνολική εικόνα της ιστοσελίδας της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα από ικανοποιητική έως πολύ ικανοποιητική, με το (47,1%) να την κρίνει ικανοποιητική και το (35,3%) πολύ ικανοποιητική.

Ένα ποσοστό όμως εκ των συμμετεχόντων (16,3%) την αξιολόγησαν ως απλά αποδεκτή, ενώ σε αντίθεση ένα πολύ μικρό ποσοστό την έκρινε ως άριστη.



Εικόνα 17. Ραβδόγραμμα συνολικής αξιολόγησης ιστοσελίδας www.dpa.gr

Περίπου οι πέντε στους δέκα εξέφρασαν την ικανοποίηση τους σε σχέση με το περιεχόμενο και τη σχεδίαση του ενημερωτικού δελτίου (newsletter) της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

Η συζήτηση τώρα κινείται γύρω από ερωτήσεις που σκοπό έχουν να αξιολογήσουν το ενημερωτικό δελτίο (newsletter) της Αρχής. Για να μπορέσει κανείς να εκφράσει την άποψη του για το περιεχόμενο και το σχεδιασμό του ενημερωτικού δελτίου θα πρέπει να το λαμβάνει. Από το σύνολο των 153 συμπληρωμένων και έγκυρων ερωτηματολογίων, 65 εξ αυτών ποσοστό (42,5%), όπως διαπιστώθηκε από το σύνολο των απαντήσεων, δεν απάντησαν το συγκεκριμένο ερώτημα. Αυτό συνεπάγεται ότι δεν ελάμβαναν το ενημερωτικό δελτίο της Αρχής, συνεπώς δεν μπορούσαν να το

αξιολογήσουν. Συμπερασματικά, ο συνολικός αριθμός των ατόμων που βαθμολόγησαν το περιεχόμενο και το σχεδιασμό του ενημερωτικού δελτίου είναι 88.

6. Λαμβάνετε το ενημερωτικό δελτίο (newsletter) της Αρχής; Εάν ναι, σε κλίμακα από το 1 μέχρι το 5, με άριστα το 5, πώς θα το βαθμολογούσατε σε σχέση με το περιεχόμενο και τη σχεδίασή του;		**Καθόλου καλό**	**Λίγο καλό**	**Μέτριο**	**Πολύ καλό**	**Άριστο**	**Σύνολο**
Οι πληροφορίες είναι ενδιαφέρουσες	Άτομα	0	1	6	47	34	88
	% του Συνόλου	0,0%	1,1%	6,8%	53,4%	38,6%	100,0%
Οι πληροφορίες είναι χρήσιμες	Άτομα	0	1	8	40	39	88
	% του Συνόλου	0,0%	1,1%	9,1%	45,5%	44,3%	100,0%
Οι σύνδεσμοι είναι ενημερωμένοι	Άτομα	0	0	12	42	34	88
	% του Συνόλου	0,0%	0,0%	13,6%	47,7%	38,6%	100,0%
Η οργάνωση και παρουσίαση είναι φιλική στην πλοήγησή του	Άτομα	0	0	19	44	25	88
	% του Συνόλου	0,0%	0,0%	21,6%	50,0%	28,4%	100,0%
Αισθητική - Σχεδιασμός	Άτομα	0	5	35	32	16	88
	% του Συνόλου	0,0%	5,7%	39,8%	36,4%	18,2%	100,0%

Πίνακας 30. Αξιολόγηση του ενημερωτικού δελτίου (newsletter) σε σχέση με το περιεχόμενο και τη σχεδίαση

Παραπάνω από τους μίσους συμμετέχοντες (53,4%) που αξιολογήσαν το ενημερωτικό δελτίο, βαθμολόγησαν ως πολύ καλό το γεγονός ότι οι πληροφορίες που παρέχει είναι ενδιαφέρουσες, ενώ ένα αντίστοιχα πολύ υψηλό ποσοστό της τάξεως του (38,6%), περίπου οι τέσσερις στους δέκα, το έκρινε ως άριστο.

Η πλειονότητα των ερωτηθέντων (45,5%) βαθμολόγησαν ως πολύ καλή την χρησιμότητα των πληροφοριών που διατίθενται μέσω του newsletter στο κοινό. Κάτι παραπάνω όμως από τέσσερις στους δέκα ποσοστό (44,3%), το μεγαλύτερο στη

βαθμίδα «Άριστο» της κλίμακας, την αξιολόγησαν ως άριστη, ενώ μέτρια την έκρινε το (9,1%) των συμμετεχόντων στην έρευνα.

Το (47,7%) των ερωτηθέντων αξιολόγησαν ως πολύ καλή την επικαιροποίηση των συνδέσμων που φιλοξενούνται στο ενημερωτικό δελτίο, ενώ ένα ποσοστό της τάξεως του (38,6%) την έκριναν ως άριστη. Ωστόσο σημαντικό είναι και το ποσοστό των ερωτηθέντων (13,6%) που βαθμολόγησαν την επικαιροποίηση των συνδέσμων ως μέτρια και αυτό γιατί είναι αρκετά μεγαλύτερο σε σύγκριση με τα αντίστοιχα ποσοστά αυτών που έκριναν ως μέτρια τόσο τη χρησιμότητα των πληροφοριών όσο και το ενδιαφέρον που παρουσιάζουν στο κοινό.

Όσον αφορά τα κριτήρια αξιολόγησης για την οργάνωση και παρουσίαση των πληροφοριών που παρέχει το ενημερωτικό δελτίο στο κοινό και την αισθητική – σχεδιασμό του, οι συμμετέχοντες στην έρευνα τα βαθμολόγησαν ως πολύ καλά με ποσοστά (50,0%) και (36,4%) αντίστοιχα.

Για τα δυο αυτά κριτήρια, όπως και στα αντίστοιχα ίδια κριτήρια για την αξιολόγηση της ιστοσελίδας της Αρχής, παρατηρείται μια σημαντική διαφοροποίηση στα ποσοστά της 5βάθμιας λεκτικής κλίμακας βαθμολόγησης σε σχέση με τα υπόλοιπα κριτήρια αξιολόγησης του ενημερωτικού δελτίου. Για μεν το κριτήριο του κατά πόσο η οργάνωση της πληροφορίας και η παρουσίαση βοηθούν στη φιλική πλοήγηση του, το ποσοστό που το βαθμολόγησε ως μέτριο είναι (21,6%), ενώ για το κριτήριο που έχει να κάνει με την αισθητική και το σχεδιασμό το ποσοστό αγγίζει το (39,8%), το μεγαλύτερο στη βαθμίδα «Μέτρια» της κλίμακας. Η μεγάλη όμως διαφοροποίηση εμφανίζεται σε εκείνους που τα αξιολόγησαν ως άριστα με ποσοστά (28,4%) και (18,2%) αντίστοιχα, όπου είναι και τα δυο χαμηλότερα στην βαθμίδα «Άριστο» της 5βάθμιας λεκτικής κλίμακας. Αξιοσημείωτο είναι επίσης το γεγονός ότι το (5,7%) βαθμολόγησε την αισθητική και το σχεδιασμό της ιστοσελίδας ως λίγο καλό, το υψηλότερο ποσοστό στην βαθμίδα «Λίγο καλό» της κλίμακας.

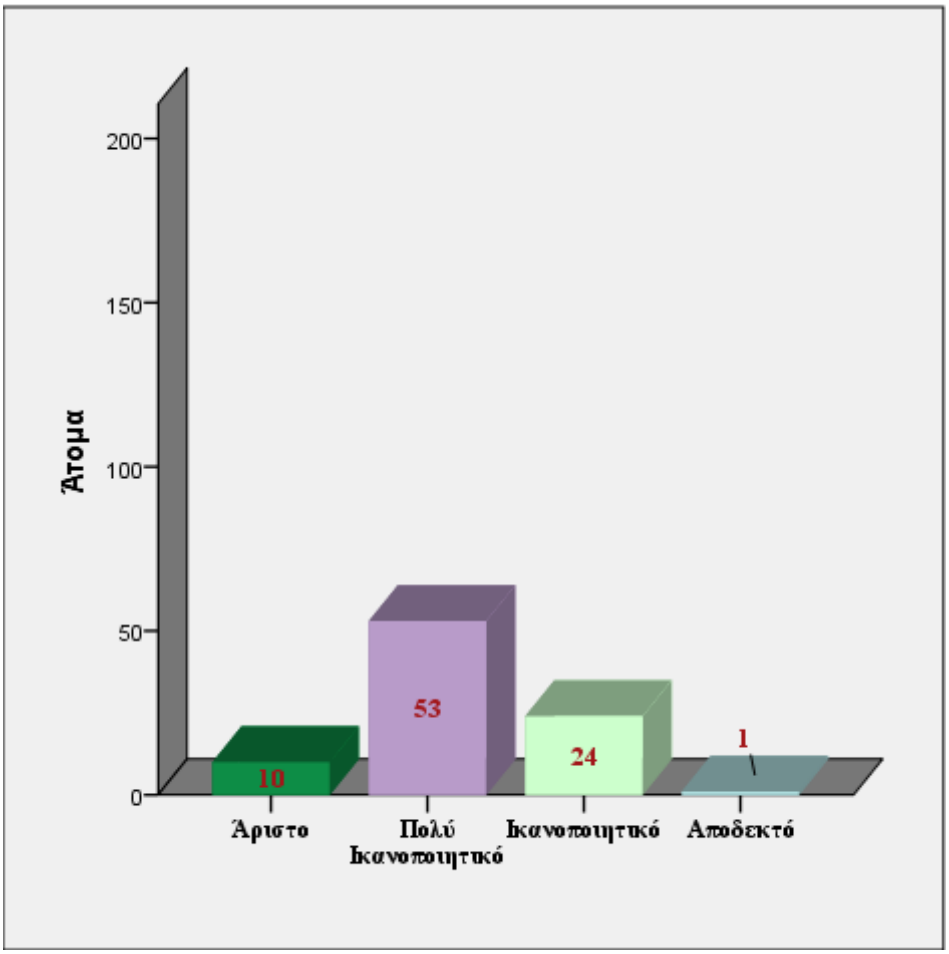
Έξι στους δέκα είναι πολύ ικανοποιημένοι από το ενημερωτικό δελτίο (newsletter) της Αρχής.

7. Αξιολογήστε συνολικά το newsletter της Αρχής.	Άτομα	Ποσοστό % του συνόλου	Ποσοστό %
Άριστο	10	6,5	11,4
Πολύ Ικανοποιητικό	53	34,6	60,2
Ικανοποιητικό	24	15,7	27,3
Αποδεκτό	1	,7	1,1
Σύνολο	88	57,5	100,0
Δεν απάντησαν γιατί δεν λαμβάνουν το newsletter	65	42,5	
Σύνολο	153	100,0	

Πίνακας 31. Συνολική αξιολόγηση του ενημερωτικού δελτίου (newsletter)

Από το πλήθος των 88 ερωτηθέντων που ελάμβαναν το ενημερωτικό δελτίο της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και ήταν σε θέση να αξιολογήσουν την συνολική εικόνα του, η πλειοψηφία αυτών, ποσοστό (71,6%), το βαθμολόγησαν από πολύ ικανοποιητικό έως άριστο, με το (60,2%) να το κρίνει πολύ ικανοποιητικό και το (11,4%) άριστο.

Ένα ποσοστό όμως εκ των συμμετεχόντων (27,3%) το αξιολόγησαν ως απλά ικανοποιητικό, ενώ σε αντίθεση ένα πολύ μικρό ποσοστό το έκρινε ως αποδεκτό.



Εικόνα 18. Ραβδόγραμμα συνολικής αξιολόγησης ενημερωτικού δελτίου (newsletter)

5.2. Συμπεράσματα

Β. Μέρος.

Από την ανάλυση των ερωτήσεων του δεύτερου μέρους προέκυψαν χρήσιμα συμπεράσματα στο κατά πόσο οι πολίτες γνωρίζουν τη νομοθεσία για την προστασία προσωπικών δεδομένων και για τις γνώσεις και δεξιότητες τους αναφορικά με τη πλοήγηση στο διαδίκτυο και τη χρήση συναφών υπηρεσιών και μέσων κοινωνικής δικτύωσης.

Δεν αποτελεί έκπληξη το γεγονός ότι ένα μεγάλο ποσοστό των ερωτηθέντων και κατά επέκταση θα μπορούσε να πει κανείς ένα μεγάλο ποσοστό των Ελλήνων πολιτών χρησιμοποιεί πλέον σε τακτική βάση τις διαδικτυακές (online) υπηρεσίες όπως

τα κοινωνικά δίκτυα και την αγορά αγαθών ή υπηρεσιών μέσω διαδικτύου. Ωστόσο, η έκθεση δείχνει σαφώς πως οι περισσότεροι εξ αυτών ανησυχούν πολύ για την καταγραφή των καθημερινών διαδικτυακών δραστηριοτήτων τους μέσω των κινητών τηλεφώνων, μέσω των καρτών πληρωμής και μέσω των ιστοσελίδων και όχι τόσο πολύ για την καταγραφή των καθημερινών δραστηριοτήτων τους μέσω καμερών, με πάνω από το ένα δέκατο να μην ανησυχούν καθόλου για το γεγονός της καταγραφής τους από κάμερες.

Είναι επίσης σημαντικό ότι οι περισσότεροι ερωτηθέντες, παρόλο που δεν αισθάνονται αρκετά άνετα με ιστοσελίδες που χρησιμοποιούν πληροφορίες σχετικά με τη διαδικτυακή δραστηριότητά που έχουν, αποδέχονται την ψηφιακή εποχή και τη συλλογή δεδομένων καθώς αποτελεί μέρος της σύγχρονης ζωής, αρκεί να είναι γνώστες των συνθηκών συλλογής και χρήσης των ηλεκτρονικών προσωπικών δεδομένων τους.

Από την άποψη αυτή, επτά στους δέκα ερωτηθέντες εκφράζουν μεγάλη δυσπιστία ως προς τα μέτρα που λαμβάνονται για την ασφαλή τήρηση των ηλεκτρονικών προσωπικών δεδομένων τους στο διαδίκτυο. Θεωρούν δε, ότι δεν έχουν τον πλήρη έλεγχο των πληροφοριών που παρέχουν σε απευθείας σύνδεση και ότι αυτό εξαρτάται από την ιστοσελίδα ή την εφαρμογή που τα διαχειρίζεται. Αφετέρου, είναι ιδιαίτερα εντυπωσιακό ότι οι εννιά στους δέκα ερωτηθέντες ανησυχούν με το γεγονός ότι δεν έχουν τον πλήρη έλεγχο των πληροφοριών που παρέχουν σε απευθείας συνδέσεις.

Το αίσθημα έλλειψης του πλήρη ελέγχου υπογραμμίζει την ανάγκη για την περαιτέρω μεταρρύθμιση του τοπίου προστασίας δεδομένων στην Ευρώπη, τόσο όσον αφορά την παροχή στις επιχειρήσεις σαφών προτύπων που πρέπει να πληρούν, όσο και για την οικοδόμηση της εμπιστοσύνης του κοινού με το διαδίκτυο και ότι τα δικαιώματά του στην πραγματικότητα προστατεύονται. Αυτό ενισχύεται και από το γεγονός ότι περίπου τα δύο τρίτα των ερωτηθέντων θεωρούν ως κατάλληλο για την διασφάλιση και ενημέρωση τους, εάν οι προσωπικές πληροφορίες που παρέχουν στο διαδίκτυο – cloud χαθούν ή κλαπούν, τις ίδιες τις διαδικτυακές εταιρείες που διαχειρίζονται τα δεδομένα καθώς και τις υπεύθυνες δημόσιες αρχές.

Η έκθεση καταδεικνύει επίσης ότι η πλειοψηφία των ερωτηθέντων έχουν ευρύτατες ανησυχίες σχετικά με τις ρυθμίσεις απορρήτου τόσο του φυλλομετρητή (browser) αναφορικά με τη λήψη cookies όσο και με τις ρυθμίσεις απορρήτου των μέσων κοινωνικής δικτύωσης. Περισσότεροι από έξι στους δέκα γνωρίζουν και κάνουν χρήση της δυνατότητας των ρυθμίσεων απορρήτου που έχουν τα προγράμματα περιήγησης, ενώ πάνω από εφτά στους δέκα προσαρμόζουν τις αρχικές ρυθμίσεις απορρήτου των διαδικτυακών μέσων κοινωνικής δικτύωσης.

Όλες αυτές οι ανησυχίες υποστηρίζουν και πάλι τη δέσμευση της Ευρωπαϊκής Ένωσης για επικαιροποίηση και βελτίωση του καθεστώτος και του νομοθετικού πλαισίου προστασίας δεδομένων και της αναβάθμισης και ουσιαστικής ενίσχυσης των αρμόδιων αρχών, με απώτερο σκοπό την αποτελεσματικότερη και ποιοτικότερη προστασία των δικαιωμάτων των πολίτων όσον αφορά τα προσωπικά δεδομένα. Την ριζική αναμόρφωση λοιπόν του νομικού πλαισίου προστασίας των προσωπικών δεδομένων που επέβαλαν οι τεχνολογικές εξελίξεις καλείται πλέον να αντιμετωπίσει ο Γενικός Κανονισμός Προστασίας των προσωπικών δεδομένων με την καθολική εφαρμογή του να ισχύει από την 25η Μαΐου 2018.

Γ. Μέρος - Ιστοσελίδα.

Από την ανάλυση των ερωτήσεων του τρίτου μέρους που αφορούσαν την αξιολόγηση για πρώτη φορά της ιστοσελίδας (www.dpa.gr) και του ενημερωτικού δελτίου (newsletter) της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα εξήχθησαν χρήσιμα συμπεράσματα για το βαθμό ικανοποίησης των πολίτων για το ενημερωτικό έργο της Αρχής μέσω της ιστοσελίδας και του ενημερωτικού δελτίου.

Το σύνολο των πολιτών που παραβρέθηκαν στη διάρκεια των τριών ενημερωτικών ημερίδων γνώριζαν την ύπαρξη της ιστοσελίδας (www.dpa.gr) και κατ' επέκταση την ύπαρξη της αρμόδιας αρχής για την προστασία των προσωπικών δεδομένων, της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, που καλείται με το έργο της να προστατεύσει και να θωρακίσει την κοινωνία και τους πολίτες στην εποχή της «ψηφιοποίησης». Παρόλα αυτά όμως το ποσοστό επισκεψιμότητας της ιστοσελίδας της Αρχής είναι αρκετά χαμηλό, αν αναλογιστεί κανείς πως κοντά στα δυο

τρίτα των ερωτηθέντων την επισκέπτονται το πολύ μια φορά τον μήνα, ενώ καθημερινά την επισκέπτεται μόλις το (6,5%) εκ των ερωτηθέντων.

Πάνω από οκτώ στους δέκα αξιολόγησαν την συνολική εικόνα της ιστοσελίδας της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα από ικανοποιητική έως πολύ ικανοποιητική. Το αίσθημα ικανοποίησης ενισχύεται και από το γεγονός ότι σε επιμέρους κριτήρια αξιολόγησης για το περιεχόμενο, τη σχεδίαση και την πλοήγηση, η πλειονότητα των ερωτηθέντων τα βαθμολόγησε από μέτρια ως πολύ καλά. Ωστόσο, η έκθεση καταδεικνύει συγκεκριμένους τομείς που χρήζουν σημαντικής βελτίωσης. Πιο συγκεκριμένα, παρατηρείται αίσθημα δυσαρέσκειας για την ομοιομορφία και την συγκεκριμένη εμφάνιση που έχει ο ιστότοπος σε όλες τις σελίδες του, με πέντε στους δέκα να την κρίνουν από μέτρια ως καθόλου καλή, για την οργάνωση και παρουσίαση της πληροφορίας, με έναν στους τρείς να την κρίνει από μέτρια ως καθόλου καλή, καθώς και για την αισθητική και το σχεδιασμό της ιστοσελίδας, με εφτά στους δέκα να την αξιολογούν από μέτρια ως καθόλου καλή.

Είναι επίσης σημαντικές και χρήζουν αναφοράς, οι παρατηρήσεις που έγιναν για τη βελτίωση της ιστοσελίδας, στο πεδίο ελεύθερου σχολιασμού που υπήρχε στο ερωτηματολόγιο. Παρατηρήσεις που ενισχύουν το αίσθημα δυσαρέσκειας των πολιτών για την σχεδίαση και την δυνατότητα εύκολης πλοήγησης.

Παράθεση παρατηρήσεων ερωτηθέντων για τη βελτίωση της ιστοσελίδας (www.dpa.gr):

«Δεν είναι ενημερωμένη η αγγλική έκδοση της ιστοσελίδας.

Με το διαθέσιμο περιεχόμενο, είναι κρίμα να έχει αισθητική 90΄ς. Ένας πιο μοντέρνος σχεδιασμός θα ενέπνεε περισσότερη εμπιστοσύνη ακόμα και σε μη νομικούς.

Ο μηχανισμός αναζήτησης μπορεί να αναβαθμιστεί (κριτήρια για καλύτερα αποτελέσματα).

Να ανανεωθεί ως «feel and view» και να γίνει πιο φιλική προς τον χρήστη και με συνδέσμους σε άλλες σχετικές ιστοσελίδες πιο εμφανείς και περισσότερους.

Χρήζει βελτίωσης η δυνατότητα αναζήτησης αποφάσεων της Αρχής.

Πολλές πρακτικές λεπτομέρειες απουσιάζουν. Η ιστοσελίδα ενημερώνεται μη επαρκώς και με μεγάλη καθυστέρηση.

Πολύ καλό το επίπεδο, πάντα υπάρχουν γενικά περιθώρια βελτίωσης, για τα οποία ευχαριστούμε πολύ εκ των προτέρων.

Δεν ενημερώνεται αρκετά συχνά. Δεν είναι αρκετά κείμενα στα αγγλικά.

Συμπλήρωση της ενότητας σχετικά με τις υποχρεώσεις του υπευθύνου επεξεργασίας.

Παρουσιάζονται συχνά προβλήματα «ταχύτητας». Επίσης, πρέπει οι θεματικές ενότητες να εμπλουτιστούν και να είναι πιο αποτελεσματική η αναζήτηση.

Αναζήτηση με «λέξεις κλειδιά» μπορεί να μη δώσει αποτέλεσμα, ενώ αν γίνει αναζήτηση από το χρήστη της ιστοσελίδας δια πλοηγήσεως π.χ. στις αποφάσεις «βήμα – βήμα» μπορεί να οδηγήσει σε εύρεση του αντικειμένου που ψάχνει ο χρήστης. Η αναζήτηση καλύπτει το περιεχόμενο των αποφάσεων;

Θα ήταν ιδιαίτερα χρήσιμο να υπάρχει συνεχής ενημέρωση για ζητήματα της επικαιρότητας (π.χ. privacy shield) με αναφορές σε νομολογία κ.λπ..

Ως προς το περιεχόμενο θα έπρεπε να υπάρχει εκτενέστερη αναφορά στο GDPR και στον υπό διαβούλευση κανονισμό e-privacy.

Λείπουν σχόλια σε επίκαιρα θέματα και σχετική αρθρογραφία διεθνής και πανελλαδική».

Γ. Μέρος - Ενημερωτικό δελτίο (newsletter).

Το «newsletter» αποτελεί ουσιαστικά ενημερωτικό δελτίο προώθησης των υπηρεσιών και του έργου της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, και κατ' επέκταση της ιστοσελίδας «www.dpa.gr» της Αρχής. Αποστέλλεται μέσω ηλεκτρονικού ταχυδρομείου, «e-mail newsletter», στους επισκέπτες που γράφτηκαν σε αυτό, περιστασιακά ή ανά τακτά χρονικά διαστήματα και απαρτίζεται από ειδήσεις, ανακοινώσεις, αναλύσεις, πληροφόρηση, χρήσιμες συμβουλές, απαντήσεις σε συχνές ερωτήσεις, υπενθυμίσεις ή ακόμη και προειδοποιήσεις, διατηρώντας πάντοτε τον ενημερωτικό του χαρακτήρα.

Σήμερα η έκδοση ενός «e-mail newsletter» τείνει να αποτελέσει κανόνα. Οι λόγοι για τους οποίους έγιναν τόσο δημοφιλή τα «e-mail newsletter» είναι γιατί τα email αποτελούν τη μόνη εφαρμογή τύπου «push technology» που εφαρμόζεται με επιτυχία. Με την δυνατότητα αυτή, δημιουργείται ένα δυναμικό κανάλι επικοινωνίας

με σκοπό την ενημέρωση του κοινού και αποφεύγεται ο παθητικός τρόπος επίσκεψης της ιστοσελίδας της Αρχής. Με τον τρόπο αυτό αυξάνεται δραματικά η δημοτικότητα της ιστοσελίδας «www.dpa.gr» και υπενθυμίζεται συνέχεια στο κοινό η ύπαρξη και το έργο της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

Όμως, η έκθεση δείχνει πως από το σύνολο των 153 συμπληρωμένων και έγκυρων ερωτηματολογίων, λίγο πάνω από ένα στα τρία, δεν είχε αξιολόγηση για το ενημερωτικό δελτίο. Γνώριζαν δηλαδή την ύπαρξη του «newsletter» της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και κατ' επέκταση το ελάμβαναν, μόλις οι 88 εκ των ερωτηθέντων. Αυτό από μόνο του καταδεικνύει την έλλειψη και το κενό ενημέρωσης και επικοινωνίας που υπάρχει σε αυτό το σημείο με τους πολίτες. Δεν αποτελεί έκπληξη το γεγονός αυτό αν αναλογιστεί κανείς και το αρκετά χαμηλό ποσοστό επισκεψιμότητας της ιστοσελίδας «www.dpa.gr».

Παρόλο το κενό ενημέρωσης και επικοινωνίας που παρατηρήθηκε να υπάρχει μέσω του ενημερωτικού δελτίου, η ανάλυση των ερωτηματολογίων αναδεικνύει την μεγάλη ικανοποίηση των συμμετεχόντων στην έρευνα, για το περιεχόμενο και τη σχεδίαση του ενημερωτικού δελτίου. Πάνω από εφτά στους δέκα αξιολόγησαν την συνολική εικόνα του «newsletter» της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα από πολύ ικανοποιητική έως άριστη.

Η πολύ καλή εντύπωση που αφήνει το ενημερωτικό δελτίο στους πολίτες ενισχύεται και από το γεγονός ότι σε επιμέρους κριτήρια αξιολόγησης για το περιεχόμενο και την οργάνωση, η πλειονότητα των ερωτηθέντων τα βαθμολόγησε από πολύ καλά έως άριστα. Ωστόσο, η έκθεση καταδεικνύει έναν συγκεκριμένο τομέα που χρήζει προσοχής και βελτίωσης. Πιο συγκεκριμένα, παρατηρείται διαφοροποίηση στον βαθμό ικανοποίησης, σε σχέση με τα άλλα κριτήρια, του κριτηρίου αξιολόγησης για την αισθητική και τον σχεδιασμό, με την πλειονότητα των ερωτηθέντων να το βαθμολογεί από μέτριο έως πολύ καλό.

Όπως στην περίπτωση αξιολόγησης της ιστοσελίδας «www.dpa.gr», έτσι και εδώ, οι παρατηρήσεις που έγιναν για τη βελτίωση του ενημερωτικού δελτίου στο πεδίο ελεύθερου σχολιασμού που υπήρχε στο ερωτηματολόγιο, είναι σημαντικές και χρήζουν αναφοράς. Παρατηρήσεις που θα βοηθήσουν στην ποιοτική αναβάθμιση του newsletter

και γενικά στην βελτίωση του επιπέδου επικοινωνίας και υπηρεσιών της Αρχής προς τους πολίτες.

Παράθεση παρατηρήσεων ερωτηθέντων για τη βελτίωση του «newsletter»:

«Σύνδεσμοι προς τις αποφάσεις, και περισσότερες Ερωτήσεις και Απαντήσεις.

Χρειάζεται να ανανεωθεί η αισθητική του και να γίνει πιο φιλικό προς τον αναγνώστη.

Το newsletter περιλαμβάνει πληροφορίες ή υποθέσεις που δεν ενδιαφέρουν παρά μόνο συγκεκριμένους υπευθύνους και κυρίως φορείς του δημοσίου. Επίσης, το newsletter δεν στέλνεται τακτικά και σε όλους όσους έχουν δηλώσει ότι ενδιαφέρονται να το λαμβάνουν.

Ίσως περισσότερες αναφορές σε ευρωπαϊκές και διεθνείς εξελίξεις πέραν των θεσμικών οργάνων της Ευρωπαϊκής Ένωσης.

Θα χρησίμευε πολύ να ήταν πιο «updated» με πολύ επίκαιρα ζητήματα σε ειδική ενότητα».

5.3. Μελλοντική έρευνα

Τα ηλεκτρονικά προσωπικά δεδομένα είναι ένα αγαθό που πρέπει να διαφυλάσσεται και να μην υποτιμάτε η αξία του. Το διαδίκτυο (παρά τα αναμφισβήτητα πλεονεκτήματά του) αυξάνει, εκ φύσεως, τους κινδύνους παράνομης επεξεργασίας τους. Ο κάθε ένας από εμάς, συνεπώς, πρέπει να είναι ενήμερος για τους κινδύνους και να χρησιμοποιεί πάντοτε το διαδίκτυο με σύνεση: η πλήρης ευαισθητοποίηση γύρω από τα προσωπικά δεδομένα είναι το πρώτο, πολύ σημαντικό, βήμα προς αυτήν την κατεύθυνση.

Η ανωτέρω προσπάθεια καταγραφής των γνώσεων, συνεπώς και της ευαισθητοποίησης, που έχουν οι πολίτες σχετικά με τα προσωπικά δεδομένα και την πλοήγηση στο διαδίκτυο έγινε με γνώμονα το ισχύων νομικό πλαίσιο προστασίας των δεδομένων προσωπικού χαρακτήρα. Ωστόσο, οι τεράστιες δυνατότητες της τεχνολογίας της πληροφορικής και οι τεχνολογικές εξελίξεις επέβαλαν την ριζική

αναμόρφωση του νομικού πλαισίου. Από την 25η Μαΐου 2018 τίθεται σε καθολική εφαρμογή ο Γενικός Κανονισμός για την Προστασία των Δεδομένων. Οποιαδήποτε προσπάθεια διεξαγωγής μελλοντικής έρευνας θα πρέπει πλέον να γίνει με βάση τον Γενικό Κανονισμό Προστασίας Δεδομένων. Έρευνα, που να καταδεικνύει το κατά πόσο οι πολίτες αλλά και οι φορείς ιδιωτικού και δημόσιου φορέα είναι ενήμεροι για τις ισχύουσες αλλαγές που εισαγάγει, αλλά και το αν τελικά καταφέρει να επιτύχει την ενίσχυση του αισθήματος ασφάλειας στους πολίτες - χρήστες του διαδικτύου, ούτως ώστε να το χρησιμοποιούν για βελτίωση της ζωής τους και να μην το αντιμετωπίζουν σαν έναν μελλοντικό παράγοντα καταδυνάστευσης και καταπάτησης των ηλεκτρονικών προσωπικών δεδομένων και συνεπώς των ελευθεριών τους.

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα είναι ο αρμόδιος φορέας για την εφαρμογή της ισχύουσας νομοθεσίας για τα προσωπικά δεδομένα στην Ελλάδα (νόμοι 2472/1997 και 3471/2006), αλλά και από την 25η Μαΐου 2018 για την εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων. Τα ευρήματα αυτής της έρευνας κατέδειξαν το σημαντικό έργο που επιτελεί η Αρχή με το να παρέχει πληροφορίες και να ενημερώνει τους πολίτες για θέματα προσωπικών δεδομένων αλλά και την ουσιαστική ανανέωση που οφείλει να κάνει στα μέσα προώθησης των υπηρεσιών και του έργου της (ιστοσελίδα (www.dpa.gr) και ενημερωτικό δελτίο (newsletter)). Ενόψει και της εφαρμογής του Γενικού Κανονισμού η δημοτικότητα της ιστοσελίδας και του ενημερωτικού δελτίου θα αυξηθεί σημαντικά. Ενδιαφέρον θα είχε λοιπόν, μελλοντική έρευνα ικανοποίησης που θα διεξαγόταν μετά και την υιοθέτηση όλων αυτών των αλλαγών, αναβαθμίσεων σε όσο το δυνατόν όμως μεγαλύτερο και επαρκώς αντιπροσωπευτικότερο δείγμα πληθυσμού. Η αλληλεπίδραση αυτή μέσω των ερωτηματολογίων ικανοποίησης, αξιολόγησης θα οδηγούσε βαθμιαία στη δημιουργία πιστού αναγνωστικού κοινού και θα αναπτυσσόταν γρηγορότερα μία σχέση εμπιστοσύνης με τους πολίτες.

6. ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Κ. Λιμνιώτης, Α. Μπούρκα, Γ. Παναγοπούλου, ειδικοί επιστήμονες ΑΠΔΠΧ, «Προσωπικά δεδομένα και Διαδίκτυο», 3ο τεύχος του δημιναίου ενημερωτικού δελτίου του saferinternet.gr, 04 Ιουλίου 2011, [online] <http://saferinternet.gr/index.php?action=download&objId=File411>.

[2] Δημήτριος Δρούτσας, Ευρωβουλευτής, τ. Υπουργός Εξωτερικών, «Γενική εισαγωγή στο σχέδιο Κανονισμού και Οδηγίας», Κείμενα Εισηγήσεων Επετειακή Διημερίδα 15 Χρόνια Λειτουργίας της ΑΠΔΠΧ, 2014 σελ 85-86.

[3] Ευρωπαϊκή Επιτροπή, [online] <https://europa.eu/european-union/about-eu/institutions-bodies/european-commission_el>.

[4] European Commission, Special Eurobarometer 431 “Data protection”, European Union, 2015.

[5] Λίλιαν Μήτρου, Καθηγήτρια στο Πανεπιστήμιο Αιγαίου (Τμήμα Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων), «Το δίκαιο στην κοινωνία της πληροφορίας», Εκδόσεις Σάκκουλα 2002.

[6] Beniger, James R, (1986), The Control Revolution: Technological and Economic Origins of the Information Society, Cambridge, Mass.: Harvard University Press.

[7] Ιωάννης Τσουκαλάς, Ευρωβουλευτής, Ομότιμος Καθηγητής ΑΠΘ, «Ιδιωτικότητα και ανωνυμία στην Κοινωνία της Πληροφορίας», Κείμενα Εισηγήσεων Επετειακή Διημερίδα 15 Χρόνια Λειτουργίας της ΑΠΔΠΧ, 2014 σελ 105-107.

[8] Gunter Ollmann, The Vishing Guide, [δημοσίευση 2007 / τελευταία ενημέρωση 2013] [online] <http://www.windowsecurity.com/whitepapers/Phishing/Vishing-Guide.html>.

[9] Centre for the Protection of National Infrastructure, www.cpni.gov.uk, [online] <https://www.cpni.gov.uk/system/files/documents/87/93/spear-phishing-understanding-the-threat.pdf>.

[10] InfoSec Institute, “The Most Popular Social Network Phishing Schemes”, [online] <http://resources.infosecinstitute.com/the-most-popular-social-network-phishing-schemes/>.

[11] Kaspersky Lab, https://www.kaspersky.com, [online] <https://www.kaspersky.com/blog/1-in-5-phishing-attacks-targets-facebook/5180/>.

[12] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, www.dpa.gr, [online] <http://www.dpa.gr/portal/page?_pageid=33,127384&_dad=portal&_schema=PORTAL>.

[13] Infographic έρευνας «Παιδιά και διαδίκτυο», 13 Φεβρουαρίου 2015, [online] <https://communicationeffect.com/cyber-crime-authority-survey/>.

[14] «Κρατώντας τα παιδιά μας ασφαλή στο Διαδίκτυο», http://www.safekids.gr, 1 Ιουνίου 2015, [online]<http://www.safekids.gr/%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1/%CE%BA%CF%81%CE%B1%CF%84%CF%8E%CE%BD%CF%84%CE%B1%CF%82-%CF%84%CE%B1-%CF%80%CE%B1%CE%B9%CE%B4%CE%B9%CE%AC-%CE%BC%CE%B1%CF%82-%CE%B1%CF%83%CF%86%CE%B1%CE%BB%CE%AE-%CF%83%CF%84%CE%BF-%CE%B4%CE%B9%CE%B1%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%BF >.

[15] Ελληνικό Κέντρο Ασφαλούς Διαδικτύου, http://saferinternet4kids.gr/, [online] <http://saferinternet4kids.gr/category/paidia/>.

[16] Ευρωπαϊκή Ένωση, Κώδικας επιγραμμικών δικαιωμάτων στην ΕΕ, Λουξεμβούργο 2012, [online] <https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/Code%20EU%20online%20rights%20EL%20final.pdf>.

[17] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, [online] <http://www.dpa.gr>.

[18] Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, [online] <http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=8194&Itemid=378&lang=>.

[19] European Independent Data Protection Authority, [online] <https://edps.europa.eu/about-edps/members-mission/supervisors_en>.

[20] Ευρωπαίος Επόπτης Προστασίας Δεδομένων ΕΕΔΠ, [online] <https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor_el>.

[21] EU Whoiswho, [online] <(http://europa.eu/whoiswho/public/index.cfm?lang=el>.

[22] Φόρμα καταγγελίας ΕΕΔΠ, [online] <https://edps.europa.eu/node/75>.

[23] Μιλτιάδης Χαλικιάς, Αναπληρωτής Καθηγητής ΑΕΙ Πειραιά ΤΤ, Αλεξάνδρα Μανωλέσου, Msc Biostatistics, Παναγιώτα Λάλου, Phd Mathematics, «Μεθοδολογία Έρευνας και Εισαγωγή στη Στατιστική Ανάλυση Δεδομένων με το IBM SPSS STATISTICS», Εκδόσεις ΣΕΑΒ 2015.

[24] Γ. Σαραφίδου, [online] <http://eclass.uth.gr/eclass/modules/document/file.php/SEAA187/%CE%9C%CE%AC%CE%B8%CE%B7%CE%BC%CE%B1%2013-5.ppt>.

[25] Γιάννης Δ. Κατερέλος, «Εισαγωγή στην κοινωνική έρευνα ΙΙ», Πάντειο Πανεπιστήμιο Κοινωνικών και Πολιτικών Επιστημών 2015, [online] <http://openeclass.panteion.gr/modules/document/file.php/TMD223/600094.pdf>.

[26] Τσαγρής Μιχαήλ, «Στατιστική με τη χρήση του IBM SPSS 22», 2014

[27] Dr.. Ευθυμία Νικήτα, «Έννοιες στατιστικής και εφαρμογές με το SPSS», 2012

[28] Νέλλας Ε., Ε.Ε.ΔΙ.Π., «Ανάλυση Δεδομένων με Χρήση του Στατιστικού Πακέτου SPSS για Windows», Γεωπονικό Πανεπιστήμιο Αθηνών Τμήμα Αγροτικής Οικονομίας & Ανάπτυξης Εργαστήριο Διοίκησης(Μανατζμεντ) Γεωργικών Επιχειρήσεων & Εκμεταλλεύσεων, 2005

7. ΠΑΡΑΡΤΗΜΑΤΑ

Ερωτηματολόγιο

Το παρόν ειδικό ερωτηματολόγιο αποτελεί μέρος της έρευνας που διεξάγεται στο πλαίσιο της διπλωματικής εργασίας του κ. Κωνσταντίνου Αϊδίνη (πληροφορικού) υπαλλήλου της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα με θέμα «**Πλοήγηση στο διαδίκτυο και ηλεκτρονικά προσωπικά δεδομένα. Μέτρηση βαθμού ικανοποίησης χρηστών της ιστοσελίδας και του newsletter της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα**» για την απόκτηση του μεταπτυχιακού τίτλου σπουδών Αυτοματισμός Παραγωγής και Υπηρεσιών του Τμήματος Αυτοματισμού του ΑΤΕΙ Πειραιά.

Σκοπός της έρευνας είναι να αντληθούν χρήσιμα συμπεράσματα σχετικά με το κατά πόσο οι πολίτες γνωρίζουν τη νομοθεσία για την προστασία προσωπικών δεδομένων καθώς και τις γνώσεις και δεξιότητές τους αναφορικά με την πλοήγηση στο διαδίκτυο και τη χρήση συναφών υπηρεσιών και μέσων κοινωνικής δικτύωσης. Επίσης, επιχειρείται η αξιολόγηση της ιστοσελίδας (www.dpa.gr) και του ενημερωτικού δελτίου (newsletter) της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

Ο συνολικός χρόνος που απαιτείται για τη συμπλήρωσή του δεν αναμένεται να ξεπεράσει τα 10 λεπτά. Παρακαλούμε να απαντήσετε σε όλες τις ερωτήσεις επιλέγοντας μία μόνο από τις πολλαπλές επιλογές που δίνονται ως πιθανές απαντήσεις σε κάθε επιμέρους ερώτηση. Σύμφωνα με την ερευνητική δεοντολογία, οι απαντήσεις σας είναι εμπιστευτικές, ενώ τα στοιχεία που παρέχετε θα χρησιμοποιηθούν μόνο για τη στατιστική ανάλυση και την εξαγωγή συμπερασμάτων στην παρούσα έρευνα.

Το ερωτηματολόγιο αποτελεί το κύριο μέσο άντλησης πληροφοριών και για το λόγο αυτό η συμβολή σας είναι ιδιαιτέρως σημαντική.

Σας ευχαριστούμε πολύ εκ των προτέρων για τη συνδρομή σας στην ολοκλήρωση της έρευνας.

Α. Μέρος

Το πρώτο μέρος περιλαμβάνει δημογραφικές ερωτήσεις.

Β. Μέρος

Το δεύτερο μέρος εμπεριέχει ερωτήσεις στο κατά πόσο οι πολίτες γνωρίζουν τη νομοθεσία για την προστασία προσωπικών δεδομένων και στις γνώσεις και δεξιότητες αναφορικά με τη πλοήγησή τους στο διαδίκτυο και τη χρήση συναφών υπηρεσιών και μέσων κοινωνικής δικτύωσης.

Πολλές ερωτήσεις σχετικά με το διαδίκτυο και τα μέσα κοινωνικής δικτύωσης έχουν βασιστεί σε αντίστοιχες ερωτήσεις από δημοσκοπήσεις του Ευρωβαρομέτρου (Special Eurobarometer 431 Data Protection 2015).

Γ. Μέρος

Το τρίτο μέρος επικεντρώνεται σε ερωτήσεις που αφορούν στην ιστοσελίδα (www.dpa.gr) και το ενημερωτικό δελτίο (newsletter) της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και στο κατά πόσο οι πολίτες γνωρίζουν την ύπαρξή τους. Ποια η γνώμη τους για το περιεχόμενο, τη σχεδίαση τους, την πλοήγηση στην ιστοσελίδα και την ανάγνωση του newsletter.

Α. Μέρος

1. **Φύλο**

☐ Άνδρας

☐ Γυναίκα

2. **Ηλικία**

☐ Έως 15

☐ 16-30

☐ 31-45

☐ 46 - 60

☐ 60 και άνω

3. **Επίπεδο εκπαίδευσης**

☐ Πρωτοβάθμια

☐ Δευτεροβάθμια

☐ Τριτοβάθμια

☐ Μεταπτυχιακό – Διδακτορικό

Β. Μέρος

1. **Σήμερα, πολλές από τις καθημερινές μας δραστηριότητες καταγράφονται με διάφορους τρόπους, όπως μέσω καμερών, καρτών πληρωμής, ιστοσελίδων, κλπ. Πόσο ανήσυχοι ή όχι είστε για αυτό; (*1=ΚΑΘΟΛΟΥ 2=ΛΙΓΟ 3=ΑΡΚΕΤΑ 4=ΠΟΛΥ*)**

	1	2	3	4
Μέσω καμερών	☐	☐	☐	☐
Μέσω καρτών πληρωμής	☐	☐	☐	☐
Μέσω χρήσης κινητού τηλεφώνου (smart phone)	☐	☐	☐	☐
Στο Internet	☐	☐	☐	☐

2. **Όπως ίσως γνωρίζετε, μερικές online επιχειρήσεις είναι σε θέση να παρέχουν δωρεάν υπηρεσίες, όπως οι μηχανές αναζήτησης, δωρεάν λογαριασμούς e-mail, κλπ, χάρη στα έσοδα που λαμβάνουν από τους διαφημιστές που προσπαθούν να προσεγγίσουν τους χρήστες των ιστοσελίδων αυτών. Πόσο άνετα νιώθετε με το γεγονός ότι οι εν λόγω ιστοσελίδες χρησιμοποιούν πληροφορίες σχετικά με την online δραστηριότητά σας για να προσαρμόσουν διαφημίσεις ή περιεχόμενο σύμφωνα με τα χόμπι και τα ενδιαφέροντά σας;**

☐ Πολύ άνετα

☐ Αρκετά άνετα

☐ Αρκετά άβολα

☐ Πολύ άβολα

☐ Δεν ξέρω

3. **Θα λέγατε ότι είστε γενικά ενήμερος σχετικά με τις συνθήκες της συλλογής δεδομένων και με τις περαιτέρω χρήσεις των ηλεκτρονικών προσωπικών δεδομένων σας;**

☐ Καθόλου

☐ Λίγο

☐ Αρκετά

☐ Πολύ

4. **Πιστεύετε ότι όταν δίνετε προσωπικά σας δεδομένα στο διαδίκτυο (για αγορά αγαθών ή υπηρεσιών μέσω διαδικτύου ή λοιπές συναλλαγές), η τήρησή τους είναι ασφαλής;**

☐ Πολύ σίγουρος

☐ Αρκετά σίγουρος

☐ Σίγουρος

☐ Καθόλου σίγουρος

☐ Δεν γνωρίζω

5. **Πόσο έλεγχο αισθάνεστε ότι έχετε στις πληροφορίες που παρέχετε σε απευθείας σύνδεση (online), π.χ. η ικανότητα να διορθώσετε, να αλλάξετε ή να διαγράψετε αυτές τις πληροφορίες;**

☐ Απόλυτο έλεγχο

☐ Μερικό έλεγχο

☐ Καθόλου έλεγχο

☐ Εξαρτάται από την ιστοσελίδα ή την εφαρμογή

☐ Δεν γνωρίζω

6. **Σε περίπτωση που δεν έχετε τον «*απόλυτο έλεγχο*» των πληροφοριών που παρέχετε στο διαδίκτυο, πόσο σας απασχολεί το γεγονός αυτό;**

☐ Με απασχολεί πολύ

☐ Με απασχολεί αρκετά

☐ Δεν με απασχολεί πολύ

☐ Δεν με απασχολεί καθόλου

☐ Δεν ξέρω

7. **Ποιος νομίζετε ότι θα πρέπει να σας διαβεβαιώσει ότι οι προσωπικές πληροφορίες που παρέχετε στο διαδίκτυο συλλέγονται, αποθηκεύονται και ανταλλάσσονται με ασφάλεια; (Μπορείτε να επιλέξετε παραπάνω από μια απαντήσεις)**

☐Online εταιρείες - Θα πρέπει να είναι υπεύθυνες, διότι θα χρειαστεί να εξασφαλίσουν ότι επεξεργάζονται πληροφορίες με ασφάλεια

☐ Εσύ - Θα πρέπει να ασχοληθείς με τα δικά σου στοιχεία

☐ Δημόσιες αρχές - Θα πρέπει να διασφαλίσουν ότι τα δεδομένα των πολιτών προστατεύονται

☐ Άλλοι

☐ Ποτέ δεν παρέχω προσωπικές πληροφορίες στο διαδίκτυο

☐ Δεν ξέρω

8. **Ποια δεδομένα σας αν χαθούν ή κλαπούν θα σας ανησυχούσαν περισσότερο;**

☐ Δεδομένα που αποθηκεύονται στον υπολογιστή

☐ Δεδομένα που αποθηκεύονται στο κινητό ή στο tablet

☐ Δεδομένα που αποθηκεύονται στο διαδίκτυο ή στο cloud

☐ Άλλο

☐ Δεν ξέρω

9. **Χρησιμοποιείτε τις ρυθμίσεις απορρήτου του φυλλομετρητή σας (browser) αναφορικά με τη λήψη cookies κατά την είσοδό σας σε ιστοσελίδες;**

☐ Ναι

☐ Όχι

☐ Δεν γνωρίζω

10. **Κάνετε χρήση μέσων κοινωνικής δικτύωσης (Facebook, Twitter, Linkedin, Instagram, Snapchat κλπ.);**

☐ Πολύ συχνά

☐ Συχνά

☐ Σχεδόν καθόλου

☐ Καθόλου

☐ Δεν γνωρίζω

11. **Όταν χρησιμοποιείτε μέσα κοινωνικής δικτύωσης (Facebook, Twitter, Linkedin, Instagram, Snapchat κλπ.), προσαρμόζετε τις αρχικές ρυθμίσεις απορρήτου;**

☐ Πολύ

☐ Αρκετά

☐ Ελάχιστα

☐ Καθόλου

☐ Δεν γνωρίζω

12. **Πόσο εύκολο ή δύσκολο σας είναι να βρείτε και να χρησιμοποιήσετε τις ρυθμίσεις απορρήτου στα μέσα κοινωνικής δικτύωσης (Facebook, Twitter, Linkedin, Instagram, Snapchat κλπ.);**

☐ Πολύ εύκολο

☐ Αρκετά εύκολο

☐ Εύκολο

☐ Δύσκολο

☐ Αρκετά δύσκολο

☐ Πολύ δύσκολο

☐ Δεν γνωρίζω

Γ. Μέρος

1. **Έχετε ποτέ επισκεφθεί την ιστοσελίδα (*www.dpa.gr)* της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα;**

   ☐ Ναι

   ☐ Όχι

2. **Εάν επισκέπτεστε την ιστοσελίδα (*www.dpa.gr*) της Αρχής πόσο συχνά το κάνετε;**

   ☐ Καθημερινά

   ☐ Μία φορά την εβδομάδα

   ☐ Μία φορά τον μήνα

   ☐ Λιγότερο από μία φορά τον μήνα

3. **Σε κλίμακα από το 1 μέχρι το 5, με άριστα το 5, πώς θα βαθμολογούσατε την ιστοσελίδα της Αρχής σε σχέση με το περιεχόμενο; (1=ΚΑΘΟΛΟΥ ΚΑΛΟ, 2=ΛΙΓΟ ΚΑΛΟ, 3=ΜΕΤΡΙΟ, 4=ΠΟΛΥ ΚΑΛΟ, 5=ΑΡΙΣΤΟ)**

	1	2	3	4	5
Οι πληροφορίες είναι επαρκείς	☐	☐	☐	☐	☐
Οι πληροφορίες είναι χρήσιμες	☐	☐	☐	☐	☐
Οι σύνδεσμοι είναι ενημερωμένοι	☐	☐	☐	☐	☐
Θεωρείτε φιλική τη δυνατότητα επικοινωνίας	☐	☐	☐	☐	☐

4. Σε κλίμακα από το 1 μέχρι το 5, με άριστα το 5, πώς θα βαθμολογούσατε την ιστοσελίδα της Αρχής σε σχέση με την σχεδίαση και την πλοήγηση; (1=ΚΑΘΟΛΟΥ ΚΑΛΗ, 2=ΛΙΓΟ ΚΑΛΗ, 3=ΜΕΤΡΙΑ, 4=ΠΟΛΥ ΚΑΛΗ, 5=ΑΡΙΣΤΗ)

	1	2	3	4	5
Φιλικότητα στη χρήση (Ο ιστότοπος έχει μια ομοιομορφία και μια συγκεκριμένη εμφάνιση σε όλες τις σελίδες του)	☐	☐	☐	☐	☐
Αναγνωσιμότητα (Οι σελίδες έχουν ευκρινείς γραμματοσειρές και χρώματα)	☐	☐	☐	☐	☐
Ταχύτητα (Οι σελίδες φορτώνουν γρήγορα)	☐	☐	☐	☐	☐
Οργάνωση της πληροφορίας (Η οργάνωση και παρουσίαση είναι φιλική στην πλοήγησή του. Βρίσκετε εύκολα αυτό που θέλετε)	☐	☐	☐	☐	☐
Αισθητική - Σχεδιασμός	☐	☐	☐	☐	☐

5. Αξιολογήστε συνολικά την ιστοσελίδα της Αρχής.

☐ Άριστη

☐ Πολύ Ικανοποιητική

☐ Ικανοποιητική

☐ Αποδεκτή

☐ Ανεπαρκής

Σε περίπτωση που την κρίνετε ανεπαρκή παρακαλώ σχολιάστε. Ευπρόσδεκτες τυχόν περαιτέρω παρατηρήσεις για τη βελτίωσή της.

6. **Λαμβάνετε το ενημερωτικό δελτίο (newsletter) της Αρχής; Εάν ναι, σε κλίμακα από το 1 μέχρι το 5, με άριστα το 5, πώς θα το βαθμολογούσατε σε σχέση με το περιεχόμενο και τη σχεδίασή του; (1=ΚΑΘΟΛΟΥ ΚΑΛΟ, 2=ΛΙΓΟ ΚΑΛΟ, 3=ΜΕΤΡΙΟ, 4=ΠΟΛΥ ΚΑΛΟ, 5=ΑΡΙΣΤΟ)**

	1	2	3	4	5
Οι πληροφορίες είναι ενδιαφέρουσες	☐	☐	☐	☐	☐
Οι πληροφορίες είναι χρήσιμες	☐	☐	☐	☐	☐
Οι σύνδεσμοι είναι ενημερωμένοι	☐	☐	☐	☐	☐
Η οργάνωση και παρουσίαση είναι φιλική στην πλοήγησή του	☐	☐	☐	☐	☐
Αισθητική - Σχεδιασμός	☐	☐	☐	☐	☐

7. **Αξιολογήστε συνολικά το newsletter της Αρχής.**

☐ Άριστο

☐ Πολύ Ικανοποιητικό

☐ Ικανοποιητικό

☐ Αποδεκτό

☐ Ανεπαρκές

Σε περίπτωση που το κρίνετε ανεπαρκές παρακαλώ σχολιάστε. Ευπρόσδεκτες τυχόν περαιτέρω παρατηρήσεις για τη βελτίωσή του.

Paper - Ελληνικό

Πλοήγηση στο διαδίκτυο και ηλεκτρονικά προσωπικά δεδομένα - Μέτρηση βαθμού ικανοποίησης χρηστών της ιστοσελίδας και του newsletter της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

ΑΪΔΙΝΗΣ ΚΩΝΣΤΑΝΤΙΝΟΣ
Τμήμα Μηχανικών Αυτοματισμού
Πανεπιστήμιο Εφαρμοσμένων Επιστημών Πειραιά
Π.Ράλλη & Θηβών 250, Αθήνα, 12244
ΕΛΛΑΔΑ
Kaidinis1@gmail.com

Περίληψη: - Τα τελευταία χρόνια η ανθρωπότητα ζει σε κλίμα αβεβαιότητας όσον αφορά την προστασία των προσωπικών δεδομένων. Η προστασία της ιδιωτικής ζωής θα αφορά, στο εξής, όχι μόνον το περιεχόμενο, αλλά και τα μεταδεδομένα που προκύπτουν από τις ηλεκτρονικές επικοινωνίες. Στην Ελλάδα η συμβολή της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) στη διαμόρφωση ενός φιλικού στην προστασία δεδομένων περιβάλλοντος είναι μεγάλη. Η μόνη βιώσιμη άμυνα έναντι των κινδύνων της ιδιωτικότητας είναι η ενδυνάμωση των «ψηφιακών πολιτών», η οποία επιτυγχάνεται μέσω της ενημέρωσης και της εκπαίδευσής τους για τους ψηφιακούς κινδύνους, τα δικαιώματα και τις υποχρεώσεις τους.

Με επίκεντρο λοιπόν τους «ψηφιακούς πολίτες», η συγκεκριμένη μελέτη έχει ως αντικείμενό της την προστασία της ιδιωτικής ζωής σε συνάρτηση με την ψηφιακή παγκοσμιοποίηση και την ραγδαία εξέλιξη των ηλεκτρονικών επικοινωνιών. Το βασικό ερώτημα στο οποίο θα προσπαθήσει να δώσει απάντηση η παρούσα εργασία είναι αν υπάρχει προστασία δεδομένων στην νέα εποχή των Τεχνολογιών Πληροφορικής και Επικοινωνιών που διανύει η ανθρωπότητα.

Πιο συγκεκριμένα, σκοπός της παρούσας διατριβής είναι να αντληθούν χρήσιμα συμπεράσματα σχετικά με το κατά πόσο οι πολίτες γνωρίζουν τη νομοθεσία για την προστασία προσωπικών δεδομένων, και κατέχουν τις απαραίτητες γνώσεις και δεξιότητες αναφορικά με την πλοήγηση στο διαδίκτυο και τη χρήση συναφών υπηρεσιών και μέσων κοινωνικής δικτύωσης.

Επίσης, επιχειρείται για πρώτη φορά η αξιολόγηση της ιστοσελίδας (www.dpa.gr) και του ενημερωτικού δελτίου (newsletter) της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και στο κατά πόσο οι πολίτες γνωρίζουν την ύπαρξή τους. Η αξιολόγηση αφορά στο ποια είναι η γνώμη των πολιτών για το περιεχόμενο, τη σχεδίαση και την πλοήγηση της ιστοσελίδας και την ανάγνωση του ενημερωτικού δελτίου.

Για την επίτευξη του ανωτέρου στόχου καταρτίσθηκε ειδικό ερωτηματολόγιο, που αποτέλεσε το κύριο μέσο άντλησης πληροφοριών για την υλοποίηση της μελέτης. Το ειδικό ερωτηματολόγιο αποτελείται από τρία μέρη: Α. Δημογραφικές ερωτήσεις, Β. Βαθμός ενημέρωσης των πολιτών σχετικά με το ισχύον νομοθετικό πλαίσιο για την προστασία των προσωπικών δεδομένων και με τις γνώσεις και δεξιότητές τους αναφορικά με τη πλοήγηση στο διαδίκτυο και τη χρήση συναφών υπηρεσιών και μέσων κοινωνικής δικτύωσης, Γ. Αξιολόγηση της ιστοσελίδας και του ενημερωτικού δελτίου της Αρχής.

Η στατιστική ανάλυση πραγματοποιήθηκε με την χρήση του εξειδικευμένου στατιστικού λογισμικού Statistical Package for Social Sciences (SPSS22). Το SPSS είναι ένα στατιστικό πακέτο που έχει πολλές δυνατότητες όσον αφορά την επεξεργασία και παρουσίαση των δεδομένων μιας επιστημονικής έρευνας αλλά και μεγάλη αξιοπιστία. Οι τελευταίες εκδόσεις του SPSS έχουν γραφικό περιβάλλον, πράγμα που το καθιστά πολύ εύκολο στη χρήση του [1].
Τα συμπεράσματα που εξήχθησαν από την στατιστική ανάλυση 153 ερωτηματολογίων που συμπληρώθηκαν θα επιφέρουν αποδοτικότερη διαχείριση των πόρων της Αρχής και ποιοτικότερες υπηρεσίες προς τους πολίτες, με σκοπό να δημιουργηθούν ικανές εγγυήσεις για την ιδιωτική ζωή και να διαμορφωθεί ένα ισχυρό πλαίσιο προστασίας.
Οι πολίτες, οι εκπαιδευτικοί, οι δημόσιοι υπάλληλοι, οι μελλοντικοί προγραμματιστές και επιστήμονες και, φυσικά, οι πολιτικοί και οι νομοθέτες θα πρέπει να είναι ενημερωμένοι για την προστασία της ιδιωτικής τους ζωής και τις επιπτώσεις των διαδικτυακών συμπεριφορών τους.

Λέξεις κλειδιά: - Προσωπικά Δεδομένα, Διαδίκτυο, Ιδιωτικότητα, SPSS

1 Εισαγωγή

Όλες οι πληροφορίες που αναφέρονται σε ένα άτομο και μπορούν άμεσα ή έμμεσα να οδηγήσουν στην προσωποποίηση – αναγνώρισή του αποτελούν Προσωπικά Δεδομένα. Για παράδειγμα το ονοματεπώνυμο, η ημερομηνία γέννησης, τα στοιχεία επικοινωνίας (αριθμοί σταθερών και κινητών τηλεφωνικών συνδέσεων, λογαριασμοί ηλεκτρονικού ταχυδρομείου, emails), η διεύθυνση κατοικίας, ο αριθμός φορολογικού μητρώου (ΑΦΜ), ο αριθμός μητρώου κοινωνικής ασφάλισης (ΑΜΚΑ), ο αριθμός δελτίου ταυτότητας (ΑΔΤ), αλλά και όλα τα «ηλεκτρονικά» αποτυπώματά του, όπως ιστοσελίδες που έχει επισκεφθεί, τα «like's», τα «post» και κάθε είδους αναρτήσεις σε όλα τα δίκτυα κοινωνικής δικτύωσης (Facebook, Twitter, Instagram, LinkID, κλπ), οι φωτογραφίες και τα βίντεο που «τράβηξε» και «ανέβασε» με φιλικά πρόσωπα είναι κάποια μόνο ενδεικτικά παραδείγματα αναφορικά με το τι θεωρείται προσωπικό δεδομένο στην καθημερινή ζωή του ατόμου.
Τα προσωπικά δεδομένα αφορούν και σε ιδιαίτερα ευαίσθητα στοιχεία της ιδιωτικής ζωής, όπως στις πολιτικές πεποιθήσεις, στο θρήσκευμα, στην ερωτική ζωή και στο σεξουαλικό προσανατολισμό ή και στην υγεία. Είναι εύκολο να δει κανείς ότι η ιδιωτική ζωή είναι άμεσα συνυφασμένη με τα προσωπικά δεδομένα. Αρκεί να αναλογιστεί κανείς ότι για όλους υπάρχουν πληροφορίες που δεν θα ήθελαν να μοιραστούν με άλλους ανθρώπους (όχι απαραίτητα επειδή πρέπει να κρατηθούν κρυφές, αλλά επειδή, με απλά λόγια, αποτελούν αποκλειστικά προσωπική υπόθεση). Αν αυτές οι ιδιωτικές πληροφορίες βρεθούν σε λάθος χέρια, κανείς δεν ξέρει ποτέ πώς θα χρησιμοποιηθούν. Η ιδιωτικότητα είναι πολύτιμη: η προστασία της ιδιωτικότητας επιτυγχάνεται με την διαφύλαξη των προσωπικών δεδομένων [2].
Ακόμα πιο επιτακτική γίνεται όμως η προστασία των προσωπικών δεδομένων του ατόμου κατά την πλοήγησή του στο διαδίκτυο, καθώς η διαρκή εξέλιξή του τα τελευταία χρόνια, η ευρεία αποδοχή του και χρήση του από όλες σχεδόν τις πληθυσμιακές ομάδες και οι νέες υπηρεσίες που παρέχει, δίνει τη δυνατότητα στους διαχειριστές (κακόβουλους και μη) των υποδομών του διαδικτύου να έχουν πρόσβαση στα προσωπικά δεδομένα των χρηστών. Η επεξεργασία των προσωπικών δεδομένων στο διαδίκτυο είναι πλέον πολύ συχνή (πολλές φορές εν αγνοία του υποκειμένου) και ουσιαστικά, αναπόφευκτη. Για παράδειγμα, κάθε φορά κατά τη διαδικασία πρόσβασης στο

διαδίκτυο με τη χρήση οποιασδήποτε «έξυπνης» συσκευής (υπολογιστή, φορητό υπολογιστή, κινητό τηλέφωνο, ταμπλέτα), ο πάροχος πρόσβασης διαδικτύου αναθέτει στη συσκευή αυτή έναν αριθμό που ονομάζεται διεύθυνση πρωτοκόλλου διαδικτύου (διεύθυνση IP). Η διεύθυνση IP είναι απαραίτητη για την πρόσβαση στο διαδίκτυο. Παρόλο που η εν λόγω συσκευή ενδεχομένως να χρησιμοποιείται από πολλά άτομα (π.χ. από όλα τα μέλη μιας οικογένειας) και παρά το γεγονός ότι η διεύθυνση IP είναι διαφορετική σε κάθε σύνδεση στο διαδίκτυο, εν τούτοις και αυτή αποτελεί προσωπικό δεδομένο, ακριβώς γιατί μπορεί, έστω και υπό προϋποθέσεις ή/και σε συνδυασμό με άλλες πληροφορίες, να ταυτοποιήσει το χρήστη της συσκευής για κάποια δεδομένη χρονική στιγμή. Για όλους τους παραπάνω λόγους, λοιπόν, η λήψη κατάλληλων μέτρων για την προστασία των προσωπικών δεδομένων έχει αποκτήσει ιδιαίτερη βαρύτητα και σημασία [2].

2 Τι ισχύει για την προστασία των προσωπικών δεδομένων

Καθημερινά συλλέγονται, επεξεργάζονται και αναλύονται δεδομένα ατόμων. Ποια είναι η ορθή χρήση τους; Τι θα πρέπει να τηρείται κατά την συλλογή και την επεξεργασία τους, χωρίς να προσβάλλονται τα δικαιώματα των υποκειμένων των δεδομένων; Πώς μπορούν να προστατευθούν;

Αρχικά, η Ευρωπαϊκή Ένωση, με το άρθρο 8 του Χάρτη Θεμελιωδών Δικαιωμάτων, υποστήριξε το δικαίωμα των ατόμων στην προστασία των προσωπικών τους δεδομένων. Για το σκοπό αυτό, εξέδωσε και αντίστοιχη Οδηγία 95/46/ΕΚ. Ωστόσο, η σημαντική τεχνολογική πρόοδος που σημειώθηκε έκτοτε και συνεχίζει και μέχρι τις μέρες μας, αναγκάζει την Ευρωπαϊκή Ένωση να εγκρίνει και να επικαιροποιεί συνεχώς κανόνες που καθορίζουν τον τρόπο με τον οποίο πρέπει να προστατεύονται τα προσωπικά δεδομένα.

Στην Ελλάδα, όπως και στα υπόλοιπα κράτη μέλη της Ευρωπαϊκής Ένωσης, υπάρχει ειδική νομοθεσία που προστατεύει τα άτομα από την ανεξέλεγκτη χρήση των προσωπικών τους δεδομένων. Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα είναι ο αρμόδιος φορέας για την εφαρμογή αυτής της νομοθεσίας στην Ελλάδα (νόμοι 2472/1997 και 3471/2006).

Η σημερινή νομοθεσία θεσπίστηκε το 1995, μία εποχή εντελώς διαφορετική, με πολύ λιγότερες προκλήσεις για τα προσωπικά δεδομένα. Το διαδίκτυο βρισκόταν σε εμβρυακό επίπεδο ανάπτυξης, οι μηχανές αναζήτησης και τα δίκτυα κοινωνικής δικτύωσης δεν υπήρχαν ούτε καν σαν ιδέα στο μυαλό των δημιουργών τους.

Σήμερα, ο τρόπος συλλογής, υποβολής σε επεξεργασία και η πρόσβαση σε δεδομένα δεν μοιάζει σε τίποτα με τις μεθόδους που χρησιμοποιήθηκαν πριν από περίπου δύο δεκαετίες. Επιπλέον, σε κάθε ένα από τα 28 κράτη μέλη, οι εθνικές αρχές επιβολής του νόμου έχουν μεταφέρει τους κανόνες με διαφορετικό τρόπο στο εσωτερικό τους και προσαρμόζουν το επίπεδο προστασίας προσωπικών δεδομένων σύμφωνα με την εκάστοτε υπόθεση (διασυνοριακή, εσωτερική, Europol, Eurojust, Prum). Το γεγονός αυτό οδηγεί σε απόκλιση στην εφαρμογή των κανόνων προστασίας των προσωπικών δεδομένων, ενώ ταυτόχρονα δημιουργεί σημαντικό διοικητικό φόρτο στις επιχειρήσεις, καθώς αυτή η πανευρωπαϊκή διαφορά είναι μη βιώσιμη [3].

Μέσα σε αυτή την τεχνολογική έκρηξη που βιώνει όλος ο κόσμος και με έντονη την απειλή της τρομοκρατίας και του οργανωμένου εγκλήματος, ξεκίνησαν συζητήσεις σε ευρωπαϊκό επίπεδο σχετικά με τον καλύτερο συνδυασμό του σεβασμού της ασφάλειας και της ιδιωτικής ζωής.

Η υιοθέτηση της ψηφιακής τεχνολογίας από τους πολίτες, σχεδόν για το σύνολο των αναγκών τους, συνεχίζεται με αμείωτο ρυθμό. Τα κοινωνικά μέσα δικτύωσης και μια μεγάλη σειρά άλλων ηλεκτρονικών

υπηρεσιών είναι πλέον διαδεδομένη. Η ψηφιακή ταυτότητα γίνεται πλέον ένα σημαντικό κομμάτι της καθημερινότητας του ατόμου, γεγονός που αναπόφευκτα το οδηγεί να μοιραστεί τουλάχιστον κάποιες βασικές προσωπικές πληροφορίες του με τους παρόχους υπηρεσιών.

Μέσα σε αυτό το συνεχώς τεχνολογικά εξελισσόμενο περιβάλλον, οι κίνδυνοι είναι υπαρκτοί και εξελίσσονται ταυτόχρονα. Η σχετικά πρόσφατη αποκάλυψη υπόθεσης στην Ελλάδα, όπου ιδιώτης κατάφερε να υποκλέψει φορολογικά και άλλα προσωπικά δεδομένα 9.000.000 πολιτών, με σκοπό να τα πουλήσει σε ιδιωτικές εταιρίες, αποτελεί ένα τρανταχτό παράδειγμα της επιτακτικής ανάγκης για ένα πιο αυστηρό νομικό πλαίσιο του καθεστώτος προστασίας προσωπικών δεδομένων στην Ευρωπαϊκή Ένωση. Οι παρόντες κανόνες προστασίας στην Ευρωπαϊκή Ένωση θεωρούνται πλέον απαρχαιωμένοι [3].

Προκειμένου να εξελίξει τους κανόνες αυτούς, από το 2012 η Ευρωπαϊκή Επιτροπή (η Ευρωπαϊκή Επιτροπή είναι το πολιτικά ανεξάρτητο εκτελεστικό όργανο της Ευρωπαϊκής Ένωσης. Είναι το μόνο αρμόδιο όργανο για την κατάρτιση προτάσεων για νέα ευρωπαϊκή νομοθεσία, και εφαρμόζει τις αποφάσεις του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της Ευρωπαϊκής Ένωσης [4]) συμμετέχει στη διαδικασία μεταρρύθμισης της προστασίας δεδομένων σε ολόκληρη την Ευρωπαϊκή Ένωση. Τα τελευταία έτη, η ολοκλήρωση αυτής της μεταρρύθμισης έχει καταστεί προτεραιότητα πολιτικού επιπέδου. Στόχος αυτής της μεταρρύθμισης είναι να ενισχυθούν τα δικαιώματα των ατόμων και να τους δοθεί η δυνατότητα να έχουν καλύτερο έλεγχο των δικών τους δεδομένων. Επιπροσθέτως, καθώς η Επιτροπή δίνει ιδιαίτερη βάση στην τόνωση της ψηφιακής ενιαίας αγοράς και στα οφέλη της ψηφιακής οικονομίας [5], η απλοποίηση του κανονιστικού πλαισίου για τις επιχειρήσεις ως προς τη χρήση των προσωπικών δεδομένων κρίνεται απαραίτητη.

Καθώς λοιπόν, η προστασία των προσωπικών δεδομένων είναι ένα πολύ ευαίσθητο θέμα για την ευρωπαϊκή κοινή γνώμη, γιατί αγγίζει την καθημερινότητα όλων, το βασικό στοιχείο της δέσμης μεταρρυθμίσεων για την προστασία των δεδομένων είναι ένας Γενικός Κανονισμός για την προστασία των δεδομένων (General Data Protection Regulation GDPR).

Την ριζική αναμόρφωση του νομικού πλαισίου προστασίας των προσωπικών δεδομένων επέβαλαν οι τεχνολογικές εξελίξεις. Σήμερα, η κοινωνία βρίσκεται μπροστά σε νέες προκλήσεις στις οποίες η Ευρωπαϊκή Επιτροπή και κατ' επέκταση η Ευρωπαϊκή Ένωση καλείται να αντιμετωπίσει με την δημοσίευση του νέου Γενικού Κανονισμού Προστασίας των προσωπικών δεδομένων.

Την 27η Απριλίου 2016 ψηφίστηκε ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΕΕ) 2016/679 που αποτελεί το κύριο νομοθέτημα της νέας δέσμης κανόνων. Την 24η Μαΐου 2016 τέθηκε σε ισχύ. Η διαδικασία ενσωμάτωσης του Κανονισμού στο εθνικό δίκαιο του κάθε κράτους μέλους πρέπει να έχει ολοκληρωθεί μέχρι την 6η Μαΐου 2018, με σκοπό η καθολική εφαρμογή της να ισχύσει από την 25η Μαΐου 2018.

Ο Γενικός Κανονισμός για την προστασία των προσωπικών δεδομένων αντικαθιστά την Οδηγία 46 του 1995 που ενσωματώθηκε στην ελληνική νομοθεσία με το ν. 2472/1997. Ο Γενικός Κανονισμός για την Προστασία των Δεδομένων δεν αποτελεί απλή επικαιροποίηση της Οδηγίας, αλλά ένα νέο κατ' ουσία νομοθέτημα προς την κατεύθυνση της διαμόρφωσης ενός ισχυρότερου και πιο συνεκτικού νομικού πλαισίου που θα έχει ομοιόμορφη εφαρμογή σε όλη την επικράτεια της Ευρωπαϊκής Ένωσης.

Ο Γενικός Κανονισμός για την προστασία των προσωπικών δεδομένων έχει ως σκοπό να καλυφθούν οι ανάγκες και να αντιμετωπιστούν οι κίνδυνοι που

προκύπτουν στο τεχνολογικό περιβάλλον του 21ου αιώνα από την ανταλλαγή προσωπικών δεδομένων στο δεύτερο πλαίσιο της παγκοσμιοποίησης, τη ραγδαία εξέλιξη των μέσων κοινωνικής δικτύωσης και των τεχνολογιών των Μεγάλων Δεδομένων (Big Data) και του Διαδικτύου των Πραγμάτων (Internet of things IoT).
Σε γενικές γραμμές, ο Γενικός Κανονισμός διευρύνει τα δικαιώματα των υποκειμένων των προσωπικών δεδομένων, δηλαδή των φυσικών προσώπων, και αυξάνει τις υποχρεώσεις των υπευθύνων επεξεργασίας των δεδομένων. Με λίγα λόγια, δημιουργεί ένα νέο νομικό πλαίσιο.

3 Προσωπικά δεδομένα και διαδίκτυο

Καθώς οι Τεχνολογίες Πληροφορικής και Επικοινωνιών καθίστανται πανταχού παρούσες, διεισδύοντας σε κάθε πτυχή της επαγγελματικής και προσωπικής ζωής του ατόμου, άνθρωποι και επιχειρήσεις καθίστανται ολοένα και πιο ευάλωτοι σε παραβιάσεις των προσωπικών τους δεδομένων. Η ιδιωτικότητα αναδεικνύεται ως ένας από τους σημαντικότερους κινδύνους που αντιμετωπίζει η συνεχώς αναπτυσσόμενη «κοινωνία της πληροφορίας».
Ως «κοινωνία της πληροφορίας» θα μπορούσε να ορισθεί η κοινωνία εκείνη, όπου οι τεχνολογίες πληροφορικής και επικοινωνιών επηρεάζουν το σύνολο των ανθρώπινων δραστηριοτήτων [6]. Με άλλα λόγια, είναι η κοινωνία εκείνη όπου η παραγωγή, διανομή, χρήση, ενσωμάτωση και διαχείριση πληροφοριών αποτελεί σημαντική οικονομική, πολιτική και πολιτιστική δραστηριότητα. Δια μέσου της χρήσης της πληροφορικής (IT) η κοινωνία της πληροφορίας έχει ως σκοπό να κερδίσει ανταγωνιστικό πλεονέκτημα διεθνώς, με δημιουργικό και παραγωγικό τρόπο. Οι άνθρωποι που έχουν τα μέσα να συμμετέχουν σε αυτή τη μορφή κοινωνίας ορισμένες φορές ονομάζονται «ψηφιακοί πολίτες». Σύμφωνα με την οικονομία της γνώσης, ο πλούτος δημιουργείται μέσα από την οικονομική εκμετάλλευση της κατανόησης. Αυτή αποτελεί και μια από τις δωδεκάδες ετικέτες που υποδηλώνουν ότι οι σύγχρονοι άνθρωποι μπαίνουν σε μία νέα μορφή κοινωνίας [7].
Η ψηφιακή πληροφορία αποτελεί από τη φύση της μια τεχνολογική καινοτομία, η οποία αμφισβητεί τις κρατούσες αντιλήψεις σχετικά με την ιδιοκτησία και την ιδιωτικότητα και ανατρέπει παραδοσιακές συνήθειες [8].
Από τη μια, όλο και περισσότερες ενέργειες στην καθημερινότητα του ατόμου προϋποθέτουν τη χρήση του διαδικτύου, από την άλλη, όλο και περισσότερες από τις ψηφιακές συσκευές που χρησιμοποιεί συνδέονται σε αυτό. Το «Internet of Things – IoT - Διαδίκτυο των Πραγμάτων» υπόσχεται ότι θα συνδέσει στο διαδίκτυο όχι μόνο τα κινητά τηλέφωνα, τις ταμπλέτες και τις κάμερες, αλλά ακόμη και τα αυτοκίνητα, τους «έξυπνους μετρητές» ηλεκτρικής ενέργειας, τα ψυγεία, τα ηχεία ή και το σύστημα ασφαλείας του σπιτιού. Ενδεικτικά αναφέρεται πρόσφατη μελέτη της εταιρείας ερευνών Gartner, Inc. (εταιρεία έρευνας και συμβουλευτικής) σύμφωνα με την οποία υπολογίζεται ότι ο αριθμός των συνδεδεμένων συσκευών θα φτάσει τον αριθμό των 26 δισεκατομμυρίων μέχρι το έτος 2020. Αυτό σημαίνει ότι κάθε άνθρωπος στον πλανήτη θα διαθέτει κατά μέσο όρο τρεις συσκευές που μπορούν να υποστηρίξουν το IoT. Παράλληλα, προβλέπει ότι το IoT θα επιφέρει μία συνολική οικονομική πρόσθετη αξία της τάξης των 1,9 τρισεκατομμυρίων δολαρίων, ενώ οι πληροφορίες που θα διαχειρίζονται οι επιχειρήσεις θα αυξηθεί έως και 14 φορές.
Στον πιο απλουστευμένο ορισμό του, το Διαδίκτυο των Πραγμάτων είναι η εφαρμογή διατάξεων αισθητήρων, τεχνολογίας πληροφοριών και δικτυακών τεχνολογιών για τη σύνδεση δισεκατομμυρίων συσκευών μικρών ή μεγάλων σε όλο τον κόσμο τόσο μεταξύ

τους όσο και με τον κατασκευαστή, για να λαμβάνουν και να μεταδίδουν σχετικά δεδομένα με στόχο να προσφέρουν περισσότερες προσωποποιημένες υπηρεσίες.

Με απλά λόγια το Διαδίκτυο των Πραγμάτων είναι το τεχνολογικό μέλλον που έρχεται για να κάνει τη ζωή του ατόμου πιο εύκολη. Η ποσότητα της ψηφιακής πληροφορίας πλέον αποκτά εκρηκτικές διαστάσεις. Η ραγδαία αυτή ανάπτυξη του «ψηφιακού κόσμου» οφείλεται κυρίως στην έκρηξη της κοινωνικής δικτύωσης, της ψηφιακής φωτογραφίας και του ψηφιακού βίντεο. Περίπου το 70 τοις εκατό των ψηφιακών δεδομένων παράγονται μεμονωμένα από ιδιώτες. Τα περισσότερα από αυτά βρίσκονται αποθηκευμένα σε ιστοσελίδες μεγάλων ιδιωτικών εταιρειών, όπως το YouTube [8].

Στην πραγματικότητα, ιδιώτες που πρόθυμα μοιράζονται τα προσωπικά τους δεδομένα είναι οι βασικοί υποστηρικτές των περισσότερων από τις καινοτόμες επιχειρήσεις του διαδικτύου. Οι χρήστες δεν φαίνεται να ενοχλούνται από την εκμετάλλευση των προσωπικών τους δεδομένων. Αυτό είναι το τίμημα που πληρώνουν για τις τρομακτικές και ασύλληπτες ψηφιακές εμπειρίες που το διαδίκτυο τους προσφέρει.

Η διαφύλαξη αυτού του τόσο μεγάλου πληροφοριακού όγκου (Μεγάλα Δεδομένα – Big Data και Ανοικτά Δεδομένα – Open Data) και η διασφάλιση του δικαιώματος των πολίτων να έχουν τον έλεγχο των ψηφιακών δεδομένων τους, αποτελούν προϋπόθεση για τη χρήση των καινοτομιών των Τεχνολογιών Πληροφορικής και Επικοινωνιών προς όφελος της ανθρωπότητας. Και οι δύο τύποι δεδομένων μπορούν να μεταμορφώσουν τον κόσμο.

Το νέο ψηφιακό περιβάλλον των Μεγάλων και Ανοικτών Δεδομένων επιδρά στην ιδιωτικότητα του ατόμου. Αρκεί κάποιος να σκεφτεί την πολύ μεγαλύτερη κλίμακα έκθεσης των προσωπικών δεδομένων, βάσει των νέων δυνατοτήτων αναζήτησης, ανάλυσης και διασύνδεσής τους, που μπορεί να οδηγήσει ακόμα και στη λήψη αυτοματοποιημένων αποφάσεων, χωρίς δυνατότητα ελέγχου από το ίδιο το άτομο. Γεννιούνται πλέον καινούργιες απαιτήσεις για την προστασία της ιδιωτικότητας, με επίκεντρο κυρίως την ενδυνάμωση των χρηστών του διαδικτύου μέσω νέων μηχανισμών ενημέρωσης και συγκατάθεσης.

Η μετάβαση, όμως, στον κυβερνοχώρο επιφέρει πρόσθετη πολυπλοκότητα. Οι ψηφιακές κοινότητες δεν διαφέρουν πολύ από τις παραδοσιακές. Αντιμετωπίζουν παρόμοιους κινδύνους, γι' αυτό το λόγο πρέπει να λαμβάνουν ανάλογες προφυλάξεις και να συμμορφώνονται με τις ίδιες αρχές. Τα ψηφιακά προσωπικά δεδομένα συλλέγονται με τρόπους που συχνά αδυνατεί ο ανθρώπινος νους να αντιληφθεί.

Το διακύβευμα πλέον δεν είναι μόνο η ιδιωτικότητα, αλλά ακόμη και η ίδια η έννοια της ατομικότητας, του προνομίου να είναι ο κάθε άνθρωπος μοναδικός.

Σχεδόν το μεγαλύτερο μέρος από το πλήθος των καθημερινών δραστηριοτήτων ενός ατόμου στο διαδίκτυο συνεπάγεται επεξεργασία των προσωπικών δεδομένων του. Χαρακτηριστικά παραδείγματα αποτελούν τα εξής:

- Κατά την διάρκεια ανάγνωσης της ηλεκτρονικής αλληλογραφίας (emails).
- Κατά την διάρκεια σύνδεσης στο διαδίκτυο μέσω προγραμμάτων πλοήγησης.
- Κατά την αναζήτηση πληροφοριών μέσω των μηχανών αναζήτησης.
- Κατά την συμπλήρωση ηλεκτρονικών φορμών.
- Κατά το «ανέβασμα» προσωπικών πληροφοριών σε υπηρεσίες κοινωνικής δικτύωσης (Facebook, Twitter, Instagram κ.τ.λ.).

Όλα τα προαναφερθέντα αποτελούν χαρακτηριστικά παραδείγματα και αποτυπώνουν το μέγεθος της επεξεργασίας των προσωπικών δεδομένων που λαμβάνει χώρα στο διαδίκτυο.

Αυτό που είναι άκρως σημαντικό και επιβάλλεται να συνειδητοποιήσει ο χρήσης του διαδικτύου είναι ότι, αν τα προσωπικά του δεδομένα πέσουν σε λάθος χέρια, ενδεχομένως να βρεθεί σε εξαιρετικά δυσμενή θέση στο μέλλον. Πώς όμως είναι δυνατόν τα προσωπικά δεδομένα να χρησιμοποιηθούν εναντίον του ατόμου που τα δημοσιοποιεί με σκοπό να το βλάψουν; Στο διαδίκτυο, δεν είναι δυνατόν να προβλέψει ή να φανταστεί κανείς το πώς και το πότε θα χρησιμοποιηθούν τα προσωπικά του δεδομένα. Οι προτιμήσεις ή οι απόψεις που δηλώνει κάποιος σήμερα, π.χ. σε ένα ιστολόγιο ή στο προφίλ του σε μία υπηρεσία κοινωνικής δικτύωσης, ενδεχομένως να επηρεάσουν αρνητικά τη μελλοντική του επαγγελματική πορεία ή τις προσωπικές του σχέσεις. Στο μέλλον, για παράδειγμα, δεν μπορεί να αποκλειστεί το γεγονός ότι πιθανοί εργοδότες θα αναζητούν πληροφορίες για υποψήφιους υπαλλήλους τους στο διαδίκτυο. «Τα γραπτά μένουν», γι' αυτό θα πρέπει, οι δημοσιεύσεις και οι αναρτήσεις πληροφοριών στο διαδίκτυο να είναι αρκετά προσεκτικές γιατί είναι πολύ δύσκολο να διαγραφούν πλήρως [2].

Αναλυτικότερες πληροφορίες, για το πώς χρησιμοποιούνται τα προσωπικά δεδομένα στο διαδίκτυο, καθώς και συμβουλές για την προστασία των ηλεκτρονικών προσωπικών δεδομένων, όπως και συμβουλές για την ασφαλής χρήση του διαδικτύου από τα παιδία, αναφέρονται στη μεταπτυχιακή διατριβή [9].

4 Προβληματισμός

Φαίνεται λοιπόν πως διανύουμε μια νέα εποχή στις Τεχνολογίες Πληροφορικής και Επικοινωνιών. Εύκολα λοιπόν κάποιος μπορεί να συνειδητοποιήσει τις προκλήσεις, αλλά και τους κινδύνους που προκύπτουν από την ανταλλαγή οικονομικών και εμπορικών δεδομένων στο πλαίσιο της παγκοσμιοποίησης, την ανάπτυξη της ψηφιακής οικονομίας και την αλματώδη εξέλιξη των υπηρεσιών κοινωνικής δικτύωσης αλλά και των τεχνολογιών των «Μεγάλων Δεδομένων (Big Data) και Ανοικτών Δεδομένων – Open Data» και του «Διαδικτύου των Πραγμάτων» (Internet of thingsIoT)», τα οποία αποτελούν μια πραγματικότητα που έχει άμεσο αντίκτυπο στην ιδιωτική ζωή του καθενός. Καθίσταται πλέον επιβεβλημένη η ανάγκη θεσμοθέτησης ισχυρών κανόνων για την προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής του ατόμου.

Ορμώμενος λοιπόν από αυτές τις ραγδαίες εξελίξεις, αλλά και από την επαγγελματική μου ιδιότητα ως υπάλληλος Πληροφορικής της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, επέλεξα να ασχοληθώ διεξοδικά με την πλοήγηση στο διαδίκτυο και τα ηλεκτρονικά προσωπικά δεδομένα στο πλαίσιο ανάπτυξης της μεταπτυχιακής μου διατριβής.

Η έρευνα αρχικά εξετάζει το επίπεδο ελέγχου που θεωρούν ότι έχουν οι ερωτηθέντες πάνω στα ηλεκτρονικά προσωπικά τους δεδομένα, τις ανησυχίες τους για τυχόν αντιληπτή έλλειψη ελέγχου αυτών και το γεγονός της παρακολούθησης των δραστηριοτήτων τους.

Στη συνέχεια, αντιμετωπίζει το επίπεδο γνώσεων των ερωτηθέντων όσον αφορά τους όρους συλλογής δεδομένων και τη στάση τους στην παροχή προσωπικών πληροφοριών.

Οι προσδοκίες των πολιτών αξιολογούνται επίσης στο κατά πόσο εμπιστεύονται διάφορες αρχές και ιδιωτικούς ή δημόσιους φορείς για την προστασία των προσωπικών πληροφοριών τους και ποια προσωπικά τους δεδομένα αν χαθούν ή κλαπούν θα τους ανησυχούσαν περισσότερο.

Επιπροσθέτως μελετάει, το επίπεδο συνειδητοποίησης των ρυθμίσεων απορρήτου σε ιστό τόπους κοινωνικής δικτύωσης, με τους ερωτηθέντες να ρωτιούνται πόσο εύκολο είναι να το βρουν για να αλλάξουν τις ρυθμίσεις του.

Στο τελευταίο τμήμα της ασχολείται με το κατά πόσο οι ερωτηθέντες γνωρίζουν την εθνική δημόσια αρχή που είναι υπεύθυνη για την προστασία των προσωπικών δεδομένων και το επίπεδο ικανοποίησης

τους όσον αφορά την ιστοσελίδα και το ενημερωτικό δελτίο της (newsletter).

5 Το ερωτηματολόγιο

Ο πιο διαδεδομένος τρόπος συγκέντρωσης πρωτογενών πληροφοριών είναι αυτός που επιτυγχάνεται με τη χρησιμοποίηση ερωτηματολογίων, στα οποία καταχωρούνται από τους ερωτώμενους ή από τους ερευνητές οι σχετικές πληροφορίες.

Υπάρχουν πληθώρα είδη ερωτηματολογίων που έχουν ήδη εφαρμοστεί σε πολλές έρευνες. Οι διαφοροποιήσεις μεταξύ των ερωτηματολογίων υπάρχουν όχι μόνο αναφορικά με το αντικείμενο μελέτης τους αλλά και με την μορφή τους, καθώς κάποια ερωτηματολόγια βασίζονται μόνο σε εικόνες και δεν χρησιμοποιούν καθόλου τον γραπτό λόγο εν αντιθέσει με άλλα που χρησιμοποιούν μόνο τον γραπτό λόγο.

Το ερωτηματολόγιο αποτελεί το θεμελιώδες στοιχείο σε κάθε δειγματοληπτική έρευνα, αλλά και στα πειράματα, στις έρευνες πεδίου και σε άλλες δραστηριότητες όπου απαιτείται η συγκέντρωση πληροφοριών, στοιχείων και δεδομένων. Η κατασκευή λοιπόν ενός ερωτηματολογίου είναι πολύ σημαντική, επειδή αυτό παρέχει ουσιαστικά τα δεδομένα της έρευνας.

Η διαδικασία ανάπτυξης και σύνταξης ενός ερωτηματολογίου αποτελεί ίσως το δυσκολότερο στάδιο μιας έρευνας, μιας και η επιτυχία της έρευνας εξαρτάται άμεσα από αυτό. Αν και δεν υπάρχει ένα σαφές και αναλυτικό μεθοδολογικό πλαίσιο για το σχεδιασμό του ερωτηματολογίου μιας οποιασδήποτε έρευνας, θα πρέπει σε γενικές γραμμές να τηρούνται κάποιοι βασικοί κανόνες για να είναι αξιοποιήσιμη η πληροφορία που προκύπτει. Περισσότερες λεπτομέρειες για τους κανόνες σύνταξης ενός ερωτηματολογίου αναφέρονται στη μεταπτυχιακή διατριβή [9].

Για την επίτευξη του στόχου της έρευνας καταρτίσθηκε ειδικό ερωτηματολόγιο, που αποτέλεσε το κύριο μέσο άντλησης πληροφοριών για την υλοποίηση της μελέτης και αποτελείται από τρία μέρη.

Το πρώτο μέρος περιλαμβάνει γενικές ερωτήσεις με σκοπό να αποτυπωθούν τα δημογραφικά χαρακτηριστικά του προς μελέτη πληθυσμού.

Το δεύτερο μέρος εμπεριέχει ερωτήσεις στο κατά πόσο οι πολίτες γνωρίζουν τη νομοθεσία για την προστασία προσωπικών δεδομένων και στις γνώσεις και δεξιότητες αναφορικά με τη πλοήγησή τους στο διαδίκτυο και τη χρήση συναφών υπηρεσιών και μέσων κοινωνικής δικτύωσης.

Τέλος το τρίτο μέρος επικεντρώνεται σε ερωτήσεις που αφορούν στην ιστοσελίδα (www.dpa.gr) και το ενημερωτικό δελτίο (newsletter) της ΑΠΔΠΧ και στο κατά πόσο οι πολίτες γνωρίζουν την ύπαρξή τους.

Οι συγκεκριμένες προτιμήσεις εκφράζονται με τη βοήθεια μιας προκαθορισμένης κλίμακας ικανοποίησης. Οι κλίμακες ικανοποίησης που συνήθως χρησιμοποιούνται είναι οι λεκτικές των 4 ή 5 βαθμίδων και οι γραφικές με τα πρόσωπα, οι οποίες είναι πιο ευχάριστες και λιγότερο συνηθισμένες, προκαλώντας το ενδιαφέρον των ερωτηθέντων. Κάθε έρευνα χρησιμοποιεί την κλίμακα εκείνη που της επιτρέπει να βγάλει σωστά και ασφαλή αποτελέσματα ανάλογα με το μοντέλο επεξεργασίας των στοιχείων που χρησιμοποιεί.

Για το σκοπό της συγκεκριμένης έρευνας χρησιμοποιήθηκε η λεκτική κλίμακα των 4 ή 5 βαθμίδων. Το μέγεθος αυτό της (4-βάθμιας) ή της (5-βάθμιας) κλίμακας κρίθηκε κατάλληλο γιατί αφενός δεν είναι ιδιαίτερα μικρό και εξασφαλίζεται η ακρίβεια των αποτελεσμάτων και αφετέρου ούτε πολύ μεγάλο με αποτέλεσμα ο ερωτηθέντας να μην συναντήσει δυσκολία στην ερμηνεία και στη διάκριση των επιπέδων της κλίμακας. Αντιθέτως τοποθετώντας πολλά επίπεδα μπορεί κανείς να συναντήσει δυσκολία στην εκτίμηση της διαφοράς ανάμεσα στα επίπεδα της κλίμακας.

Στο ειδικό ερωτηματολόγιο της έρευνας εκτός από τις ερωτήσεις ικανοποίησης συμπεριλαμβάνονται επίσης και ερωτήσεις μονής επιλογής.

Το συγκεκριμένο ερωτηματολόγιο εξετάζει μόνο τις γνώσεις και δεξιότητες αναφορικά με την πλοήγηση στο διαδίκτυο και τη χρήση συναφών υπηρεσιών και μέσων κοινωνικής δικτύωσης. Το φάσμα των ερωτήσεων που αφορούν τα προσωπικά δεδομένα και το διαδίκτυο είναι πολύ μεγάλο και δεν θα μπορούσαν να συμπεριληφθούν σε ένα και μοναδικό ερωτηματολόγιο. Αυτό είναι λογικό αν σκεφτεί κανείς ότι μόνο για τα προσωπικά δεδομένα υπάρχουν αντίστοιχες δημοσκοπήσεις του Ευρωβαρομέτρου. Πολλές ερωτήσεις της συγκεκριμένης έρευνας σχετικά με το διαδίκτυο και τα μέσα κοινωνικής δικτύωσης έχουν βασιστεί σε αντίστοιχες ερωτήσεις του Special Eurobarometer 431 Data Protection 2015 [5]. Γι' αυτό τα αποτελέσματα που θα προκύψουν αφορούν αποκλειστικά τις συγκεκριμένες ερωτήσεις.

Η έρευνα διεξήχθη στη διάρκεια των τριών ενημερωτικών ημερίδων που διοργάνωσε η ΑΠΔΠΧ στην Αίθουσα Σεμιναρίων της, Λ. Κηφισίας 1-3, Αθήνα (1ος όροφος), για τον εορτασμού της 11ης Ευρωπαϊκής Ημέρας Προστασίας Προσωπικών Δεδομένων. Κρίθηκε σκόπιμο για την εξασφάλιση της αποτελεσματικότητας και εγκυρότητας, η διεξαγωγή της έρευνας να γίνει την συγκεκριμένη χρονική περίοδο. Η συμμετοχή των ερωτηθέντων στις τρεις ενημερωτικές ημερίδες πιστοποιούσε το γεγονός ότι έστω και μια φορά έχουν περιηγηθεί στην ιστοσελίδα της Αρχής με αποτέλεσμα η γνώμη τους για το περιεχόμενο, τη σχεδίαση και την πλοήγηση στην ιστοσελίδα, θα ήταν όσο το δυνατόν πιο έγκυρη με αποτέλεσμα να προκύψουν ασφαλέστερα συμπεράσματα.

Πρόκειται δηλαδή, για περίπτωση μη πιθανοτικής δειγματοληψίας, και πιο συγκεκριμένα «Δειγματοληψία ευκαιρίας» [10], διότι η εξαγωγή του δείγματος δε βασίστηκε σε τεχνικές που χρησιμοποιούν οι νόμοι των πιθανοτήτων. Έγινε δηλαδή προσπάθεια συλλογής όσο το δυνατό μεγαλύτερου δείγματος στο οποίο υπήρχε εύκολη πρόσβαση. Αυτό το είδος δειγματοληψίας χρησιμοποιείται συνήθως σε πιλοτικές έρευνες και είναι προφανές ότι ο τρόπος αυτός συλλογής δείγματος δεν αντιπροσωπεύει επαρκώς τον πληθυσμό. Αναφορές για το τι είναι επιστημονική έρευνα, καθώς και τρόποι διεξαγωγής ερευνών, στη μεταπτυχιακή διατριβή [9].

Για τους λόγους που προ αναφέρθηκαν, η συλλογή του δείγματος προέκυψε από το πλήθος των συμμετεχόντων και στις τρεις ενημερωτικές ημερίδες. Διανεμήθηκαν προς συμπλήρωση 200 ειδικά ερωτηματολόγια και σύμφωνα με την ερευνητική δεοντολογία, οι απαντήσεις των συμμετεχόντων στην έρευνα είναι εμπιστευτικές, ενώ τα στοιχεία που παρείχαν χρησιμοποιήθηκαν μόνο για τη στατιστική ανάλυση και την εξαγωγή συμπερασμάτων στην παρούσα έρευνα. Κατά την συλλογή των ερωτηματολογίων δόθηκαν και οι απαραίτητες διευκρινήσεις σε περιπτώσεις απορίων σχετικά με την συμπλήρωση του ερωτηματολογίου. Από τα 200 ερωτηματολόγια που διανεμήθηκαν συμπληρώθηκαν και ήταν έγκυρα τα 153.

6 Συμπεράσματα

6.1 Μέρος Α

Από το προφίλ των ατόμων που συμπλήρωσαν το ειδικό ερωτηματολόγιο με βάση το φύλο, την ηλικία και το μορφωτικό επίπεδο, παρατηρεί κανείς πως το πλήθος των ερωτηθέντων ήταν γυναίκες, η ηλικιακή ομάδα με τη μεγαλύτερη αντιπροσώπευση ήταν μεταξύ 31 - 45 χρονών, ενώ η πλειονότητα των ερωτηθέντων δήλωσαν ότι είναι κάτοχοι μεταπτυχιακού – διδακτορικού τίτλου σπουδών. Περισσότερες λεπτομέρειες αναφορικά με το προφίλ των συμμετεχόντων παρουσιάζονται στη μεταπτυχιακή διατριβή [9].

6.2 Μέρος Β

Από την ανάλυση των ερωτήσεων του δεύτερου μέρους προέκυψαν χρήσιμα συμπεράσματα στο κατά πόσο οι πολίτες γνωρίζουν τη νομοθεσία για την προστασία προσωπικών δεδομένων και για τις γνώσεις και δεξιότητες τους αναφορικά με τη πλοήγηση στο διαδίκτυο και τη χρήση συναφών υπηρεσιών και μέσων κοινωνικής δικτύωσης.

Δεν αποτελεί έκπληξη το γεγονός ότι ένα μεγάλο ποσοστό των ερωτηθέντων και κατά επέκταση θα μπορούσε να πει κανείς ένα μεγάλο ποσοστό των Ελλήνων πολιτών χρησιμοποιεί πλέον σε τακτική βάση τις διαδικτυακές (online) υπηρεσίες όπως τα κοινωνικά δίκτυα και την αγορά αγαθών ή υπηρεσιών μέσω διαδικτύου. Ωστόσο, η έκθεση δείχνει σαφώς πως οι περισσότεροι εξ αυτών ανησυχούν πολύ για την καταγραφή των καθημερινών διαδικτυακών δραστηριοτήτων τους μέσω των κινητών τηλεφώνων, μέσω των καρτών πληρωμής και μέσω των ιστοσελίδων και όχι τόσο πολύ για την καταγραφή των καθημερινών δραστηριοτήτων τους μέσω καμερών, με πάνω από το ένα δέκατο να μην ανησυχούν καθόλου για το γεγονός της καταγραφής τους από κάμερες.

Είναι επίσης σημαντικό ότι οι περισσότεροι ερωτηθέντες, παρόλο που δεν αισθάνονται αρκετά άνετα με ιστοσελίδες που χρησιμοποιούν πληροφορίες σχετικά με τη διαδικτυακή δραστηριότητά που έχουν, αποδέχονται την ψηφιακή εποχή και τη συλλογή δεδομένων καθώς αποτελεί μέρος της σύγχρονης ζωής, αρκεί να είναι γνώστες των συνθηκών συλλογής και χρήσης των ηλεκτρονικών προσωπικών δεδομένων τους.

Από την άποψη αυτή, επτά στους δέκα ερωτηθέντες εκφράζουν μεγάλη δυσπιστία ως προς τα μέτρα που λαμβάνονται για την ασφαλή τήρηση των ηλεκτρονικών προσωπικών δεδομένων τους στο διαδίκτυο. Θεωρούν δε, ότι δεν έχουν τον πλήρη έλεγχο των πληροφοριών που παρέχουν σε απευθείας σύνδεση και ότι αυτό εξαρτάται από την ιστοσελίδα ή την εφαρμογή που τα διαχειρίζεται. Αφετέρου, είναι ιδιαίτερα εντυπωσιακό ότι οι εννιά στους δέκα ερωτηθέντες ανησυχούν με το γεγονός ότι δεν έχουν τον πλήρη έλεγχο των πληροφοριών που παρέχουν σε απευθείας συνδέσεις.

Το αίσθημα έλλειψης του πλήρη ελέγχου υπογραμμίζει την ανάγκη για την περαιτέρω μεταρρύθμιση του τοπίου προστασίας δεδομένων στην Ευρώπη, τόσο όσον αφορά την παροχή στις επιχειρήσεις σαφών προτύπων που πρέπει να πληρούν, όσο και για την οικοδόμηση της εμπιστοσύνης του κοινού με το διαδίκτυο και ότι τα δικαιώματά του στην πραγματικότητα προστατεύονται. Αυτό ενισχύεται και από το γεγονός ότι περίπου τα δύο τρίτα των ερωτηθέντων θεωρούν ως κατάλληλο για την διασφάλιση και ενημέρωση τους, εάν οι προσωπικές πληροφορίες που παρέχουν στο διαδίκτυο – cloud χαθούν ή κλαπούν, τις ίδιες τις διαδικτυακές εταιρείες που διαχειρίζονται τα δεδομένα καθώς και τις υπεύθυνες δημόσιες αρχές.

Η έκθεση καταδεικνύει επίσης ότι η πλειοψηφία των ερωτηθέντων έχουν ευρύτατες ανησυχίες σχετικά με τις ρυθμίσεις απορρήτου τόσο του φυλλομετρητή (browser) αναφορικά με τη λήψη cookies όσο και με τις ρυθμίσεις απορρήτου των μέσων κοινωνικής δικτύωσης. Περισσότεροι από έξι στους δέκα γνωρίζουν και κάνουν χρήση της δυνατότητας των ρυθμίσεων απορρήτου που έχουν τα προγράμματα περιήγησης, ενώ πάνω από εφτά στους δέκα προσαρμόζουν τις αρχικές ρυθμίσεις απορρήτου των διαδικτυακών μέσων κοινωνικής δικτύωσης.

Όλες αυτές οι ανησυχίες υποστηρίζουν και πάλι τη δέσμευση της Ευρωπαϊκής Ένωσης για επικαιροποίηση και βελτίωση του καθεστώτος και του νομοθετικού πλαισίου προστασίας δεδομένων και της αναβάθμισης και ουσιαστικής ενίσχυσης των αρμόδιων αρχών, με απώτερο σκοπό την αποτελεσματικότερη και ποιοτικότερη προστασία των δικαιωμάτων των πολίτων όσον αφορά τα προσωπικά δεδομένα. Την

ριζική αναμόρφωση λοιπόν του νομικού πλαισίου προστασίας των προσωπικών δεδομένων που επέβαλαν οι τεχνολογικές εξελίξεις καλείται πλέον να αντιμετωπίσει ο Γενικός Κανονισμός Προστασίας των προσωπικών δεδομένων με την καθολική εφαρμογή του να ισχύει από την 25η Μαΐου 2018.

6.3 Μέρος Γ - Ιστοσελίδα

Από την ανάλυση των ερωτήσεων του τρίτου μέρους που αφορούσαν την αξιολόγηση για πρώτη φορά της ιστοσελίδας (www.dpa.gr) και του ενημερωτικού δελτίου (newsletter) της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα εξήχθησαν χρήσιμα συμπεράσματα για το βαθμό ικανοποίησης των πολίτων για το ενημερωτικό έργο της Αρχής μέσω της ιστοσελίδας και του ενημερωτικού δελτίου. Το σύνολο των πολιτών που παραβρέθηκαν στη διάρκεια των τριών ενημερωτικών ημερίδων γνώριζαν την ύπαρξη της ιστοσελίδας (www.dpa.gr) και κατ' επέκταση την ύπαρξη της αρμόδιας αρχής για την προστασία των προσωπικών δεδομένων, της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, που καλείται με το έργο της να προστατεύσει και να θωρακίσει την κοινωνία και τους πολίτες στην εποχή της «ψηφιοποίησης». Παρόλα αυτά όμως το ποσοστό επισκεψιμότητας της ιστοσελίδας της Αρχής είναι αρκετά χαμηλό, αν αναλογιστεί κανείς πως κοντά στα δυο τρίτα των ερωτηθέντων την επισκέπτονται το πολύ μια φορά τον μήνα, ενώ καθημερινά την επισκέπτεται μόλις το (6,5%) εκ των ερωτηθέντων.

Πάνω από οκτώ στους δέκα αξιολόγησαν την συνολική εικόνα της ιστοσελίδας της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα από ικανοποιητική έως πολύ ικανοποιητική. Το αίσθημα ικανοποίησης ενισχύεται και από το γεγονός ότι σε επιμέρους κριτήρια αξιολόγησης για το περιεχόμενο, τη σχεδίαση και την πλοήγηση, η πλειονότητα των ερωτηθέντων τα βαθμολόγησε από μέτρια ως πολύ καλά. Ωστόσο, η έκθεση καταδεικνύει συγκεκριμένους τομείς που χρήζουν σημαντικής βελτίωσης. Πιο συγκεκριμένα, παρατηρείται αίσθημα δυσαρέσκειας για την ομοιομορφία και την συγκεκριμένη εμφάνιση που έχει ο ιστότοπος σε όλες τις σελίδες του, με πέντε στους δέκα να την κρίνουν από μέτρια ως καθόλου καλή, για την οργάνωση και παρουσίαση της πληροφορίας, με έναν στους τρείς να την κρίνει από μέτρια ως καθόλου καλή, καθώς και για την αισθητική και το σχεδιασμό της ιστοσελίδας, με εφτά στους δέκα να την αξιολογούν από μέτρια ως καθόλου καλή.

Είναι επίσης σημαντικές και χρήζουν αναφοράς, οι παρατηρήσεις που έγιναν για τη βελτίωση της ιστοσελίδας, στο πεδίο ελεύθερου σχολιασμού που υπήρχε στο ερωτηματολόγιο, παρατηρήσεις που ενισχύουν το αίσθημα δυσαρέσκειας των πολιτών για την σχεδίαση και την δυνατότητα εύκολης πλοήγησης.

6.4 Μέρος Γ - Ενημερωτικό δελτίο

Το «newsletter» αποτελεί ουσιαστικά ενημερωτικό δελτίο προώθησης των υπηρεσιών και του έργου της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, και κατ' επέκταση της ιστοσελίδας «www.dpa.gr» της Αρχής. Αποστέλλεται μέσω ηλεκτρονικού ταχυδρομείου, «e-mailnewsletter», στους επισκέπτες που γράφτηκαν σε αυτό, περιστασιακά ή ανά τακτά χρονικά διαστήματα και απαρτίζεται από ειδήσεις, ανακοινώσεις, αναλύσεις, πληροφόρηση, χρήσιμες συμβουλές, απαντήσεις σε συχνές ερωτήσεις, υπενθυμίσεις ή ακόμη και προειδοποιήσεις, διατηρώντας πάντοτε τον ενημερωτικό του χαρακτήρα.

Σήμερα η έκδοση ενός «e-mailnewsletter» τείνει να αποτελέσει κανόνα. Οι λόγοι για τους οποίους έγιναν τόσο δημοφιλή τα «e-mailnewsletter» είναι γιατί τα email αποτελούν τη μόνη εφαρμογή τύπου

«pushtechnology» που εφαρμόζεται με επιτυχία. Με την δυνατότητα αυτή, δημιουργείται ένα δυναμικό κανάλι επικοινωνίας με σκοπό την ενημέρωση του κοινού και αποφεύγεται ο παθητικός τρόπος επίσκεψης της ιστοσελίδας της Αρχής. Με τον τρόπο αυτό αυξάνεται δραματικά η δημοτικότητα της ιστοσελίδας «www.dpa.gr» και υπενθυμίζεται συνέχεια στο κοινό η ύπαρξη και το έργο της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

Όμως, η έκθεση δείχνει πως από το σύνολο των 153 συμπληρωμένων και έγκυρων ερωτηματολογίων, λίγο πάνω από ένα στα τρία, δεν είχε αξιολόγηση για το ενημερωτικό δελτίο. Γνώριζαν δηλαδή την ύπαρξη του «newsletter» της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και κατ' επέκταση το ελάμβαναν, μόλις οι 88 εκ των ερωτηθέντων. Αυτό από μόνο του καταδεικνύει την έλλειψη και το κενό ενημέρωσης και επικοινωνίας που υπάρχει σε αυτό το σημείο με τους πολίτες. Δεν αποτελεί έκπληξη το γεγονός αυτό αν αναλογιστεί κανείς και το αρκετά χαμηλό ποσοστό επισκεψιμότητας της ιστοσελίδας «www.dpa.gr».

Παρόλο το κενό ενημέρωσης και επικοινωνίας που παρατηρήθηκε να υπάρχει μέσω του ενημερωτικού δελτίου, η ανάλυση των ερωτηματολογίων αναδεικνύει την μεγάλη ικανοποίηση των συμμετεχόντων στην έρευνα, για το περιεχόμενο και τη σχεδίαση του ενημερωτικού δελτίου. Πάνω από εφτά στους δέκα αξιολόγησαν την συνολική εικόνα του «newsletter» της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα από πολύ ικανοποιητική έως άριστη.

Η πολύ καλή εντύπωση που αφήνει το ενημερωτικό δελτίο στους πολίτες ενισχύεται και από το γεγονός ότι σε επιμέρους κριτήρια αξιολόγησης για το περιεχόμενο και την οργάνωση, η πλειονότητα των ερωτηθέντων τα βαθμολόγησε από πολύ καλά έως άριστα. Ωστόσο, η έκθεση καταδεικνύει έναν συγκεκριμένο τομέα που χρήζει προσοχής και βελτίωσης. Πιο συγκεκριμένα, παρατηρείται διαφοροποίηση στον βαθμό ικανοποίησης, σε σχέση με τα άλλα κριτήρια, του κριτηρίου αξιολόγησης για την αισθητική και τον σχεδιασμό, με την πλειονότητα των ερωτηθέντων να το βαθμολογεί από μέτριο έως πολύ καλό.

Όπως στην περίπτωση αξιολόγησης της ιστοσελίδας «www.dpa.gr», έτσι και εδώ, τα συμπεράσματα που εξήχθησαν θα βοηθήσουν στην ποιοτική αναβάθμιση της ιστοσελίδας και του newsletter με απώτερο σκοπό τη βελτίωση του επιπέδου επικοινωνίας και υπηρεσιών της Αρχής προς τους πολίτες.

Αναλυτική παρουσίαση, με πίνακες και ραβδογράμματα των αποτελεσμάτων του ερωτηματολογίου για το δεύτερο και τρίτο μέρος, παρουσιάζονται στη μεταπτυχιακή διατριβή [9].

7 Μελλοντική έρευνα

Τα ηλεκτρονικά προσωπικά δεδομένα είναι ένα αγαθό που πρέπει να διαφυλάσσεται και να μην υποτιμάτε η αξία του. Το διαδίκτυο (παρά τα αναμφισβήτητα πλεονεκτήματά του) αυξάνει, εκ φύσεως, τους κινδύνους παράνομης επεξεργασίας τους. Ο κάθε ένας από εμάς, συνεπώς, πρέπει να είναι ενήμερος για τους κινδύνους και να χρησιμοποιεί πάντοτε το διαδίκτυο με σύνεση: η πλήρης ευαισθητοποίηση γύρω από τα προσωπικά δεδομένα είναι το πρώτο, πολύ σημαντικό, βήμα προς αυτήν την κατεύθυνση.

Η ανωτέρω προσπάθεια καταγραφής των γνώσεων, συνεπώς και της ευαισθητοποίησης, που έχουν οι πολίτες σχετικά με τα προσωπικά δεδομένα και την πλοήγηση στο διαδίκτυο έγινε με γνώμονα το ισχύων νομικό πλαίσιο προστασίας των δεδομένων προσωπικού χαρακτήρα. Ωστόσο, οι τεράστιες δυνατότητες της τεχνολογίας της πληροφορικής και οι τεχνολογικές εξελίξεις επέβαλαν την ριζική αναμόρφωση του νομικού πλαισίου. Από

την 25η Μαΐου 2018 τίθεται σε καθολική εφαρμογή ο Γενικός Κανονισμός για την Προστασία των Δεδομένων. Οποιαδήποτε προσπάθεια διεξαγωγής μελλοντικής έρευνας θα πρέπει πλέον να γίνει με βάση τον Γενικό Κανονισμό Προστασίας Δεδομένων. Έρευνα, που να καταδεικνύει το κατά πόσο οι πολίτες αλλά και οι φορείς ιδιωτικού και δημόσιου φορέα είναι ενήμεροι για τις ισχύουσες αλλαγές που εισαγάγει, αλλά και το αν τελικά καταφέρει να επιτύχει την ενίσχυση του αισθήματος ασφάλειας στους πολίτες - χρήστες του διαδικτύου, ούτως ώστε να το χρησιμοποιούν για βελτίωση της ζωής τους και να μην το αντιμετωπίζουν σαν έναν μελλοντικό παράγοντα καταδυνάστευσης και καταπάτησης των ηλεκτρονικών προσωπικών δεδομένων και συνεπώς των ελευθεριών τους.

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα είναι ο αρμόδιος φορέας για την εφαρμογή της ισχύουσας νομοθεσίας για τα προσωπικά δεδομένα στην Ελλάδα (νόμοι 2472/1997 και 3471/2006), αλλά και από την 25η Μαΐου 2018 για την εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων. Τα ευρήματα αυτής της έρευνας κατέδειξαν το σημαντικό έργο που επιτελεί η Αρχή με το να παρέχει πληροφορίες και να ενημερώνει τους πολίτες για θέματα προσωπικών δεδομένων αλλά και την ουσιαστική ανανέωση που οφείλει να κάνει στα μέσα προώθησης των υπηρεσιών και του έργου της (ιστοσελίδα (www.dpa.gr) και ενημερωτικό δελτίο (newsletter)). Ενόψει και της εφαρμογής του Γενικού Κανονισμού η δημοτικότητα της ιστοσελίδας και του ενημερωτικού δελτίου θα αυξηθεί σημαντικά. Ενδιαφέρον θα είχε λοιπόν, μελλοντική έρευνα ικανοποίησης που θα διεξαγόταν μετά και την υιοθέτηση όλων αυτών των αλλαγών, αναβαθμίσεων σε όσο το δυνατόν όμως μεγαλύτερο και επαρκώς αντιπροσωπευτικότερο δείγμα πληθυσμού. Η αλληλεπίδραση αυτή μέσω των ερωτηματολογίων ικανοποίησης, αξιολόγησης θα οδηγούσε βαθμιαία στη δημιουργία πιστού αναγνωστικού κοινού και θα αναπτυσσόταν γρηγορότερα μία σχέση εμπιστοσύνης με τους πολίτες.

8 Ευχαριστίες

Για την ολοκλήρωσή της μεταπτυχιακής μου έρευνας βοήθησαν πολλοί άνθρωποι τους οποίους οφείλω να ευχαριστήσω.

Πρώτα από όλα οφείλω πολλά ευχαριστώ στον καθηγητή κύριο Χρήστο Δρόσο για την άρτια συνεργασία, την υποστήριξη και την απεριόριστη υπομονή του.

Εν συνεχεία, οφείλω πολλά ευχαριστώ στους συναδέλφους μου που με βοήθησαν στη σύνταξη του ειδικού ερωτηματολογίου.

Επίσης, θα ήθελα να ευχαριστήσω όλα τα άτομα εκείνα που είχαν την διάθεση και υπομονή να συμπληρώσουν το ειδικό αυτό ερωτηματολόγιο της έρευνας, βοηθώντας στην συγκέντρωση πολύτιμων πληροφοριών για την ολοκλήρωση της μεταπτυχιακής μου διατριβής.

Τέλος οφείλω πολλά ευχαριστώ στην οικογένεια μου για την αμέριστη συμπαράσταση και υπομονή που έδειξε κατά τη διάρκεια όλου του κύκλου των μεταπτυχιακών μου σπουδών καθώς και στο φίλο μου Ντόντο Κωνσταντίνο που με παρότρυνε να παρακολουθήσω το μεταπτυχιακό πρόγραμμα το οποίο αν και είχε τις δυσκολίες του, θεωρώ ότι με βοήθησε να διευρύνω τους ορίζοντες μου.

Βιβλιογραφικές αναφορές:

[1] Τσαγρής Μιχαήλ, *Στατιστική με τη χρήση του IBM SPSS 22*, 2014

[2] Κ. Λιμνιώτης, Α. Μπούρκα, Γ. Παναγοπούλου, ειδικοί επιστήμονες ΑΠΔΠΧ, *Προσωπικά δεδομένα και Διαδίκτυο*, 3ο τεύχος του δημιναίου ενημερωτικού δελτίου του saferinternet.gr, 04 Ιουλίου 2011, [online] <http://saferinternet.gr/index.php?action=download&objId=File411>.

[3] Δημήτριος Δρούτσας, Ευρωβουλευτής, τ. Υπουργός Εξωτερικών, *Γενική εισαγωγή στο σχέδιο Κανονισμού και Οδηγίας*, Κείμενα Εισηγήσεων Επετειακή Διημερίδα 15 Χρόνια Λειτουργίας της ΑΠΔΠΧ, 2014 σελ 85-86.

[4] Ευρωπαϊκή Επιτροπή, [online] <*https://europa.eu/european-union/about-eu/institutions-bodies/european-commission_el*>.

[5] European Commission, *Special Eurobarometer 431 "Data protection"*, European Union, 2015.

[6] Λίλιαν Μήτρου, Καθηγήτρια στο Πανεπιστήμιο Αιγαίου (Τμήμα Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων), *Το δίκαιο στην κοινωνία της πληροφορίας*, Εκδόσεις Σάκκουλα 2002.

[7] Beniger, James R, (1986), *The Control Revolution: Technological and Economic Origins of the Information Society*, Cambridge, Mass.: Harvard University Press.

[8] Ιωάννης Τσουκαλάς, Ευρωβουλευτής, Ομότιμος Καθηγητής ΑΠΘ, *Ιδιωτικότητα και ανωνυμία στην Κοινωνία της Πληροφορίας*, Κείμενα Εισηγήσεων Επετειακή Διημερίδα 15 Χρόνια Λειτουργίας της ΑΠΔΠΧ, 2014 σελ 105-107.

[9] Αϊδίνης Κωνσταντίνος, *Πλοήγηση στο διαδίκτυο και ηλεκτρονικά προσωπικά δεδομένα - Μέτρηση βαθμού ικανοποίησης χρηστών της ιστοσελίδας και του newsletter της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα*, Μεταπτυχιακή Διατριβή, 2018.

[10] ΜιλτιάδηςΧαλικιάς, ΑναπληρωτήςΚαθηγητήςΑΕΙΠειραιά ΤΤ, ΑλεξάνδραΜανωλέσου, MscBiostatistics, ΠαναγιώταΛάλου, PhdMathematics, *Μεθοδολογία Έρευνας και Εισαγωγή στη Στατιστική Ανάλυση Δεδομένων με το IBMSPSSSTATISTICS*, ΕκδόσειςΣΕΑΒ 2015.

Paper - Αγγλικό

Online Browsing and Online Personal Data - Measuring the Degree of User Satisfaction Concerning the Website and Newsletter of the Personal Data Protection Authority

AIDINIS KONSTANTINOS
Department of Automation Engineering
Piraeus University of Applied Sciences
P.Ralli&Thivon 250, Athens, 12244
GREECE
Kaidinis1@gmail.com

Abstract: - In recent years, humanity has been living in a state of uncertainty regarding the protection of personal data. Protection of privacy will henceforth concern not only content but also metadata resulting from electronic communications. In Greece, the contribution of the Personal Data Protection Authority (DPA) to the development of a data friendly environment is great. The only sustainable defense against the dangers of privacy is the empowerment of "digital citizens", which is achieved through information and education about digital hazards, rights and obligations.

Focusing on "digital citizens", this study's scope is the protection of privacy in connection with digital globalization and accordingly the rapid development of electronic communications. The key question to be addressed in the present work is whether data protection actually exists in the new era of Information and Communication Technologies that mankind is experiencing.

More specifically, the purpose of this dissertation is to draw useful conclusions as to whether citizens are aware of the data protection legislation and possess the necessary knowledge and skills regarding navigation and the use of related services and social media.

It is also being attempted for the first time to evaluate the website (www.dpa.gr) and the newsletter of the Personal Data Protection Authority and to conclude whether citizens are aware of their existence. What is really evaluated, concerns the citizens' opinion about the content, design and navigation of the website as well as reading the newsletter.

In order to achieve this goal, a specific questionnaire was designed, from which information was obtained for the implementation of the study. The specific questionnaire consists of three parts: A. Demographic questions, B. Degree of informing citizens about the current legal framework for the protection of personal data and possession of the necessary knowledge and skills regarding navigation and the use of related services and social media, C. Evaluation of the Authority's website and newsletter.

The statistical analysis was conducted using the Statistical Package for Social Sciences (SPSS22). SPSS is a statistical package that has a lot of potential in terms of processing and presenting the data of a scientific research and also great reliability. The latest versions of SPSS have a graphical environment, making it very easy to use [1].

The conclusions drawn from the statistical analysis of 153 completed questionnaires will result in a more efficient management of the Authority's resources and in better services towards citizens in order to create adequate safeguards for privacy and a strong framework of protection. Citizens, educators, civil servants, future developers and scientists and, of course, politicians and legislators should be aware of the protection of their privacy and the impact of their internet behaviors.

Key-Words: -Personal Data, Internet, Privacy, SPSS

1 Introduction

All information that refers to an individual and can directly or indirectly lead to his / her personalization - recognition is considered as Personal Data. For example, name, date of birth, contact details (fixed and mobile phone numbers, e-mail accounts, emails), home address, tax ID number, social security number (SMA) Identity Card (ID), but also all its "electronic" footprints, such as visited websites, "like's", "post" and all sorts of posts on all social networking sites (Facebook, Twitter, Instagram, LinkID, etc.) the videos that "were shot" and "uploaded" with friendly faces are just some indicative examples of what is considered personal data in the everyday life of an individual.

Personal data also relate to particularly sensitive elements of privacy, such as political beliefs, religion, erotic life and sexual orientation or health. It is easy to see that privacy is directly interwoven with personal data. That is to consider that there is enough information out there for everyone that would not like to share with other people (not necessarily because they have to be kept secret, but simply because they are purely personal). If this private information is found in the wrong hands, no one ever knows when and how can be used. Privacy is valuable: privacy is achieved by preserving personal data [2].

Even more compelling is the protection of an individual's privacy while navigating on the Internet, as the constant evolution over the last few years, the wide acceptance and use by almost all population groups and the new services it provides enables malicious and non-malicious web infrastructure administrators to access their users' personal data. The processing of personal data on the internet is now very common (often without the knowledge of the subject) and essentially, inevitable. The IP address is essential to access the internet. Although this device may be used by many people (eg all family members) and despite the fact that the IP address is different on every internet connection, it is also a personal data, precisely because may, even under conditions and / or in conjunction with other information, identify the user of the device for a given time. For all the above reasons, therefore, the adoption of appropriate measures for the protection of personal data has gained particular weight and importance [2].

2 What applies to the protection of personal data

Everyday data is collected, processed and analyzed. What is their correct use? What should be kept when collecting and processing them without affecting the rights of the data subjects? How can they be protected? Initially, the European Union, in Article 8 of the Charter of Fundamental Rights, supported the right of individuals to the protection of their personal data. For this purpose, it was also issued a corresponding Directive 95/46 / EC. However, the significant technological progress since then, which has continued to date, forces the European Union to constantly approve and update rules defining the way in which personal data must be protected.

In Greece, as in the other Member States of the European Union, there is a specific legislation that protects individuals from the uncontrolled use of their personal data. The Personal Data Protection Authority is the body responsible for implementing this legislation in Greece (Laws 2472/1997 and 3471/2006).

Today's legislation was introduced in 1995, a completely different era, with far fewer challenges for personal data. The internet was at an embryonic level of development, search engines and social networks did not

even exist as an idea in the minds of their creators.

Today, the way of collecting, processing and accessing data is nothing like the methods used about two decades ago. Moreover, in each of the 28 Member States, national law enforcement authorities have transposed the rules differently within their borders and adjust the level of personal data protection according to the case (cross-border, internal, Europol, Eurojust, Prum). This leads to a divergence in the application of the rules on the protection of personal data, while at the same time creating a significant administrative burden on businesses, as this pan-European dispute is unsustainable [3].

Throughout this technological explosion that the whole world is experiencing and with the strong threat of terrorism and organized crime, debates have begun at European level on the best combination of respect for security and privacy.

The adoption of digital technology by the citizens, almost for all their needs, continues at a steady pace. Social networking tools and a wide range of other online services are now widespread. Digital identity is now an important part of a person's daily life, which inevitably leads him to share at least some basic personal information with his service providers.

Within this continuously technologically evolving environment, the dangers are real and evolve at the same time. The relatively recent case disclosure in Greece where a private individual managed to seize tax and other personal data of 9,000,000 citizens in order to sell them to private companies is a shining example of the urgent need for a stricter legal framework for the data protection regime in the European Union.

These protection rules in the European Union are now considered obsolete [3].

In order to develop these rules, from 2012 the European Commission (the European Commission is the politically independent executive body of the European Union. It is the only body responsible for drawing up proposals for new European legislation, and implements decisions of the European Parliament and the Council of the European Union [4]) is involved in the process of data protection reform throughout the European Union. In recent years, the completion of this reform has become a political priority. The aim of this reform is to strengthen the rights of individuals and to enable them to have better control over their own data. In addition, as the Commission provides a special basis for stimulating the digital single market and the benefits of the digital economy [5], simplification of the regulatory framework for business with regard to the use of personal data is deemed necessary.

Since, therefore, the protection of personal data is a very sensitive issue for European public opinion, since it touches everyone's everyday life, the key element of the data protection reform package is a General Data Protection Regulation GDPR.

The radical overhaul of the legal framework for the protection of personal data has led to technological developments. Today, society faces new challenges to which the European Commission and, by extension, the European Union is called upon to tackle with the publication of the new General Data Protection Regulation.

The General Regulation on the Protection of Personal Data replaces Directive 46 of 1995, which was incorporated into the Greek law by Law 2472/1997. The General Data Protection Regulation is not a mere update of the Directive but a new substantive law towards a stronger and more coherent legal framework that will be uniformly applied throughout the European Union.

The General Regulation on the protection of personal data aims to meet the needs and address the risks arising in the 21st century technological environment from the exchange of personal data in the second context of globalization, the rapid development of social media and technologies the Big Data and the Internet of Things (Internet of Things).

On April 27, 2016, the General Data Protection Regulation (EU) 2016/679 was

adopted, which is the main piece of legislation in the new set of rules. On May 24, 2016 came into force. The process of transposing the Regulation into the national law of each Member State must be completed by 6 May 2018 with a view to its universal application from 25 May 2018.

3 Personal data and the Internet

As Information and Communication Technologies become ubiquitous by penetrating every aspect of a person's professional and personal life, people and businesses are becoming more and more vulnerable to violations of their personal data. Privacy is emerging as one of the most important risks faced by the ever-growing "information society".

An "information society" could be defined as a society where information and communication technologies affect all human activities [6]. In other words, it is this society that the production, distribution, uses and integration, management of information is an important economic, political and cultural activity. Through the use of information technology (IT), the information society aims to gain a competitive advantage internationally, creatively and productively. People who have the means to participate in this form of society are sometimes called 'digital citizens'. According to the knowledge economy, wealth is created through economic exploitation of understanding. This is also one of the dozens of labels that suggest that modern humans are entering a new form of society [7].

Digital information is, by its nature, a technological innovation that challenges existing perceptions of ownership and privacy and overturns traditional habits [8].

On the one hand, more and more actions in everyday life of the person presuppose the use of the internet, on the other hand, more and more of the digital devices they use are associated with it. "Internet of Things - IoT - Internet of Things" promises to connect not only mobile phones, tablets and cameras to the internet, but even cars, "smart meters" of electricity, refrigerators, loudspeakers or the entire home security system. Indicatively, a recent study by research firm Gartner, Inc. (research and advisory firm) estimates that the number of connected devices will reach 26 billion by 2020. This means that every person on the planet will have an average of three devices that can support the IOT. At the same time, it predicts that the IoT will bring about a total financial added value of $ 1.9 trillion, while information managed by businesses will increase up to 14 times.

In its more streamlined definition, the Internet of Things is the implementation of sensor, information technology and network technologies to connect billions of small or large devices around the world to each other and to the manufacturer to receive and transmit relevant data with the aim of offering more personalized services.

Simply put, the Internet of Things is the technological future that comes to make life easier for the individual. The amount of digital information now acquires explosive dimensions. This rapid growth of the "digital world" is mainly due to the explosion of social networking, digital photography and digital video. Approximately 70 percent of digital data is produced individually by individuals. Most of these are stored on websites of large private companies, such as YouTube [8].

In fact, individuals who willingly share their personal data are the main supporters of most of the innovative businesses of the internet. Users do not seem to be bothered by the exploitation of their personal data. This is the price they pay for the terrifying and unimaginable digital experiences the internet offers them.

Preserving this large volume of information (Big Data and Open Data) and safeguarding the right of citizens to control their digital data is a prerequisite for the use of ICT innovations to the benefit of humanity. Both types of data can transform the world.

The new digital environment of Large and Open Data affects the privacy of the individual. It is enough to think of the much larger scale of personal data exposure based on their new search, analysis and interconnection capabilities, which can even lead to automated decisions without the control of the individual himself. New privacy requirements are now being born, focusing mainly on empowering internet users through new information and consent mechanisms.

But the transition to cyberspace brings additional complexity. Digital communities do not differ greatly from traditional ones. They face similar risks, so they have to take similar precautions and comply with the same principles. Digital personal data is collected in ways that the human mind often fails to perceive.

The challenge now is not only privacy, but even the very concept of individuality, the privilege of being the only individual.

Almost the bulk of a person's daily activities on the internet involve processing his or her personal data. Typical examples are:

- While reading emails.
- When connecting to the Internet through browsers.
- When searching for information through search engines.
- When filling in electronic forms.
- When uploading personal information to social networking services (Facebook, Twitter, Instagram, etc.).

All of the above are exemplary examples and reflect the size of the processing of personal data that takes place on the Internet.

What is extremely important and the user of the Internet must be aware of is that if his/her personal data result into the wrong hands, he may be in a very unfavorable position in the future. How, however, is it possible for personal data to be used against the person who discloses them in order to harm it? On the Internet, it is not possible to predict or imagine how and when their personal data will be used.

The preferences or views that someone expresses today e.g. on a blog or profile in a social networking service, may negatively affect his / her future career path or personal relationships. In the future, for example, it cannot be ruled out that potential employers will seek information about their prospective employees on the Internet. "Writings are left", so publications and online postings should be it is very difficult to delete them completely [2].

More detailed information on how personal data are used on the internet, as well as tips on protecting electronic personal data, as well as tips on how to use the internet safely from children, are listed in the postgraduate dissertation [9].

4 Reflections

So it seems that we are in a new age in Information and Communication Technologies. So it is easy to be aware of the challenges and the dangers that arise from the exchange of economic and commercial data in the context of globalization, the development of the digital economy and the rapid development of social networking services as well as of the technologies of "Big Data Data) and Open Data and the Internet of Things, which are a reality that has a direct impact on everyone's privacy. There is now an ultimate need to establish robust rules for the protection of personal data and privacy.

I chose to thoroughly deal with internet surfing and electronic personal data as part of the development of my postgraduate dissertation, driven by these rapid developments, as well as by my professional status as a Data Protection Officer of the Personal Data Protection Authority.

The survey initially examines the level of control that respondents feel about having their electronic personal data, their concerns about any perceived lack of control, and the fact of monitoring their activities.

Subsequently, it addresses the level of knowledge of respondents regarding the

terms of data collection and their attitude to the provision of personal information.
Citizens' expectations are also assessed on whether they trust different authorities and private or public bodies to protect their personal information, and which personal data, if lost or stolen, would worry them more.
In addition, it examines the level of awareness of privacy settings in social networking sites, with respondents asking how easy it is to find it to change their settings.
In the last section of dissertation, it deals with whether respondents are aware of the national public data protection authority and their level of satisfaction with the Authority's website and newsletter.

5 The questionnaire

The most common way to collect primary information is the use of questionnaires that are completed by respondents or researchers as relevant information.
There are a number of types of questionnaires already applied in many surveys. Differences between questionnaires exist not only in terms of their subject matter but also in their form, as some questionnaires are based on images only and do not use the written language at all, as opposed to others using only the written discourse.
The questionnaire is the fundamental element in each sampling survey, but also in experiments, field investigations and other activities where information and data are required. The construction of a questionnaire is therefore very important, because it essentially provides the research data.
The process of developing and compiling a questionnaire is probably the most difficult stage of a survey, since the success of research depends directly on it. Although there is no clear and detailed methodological framework for designing the questionnaire of any research, some basic rules should generally be respected to make the resulting information useful. More details about the rules for compiling a questionnaire are mentioned in the thesis [9].
In order to achieve the objective of the survey, a specific questionnaire was drawn up, which was the main tool for obtaining information on the implementation of the study and consists of three parts.
The first part contains general questions in order to capture the demographic characteristics of the population to be studied.
The second part has questions about whether citizens are aware of the data protection laws and the knowledge and skills regarding their Internet surfing and the use of related services and social media.
Finally, the third part focuses on questions related to the website (www.dpa.gr) and the newsletter of the DPA and on whether citizens know the Authority's existence.
These preferences are expressed by means of a predetermined satisfaction scale. Satisfaction scales commonly used are 4 or 5-grade verbs, and graphical ones with faces, which are more enjoyable and less common, provoking the interest of respondents. Each survey uses the scale that allows it to produce correct and safe results depending on the data processing model it uses.
For the purpose of this research, the 4 or 5-step verbal scale was used. This magnitude of the (4-level) or (5-scale) scale was judged to be appropriate because it is not too small and ensures the accuracy of the results and not too large, so that the respondent does not encounter difficulty in interpreting and distinguishing levels. Conversely, by placing many levels one can find it difficult to estimate the difference between the levels of the scale.
In the survey are also included specific questionnaire in addition to satisfaction questions and one-time questions.
This questionnaire only examines the knowledge and skills related to web surfing and the use of related services and social

media. The range of questions concerning personal data and the internet is very large and could not be included in a single questionnaire. This is sensible if you think that there are available Euro barometer polls only for personal data. Many questions of this research related to the Internet and social media have been based on corresponding questions from the Special Eurobarometer 431 Data Protection 2015 [5]. That is why the results that will arise relate only to the specific questions.

The survey was carried out during the three informative days organized by DPA in its seminar room, 1-3 Kifissias Avenue, Athens (1st floor), celebrating the 11th European Day for the Protection of Personal Data. It was considered appropriate that the research would be conducted at that time in order to ensure its effectiveness and validity. The attendance of the respondents at the three informative workshops certified the fact that once they browsed on the Authority's website, in result their opinion on content, design and navigation on the website would be as valid as possible, resulting in safer conclusions.

In other words, this is a case of non-probable sampling, and in particular "Sampling of Opportunity" [10], the extraction of the sample was not based on techniques used by the probability laws. In other words, it was an attempt to collect as much as possible a sample in which there was easy access.

This type of sampling is usually used in pilot surveys and it is obvious that this sample collection does not adequately represent the population. References to what are scientific research, and ways of conducting research, can be found in the postgraduate dissertation [9].

For the reasons outlined above, the sample collection was obtained from the crowd of participants at all three informative days. 200 specific questionnaires were distributed to complement, and according to research ethics, the respondents' responses to the survey were confidential, and the data they provided were used only for statistical analysis and conclusions in this research. Questionnaires were also provided with the necessary clarifications in case of questions concerning the completion of the questionnaire. Of the 200 questionnaires distributed, 153 were filled in and validated.

6 Conclusions

6.1 Part A

From the profile of the persons who completed the gender, age and educational questionnaire, one observes that most of respondents were women, from which the age group largely represented was between 31 - 45 years old; while the majority of respondents said they had a postgraduate - doctoral degree. More details on the profile of the participants are presented in the postgraduate dissertation [9].

6.2 Part B

The analysis of the questions of the second part has produced useful conclusions on whether citizens are aware of the legislation on data protection and their knowledge and skills regarding internet surfing and the use of related services and social media.

It is no surprise that a large percentage of respondents and, by extension, a large percentage of Greek citizens can now use online services such as social networking and the purchasing of goods or services over the Internet. However, the report clearly shows that most of them are very concerned about the recording of their daily online activities via mobile phones, via payment cards and through the web pages, and not so much for recording their daily activities through cameras, from whom more than one tenth not to worry at all about the fact that they were recorded by cameras.

It is also important that most respondents, although they do not feel comfortable enough with websites that use information about their online activity, accept the “digital age” and the collection of data as part of modern life, as long as they are aware

of the conditions of collection and use of their electronic personal data.
In this respect, seven out of ten respondents are very distrustful about the measures taken to securely keep their electronic personal data online. They think they do not have full control over the information they provide online and that that depends on the website or the application that manages this information. On the other hand, it is particularly striking that nine out of ten respondents are concerned that they do not have full control of the information they provide on the internet.
The feeling of lack of full control underlines the need for further reform of the data protection landscape in Europe, both in terms of providing businesses with clear standards that they have to meet, and of building public trust with the internet, and that the rights are actually protected. This is also supported by the fact that about two-thirds of respondents find it suitable to secure and update them if the personal information they provide on the Internet - cloud is lost or stolen - the internet companies that manage the data themselves along with the responsible public authorities.
The report also shows that the majority of respondents have widespread concerns about the confidentiality settings of both the browser and cookies as well as the privacy settings of the social media. More than six out of ten know and make use of the privacy settings of browsers, and more than seven out of ten adjust the privacy settings of online social media.
All these concerns support the European Union's commitment to updating and improving the status and the legal framework for data protection and the upgrading and effective strengthening of the competent authorities with a view to more effective and better protection of the rights of citizens with regard to personal data. The radical overhaul of the legal framework for the protection of personal data imposed by technological developments is therefore now called upon to address the General Regulation on the Protection of Personal Data with its universal application in force from 25 May 2018.

6.3 Part C - Website

From the analysis of the third party's questions regarding the first evaluation of the website (www.dpa.gr) and the newsletter of the Personal Data Protection Authority, useful conclusions were drawn about the degree of satisfaction of the citizens for the information project of the Authority through the website and newsletter.
All the citizens who attended during the three informative days were aware of the existence of the website (www.dpa.gr) and by extension the existence of the competent authority for the protection of personal data, the Data Protection Authority, task of which is to protect and shield society and citizens in the era of "digitization". Nevertheless, the percentage of traffic on the Authority's website is quite low, considering that almost two-thirds of respondents visit it at least once a month, while only 6,5% of respondents visit it daily.
More than eight out of ten rated the overall image of the Personal Data Protection Authority website satisfactory to very satisfactory. The feeling of satisfaction is also reinforced by the fact that in individual evaluation criteria for content, design and navigation, the majority of respondents rated them moderately to very good. However, the report demonstrates specific areas that need to be significantly improved. More specifically, there is a feeling of dissatisfaction with the uniformity and the specific appearance of the site on all its pages, with five out of ten judging it from moderate to no good for organizing and presenting the information, with one in three being judges from moderate to not good, as well as the aesthetics and design of the website, with seven out of ten evaluating it from moderate to not good.

Important and relevant comments in the free annotation field of the questionnaire were made to improve the site. These observations that were mentioned above enhance citizens' dissatisfaction with the design of the site and the ability to navigate easily.

6.4 Part C - Newsletter

The "newsletter" is essentially a newsletter for the promotion of the services and the work of the Data Protection Authority and, by extension, of the Authority's website www.dpa.gr. It is sent by e-mail, "e-mailnewsletter", to visitors written on it, occasionally or at regular intervals, and consists of news, announcements, analyses, information, useful tips, answers to frequently asked questions, reminders or even warnings, keeping always its informative character.

Nowadays the publication of an "e-mailnewsletter" tends to become a rule. The reasons why the e-mailnewsletter has become so popular is because email is the only push-technology application that is successfully implemented. With this feature, a dynamic communication channel is created to inform the public and avoid the passive way of visiting the Authority's website. This dramatically increases not only the popularity of the website "www.dpa.gr" and the existence but also the work of the Personal Data Protection Authority is constantly reminded to the public. But the report shows that out of a total of 153 completed and valid questionnaires, just over one in three provided no evaluation for the newsletter. The respondents knew the existence of the "newsletter" of the Personal Data Protection Authority but only 88 of them received it. This alone demonstrates the lack of information and communication that exists at this point between the Authority and the citizens. This is not surprising if you also consider the low percentage of traffic on the site "www.dpa.gr". Despite the information and communication gap observed through the newsletter, the analysis of the questionnaires highlights the great satisfaction of the participants in the survey, the content and the design of the newsletter. More than seven out of ten rated the overall picture of the "newsletter" of the Data Protection Authority from very satisfactory to excellent.

The very good impression that the newsletter makes to citizens is also supported by the fact that in individual evaluation criteria for content and organization, the majority of respondents rated them very well to excellent. However, the report shows a specific area that needs attention and improvement. More specifically, the degree of satisfaction with the other criteria of the assessment criterion for aesthetics and design is observed, with the majority of respondents rating it from medium to very good.

As in the case of the evaluation of the website www.dpa.gr, the conclusions drawn here will help to improve the quality of the website and the newsletter with the ultimate goal of improving the level of communication and services of the Authority towards the citizens.

A detailed presentation, with tables and bar graphs of the results of the questionnaire for the second and third part, is presented in the dissertation [9].

7 Future Research

Electronic personal data is a good that must be preserved and in no way should its value be underestimated. The internet (despite its undeniable advantages) naturally increases the risks of illegal processing. Each of us, therefore, must be aware of the dangers and always use the internet wisely: full awareness of personal data is the first, very important step towards this direction.

The above attempt to capture the knowledge and therefore the awareness of the citizens about personal data and internet surfing was based on the current legal framework for the

protection of personal data. However, the huge potential of IT and technological developments has forced the radical overhaul of the legal framework. Since May 25, 2018, the General Data Protection Regulation will be universally applicable. Any attempt to conduct a future investigation should now be made on the basis of the General Data Protection Regulation. A survey to show whether citizens and public and private operators are aware of the changes they are introducing, but also whether they ultimately succeed in enhancing their sense of security for Internet users, so that they use it to improve their lives and not to treat it as a future factor of oppression and encroachment on electronic personal data and hence their freedoms.

The Personal Data Protection Authority is the body responsible for the implementation of the applicable legislation on personal data in Greece (Laws 2472/1997 and 3471/2006), but also since 25 May 2018 for the application of the General Data Protection Regulation. The findings of this research have highlighted the important work being done by the Authority by providing information and informing citizens about personal data. This research has also pointed out the substantial renewal that it has to be done by the Authority in the means of promoting its services and its work (website (www. dpa.gr) and a newsletter). In view of the implementation of the General Regulation, the popularity of the website and newsletter will increase significantly. Interestingly, there would be a future satisfaction survey that would take place after all these changes were adopted, upgrades to as large a population as possible and sufficiently representative. This interaction through satisfaction and evaluation questionnaires would gradually lead to the creation of a faithful readership and would develop more quickly trust with citizens.

8 Acknowledgments

For the completion of my postgraduate dissertation there are many people I owe to thank.

First of all I'd like to sincerely thank Professor Christos Drosos for his excellent cooperation, support and unlimited patience. Next, I am thankful to my colleagues who helped me to write the special questionnaire. I would also like to thank all those people who had the mood and patience to complete this specific survey questionnaire, helping me to gather valuable information for completing my postgraduate dissertation.

Finally, I owe a lot of thanks to my family for the unwavering support and patience they showed during my entire postgraduate course as well as my friend Donto Konstantinos who urged me to attend the postgraduate program which, although it had several difficulties it helped me to broaden my horizons.

References:

[1] M. Tsagris, Statistical Package for the Social Sciences, 2014.

[2] Konstantinos Limniotis, Athena Bourka, Georgia Panagopoulou, special scientists at the Data Protection Authority, Personal Data and the Internet, 3rd issue of the saferinternet.gr newsletter, 04 July 2011, [online] <http://saferinternet.gr/index.php?action=download&objId=File411>.

[3] Dimitrios Droutsas, Member of the European Parliament, former Minister of Foreign Affairs, General introduction to the draft Regulation and Directive, Texts of Proposals Anniversary Workshop 15 Years of Operation of the Data Protection Authority, 2014 pages 85-86.

[4] European Commission, [online] <https://europa.eu/european-union/about-eu/institutions-bodies/european-commission_el>.

[5] European Commission, Special Eurobarometer 431 “Data protection”, European Union, 2015.

[6] Mitrou Lilian, Professor at the University of the Aegean (Department of Information and Communication Systems Engineering), Law and Society in the 21st Century, Sakkoula Publications 2002.

[7] Beniger, James R, (1986), The Control Revolution: Technological and Economic Origins of the Information Society, Cambridge, Mass.: Harvard University Press.

[8] Ioannis Tsoukalas, Member of the European Parliament, Professor Emeritus of the Aristotle University of Thessaloniki, Privacy and anonymity in the Information Society, Texts of Proposals Anniversary Workshop 15 Years of Operation of the Data Protection Authority, 2014 pages 105-107.

[9] Aidinis Konstantinos, Online Browsing and Online Personal Data - Measuring the Degree of User Satisfaction Concerning the Website and Newsletter of the Personal Data Protection Authority, Postgraduate Thesis, 2018.

[10] Miltiadis Chalikias, Associate Professor of Piraeus University of Applied Sciences, Alexandra Manoleos, Msc Biostatistics, Panagiota Lalou, Phd Mathematics, Research Methodology and Introduction to Statistical Analysis of Data with IBM SPSS STATISTICS, SEAV 2015 Publishing.

Πρόταση μεταπτυχιακής διατριβής

ΑΝΩΤΑΤΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΕΙΡΑΙΑ Τ.Τ.
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΑΥΤΟΜΑΤΙΣΜΟΥ Τ.Ε
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΑΥΤΟΜΑΤΙΣΜΟΣ ΠΑΡΑΓΩΓΗΣ & ΥΠΗΡΕΣΙΩΝ

Πρόταση Μεταπτυχιακής Διατριβής

Όνομα Φοιτητή: Αϊδίνης Κωνσταντίνος

Όνομα Επιβλέποντα Καθηγητή: Χρήστος Δρόσος

Τίτλος διατριβής: Πλοήγηση στο διαδίκτυο και ηλεκτρονικά προσωπικά δεδομένα. Μέτρηση βαθμού ικανοποίησης χρηστών της ιστοσελίδας και του newsletter της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Dissertation Title: Surfing the web and electronic privacy. Measuring users satisfaction of the website and the newsletter of the Hellenic Data Protection Authority

ΠΕΡΙΛΗΨΗ - Abstract

Τα τελευταία χρόνια ο κόσμος ζει σε κλίμα αβεβαιότητας όσον αφορά την προστασία των προσωπικών δεδομένων. Σε αυτό συνέτειναν ιδιαίτερα οι αποκαλύψεις Σνόουντεν για γενικευμένες παρακολουθήσεις των ηλεκτρονικών επικοινωνιών από τις υπηρεσίες ασφαλείας των ΗΠΑ. Παράλληλα, στην ΕΕ παρακολουθούμε πρωτοβουλίες για την αντιμετώπιση της διεθνούς τρομοκρατίας, αλλά και για την ορθολογιστική διαχείριση του προσφυγικού προβλήματος, οι οποίες συνεπάγονται τη δημιουργία ηλεκτρονικών βάσεων δεδομένων μεγάλης κλίμακας. Από την άλλη πλευρά, η ανταλλαγή οικονομικών και εμπορικών δεδομένων στο πλαίσιο της παγκοσμιοποίησης, η ανάπτυξη της ψηφιακής οικονομίας, η ραγδαία εξέλιξη των μέσων κοινωνικής δικτύωσης αποτελούν μια πραγματικότητα που επηρεάζει άμεσα την ιδιωτική ζωή του καθενός. Η προστασία της ιδιωτικής ζωής θα αφορά, στο εξής,

όχι μόνον το περιεχόμενο, αλλά και τα μεταδεδομένα που προκύπτουν από τις ηλεκτρονικές επικοινωνίες. Σκοπός της παρούσας διατριβής είναι να αντληθούν χρήσιμα συμπεράσματα, με την βοήθεια ειδικού ερωτηματολογίου, σχετικά με το κατά πόσο οι πολίτες γνωρίζουν τη νομοθεσία για την προστασία προσωπικών δεδομένων καθώς και τις γνώσεις και δεξιότητές τους αναφορικά με την πλοήγηση στο διαδίκτυο και τη χρήση συναφών υπηρεσιών και μέσων κοινωνικής δικτύωσης. Επίσης, επιχειρείται για πρώτη φορά η αξιολόγηση της ιστοσελίδας (www.dpa.gr) και του ενημερωτικού δελτίου (newsletter) της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) και στο κατά πόσο οι πολίτες γνωρίζουν την ύπαρξή τους. Ποια η γνώμη τους για το περιεχόμενο, τη σχεδίαση τους, την πλοήγηση στην ιστοσελίδα και την ανάγνωση του newsletter. Το αντικείμενο της μελέτης, το οποίο εμπίπτει με το Π.Μ.Σ, δεδομένου ότι πραγματεύεται την προστασία της ιδιωτικής ζωής σε συνάρτηση με την ψηφιακή παγκοσμιοποίηση και την ραγδαία εξέλιξη των ηλεκτρονικών επικοινωνιών, θα προσπαθήσει να δώσει απάντηση στο ερώτημα αν υπάρχει προστασία δεδομένων στην εποχή μας που χαρακτηρίζεται από την κυριαρχία της τεχνολογίας, τον ψηφιακό κόσμο. Στην Ελλάδα η συμβολή της ΑΠΔΠΧ στη διαμόρφωση ενός φιλικού στην προστασία δεδομένων περιβάλλοντος είναι μεγάλη. Η μόνη βιώσιμη άμυνα έναντι των κινδύνων της ιδιωτικότητας είναι η ενδυνάμωση των «ψηφιακών πολιτών», η οποία επιτυγχάνεται μέσω της ενημέρωσης και της εκπαίδευσής τους για τους ψηφιακούς κινδύνους, τα δικαιώματα και τις υποχρεώσεις. Τα δύο αυτά γεγονότα αποτελούν τον πρωταρχικό σκοπό αυτής της διατριβής, σε μια προσπάθεια η διαφύλαξη της ιδιωτικής ζωής στην εποχή της πληροφορίας να γίνει κατανοητή από περισσότερους ανθρώπους. Η στατιστική ανάλυση θα πραγματοποιηθεί με την χρήση του εξειδικευμένου στατιστικού λογισμικού Statistical Package for Social Sciences (SPSS 22). Τα συμπεράσματα που θα εξαχθούν από την στατιστική ανάλυση θα επιφέρουν αποδοτικότερη διαχείριση των πόρων της ΑΠΔΠΧ και ποιοτικότερες υπηρεσίες προς τους πολίτες με σκοπό να δημιουργηθούν ικανές εγγυήσεις για την ιδιωτική ζωή και να διαμορφωθεί ένα ισχυρό πλαίσιο προστασίας. Οι πολίτες, οι εκπαιδευτικοί, οι δημόσιοι υπάλληλοι, οι μελλοντικοί προγραμματιστές και επιστήμονες και, φυσικά, οι πολιτικοί και οι νομοθέτες θα πρέπει να είναι

ενημερωμένοι για την προστασία της ιδιωτικής τους ζωής και τις επιπτώσεις των διαδικτυακών συμπεριφορών τους. Υπολογίζεται ότι η μελέτη θα ολοκληρωθεί εντός ενός έτους. Η διανομή του ειδικού ερωτηματολογίου θα αποτελεί το κύριο μέσο άντλησης πληροφοριών για την υλοποίηση της μελέτης. Κατά τον τελευταίο (τέταρτο) μήνα θα πραγματοποιηθεί η συγγραφή της διατριβής και οι διορθώσεις αυτής σε συνεργασία με τον επιβλέποντα καθηγητή.

Σχέδιο Βαθμολόγησης (με ενδεικτική ποσόστωση)

Εισαγωγή	10%
Βιβλιογραφική Έρευνα	10%
Σχεδιασμός Ερευνητικής Μεθοδολογίας	10%
Παρουσίαση Αποτελεσμάτων	35%
Συμπεράσματα	20%
Αυτοαξιολόγηση	5%
Προτάσεις για περαιτέρω έρευνα	10%

Ενδεικτική Δομή

1. ΕΙΣΑΓΩΓΗ

1.1. Προσωπικά δεδομένα

1.2. Τι ισχύει για την προστασία των προσωπικών δεδομένων

1.3. Γενικός Κανονισμός για την προστασία των προσωπικών δεδομένων GDPR

1.4. Προσωπικά δεδομένα και διαδίκτυο

1.4.1. Προστασία της ιδιωτικής ζωής στην Κοινωνία της Πληροφορίας

1.4.2. Πώς χρησιμοποιούνται τα προσωπικά δεδομένα στο διαδίκτυο

1.4.3. Συμβουλές για την προστασία των προσωπικών δεδομένων στο διαδίκτυο

1.4.3.1. Phishing

1.4.3.2. Αζήτητη – Ανεπιθύμητη ηλεκτρονική επικοινωνία (Spam)

1.4.3.3. Ασφαλής χρήση του διαδικτύου: Συμβουλές για παιδιά

Σχετική βιβλιογραφία

[1] Κ. Λιμνιώτης, Α. Μπούρκα, Γ. Παναγοπούλου, ειδικοί επιστήμονες ΑΠΔΠΧ, «Προσωπικά δεδομένα και Διαδίκτυο», 3ο τεύχος του δημιναίου ενημερωτικού δελτίου του saferinternet.gr, 04 Ιουλίου 2011, [online] <http://saferinternet.gr/index.php?action=download&objId=File411>.

[2] Δημήτριος Δρούτσας, Ευρωβουλευτής, τ. Υπουργός Εξωτερικών, «Γενική εισαγωγή στο σχέδιο Κανονισμού και Οδηγίας», Κείμενα Εισηγήσεων Επετειακή Διημερίδα 15 Χρόνια Λειτουργίας της ΑΠΔΠΧ, 2014 σελ 85-86.

[3] Ευρωπαϊκή Επιτροπή, [online] <https://europa.eu/european-union/about-eu/institutions-bodies/european-commission_el>.

[4] European Commission, Special Eurobarometer 431 “Data protection”, European Union, 2015.

[5] Λίλιαν Μήτρου, Καθηγήτρια στο Πανεπιστήμιο Αιγαίου (Τμήμα Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων), «Το δίκαιο στην κοινωνία της πληροφορίας», Εκδόσεις Σάκκουλα 2002.

[6] Beniger, James R, (1986), The Control Revolution: Technological and Economic Origins of the Information Society, Cambridge, Mass.: Harvard University Press.

[7] Ιωάννης Τσουκαλάς, Ευρωβουλευτής, Ομότιμος Καθηγητής ΑΠΘ, «Ιδιωτικότητα και ανωνυμία στην Κοινωνία της Πληροφορίας», Κείμενα Εισηγήσεων Επετειακή Διημερίδα 15 Χρόνια Λειτουργίας της ΑΠΔΠΧ, 2014 σελ 105-107.

[8] Gunter Ollmann, The Vishing Guide, [δημοσίευση 2007 / τελευταία ενημέρωση 2013] [online] <http://www.windowsecurity.com/whitepapers/Phishing/Vishing-Guide.html>.

[9] Centre for the Protection of National Infrastructure, www.cpni.gov.uk, [online] <https://www.cpni.gov.uk/system/files/documents/87/93/spear-phishing-understanding-the-threat.pdf>.

[10] InfoSec Institute, “The Most Popular Social Network Phishing Schemes”, [online] <http://resources.infosecinstitute.com/the-most-popular-social-network-phishing-schemes/>.

[11] Kaspersky Lab, https://www.kaspersky.com, [online] <https://www.kaspersky.com/blog/1-in-5-phishing-attacks-targets-facebook/5180/>.

[12] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, www.dpa.gr, [online] <http://www.dpa.gr/portal/page?_pageid=33,127384&_dad=portal&_schema=PORTAL>.

[13] Infographic έρευνας «Παιδιά και διαδίκτυο», 13 Φεβρουαρίου 2015, [online] <https://communicationeffect.com/cyber-crime-authority-survey/>.

[14] «Κρατώντας τα παιδιά μας ασφαλή στο Διαδίκτυο», http://www.safekids.gr, 1 Ιουνίου 2015, [online]<http://www.safekids.gr/%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1/%CE%BA%CF%81%CE%B1%CF%84%CF%8E%CE%BD%CF%84%CE%B1%CF%82-%CF%84%CE%B1-%CF%80%CE%B1%CE%B9%CE%B4%CE%B9%CE%AC-%CE%BC%CE%B1%CF%82-%CE%B1%CF%83%CF%86%CE%B1%CE%BB%CE%AE-%CF%83%CF%84%CE%BF-%CE%B4%CE%B9%CE%B1%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%BF >.

[15] Ελληνικό Κέντρο Ασφαλούς Διαδικτύου, http://saferinternet4kids.gr/, [online] <http://saferinternet4kids.gr/category/paidia/>.

[16] Ευρωπαϊκή Ένωση, Κώδικας επιγραμμικών δικαιωμάτων στην ΕΕ, Λουξεμβούργο 2012, [online] <https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/Code%20EU%20online%20rights%20EL%20final.pdf>.

[17] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, [online] <http://www.dpa.gr>.

[18] Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, [online] <http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=8194&Itemid=378&lang=>.

[19] European Independent Data Protection Authority, [online] <https://edps.europa.eu/about-edps/members-mission/supervisors_en>.

[20] Ευρωπαίος Επόπτης Προστασίας Δεδομένων ΕΕΔΠ, [online] <https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor_el>.

[21] EU Whoiswho, [online] <(http://europa.eu/whoiswho/public/index.cfm?lang=el>.

[22] Φόρμα καταγγελίας ΕΕΔΠ, [online] <https://edps.europa.eu/node/75>.

[23] Μιλτιάδης Χαλικιάς, Αναπληρωτής Καθηγητής ΑΕΙ Πειραιά ΤΤ, Αλεξάνδρα Μανωλέσου, Msc Biostatistics, Παναγιώτα Λάλου, Phd Mathematics, «Μεθοδολογία Έρευνας και Εισαγωγή στη Στατιστική Ανάλυση Δεδομένων με το IBM SPSS STATISTICS», Εκδόσεις ΣΕΑΒ 2015.

[24] Γ. Σαραφίδου, [online] <http://eclass.uth.gr/eclass/modules/document/file.php/SEAA187/%CE%9C%CE%AC%CE%B8%CE%B7%CE%BC%CE%B1%2013-5.ppt>.

[25] Γιάννης Δ. Κατερέλος, «Εισαγωγή στην κοινωνική έρευνα ΙΙ», Πάντειο Πανεπιστήμιο Κοινωνικών και Πολιτικών Επιστημών 2015, [online] <http://openeclass.panteion.gr/modules/document/file.php/TMD223/600094.pdf>.

[26] Τσαγρής Μιχαήλ, «Στατιστική με τη χρήση του IBM SPSS 22», 2014

[27] Dr.. Ευθυμία Νικήτα, «Έννοιες στατιστικής και εφαρμογές με το SPSS», 2012

[28] Νέλλας Ε., Ε.Ε.ΔΙ.Π., «Ανάλυση Δεδομένων με Χρήση του Στατιστικού Πακέτου SPSS για Windows», Γεωπονικό Πανεπιστήμιο Αθηνών Τμήμα Αγροτικής Οικονομίας & Ανάπτυξης Εργαστήριο Διοίκησης(Μανατζμεντ) Γεωργικών Επιχειρήσεων & Εκμεταλλεύσεων, 2005

Επιτροπή Έγκρισης & Βαθμολόγησης

Δρ.Δ.Τσελές	Δρ.Κ.Αλαφοδήμος	Δρ. Χρήστος Δρόσος
Καθηγητής	Καθηγητής	Επιβλέπων-Εισηγητής
Διευθυντής Π.Μ.Σ	Πρόεδρος Τμ.Μηχ. Αυτομ.	

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ