**ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ**
**ΣΧΟΛΗ ΚΟΙΝΩΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ**
**ΤΜΗΜΑ ΚΟΙΝΩΝΙΟΛΟΓΙΑΣ**
**ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ «ΚΟΙΝΩΝΙΟΛΟΓΙΑ»**

# «ΝΕΕΣ ΤΕΧΝΟΛΟΓΙΕΣ ΚΑΙ ΕΥΑΙΣΘΗΤΑ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ: ΚΟΙΝΩΝΙΟΛΟΓΙΚΕΣ ΠΡΟΣΕΓΓΙΣΕΙΣ ΚΑΙ ΔΙΕΡΕΥΝΗΣΗ ΣΕ ΤΟΠΙΚΟ ΕΠΙΠΕΔΟ»

**ΦΟΙΤΗΤΡΙΑ**
**ΔΗΜΗΤΡΑΚΗ ΕΛΕΝΗ**

**ΤΡΙΜΕΛΗΣ ΕΠΙΤΡΟΠΗ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ**

**ΕΠΙΒΛΕΠΩΝ:** ΣΑΜΑΤΑΣ ΜΗΝΑΣ
**ΜΕΛΗ:** ΖΑΜΠΑΡΛΟΥΚΟΥ ΣΤΕΛΛΑ
ΧΑΛΑΡΗΣ ΓΕΩΡΓΙΟΣ

**ΡΕΘΥΜΝΟ 2010**

## ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

# ΠΕΡΙΛΗΨΗ

Στην τρέχουσα ύστερη νεωτερικότητα ή μετανεωτερικότητα ζούμε σε κοινωνίες πληροφοριών και παρακολούθησης όπου μέσω των νέων τεχνολογιών της τηλεματικής (ηλεκτρονικοί υπολογιστές, διαδίκτυο, κινητή τηλεφωνία, ανάλυση DNA κτλ) τα προσωπικά δεδομένα και ιδιαίτερα τα ευαίσθητα που αφορούν την ιδιωτική ζωή του ανθρώπου (ζητήματα υγείας, κοινωνικής πρόνοιας, φυλετικής και εθνικής προέλευσης, ερωτικής ζωής, πολιτικά φρονήματα, θρησκευτικές και φιλοσοφικές πεποιθήσεις, συμμετοχή σε συνδικαλιστικές οργανώσεις, ποινικές διώξεις ή καταδίκες, γενετικά δεδομένα, δηλώσεις για τα στοιχεία του αιτούντος άσυλο, τα δεδομένα των ληπτών και δωρητών οργάνων και ιστών, κτλ), γίνονται ολοένα και περισσότερο αντικείμενα εκμετάλλευσης. Είναι εκμεταλλεύσιμα για λόγους θεμιτούς όπως ο κρατικός και υπερκρατικός έλεγχος και η ασφάλεια, η κατηγοριοποίηση και η ταξινόμηση που συνεπάγεται ένταξη ή αποκλεισμό σε τάξεις και κατηγορίες με τη συναίνεση των υποκειμένων όσο και για λόγους αγοράς – κέρδους και καταναλωτικής επιρροής, καθώς και για διάφορους άλλους αθέμιτους λόγους (απάτης, εκβιασμού, παράνομου κέρδους) και μάλιστα χωρίς της συναίνεση των υποκειμένων.

Παρά το θεσμικό οπλοστάσιο για την προστασία των προσωπικών δεδομένων τα άτομα υποκείμενα παρακολούθησης ιδίως των ασθενέστερων οικονομικά τάξεων είτε λόγω άγνοιας, είτε λόγω αμέλειας ή πρόσκαιρου οφέλους διευκολύνουν την παραβίαση της ιδιωτικότητάς τους και μάλιστα των ευαίσθητων προσωπικών δεδομένων τους.

Στην παρούσα εργασία έγινε προσπάθεια διερεύνησης σε τοπικό επίπεδο σε διάφορους φορείς (όπως στρατολογικό γραφείο, ασφαλιστική εταιρεία, νοσοκομείο, αλυσίδα super market) της αποτελεσματικότητας της εφαρμογής των νόμων για την προστασία των προσωπικών δεδομένων και μάλιστα των ευαίσθητων. Απόρροια της έρευνας αυτής ήταν η διαπίστωση ότι σε τοπικό, επαρχιακό επίπεδο οι νόμοι για την προστασία των προσωπικών και των ευαίσθητων προσωπικών δεδομένων ατονούν περισσότερο, οι παραβιάσεις είναι πιο συχνές και ο έλεγχος πιο δύσκολος.

Επίσης, έπειτα από έρευνα σε δείγμα κατοίκων του Ρεθύμνου διαπιστώθηκε ότι έχουν αποδεχθεί την παρακολούθηση από ιδιωτικούς φορείς ως μέρος της καθημερινότητας τους, ενώ αμφισβητούν και αντιδρούν στην κρατική και αστυνομική παρακολούθηση. Μάλιστα φαίνεται να έχουν άγνοια των δικαιωμάτων

τους σχετικά με την επεξεργασία των προσωπικών τους δεδομένων. Παρά τις προφανείς παραβιάσεις, οι φορείς συλλογής και επεξεργασίας προσωπικών δεδομένων ισχυρίζονται ότι λειτουργούν σύμφωνα με τις επιταγές του νόμου, ενώ οι πολίτες, ιδίως αυτοί των ασθενέστερων οικονομικά τάξεων, αγνοούν το σκοπό της συλλογής και τον τρόπο επεξεργασίας των προσωπικών τους δεδομένων, και παράλληλα δείχνουν έντονη δυσπιστία σχετικά με τη χρήση τους από διάφορους φορείς αλλά και σε σχέση με την επάρκεια της νομοθεσίας για την προστασία τους. Φυσικά για όλα τα παραπάνω θέματα που διερευνήσαμε χρειάζεται περισσότερη μελέτη σ' ένα μεγαλύτερο και πιο αντιπροσωπευτικό δείγμα πληθυσμού.

**<u>Λέξεις – κλειδιά:</u>** *παρακολούθηση, Κοινωνία της Πληροφορίας, Κοινωνία της Παρακολούθησης, προσωπικά δεδομένα, ευαίσθητα προσωπικά δεδομένα, Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.*

## ABSTRACT

In current modernity or post modernity we live in information and surveillance societies where through the new telematic technologies personal data and especially sensitive personal data like health, race, religion, political beliefs etc are processed, exploited and manipulated for legal reasons with or without their subject's consent for security, categorization and classification by state and superstate. Personal data exploitation is also used for the market purposes and profit reasons, consumer profiles and even for illegal reasons.

Despite the existing data protection laws, people especially of the lower classes as surveillance subjects either from ignorance or from negligence accept their privacy violation and especially the violation of their sensitive personal data.

In our study, an empirical survey was carried out at the local level with the investigation in certain organizations (like the Draft office, insurance company, hospital, supermarket) and to inquiry the effectiveness of personal data protection laws. Our study has found that personal and sensitive personal data protection laws are not enforced, privacy law violations are more frequent and privacy law enforcement is more difficult especially at the local level.

Also our survey with some local residents from the city of Rethymno has found that they seem to accept their surveillance from private organizations as part of their everyday life while they dispute and react to state and police surveillance. Also they seem to ignore their legal rights for their personal data protection. Despite obvious privacy violations, the organizations that collect and process personal data claim that they operate according to the law, while the citizens especially of the lower classes are not aware of the collection, process and exploitation of their personal data and ignore the laws for their protection. In deed all the issues we investigated need furthermore research with a bigger and more representative sample.



**Key words:** *Surveillance, Information Society, Surveillance Society, personal data, sensitive personal data, Data Protection Authority.*

# ΕΙΣΑΓΩΓΗ

Στις αρχές του 21ου αιώνα ζούμε σε «κοινωνίες παρακολούθησης», δηλαδή σε κοινωνίες των οποίων η οργάνωση και η λειτουργία βασίζεται στη μαζική παρακολούθηση του πληθυσμού, όπου καταγράφονται πληροφορίες σχετικά με την ταυτότητα, τις κινήσεις, τις προτιμήσεις και τις δραστηριότητες των ατόμων μέσω των τεχνολογιών παρακολούθησης για λογαριασμό οργανισμών, κυβερνήσεων αλλά και επιχειρήσεων (Lyon, 2001). Οι πληροφορίες αυτές συλλέγονται, επεξεργάζονται και χρησιμοποιούνται σε βάσεις δεδομένων για τη λήψη αποφάσεων που επηρεάζουν διάφορες πτυχές της ζωής των ανθρώπων όπως η εργασία, η πρόσβαση σε υπηρεσίες, η υγεία κτλ (Ball & Murakami Wood, 2006: 1). Η καθημερινή ζωή των ανθρώπων αποτελεί αντικείμενο παρακολούθησης μέσω της χρήσης των νέων τεχνολογιών, όπου τα προσωπικά δεδομένα συλλέγονται και επεξεργάζονται είτε για λόγους ελέγχου και ασφάλειας, είτε για λόγους φροντίδας αλλά και κέρδους με τη συναίνεση τους ή χωρίς αυτήν. Ενδεικτικά παραδείγματα παρακολούθησης της καθημερινής μας ζωής είναι α) τα κλειστά κυκλώματα τηλεόρασης (CCTV) που υπάρχουν σχεδόν παντού, β) τα νέα διαβατήρια που αποτελούν πηγή προσωπικών πληροφοριών με προοπτική να λειτουργούν με microchip και με βιομετρικά δεδομένα, όπως και οι νέες ταυτότητες, γ) η οργάνωση και η λειτουργία των βιβλιοθηκών μέσω καρτών που περιέχουν προσωπικά δεδομένα για ποια βιβλία δανειστήκαμε, κτλ, δ) οι «έξυπνες» κάρτες (smart cards) των super market που καταγράφουν τις καταναλωτικές μας συνήθειες, ε) η ενδεχόμενη καταγραφή των τηλεφωνημάτων από τις εταιρείες τηλεφωνίας, η παρακολούθηση της χρήσης του διαδικτύου, κτλ.

Το φαινόμενο της παρακολούθησης υπήρχε ανέκαθεν με την πρόσωπο προς πρόσωπο παρακολούθηση. Αναπτύχθηκε όμως με την ορθολογική – γραφειοκρατική οργάνωση του κράτους και ιδίως του έθνους – κράτους για την αποτελεσματικότερη λειτουργία της κρατικής γραφειοκρατίας και την τήρηση αρχείων (Giddens, 1987). Η ανάπτυξη της τηλεματικής, ιδίως από τα μέσα της δεκαετίας του 1970, οδήγησε στην «κοινωνία της Πληροφορίας αλλά και της Παρακολούθησης». Στην εργασία αυτή χρησιμοποιούμε περισσότερο τον όρο «παρακολούθηση» από αυτόν της «επιτήρησης» διότι η επιτήρηση αφορά γενικά την τήρηση κανόνων, δηλαδή την κανονικότητα ενώ η παρακολούθηση συλλέγει και επεξεργάζεται προσωπικά και ευαίσθητα δεδομένα, δηλαδή ενδιαφέρεται για την ιδιωτικότητα, σεξουαλικότητα, κατανάλωση, υγεία, κτλ.

Πράγματι οι νέες τεχνολογίες πληροφοριών και επικοινωνίας με δυνατότητες ελέγχου και συντονισμού από απόσταση αλλά και τη δημιουργία νέων ψηφιακών τεχνικών αναγνώρισης και εντοπισμού με δορυφόρους και οπτικές ίνες συνέβαλαν στη λεγόμενη «επανάσταση των πληροφοριών», στη λεγόμενη «Κοινωνία των Δικτύων» και στη λεγόμενη «νέα παρακολούθηση» (Καστέλς, 2004; Ball & Murakami Wood, 2006: 1; Marx, 2002).

Όμως η νέα παρακολούθηση δεν είναι αποκλειστικό προϊόν των νέων τεχνολογιών, αλλά και του φόβου και της καχυποψίας που δημιουργήθηκε από τις επιθέσεις της 11ης Σεπτεμβρίου στις ΗΠΑ και την ανάγκη προστασίας ενάντια σε απειλές όπως π.χ. η τρομοκρατία, κτλ (Χάρβεϊ, 2007). Εδώ κυρίαρχο ρόλο έχει η γνώση και η επεξεργασία της πληροφορίας που πλέον γίνεται με τη βοήθεια των νέων τεχνολογιών. Έτσι, βασικά χαρακτηριστικά της νέας παρακολούθησης είναι ότι μέσω των νέων τεχνολογιών συλλογής και επεξεργασίας δεδομένων αποτελεί στοιχείο της καθημερινότητας μας, είναι συστηματική και διεξάγεται βάσει σκοπιμοτήτων, είναι δε εστιασμένη, στοχεύει δηλαδή σε αναγνωρίσιμα πρόσωπα των οποίων τα δεδομένα συλλέγονται, αποθηκεύονται, επεξεργάζονται, διαβιβάζονται, ανακτώνται, συγκρίνονται και ενδεχομένως και να εμπορεύονται (Marx, 2002).

Οι τομείς στους οποίους εφαρμόζεται η νέα παρακολούθηση ως συλλογή και επεξεργασία προσωπικών δεδομένων περιλαμβάνουν π.χ: α) την ταυτότητα των ατόμων για την ανάληψη ρίσκου και ασφάλειας όπου η συλλογή και επεξεργασία των προσωπικών δεδομένων είναι ζωτικής σημασίας, με χαρακτηριστικό παράδειγμα το διατραπεζικό σύστημα ΤΕΙΡΕΣΙΑΣ ΑΕ, β) στρατιωτικές εφαρμογές παρακολούθησης μέσω δορυφόρων και διεθνών συστημάτων επικοινωνίας, γ) το διαδίκτυο και το GPS (Global Position System), δ) την ασφάλεια αναφορικά με τις τηλεπικοινωνίες, τους υπολογιστές, τις ηλεκτρονικές εμπορικές και τραπεζικές συναλλαγές και την κοινωνική ή ιδιωτική ασφάλιση και ε) εμπορία και λαθρεμπορία προσωπικών δεδομένων από απλούς ιδιώτες. Διότι όσοι έχουν πρόσβαση σε τράπεζες δεδομένων μπορούν να εκμεταλλεύονται τα δεδομένα αυτά προς ίδιον όφελος, γεγονός που προκαλεί έλλειψη εμπιστοσύνης στους θεσμούς που με τη σειρά της καλλιεργεί την ανασφάλεια και την καχυποψία (Ball & Murakami Wood, 2006; 1 – 3).

Το θέμα μας λοιπόν προς διερεύνηση είναι αυτό της ασύδοτης επεξεργασίας των προσωπικών και ιδιαίτερα των ευαίσθητων προσωπικών δεδομένων στο πλαίσιο του «πληροφοριακού καπιταλισμού» (Information Capitalism) και της «κοινωνίας της πληροφορίας» – που είναι ταυτόχρονα και «κοινωνία της παρακολούθησης» – με την

επέκταση εφαρμογής των τεχνολογιών παρακολούθησης σε διάφορες πτυχές της καθημερινότητας κυρίως για τους σκοπούς της ασφάλειας και του ελέγχου αλλά και της φροντίδας και του κέρδους, ιδιαίτερα μετά τα γεγονότα της 11ης Σεπτεμβρίου.

Με βάση το γεγονός ότι ζούμε σε κοινωνίες των πληροφοριών και της παρακολούθησης όπου η χρήση των νέων τεχνολογιών είναι ευρέως διαδεδομένη και τα προσωπικά δεδομένα και ιδιαίτερα τα ευαίσθητα προσωπικά δεδομένα γίνονται ολοένα και πιο εκμεταλλεύσιμα για διάφορους σκοπούς, θεμιτούς ή αθέμιτους, θα προσπαθήσουμε να αποδείξουμε ότι παρά την ύπαρξη της νομοθεσίας για την προστασία των προσωπικών και των ευαίσθητων προσωπικών δεδομένων, η παραβίαση της ιδιωτικότητας και η εκμετάλλευση των ευαίσθητων προσωπικών δεδομένων του ατόμου αποτελεί καθημερινή πραγματικότητα ιδιαίτερα σε τοπικό επίπεδο, καθώς υπάρχει αδυναμία στην εφαρμογή της παραπάνω νομοθεσίας, αλλά και άγνοια ή αμέλεια από την πλευρά των υποκειμένων της παρακολούθησης, ιδίως των ασθενέστερων τάξεων.

Για τη διερεύνηση της παραπάνω βασικής μας υπόθεσης εργασίας αρχικά διεξήγαμε άτυπη εμπειρική έρευνα σε κάποιους φορείς της πόλης του Ρεθύμνου (στρατολογικό γραφείο, ασφαλιστική εταιρεία, νοσοκομείο, αλυσίδα super market) οι οποίοι για την εξυπηρέτηση των σκοπών της λειτουργίας τους συλλέγουν και επεξεργάζονται προσωπικά και ευαίσθητα προσωπικά δεδομένα, προκειμένου να διαπιστώσουμε το βαθμό της νομιμότητας της όλης αυτής διαδικασίας. Χρησιμοποιήσαμε τη μέθοδο της άτυπης συνέντευξης με τους υπεύθυνους των παραπάνω φορέων.

Στη συνέχεια, διερευνήσαμε με ερωτηματολόγιο στο τοπικό επίπεδο τις απόψεις και τις αντιλήψεις τυχαίου δείγματος κατοίκων της πόλης του Ρεθύμνου όσον αφορά την προστασία των προσωπικών και των ευαίσθητων προσωπικών τους δεδομένων. Για την έρευνα μας αυτή λάβαμε υπόψη μας, έπειτα από βιβλιογραφική ανασκόπηση και διερεύνηση μέσω του διαδικτύου έρευνες με ανάλογο αντικείμενο, και συγκεκριμένα την έρευνα του Ευρωβαρομέτρου (2008) για τη μελέτη των αντιλήψεων πολιτών των χωρών της Ευρωπαϊκής Ένωσης (ΕΕ) σχετικά με την προστασία των προσωπικών τους δεδομένων, και αυτή της Σχολής Κοινωνικών Επιστημών του Πανεπιστημίου Κρήτης που είχε σαν στόχο τη διερεύνηση της προστασίας της ιδιωτικής ζωής και των προσωπικών δεδομένων από τα μέλη της πανεπιστημιακής κοινότητας. Το ερωτηματολόγιο της έρευνας μας αποτελούσε συνδυασμό εκείνων που χρησιμοποιήθηκαν στις παραπάνω δύο έρευνες. Η ανάλυση

και η επεξεργασία των αποτελεσμάτων έγινε με τη βοήθεια του στατιστικού προγράμματος SPSS16.0.

Έτσι, η παρούσα μελέτη μας αφορά μια κοινωνιολογική διερεύνηση της επίδρασης των νέων τεχνολογιών στην προστασία των προσωπικών και ιδιαίτερα των ευαίσθητων προσωπικών δεδομένων στο τοπικό επίπεδο. Στο πρώτο κεφάλαιο αναπτύσσονται οι βασικές κοινωνιολογικές προσεγγίσεις για την «Κοινωνία της Πληροφορίας» ως «Κοινωνία της Παρακολούθησης» ενώ το δεύτερο κεφάλαιο αναφέρεται στις τεχνολογίες παραβίασης της ιδιωτικότητας του ατόμου στο πλαίσιο αυτής.

Το τρίτο και το τέταρτο κεφάλαιο αναφέρονται στην προστασία των προσωπικών και των ευαίσθητων προσωπικών δεδομένων στην ΕΕ και την Ελλάδα αντίστοιχα. Παραθέτουμε την ευρωπαϊκή όσο και την ελληνική νομοθεσία για την προστασία των προσωπικών δεδομένων, τις βασικές αρχές που πρέπει να διέπουν τη συλλογή και την επεξεργασία τους αλλά και τα δικαιώματα των υποκειμένων για την προστασία της ιδιωτικότητας. Διότι, η ΕΕ είναι αυτή που θέτει τις κατευθυντήριες γραμμές για κάθε κράτος – μέλος της, και εν προκειμένω η Ελλάδα, καλείται να τις προσαρμόσει στο δίκαιο και την κουλτούρα του. Έτσι, στα κράτη – μέλη έχουν δημιουργηθεί οι εθνικές Αρχές Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), οι οποίες έχουν σαν στόχο την προστασία της προσωπικότητας και της ιδιωτικής ζωής του ατόμου προσδιορίζοντας το πλαίσιο προστασίας των προσωπικών δεδομένων και μάλιστα των ευαίσθητων προσωπικών δεδομένων. Το πέμπτο λοιπόν κεφάλαιο αναφέρεται στη λειτουργία της Ελληνικής ΑΠΔΠΧ και στις αποφάσεις που έχει εκδώσει σε σχέση με ευαίσθητα προσωπικά δεδομένα.

Στο έκτο κεφάλαιο παραθέτουμε και αναλύουμε τα αποτελέσματα της εμπειρικής μας έρευνας που διεξήγαμε σε διάφορους φορείς του Ρεθύμνου προκειμένου να διαπιστώσουμε την αποτελεσματικότητα της εφαρμογής της νομοθεσίας για την προστασία των προσωπικών και των ευαίσθητων προσωπικών δεδομένων, αλλά και σε κατοίκους του Ρεθύμνου αναφορικά με τις αντιλήψεις τους για την προστασία των δεδομένων τους και το βαθμό αποδοχής της παραβίασης της ιδιωτικότητας τους. Διαπιστώσαμε ότι για κάποιους από τους φορείς η συλλογή και επεξεργασία των προσωπικών δεδομένων αποτελεί διαδικασία ρουτίνας με αποτέλεσμα οι υπάλληλοι να μην έχουν επίγνωση ότι διαχειρίζονται τέτοιου είδους ευαίσθητα δεδομένα, ενώ ταυτόχρονα τα υποκείμενα των δεδομένων δεν έχουν επίγνωση των δικαιωμάτων τους σε σχέση με την προστασία των προσωπικών τους

δεδομένων. Τέλος, από την έρευνα σε μικρό δείγμα κατοίκων της πόλης του Ρεθύμνου διαπιστώθηκε ότι ενώ αρκετές φορές τάσσονται γενικά υπέρ της παρακολούθησης, δυσπιστούν και δυσανασχετούν όχι από την κρατική παρακολούθηση αλλά από αυτή στο χώρο της εργασίας τους από τους εργοδότες.

Τέλος, συγκρίνουμε τα αποτελέσματα της έρευνας μας με αυτές του Ευρωβαρομέτρου και της Σχολής Κοινωνικών Επιστημών του Πανεπιστημίου Κρήτης και καταλήγουμε στα γενικά μας συμπεράσματα, που επιβεβαιώνουν τη βασική μας υπόθεση.

# ΚΕΦΑΛΑΙΟ 1$^{Ο}$
# ΚΟΙΝΩΝΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ ΚΑΙ Η ΠΑΡΑΒΙΑΣΗ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ: ΚΟΙΝΩΝΙΟΛΟΓΙΚΕΣ ΠΡΟΣΕΓΓΙΣΕΙΣ

## 1.1: Η Κοινωνία της Παρακολούθησης στο πλαίσιο του νεοφιλελευθερισμού και του νεοσυντηρητισμού

Από τη δεκαετία του 1970 παρατηρούνται εμφανείς αλλαγές στον τομέα της οικονομίας των αναπτυγμένων κοινωνιών και της μετάβασης από τη βιομηχανική εποχή στη μεταβιομηχανική εποχή βασικό χαρακτηριστικό της οποίας αποτελούν οι νέες τεχνολογίες της πληροφορίας και της επικοινωνίας. Αναδύεται δηλαδή ένα νέο είδος δικτυακής οικονομίας που χαρακτηρίζεται από ευελιξία ενώ υπάρχει ποιοτική μεταβολή στην οργάνωση της λεγόμενης δικτυακής κοινωνίας (Καστέλς, 2004).

Σύμφωνα με τον Ντάνιελ Μπελ, όπως στη βιομηχανική εποχή κινητήρια δύναμη αποτελούσαν η παραγωγή υλικών προϊόντων και το κέρδος με τη χρήση της ενέργειας και των μηχανημάτων, στη μεταβιομηχανική κοινωνία κινητήρια δύναμη αποτελούν η γνώση και η πληροφορία (Bell, 1999; Allen, 2003: 249 – 263).

Έτσι, η πληροφορία γίνεται ένα πολύτιμο στρατηγικό μέσο στη μεταβιομηχανική εποχή, ενώ στο χώρο του δικαίου διαμορφώνεται ένα νέο άυλο έννομο αγαθό, η πληροφορία των προσωπικών δεδομένων με τεράστια οικονομική, πολιτιστική και πολιτική σημασία[1]. Μάλιστα η γνώση και η πληροφορία είναι αυτές που μας «πηγαίνει πέρα από τη βιομηχανική εποχή, σε έναν κόσμο υπηρεσιών με επίκεντρο τις τεχνολογίες της πληροφορικής και των δικτυωμένων υπηρεσιών»[2] (Allen, 2003: 293).

Κυρίαρχος είναι ο ρόλος τόσο των ηλεκτρονικών υπολογιστών όσο και του διαδικτύου (internet), των δορυφόρων, των τραπεζών δεδομένων (data banks) και

[1] Η πληροφορία δηλαδή θεωρείται βασικό μέσο βελτίωσης της οικονομικής λειτουργίας αφού αποτελεί ταυτόχρονα και πρώτη ύλη αλλά και εμπόρευμα ως αποτέλεσμα της παραγωγικής διαδικασίας καθώς η γνώση «έχει αντικαταστήσει την (παραγωγική) εργασία ως πηγή αξίας που αποδίδει μελλοντικά κέρδη. (Bell, 1999: 41 και 47; Hall et al, 2003: 254 – 259, 262, 293; Καστέλς, 2005).

[2] Η επεξεργασία της πληροφορίας έχει την ικανότητα να μεταβάλλει ριζικά τους συνηθισμένους τρόπους σκέψης και δράσης όπου μέσω των νέων τεχνολογιών δίνεται η δυνατότητα αναμόρφωσης του τρόπου παραγωγής και κατανάλωσης αλλά και του τόπου στον οποίο επιτελούνται αυτές οι δραστηριότητες. Μάλιστα η πληροφορία και οι χρήσεις της θεωρούνται βασικοί συντελεστές, που έχουν αρχίσει ήδη να αναδιαμορφώνουν τις δραστηριότητες στους τομείς της μεταποίησης και του κράτους καθώς και στις ιδιωτικές υπηρεσίες, όπως ο χρηματοπιστωτικός τομέας και το εμπόριο (Allen, 2003: 259, 267 και 293).

γενικά της τηλεματικής για την επεξεργασία πληροφοριών και την παροχή άυλων ψηφιοποιημένων υπηρεσιών. Οι νέες τεχνολογίες συλλογής, επεξεργασίας και μετάδοσης πληροφοριών έχουν γίνει απαραίτητες για την οργάνωση και τη λειτουργία της μεταβιομηχανικής, «δικτυακής» κοινωνίας, με αποτέλεσμα να υπάρχει απεριόριστη δυνατότητα επεξεργασίας των στοιχείων κάθε ανθρώπινης δραστηριότητας. Δηλαδή, τα συστήματα πληροφορικής και η επεξεργασία των πληροφοριών με ψηφιακά μέσα είναι πλέον απαραίτητα στον ιδιωτικό και το δημόσιο τομέα (Καστέλς, 2005).

Η παραγωγή στο σύνολο της οργανώνεται βάσει των νέων τεχνολογιών αγνοώντας τις συνέπειες που μπορεί να έχει στην κοινωνία. Αρχικά έχουμε τη δημιουργία μεγαλύτερης οικονομικής και κοινωνικής ανισότητας αφού πλέον ο κόσμος αποτελείται από την ελίτ επαγγελματιών και των εξειδικευμένων εργαζόμενων και από την τάξη των εργαζόμενων σε υπηρεσίες υπό το καθεστώς περιστασιακής ή μερικής απασχόλησης.

Με την εμφάνιση των νέων τεχνολογιών έχουμε την παγκοσμιοποίηση της οικονομίας όπου όλος ο πλανήτης καθίσταται μία ενιαία αγορά, με τη διεθνικοποίηση των επιχειρήσεων σε παγκόσμια κλίμακα και τη «σμίκρυνση» του χώρου και του χρόνου και την έκταση στην οποία οι τύχες των ανθρώπων σε διάφορα μέρη του πλανήτη αλληλοσυνδέονται και συσχετίζονται ολοένα και περισσότερο (Allen, 2003: 293 – 296). Η οικονομική αυτή παγκοσμιοποίηση λαμβάνει χώρα στο πλαίσιο του νεοφιλελευθερισμού[3] όπου πλέον υποβαθμίζονται τα δημόσια αγαθά, ο δημόσιος τομέας συρρικνώνεται και ιδιοποιείται από τον ιδιωτικό τομέα και τα πάντα ιδιωτικοποιούνται στην προσπάθεια να δοθούν λύσεις στα κοινωνικά προβλήματα. Η παγκοσμιοποίηση της αγοράς με τη βοήθεια των νέων τεχνολογιών λειτουργεί προς όφελος του ιδιωτικού κεφαλαίου και εις βάρος του δημόσιου τομέα (Χάρβεϊ, 2007).

Στο πλαίσιο της νεοφιλελεύθερης παγκοσμιοποίησης η κοινωνία της πληροφορίας εμπορευματοποιείται και είναι ευάλωτη σε απειλές και παραβιάσεις από τις νέες τεχνολογίες, ιδιαίτερα στο ζήτημα της προστασίας των προσωπικών δικαιωμάτων και ελευθεριών γενικά, αλλά και των ευαίσθητων προσωπικών δεδομένων, ειδικότερα για λόγους ασφάλειας, ελέγχου, κέρδους και επιρροής (Ιγγλεζάκης, 2004). Διότι η «Κοινωνία της Πληροφορίας» είναι ταυτόχρονα και

[3] Ο Νεοφιλελευθερισμός είναι μία θεωρία πολιτικοοικονομικών μεθόδων που πρεσβεύει ότι η ανθρώπινη ευημερία μπορεί να προαχθεί καλύτερα με την αποδέσμευση των ατομικών επιχειρηματικών ελευθεριών και ικανοτήτων μέσα σ' ένα θεσμικό πλαίσιο που χαρακτηρίζεται από ισχυρά ατομο-ιδιοκτησιακά δικαιώματα, ελεύθερες αγορές και ελεύθερο εμπόριο (Χάρβεϊ, 2007: 24).

«Κοινωνία της Παρακολούθησης» με την έννοια της συλλογής και επεξεργασίας των πληροφοριών και ιδίως των προσωπικών δεδομένων. Επίσης τα παραπάνω συνδυάζονται με το «νεοσυντηρητισμό», ο οποίος προσπαθεί να βάλει τάξη στο χάος που προκλήθηκε από το νεοφιλελευθερισμό, επικαλούμενος την ξενοφοβία, την τρομοκρατία και την εδραίωση των κοινωνικών εξουσιών με την επίκληση παραδοσιακών θεσμών και αξιών. Ο νεοσυντηρητισμός δηλαδή προσπαθεί να κάνει συνεκτικότερη τη νεοφιλελεύθερη κοινωνία επικαλούμενος δυνητικούς εσωτερικούς και εξωτερικούς κινδύνους, χρησιμοποιώντας ακόμη και τη στρατικοποίηση ως αντίδοτο, καλλιεργώντας με τον τρόπο αυτό την καχυποψία, ενδυναμώνοντας έτσι την «Κοινωνία της Παρακολούθησης» (Χάρβεϊ, 2007: 118 – 121).

### 1.2: Οι απόψεις του Anthony Giddens

Σύμφωνα με τον Giddens (1987), η παρακολούθηση είναι βασική λειτουργία του έθνους – κράτους. Θεωρεί ότι το νεωτερικό έθνος – κράτος βασίζεται στην επιτήρηση – παρακολούθηση και στην προετοιμασία για τη χρήση της βίας και την προσφυγή στον πόλεμο. Ο τρόπος οργάνωσης της νεωτερικής κοινωνίας είναι τέτοιος που καλλιεργεί και ενισχύει την παρακολούθηση – επιτήρηση και αυτό φαίνεται από τη νομιμοποίηση της χρήσης διαφόρων μέσων για την επίτευξη της. Δηλαδή υπάρχει στρατικοποίηση του έθνους – κράτους καθιστώντας το έτοιμο να αντιδράσει προκειμένου να προστατευθεί από κάθε εσωτερική ή εξωτερική απειλή. Έτσι τα πάντα πρέπει να ελέγχονται από το κράτος, το οποίο απαιτεί από τους πολίτες την παροχή υπηρεσιών να εκχωρούν τα προσωπικά τους δεδομένα. Η μη εκχώρηση τους μπορεί να σημαίνει προσπάθεια απόκρυψής τους για κάποιο λόγο, ο οποίος πρέπει να διερευνηθεί, ως εν δυνάμει ύποπτος.

Έτσι προκύπτει το θέμα της εμπιστοσύνης που σύμφωνα με τον Giddens έχει πολλές διαστάσεις[4]. Θεωρεί ότι στη νεωτερικότητα εμπιστοσύνη υπάρχει στο πλαίσιο τόσο της γενικής επίγνωσης ότι η ανθρώπινη δραστηριότητα είναι κοινωνικό δημιούργημα και δεν απορρέει από τη φύση των πραγμάτων ή από θεϊκή επιρροή όσο και της απέραντα αυξημένης μετασχηματιστικής δύναμης των ανθρώπινων ενεργειών

[4] Ως εμπιστοσύνη ορίζεται η «πεποίθηση για την αξιοπιστία ενός προσώπου ή συστήματος, εν σχέσει προς κάποιο δεδομένο σύνολο αποτελεσμάτων ή συμβάντων, όπου αυτή η πεποίθηση εκφράζει πίστη στην εντιμότητα ή την αγάπη τρίτου ή στην ορθότητα αφηρημένων αρχών (τεχνική γνώση)» (Giddens, 2001: 51).

που προέρχεται από το δυναμικό χαρακτήρα των μοντέρνων κοινωνικών θεσμών (Giddens, 2001: 51).

Γι' αυτόν η νεωτερικότητα έχει τέσσερις διαστάσεις: α) τον καπιταλισμό δηλαδή το σύστημα εμπορευματικής παραγωγής, βασικό χαρακτηριστικό του οποίου είναι η σχέση μεταξύ της ατομικής ιδιοκτησίας του κεφαλαίου και της μισθωτής εργασίας, β) το βιομηχανισμό στον οποίο χρησιμοποιούνται άψυχες παραγωγικές δυνάμεις και μηχανές στην παραγωγική διαδικασία, γ) την επιτήρηση που αναφέρεται στις ικανότητες επιτήρησης των δραστηριοτήτων του πληθυσμού κυρίως στην πολιτική σφαίρα, τόσο με άμεσο τρόπο όσο και με έμμεσο κυρίως ασκώντας έλεγχο στην πληροφόρηση και δ) τη στρατιωτική εξουσία που αναφέρεται στον έλεγχο των μέσων άσκησης της βίας στο πλαίσιο της εκβιομηχάνισης του πολέμου (Giddens, 2001: 74 – 79).

Με την εμφάνιση των εθνών – κρατών η οργάνωση των κοινωνιών βασίζεται ως επί το πλείστον στη συλλογή και τη διαχείριση των πληροφοριών για διοικητικούς, εξουσιαστικούς και στρατιωτικούς σκοπούς, όπου πρέπει να ελέγχονται και να παρακολουθούνται τα πάντα. Ο όρος έθνος – κράτος αφενός αποτελεί γεωγραφικό προσδιορισμό και αφετέρου χρησιμοποιείται για να αποδώσει ταυτότητα στα άτομα – κατοίκους μιας συγκεκριμένης γεωγραφικής περιοχής, εντός συγκεκριμένων συνόρων. Οι συνθήκες δημιουργίας των εθνών – κρατών ήταν για σκοπούς άμυνας, προετοιμασίας και διεξαγωγής του πολέμου ενώ βασική είναι η χρήση της τεχνολογίας για την ανάπτυξη της πολεμικής βιομηχανίας. Δηλαδή, όλα τα επίπεδα της κοινωνικής και οικονομικής οργάνωσης βασίζονται στη συστηματική συλλογή πληροφοριών που αφορούν τα άτομα και τις ενέργειές τους. Ιδιαίτερα στην εποχή της ύστερης νεωτερικότητας η πληροφορία βρίσκεται στο επίκεντρο ενώ οι μηχανισμοί επιτήρησης και παρακολούθησης λειτουργούν αντιφατικά σε σχέση με τις συνταγματικές επιταγές για την προστασία του ατόμου και της ιδιωτικής του ζωής.

Διότι η παρακολούθηση στο πλαίσιο του νεωτερικού έθνους – κράτους μέσω της συλλογής και επεξεργασίας προσωπικών δεδομένων αφενός εξυπηρετεί διοικητικούς σκοπούς και αφετέρου, δίνεται η δυνατότητα με τη χρήση των νέων τεχνολογιών να παρακολουθούνται ομάδες του πληθυσμού βάσει διαφόρων κριτηρίων με αποτέλεσμα την καθημερινοποίηση του φαινομένου της

παρακολούθησης[5]. Είναι αυτό που χαρακτηρίζει ο Giddens ως «παράδοξο της ιδιωτικότητας», την αντίθεση μεταξύ «ατομικοποίησης» που αναφέρεται στα εξατομικευμένα στοιχεία αναγνώρισης του ατόμου και της «ατομικότητας» που αφορά το σκληρό πυρήνα της ιδιωτικότητάς του. Δηλαδή, το άτομο πλέον είναι αναγκασμένο να μοιράζεται τα προσωπικά του δεδομένα προκειμένου να πετύχει κάποιο στόχο του, σε βάρος της ιδιωτικότητάς του. Χαρακτηριστικό είναι το παράδειγμα των συναλλαγών μας τόσο με δημόσιους όσο και με ιδιωτικούς φορείς προκειμένου να μπορέσουμε να κάνουμε χρήση κάποιων υπηρεσιών (Giddens, 2001).

### 1.3: Οι απόψεις του Manuel Castells

Ο Manuel Castells θεωρεί ότι η καπιταλιστική αναδόμηση και η τεχνολογία διαδραματίζουν σημαντικό ρόλο στην αλλαγή της κοινωνίας ενώ σημαντικό ρόλο έχει η γνώση και η χρήση της πληροφορίας περισσότερο από κάθε άλλο οικονομικό τομέα. Από το βιομηχανικό τύπο ανάπτυξης που αναφέρεται στο παραγωγικό σύστημα που οργανώνεται με βάση την ιδιοκτησία, την αγορά, τον ανταγωνισμό και το κέρδος, έχουμε μεταβεί σε ένα «πληροφοριακό τύπο ανάπτυξης» που αυξάνει την παραγωγικότητα. Εδώ η γνώση χρησιμοποιείται για τη δημιουργία νέας γνώσης και είναι καθοριστικής σημασίας για την οικονομική ανάπτυξη ενώ η πληροφορία αποτελεί ταυτόχρονα την πρώτη ύλη και το εμπόρευμα ως αποτέλεσμα της παραγωγικής διαδικασίας.

Η οικονομία αναπτύσσεται πλέον σε παγκόσμιο επίπεδο με τη βοήθεια των νέων ψηφιακών τεχνολογιών και των δικτύων επικοινωνιών και πληροφοριών που αλλάζουν τον τρόπο διεξαγωγής της παραγωγικής διαδικασίας στο σύνολο της αλλά και της οργάνωσης της κοινωνίας. Έτσι, στις σύγχρονες δικτυακές κοινωνίες (Network Societies), σημαντικό ρόλο έχει ο πληροφοριακός τύπος ανάπτυξης (πληροφοριακός καπιταλισμός) όπου η διαχείριση της πληροφορίας μέσω δικτύων αποτελεί την κινητήρια δύναμη της παραγωγικής διαδικασίας στο σύνολο της, της διανομής, της κατανάλωσης και της διοίκησης. Η μετάδοση της πληροφορίας δεν υπόκεινται σε περιορισμούς του χώρου και του χρόνου, ούτε σε γεωγραφικούς

[5] Όπως χαρακτηριστικά αναφέρει ο Giddens: «οι δυνατότητες ενός κράτους με ολοκληρωτικό χαρακτήρα εξαρτώνται από την ύπαρξη κοινωνιών στις οποίες το κράτος μπορεί να διεισδύσει επιτυχώς στις καθημερινές δραστηριότητες της πλειονότητας των υπηκόων του. Αυτό με τη σειρά του προϋποθέτει υψηλό επίπεδο παρακολούθησης …. και κωδικοποίησης των πληροφοριών που είναι σχετικές με την επίβλεψη της συμπεριφοράς σημαντικού μέρους του πληθυσμού» (Giddens,1987: 302).

περιορισμούς εξαιτίας της ανάπτυξης των παγκόσμιων δικτύων. Η δυνατότητα συλλογής, επεξεργασίας και αναμετάδοσης των πληροφοριών είναι απεριόριστη μέσω της ύπαρξης των παγκόσμιων πληροφοριακών δικτύων που μετατρέπουν την κοινωνία, την αγορά, την εκπαίδευση κτλ σε παγκόσμια δίκτυα (Καστέλς, 2004: 256 – 263, Hall et al, 2003: 260 – 262, 303 - 305).

Σύμφωνα με τον Καστέλς «η βασικότερη από τις νέες τεχνολογίες είναι το διαδίκτυο, η κουλτούρα του οποίου αποτελεί ένα συλλογικό οικοδόμημα που υπερβαίνει τις ατομικές προτιμήσεις και επηρεάζει τις πρακτικές των παραγωγών του. Αποτελεί εργαλείο για δράση, πληροφόρηση, στρατολόγηση, οργάνωση, κυριαρχία, αντικυριαρχία, μέσο επικοινωνία κτλ. Αρχικά θεωρούνταν ότι θα υπηρετούσε τη διεύρυνση της δημοκρατίας καθώς θα λειτουργούσε ως μέσο επιτήρησης της κυβέρνησης από τους πολίτες (sousveillnace: παρακολούθηση από τα κάτω) – τους απλούς ανθρώπους. Η κυβέρνηση χρησιμοποιεί το διαδίκτυο ως πίνακα ανακοινώσεων και τα ΜΜΕ λειτουργούν επηρεάζοντας προς όποια κατεύθυνση επιθυμούν την κοινή γνώμη σε αντιδιαστολή με το διαδίκτυο που αποτελεί οριζόντιο, μη ελεγχόμενο, φθηνό κανάλι επικοινωνίας ένα προς ένα και ενός προς πολλούς ενώ λειτουργεί ως μέσο για τη δημιουργία της πολιτικής των σκανδάλων» (Καστέλς, 2005: 64 – 84, 169 – 171).

Όμως ενώ αρχικά το διαδίκτυο αποτελούσε χώρο ελεύθερης και χωρίς περιορισμούς έκφρασης του ατόμου, τώρα έχει μετατραπεί σε εργαλείο ελέγχου της συμπεριφοράς του ατόμου, των κινήσεων του όταν χρησιμοποιεί το διαδίκτυο αλλά και των προτιμήσεων του, μετατρέποντας έτσι τα ενδιαφέροντα και τις αξίες σε καθοδηγητικούς κανόνες της ανθρώπινης συμπεριφοράς (Καστέλς, 2005: 187 – 198). Όσον αφορά τα προσωπικά δεδομένα στον κυβερνοχώρο, αρχικά θεωρούνταν ότι είναι προστατευμένα εξαιτίας της ανωνυμίας της επικοινωνίας μέσω του διαδικτύου. Όμως μπορούν να παραβιαστούν αφού υπάρχει η δυνατότητα να εντοπιστούν οι κινήσεις του χρήστη στο διαδίκτυο, να συσχετιστούν και να οδηγήσουν στην ανακάλυψη της ταυτότητας του και στη δημιουργία προφίλ από τις προτιμήσεις του. Αυτό συμβαίνει λόγω της εμπορευματοποίησης του διαδικτύου μέσω της δημιουργίας λογισμικών που επιτρέπουν τον έλεγχο του. Τα λογισμικά αυτά χρησιμοποιούνται για την αναγνώριση, την επιτήρηση και την έρευνα των χρηστών του διαδικτύου (Καστέλς, 2005: 201 – 205).

Ουσιαστικά το διαδίκτυο ενισχύει την εξουσία των κυβερνήσεων και των εταιρειών για υποκλοπές και έλεγχο της κυκλοφορίας των πληροφοριών, περιορίζει

δε την προστασία των προσωπικών δεδομένων και ιδιαίτερα των ευαίσθητων. Για παράδειγμα όταν κάποιος ομοφυλόφιλος επισκέπτεται ένα chat room σεξουαλικής προτίμησης μπορεί να αναγνωριστεί η ταυτότητα του, προσβάλλεται δηλαδή η ελευθερία του με αποτέλεσμα να θυματοποιείται ως άτομο.

Το διαδίκτυο δηλαδή αποτελεί πεδίο ελεύθερης δράσης του ατόμου το οποίο μπορεί να χαρακτηριστεί χαοτικό και χωρίς περιορισμούς. Έτσι, το κράτος αδυνατεί να ελέγξει τις πληροφορίες που διοχετεύονται μέσω αυτού γεγονός που έχει ως αποτέλεσμα τη δημιουργία τεχνολογιών ανάγνωσης, επιτήρησης και έρευνας. Εξαιτίας λοιπόν της παραπάνω αδυναμίας του, το κράτος παραχωρεί μέρος των κυριαρχικών του δικαιωμάτων σε υπερεθνικές και εποπτικές αρχές προκειμένου να διατηρήσει την κυριαρχία του.

Συνοπτικά ο Καστέλς συμφωνεί με όσους υποστηρίζουν ότι ζούμε στην κοινωνία της παρακολούθησης του Μεγάλου Αδελφού και των μικρών αδελφών δηλαδή των επιχειρήσεων βασικό χαρακτηριστικό της οποίας είναι η έλλειψη κανόνων συμπεριφοράς στο διαδίκτυο αλλά και πρόβλεψης των συνεπειών της, καθώς και η εμπορευσιμότητα των προσωπικών πληροφοριών και ιδιαίτερα των ευαίσθητων (Καστέλς, 2005: 212 – 216, 207 - 209).

### 1.4: <u>Οι απόψεις του David Lyon</u>

Σύμφωνα με τον David Lyon (2003), στην εποχή μας η έννοια της παρακολούθησης και η φύση της έτσι όπως τη γνωρίζαμε στα έθνη – κράτη έχει διαφοροποιηθεί εξαιτίας της χρήσης των νέων τεχνολογιών. Οι μεταβολές στην κοινωνία μας είναι τέτοιες που επιτρέπουν την καθημερινοποίηση της παρακολούθησης, δηλαδή την παρακολούθηση των καθημερινών μας δραστηριοτήτων στην εργασία, στο σπίτι, στις αγορές, κτλ και την επιβάλλουν για λόγους ασφάλειας στις επικοινωνίες και μετακινήσεις.

Κωδικοί, συναλλαγές, επισκέψεις, τηλεφωνήματα και άλλες δραστηριότητες αποτελούν αντικείμενο παρακολούθησης ενώ διάφορα δεδομένα που μπορεί να περιλαμβάνουν βίντεο, βιομετρικά, γενετικά αλλά και ψηφιακά αρχεία μπορούν να χρησιμοποιηθούν στη δημιουργία προφίλ σε ένα δικτυωμένο σύστημα.

Σχεδόν τα πάντα έχουν οργανωθεί μέσω των νέων τεχνολογιών, ενώ έχουν δημιουργηθεί διάφορες βάσεις δεδομένων οι οποίες μπορεί να χρησιμοποιηθούν για σκοπούς π.χ. προώθησης πωλήσεων, αστυνόμευσης κτλ διευκολύνοντας τη συλλογή

και παραβίαση των προσωπικών δεδομένων εξαιτίας της δυνατότητας του διαδικτύου και των τηλεπικοινωνιών. Δηλαδή η παρακολούθηση θεωρείται πλέον κοινωνικά επιθυμητή αλλά και αναγκαία διαδικασία (Lyon, 2005: 368).

Για την επίτευξη της παρακολούθησης χρησιμοποιούνται τεχνολογίες όπως οι βιομετρικές που χρησιμοποιούν π.χ. τα δακτυλικά αποτυπώματα, την ανίχνευση ίριδας ή ακόμη και δείγματα DNA. Υπάρχουν επίσης και τα δορυφορικά συστήματα εντοπισμού GPS (Global Position Satellites), τα συστήματα γεωγραφικών πληροφοριών GIS (Geographic Information Systems) και τα κινητά τηλέφωνα μέσω των οποίων μπορεί να εντοπιστεί η γεωγραφική θέση κάποιου.

Τους σκοπούς της παρακολούθησης υπηρετούν και τα κλειστά κυκλώματα τηλεόρασης (CCTV) που χρησιμοποιούνται για την κατόπτευση πολιτικών, οικονομικών και άλλων χώρων και την αναγνώριση του προσώπου κάποιου, στοιχείο που μπορεί να χρησιμοποιηθεί για διάφορους σκοπούς (Lyon, 2003).

Τα προσωπικά δεδομένα χρησιμοποιούνται για την κατηγοριοποίηση – ταξινόμηση των ατόμων βάσει διαφόρων κριτηρίων (social sorting) που εξυπηρετούν κάποιους σκοπούς π.χ. διαφήμιση, δημόσια τάξη κτλ και έχουν μεγάλη σημασία για τις ευκαιρίες ζωής αλλά και τον αποκλεισμό των ατόμων. Δημιουργούνται δηλαδή οργανωτικές ταυτότητες που αποτελούν σημαντικούς παράγοντες για τον καθορισμό των ευκαιριών ζωής αλλά και νέοι αποκλεισμοί με βάσει υποψίες (categorical suspicion). Αυτό έχει σαν αποτέλεσμα τη συρρίκνωση του ιδιωτικού χώρου και της ιδιωτικότητας τόσο εξαιτίας του τρόπου συλλογής, προώθησης και χρήσης των προσωπικών δεδομένων όσο και εξαιτίας της αλλαγής των κοινωνικών σχέσεων που είναι πιο ρευστές, δικτυακές και αποτελούν αντικείμενο παρακολούθησης με βάση το πρόταγμα της ασφάλειας και του ελέγχου, αλλά και για λόγους φροντίδας και κέρδους (Lyon, 2003: 18 – 22).

Οφείλουμε λοιπόν να συνειδητοποιήσουμε ότι ζούμε σε κοινωνίες παρακολούθησης λαμβάνοντας υπόψη ότι η παρακολούθηση μέσω των νέων τεχνολογιών και δικτύων είναι πιο διεισδυτική από ποτέ και ότι τα προσωπικά μας δεδομένα διατίθενται και χρησιμοποιούνται και από πολυεθνικές εταιρείες, και όχι μόνο από το κράτος για την άσκηση της κυριαρχίας, του ελέγχου και της αστυνόμευσης. Χαρακτηριστικό είναι το παράδειγμα των φαρμακευτικών εταιρειών που μπορούν να έχουν πρόσβαση σε διάφορες βάσεις προσωπικών δεδομένων. Όσο για τα προσωπικά δεδομένα που συλλέγονται στην καθημερινότητα μας, μπορούν

παρά τους νόμους και περιορισμούς να αντιγραφούν, να τροποποιηθούν και να πωληθούν εξυπηρετώντας διάφορους σκοπούς (Lyon, 2003: 24 – 28).

Δηλαδή, σύμφωνα με το Lyon στις μέρες μας η παραβίαση της ιδιωτικότητας του ατόμου και των προσωπικών και ιδιαίτερα των ευαίσθητων προσωπικών του δεδομένων λαμβάνει χώρα σχεδόν σε κάθε δραστηριότητα της καθημερινής του ζωής για θετικούς αλλά και αρνητικούς λόγους π.χ. ασφάλειας, φροντίδας, ελέγχου και κέρδους αλλά και εκβιασμούς κτλ. Δηλαδή, το άτομο αντιμετωπίζεται ως εν δυνάμει ύποπτος και για το λόγο αυτό συλλέγονται διάφορες πληροφορίες που το αφορούν, ακόμα και οι ευαίσθητες. Κεντρικό ρόλο στην παρακολούθηση κατέχει η ταξινόμηση – κοινωνική κατηγοριοποίηση των ατόμων βάσει κριτηρίων (social sorting). Έτσι οι νέες τεχνολογίες χρησιμοποιούνται ως μέσο τόσο από το κράτος όσο και από την αγορά για τον εντοπισμό, την εκτίμηση και την αξιολόγηση κάθε είδους δυνητικών κινδύνων με απώτερο στόχο την ελαχιστοποίηση ή ακόμη και την εξάλειψη τους (Lyon, 2001: 46 – 47).

Χαρακτηριστικό είναι το παράδειγμα των πολιτικών ασφαλείας και παρακολούθησης που ακολουθήθηκαν ιδιαίτερα μετά την 11η Σεπτεμβρίου 2001 όπου επιδεινώθηκαν τα προβλήματα που σχετίζονται με τη συλλογή, αποθήκευση, επεξεργασία και ανταλλαγή των προσωπικών δεδομένων λόγω της αντιτρομοκρατικής νομοθεσίας στις ΗΠΑ, αλλά και στην ΕΕ. Έτσι, η συλλογή και επεξεργασία προσωπικών δεδομένων χωρίς τη συγκατάθεση των ατόμων νομιμοποιείται παντού για λόγους ασφάλειας (Lyon, 2001).

Συνοπτικά, στο πλαίσιο του Πληροφοριακού Καπιταλισμού και της Κοινωνίας των Δικτύων, δημιουργούνται προβλήματα και νέες προκλήσεις για την προστασία των δικαιωμάτων του ατόμου, την ιδιωτικότητα και τις πολιτικές ελευθερίες διότι ιδιαίτερα μετά την 11η Σεπτεμβρίου επικρατεί το λεγόμενο «πρόταγμα της ασφάλειας» (Lyon, 2003).

### 1.5: Οι απόψεις των K. Haggerty και R. Ericson: Από το «πανοπτικό» στο «ψηφιδωτό» της παρακολούθησης

Το φαινόμενο της επιτήρησης και παρακολούθησης σχετίζεται με την πειθαρχική εξουσία, με βάση την ανάλυση του Φουκώ. Το «πανοπτικό», ένα μοντέλο φυλακής βασικός εμπνευστής του όποιου ήταν ο Jeremy Bentham, χρησιμοποιήθηκε και αναλύθηκε από τον Michael Foucault στο έργο του «Πειθαρχία και τιμωρία: Η

γένεση της φυλακής». Το κτίριο της φυλακής έχει κυκλικό σχήμα. Στο κέντρο του υπάρχει ο πύργος ελέγχου γύρω από τον οποίο είναι κτισμένα τα κελιά των κρατουμένων με παράθυρα που βλέπουν προς το κέντρο, δηλαδή τον πύργο ελέγχου. Οι κρατούμενοι αισθάνονται ότι παρακολουθούνται διαρκώς τόσο συλλογικά όσο και ατομικά από κάποιον παρατηρητή, ο οποίος βρίσκεται στον πύργο ελέγχου χωρίς όμως να φαίνεται από αυτούς. Διότι, ο πύργος ελέγχου διαθέτει μόνωση αλλά και ειδικά στόρια ώστε να μην βγαίνει προς τα έξω είτε φως είτε ήχος που να προδίδει την παρουσία του παρατηρητή. Η ουσία λοιπόν του «πανοπτικού» δεν είναι άλλη από την εσωτερίκευση του πανοπτικού ελέγχου από τα υποκείμενα. Δηλαδή, η όλη αρχιτεκτονική της φυλακής υποβάλλει στους κρατούμενους την αίσθηση του συνεχούς πανοπτικού ελέγχου είκοσι τέσσερις ώρες του εικοσιτετράωρο άσχετα με το αν αυτό πράγματι συμβαίνει. Τους αναγκάζει δηλαδή να συμπεριφέρονται σύμφωνα με τους κανόνες της φυλακής, να πειθαρχούν φοβούμενοι τις συνέπειες με αποτέλεσμα αποδέχονται τον έλεγχο και την πειθαρχική εξουσία. Δηλαδή η άσκηση κοινωνικού ελέγχου επιφέρει την υιοθέτηση κοινωνικά αποδεκτών κανόνων και συμπεριφορών. Έτσι το πανοπτικό λειτουργεί ως πολλαπλασιαστής της εξουσίας στα πλαίσια οποιουδήποτε θεσμού.

Σύμφωνα όμως με τον Giddens (1987), η εφαρμογή της πειθαρχικής εξουσίας του πανοπτικού δεν μπορεί να γενικευτεί σε όλους τους θεσμούς καθώς υπάρχουν θεσμοί στους οποίους τα άτομα μετέχουν οικειοθελώς, δεν είναι έγκλειστοι. Έτσι γι' αυτόν κεντρικής σημασίας είναι η δημιουργία νέων σχέσεων εξουσίας στα πλαίσια μιας πειθαρχικής κοινωνίας. Μάλιστα στο πλαίσιο των σχέσεων αυτών, μία μετεξέλιξη του πανοπτικού αποτελεί ο συνοπτισμός, δηλαδή η κατάσταση στην οποία οι πολλοί παρακολουθούν τους λίγους (Mathieson, 1997: 217).

Οι Haggerty και Ericson θεωρούν ότι πλέον το «πανοπτικό» είναι ένα απαρχαιωμένο ιεραρχικό μοντέλο παρακολούθησης από πάνω προς τα κάτω, αφού αναφέρεται καθαρά στην άνιση σχέση φύλακα και φυλακισμένου, παρατηρητή και παρακολουθούμενου στο πλαίσιο της πειθαρχικής εξουσίας και κοινωνίας. Το «πανοπτικό» έχει εξελιχθεί σε «ψηφιδωτό» της παρακολούθησης που είναι η σκόπιμη συλλογή, επεξεργασία και σύνθεση διαφόρων πληροφοριών από διάφορες δραστηριότητες του ατόμου, με απώτερο σκοπό της δημιουργία προφίλ. Βασική του διαφορά με το «πανοπτικό» αποτελεί το γεγονός ότι δεν αφορά την οπτική παρακολούθηση αλλά τη συλλογή και επεξεργασία και σύνθεση – συναρμολόγηση δεδομένων βάσει των ψηφιακών ιχνών που συλλέγονται από διάφορες πηγές.

Δηλαδή, βασικό χαρακτηριστικό της σύγχρονης παρακολούθησης αποτελεί η χρήση πρακτικών και τεχνολογιών παρακολούθησης για τη δημιουργία του πληροφοριακού προφίλ.

Οι Haggerty και Ericson, θεωρούν ότι είμαστε μάρτυρες μιας σύγκλισης αυτών που κάποτε ήταν συστήματα διακριτικής παρακολούθησης ώστε πλέον να μπορούμε να κάνουμε λόγο για ένα αναδυόμενο «ψηφιδωτό παρακολούθησης» ή συναρμολόγημα (surveillance assemblage) π.χ. στην περίπτωση του ανθρώπινου σώματος χωρίζοντάς το σε μία σειρά διακριτικών ροών, επανασυγκροτείται σε ευδιάκριτες συνθέσεις δεδομένων που μπορούν να εξεταστούν προσεκτικά και να επεξεργαστούν (Haggerty, K. & Ericson, R., 2000: 606).

Σύμφωνα με τον Patton, τα «ψηφιδωτά» αυτά αποτελούνται από μία πολυπλοκότητα ετερογενών πληροφοριών, των οποίων η ενότητα προκύπτει αποκλειστικά και μόνο από το γεγονός ότι λειτουργούν ως μία συνθετική οντότητα. Κάθε ψηφιδωτό αυτό καθαυτό απαρτίζεται από διαφορετικά διακριτικά προφίλ που λειτουργούν ως πληροφοριακοί σωσίες (data doubles) (Haggerty, K. & Ericson, R., 2000: 608; Patton, 1994: 158).

Αν στο «ψηφιδωτό» προστεθεί η δυνατότητα συσχέτισης των προσωπικών δεδομένων σε ταχύτατο χρονικό διάστημα, μπορούν να κατασκευαστούν προφίλ των υπό παρακολούθηση ατόμων και ταξινομούνται ανάλογα (categorical suspects) με ότι αυτό συνεπάγεται, δηλαδή αποκλεισμό, διακρίσεις κτλ. Έτσι από την πανοπτική, πειθαρχική εξουσία έχουμε περάσει σε νέες μορφές παρακολούθησης που επεκτείνονται σε κάθε ανθρώπινη λειτουργία και δράση (π.χ. σεξουαλικότητα, υγεία, κατανάλωση, κτλ) όπως οι ρίζες και τα αναρριχητικά φυτά, καταργώντας κάθε ιδιωτικότητα.

### 1.6: <u>Το δικαίωμα στην ιδιωτικότητα, η παραβίαση και το τέλος αυτής</u>

Σύμφωνα με τη βιβλιογραφική ανασκόπηση που διεξήχθη από τον Ken Gormley, η ιδιωτικότητα μπορεί να κατανοηθεί ως: α) «έκφραση της προσωπικότητας κάποιου εστιάζοντας στο δικαίωμα του ατόμου να ορίζει την ουσία του ως ανθρώπινο ων», β) «αυτονομία», γ) «η ικανότητα του ατόμου να καθορίζει τις πληροφορίες που το αφορούν και τον έλεγχο των σχέσεων του με τους άλλους ανθρώπους», και δ) το δικαίωμα του ατόμου στη «μυστικότητα, την ανωνυμία και τη μοναχικότητα». Παρόλα αυτά οι παραπάνω ορισμοί δεν μπορούν να καλύψουν όλο

το εύρος της ιδιωτικότητας όπως π.χ. ο δικαίωμα του ατόμου να αποκλείει άλλους από την εισβολή στο φυσικό του χώρο αλλά και τον αγώνα για έλεγχο ανάμεσα στο άτομο και την κοινωνία (Gormley, 1997: 19 – 20).

Η έννοια της ιδιωτικότητας[6] αναφέρεται επίσης σε μία ανθρώπινη αξία που αποτελείται: α) από το δικαίωμα στη μοναχικότητα, δηλαδή στο δικαίωμα του ατόμου να παραμένει μόνο, χωρίς να παρενοχλείται από κάτι, β) την ανωνυμία δηλαδή στο δικαίωμα του να παραμένει ανώνυμο ανάμεσα στο ευρύ κοινό και σε δημόσιους χώρους, γ) τις ιδιωτικές σχέσεις δηλαδή στο δικαίωμα του να κάνει κάτι ιδιωτικά – όχι δημόσια και δ) το δικαίωμα στο να τηρεί επιφυλάξεις, να ελέγχει δηλαδή τις προσωπικές του πληροφορίες καθώς επίσης και τις μεθόδους διάδοσης τους, δηλαδή τον «πληροφοριακό αυτοκαθορισμό»[7].

Έτσι, τα προβλήματα που δημιουργούνται από τη χρήση των νέων τεχνολογιών αναφορικά με την ιδιωτικότητα και την προστασία της αφορούν α) την ιδιωτικότητα σε σχέση με το χώρο, δηλαδή τον περιορισμό της εισβολής στο χώρο του σπιτιού, της εργασίας, στους δημόσιους χώρους, κτλ, β) την ιδιωτικότητα αναφορικά με τη δυνατότητα εντοπισμού της θέσης του ατόμου μέσω της τεχνολογίας του Global Position System (GPS) και των δορυφορικών συστημάτων, γ) την ιδιωτικότητα αναφορικά με το ανθρώπινο σώμα, καθώς πρέπει να υπάρχει σεβασμός ως προς την ακεραιότητά του και χρήσης βιομετρικών και γενετικών δεδομένων, δ) την προσωπική ιδιωτικότητα που αναφέρεται στην προστασία του ατόμου έναντι π.χ. σωματικών ελέγχων και της συλλογής προσωπικών πληροφοριών, ε) την ιδιωτικότητα στις επικοινωνίες και στ) την ιδιωτικότητα αναφορικά με τις προσωπικές μας προτιμήσεις, ιδέες και σχέσεις με άλλους (Westin, 1997).

Συνεπώς η ιδιωτικότητα είναι αυτή που καθορίζει την ελευθερία του ατόμου και αναγνωρίζει τον προσωπικό χώρο όπου κάποιος να μπορεί να δρα και να μοιράζεται με τους άλλους. Έτσι, η ιδιωτικότητα εξισούται με την ελευθερία του ανθρώπου, πράγμα που σημαίνει ότι οφείλουμε να την περιφρουρούμε από τη χρήση των νέων τεχνολογιών.

Το ερώτημα που προκύπτει σήμερα είναι πότε, πως και ποιες πληροφορίες, και ιδιαίτερα οι ευαίσθητες, πρέπει να προστατεύονται από την ευρεία χρήση

[6] Σύμφωνα με τον Westin «κάθε άτομο πρέπει, μέσα στο ευρύτερο πλαίσιο της κουλτούρας του, την κοινωνική θέση και την προσωπική του κατάσταση, να προσαρμόζεται διαρκώς ανάμεσα στην ανάγκη για μοναχικότητα και συντροφικότητα, για στενή σχέση και γενική κοινωνική επαφή, για ανωνυμία και υπεύθυνη συμμετοχή στην κοινωνία, για επιφύλαξη και αποκάλυψη» (Westin, 1997: 31).
[7] Η έννοια του πληροφοριακού αυτοκαθορισμού αναλύεται παρακάτω, σ. 61.

συστημάτων παρακολούθησης όπως οι βάσεις δεδομένων, οι ψηφιακές κάμερες, τα CCTV, το διαδίκτυο, κτλ. Έτσι σύμφωνα με τον Χαλαζωνίτη (1995: 303 - 318), ευαίσθητα προσωπικά δεδομένα θεωρούνται όλα τα δεδομένα και οι πληροφορίες που «ενδιαφέρουν τους τρίτους και αυτός-ή που τον-την αφορούν δεν επιθυμεί την κοινοποίηση τους». Συγκεκριμένα, ως ευαίσθητα προσωπικά δεδομένα θεωρούνται αυτά που αφορούν «ζητήματα υγείας, κοινωνικής πρόνοιας, φυλετικής και εθνικής προέλευσης, ερωτικής ζωής, πολιτικά φρονήματα, θρησκευτικές και φιλοσοφικές πεποιθήσεις, συμμετοχή σε συνδικαλιστικές οργανώσεις, ποινικές διώξεις ή καταδίκες, γενετικά και ιατρικά δεδομένα, δηλώσεις για τα στοιχεία του αιτούντος άσυλο, τα δεδομένα των ληπτών και δωρητών οργάνων και ιστών κτλ»[8].

Τα παραπάνω τεχνολογικά μέσα παρακολούθησης έχουν σαν στόχο τη συλλογή διαφόρων ευαίσθητων προσωπικών δεδομένων, από τα αρχεία τραπεζικών συναλλαγών, αρχεία με ιατρικά ιστορικά, αρχεία του στρατού και της αστυνομίας, ασφάλισης, λογαριασμών τηλεφωνημάτων, κρατήσεις σε αεροπορικές εταιρείες, θεωρήσεις και εκδόσεις διαβατηρίων, κινήσεις πιστωτικών καρτών, κά.

Όμως συχνά τα προσωπικά μας δεδομένα συλλέγονται χωρίς τη συγκατάθεση μας, ενώ πολλές φορές εκούσια ή αναγκαστικά διαβιβάζονται εκχωρώντας ανεκτίμητες πληροφορίες σε εταιρείες για σκοπούς μάρκετινγκ αλλά και σε κυβερνητικές υπηρεσίες. Σύμφωνα μάλιστα με τον Stamatellos, στην κοινωνία της πληροφορίας και της παρακολούθησης όπου το μόνο που έχει αξία είναι η πληροφορία, οι άνθρωποι αντιμετωπίζονται περισσότερο σαν ένα σύνολο πληροφοριών παρά σαν ανθρώπινα όντα (Stamatellos, xx: 25-26). Επειδή η ιδιωτικότητα και η προστασία των προσωπικών δεδομένων από τα υποκείμενα ποικίλει και θεωρείται προσωπικό ζήτημα, οι κοινωνιολόγοι σε αντίθεση με τους νομικούς, εξετάζουν την παρακολούθηση, δηλαδή τα κίνητρα και τις συνέπειες αυτών που συλλέγουν και εκμεταλλεύονται τα προσωπικά δεδομένα (Lyon, 2003).

[8] Ο διαχωρισμός των εννοιών «προσωπικά δεδομένα» και «ευαίσθητα προσωπικά δεδομένα» εξαρτάται από το πολιτιστικό και κοινωνικό πλαίσιο στο οποίο αναφέρονται. Στη χώρα μας, δεδομένου του προηγούμενου αυταρχικού κράτους στην περίοδο της Χούντας, ευαίσθητα θεωρούνται τα δεδομένα που αφορούν αποκλειστικά την ιδιωτική ζωή του ατόμου αλλά και τα πολιτικά φρονήματα (Σαματάς, 2005).

### 1.7: Η νέα ηλεκτρονική παρακολούθηση

Σύμφωνα με τον Gary Marx (2002), την πρόσωπο με πρόσωπο παρακολούθηση έχει διαδεχθεί η αποκαλούμενη «νέα παρακολούθηση» βασικό χαρακτηριστικό της οποίας αποτελεί η ευρεία χρήση των νέων τεχνολογιών. Δηλαδή, η νέα παρακολούθηση διεξάγεται με τη συλλογή και επεξεργασία μεγάλης ποσότητας δεδομένων (π.χ. βιομετρικά δεδομένα, χρήση του διαδικτύου, των ΑΤΜ κτλ) σε ταχύτατο χρόνο, αυτόματα και από απόσταση. Τα δεδομένα αυτά συλλέγονται, επεξεργάζονται και μεταδίδονται σε τεράστιες βάσεις δεδομένων και χρησιμοποιούνται τόσο από το κράτος όσο και από ιδιώτες για διάφορους σκοπούς όπως π.χ. η δημιουργία προφίλ, η κοινωνική κατηγοριοποίηση – ταξινόμηση (social sorting) που μπορεί να οδηγήσουν στη δημιουργία νέων διακρίσεων και αποκλεισμών (Lyon, 2003: 13 – 14).

Καθημερινά γινόμαστε αντικείμενο παρακολούθησης κυρίως με τη χρήση των τεχνολογιών, χωρίς αυτό να σημαίνει ότι τα τεχνολογικά συστήματα είναι εξ αρχής «καλά» ή «κακά». Αυτό εξαρτάται από τη χρήση τους. Ο συνηθέστερος λόγος παρακολούθησης είναι η άσκηση ελέγχου ή επιρροής σε όλα τα κοινωνικά επίπεδα – από μέρους του κράτους, της αγοράς κτλ – με τη βοήθεια των νέων τεχνολογιών (Ρόμπινς & Ουέμπστερ, 2002: 20; Hall et al., 2003).

Παλαιότερα το κράτος ασκούσε καταπιεστικές μορφές αστυνόμευσης και παρακολούθησης με βάση πληροφοριοδότες και οπτική παρακολούθηση. Σήμερα αναπτύσσονται σταδιακά νέες ήπιες μορφές άσκησης ελέγχου, όπως: α) η αναζήτηση εθελοντών επικαλούμενοι την ιδιότητα του πολίτη και τον πατριωτισμό, π.χ. με το πρόγραμμα "Watch your car" όπου οι ιδιοκτήτες των αυτοκινήτων τοποθετούν μία ηλεκτρονική συσκευή στο αυτοκίνητο τους που επιτρέπει στην αστυνομία σε κάθε περιοχή των ΗΠΑ να σταματήσουν το αυτοκίνητο αν κυκλοφορεί όταν η ώρα είναι περασμένη, β) η τοποθέτηση καμερών στα ταξί δίνοντας τη δυνατότητα στην αστυνομία να τα ελέγχει επεκτείνοντας τον έλεγχο και στους επιβάτες, γ) η χρήση πινακίδων με την ένδειξη ότι «με την είσοδο σας δίνετε τη συγκατάθεση σας να υποβληθείτε σε έλεγχο», δ) το εμπόριο προσωπικών πληροφοριών με ανταμοιβή και ευκολίες στον ιδιωτικό τομέα και ε) η χρήση κρυφών ή περιορισμένης ορατότητας τεχνολογιών για τη συλλογή πληροφοριών, κτλ (Marx, 2005).

Οι συνηθέστερες τεχνολογίες παρακολούθησης είναι οι τηλεπικοινωνίες[9], τα συστήματα βιντεοπαρακολούθησης, οι βάσεις δεδομένων, τα βιομετρικά δεδομένα αλλά και οι τεχνολογίες εντοπισμού, παρακολούθησης και κατηγοριοποίησης. Στις μέρες μας η χρήση καμερών κλειστού κυκλώματος παρακολούθησης (CCTV) είναι ιδιαίτερα διαδεδομένη. Τέτοια κυκλώματα είναι εγκατεστημένα σχεδόν σε όλα τα δημόσια κτήρια, σε τράπεζες, σε καταστήματα, κτλ προς αποφυγή της εγκληματικότητας και της τρομοκρατίας καταγράφοντας κάθε περαστικό αλλά και συγκρίνοντας τις εικόνες με άλλες σε τράπεζες δεδομένων.

Η χρήση υπολογιστών και οι τράπεζες δεδομένων (data bases) έχουν συμβάλλει στην πιο χαρακτηριστική μορφή της νέας παρακολούθησης που είναι η «αρχειοπαρακολούθηση» που αποτελεί βασικό χαρακτηριστικό της «κοινωνίας της παρακολούθησης», η ύπαρξη της οποίας δικαιολογείται για λόγους αποτελεσματικότητας αφού χιλιάδες δεδομένα μπορούν από απόσταση να συλλεχθούν, να ταξινομηθούν και να συγκριθούν ταχύτατα και με μεγαλύτερη ακρίβεια. Ο όρος «αρχειοπαρακολούθηση» αναφέρεται στις πρακτικές παρακολούθησης δεδομένων. Εφαρμόζονται για τη συλλογή, αποθήκευση και επεξεργασία μεγάλης ποσότητας προσωπικών και άλλων δεδομένων και αποτελεί εξέλιξη της ορθολογικής γραφειοκρατικής οργάνωσης που ανέλυσε ο Βέμπερ. Οι συνηθέστερες μορφές αρχειοπαρακολούθησης είναι στο marketing, την ιατρική, την αστυνόμευση και τον έλεγχο των συνόρων (Clarke, 1997).

Η δυνατότητα της αρχειοπαρακολούθησης έχει εξελιχθεί με τη βοήθεια των νέων τεχνολογιών ώστε να αφορά όχι μόνο τη συλλογή και την αποθήκευση των πληροφοριών[10] των πολιτών αλλά και τη διασταύρωση διαφόρων δεδομένων (data matching) για σκοπούς ταυτοποίησης, δημιουργίας προφίλ ακόμα και της πρόβλεψης της συμπεριφοράς των ατόμων δημιουργώντας με τον τρόπο αυτό νέες κατηγοριοποιήσεις και τη δημιουργία ομάδων υπόπτων (categorical suspects), αποκλεισμούς αλλά και διακρίσεις ή ακόμη και προκαταλήψεις. Σχεδόν όλα τα συστήματα που χρησιμοποιούν προσωπικά δεδομένα μπορούν να ευνοήσουν και να αποκλείσουν κάποιους, να μειώσουν τις ευκαιρίες ζωής τους ή ακόμη και να τους

[9] Η παρακολούθηση στον τομέα των τηλεπικοινωνιών αφορά το βαθμό που άτομα, οργανισμοί και δίκτυα μπορούν να καταγράφουν, να συλλέγουν και να αποθηκεύουν πληροφορίες για τις κλήσεις και το περιεχόμενο της τηλεπικοινωνιακής συναλλαγής τόσο ανάμεσα σε τεχνολογικές συσκευές όσο και ανάμεσα σε ανθρώπους και συσκευές.

[10] Υπάρχει επιπλέον η δυνατότητα πρόσβασης και σύγκρισης μέσω των νέων τεχνολογιών για σκοπούς μάρκετινγκ, βιογενετικής αλλά και καταναλωτικής παρακολούθησης προσωπικών δεδομένων που αφορούν φορολογικά θέματα, ιατρικά αλλά και θέματα ασφάλισης (Κριάρη – Κατράνη, 1999).

αποκλείσουν από την κοινωνική και πολιτική συμμετοχή. Με τον τρόπο αυτό παραβιάζεται η ιδιωτικότητα του ατόμου ενώ ταυτόχρονα χειραγωγείται η συμπεριφορά του σε βάρος της αυτονομίας, της αυτοδιάθεσης και του αυτοκαθορισμού του (Lyon, 1994, 2001, 2007: 180 – 184; Marx, 2002; Σαματάς, 2005: 489 – 491, 499).

Η αρχειοπαρακολούθηση διακρίνεται σε: α) προσωπική που περιλαμβάνει την ανάλυση των προσωπικών αρχείων ατόμων που έχουν τραβήξει την προσοχή για κάποιο λόγο προγενέστερα, και μαζική που στοχεύει στη δημιουργία ομάδων με προοπτική την εύρεση εκείνων που αξίζει να αποτελέσουν αντικείμενο της ατομικής αρχειοπαρακολούθησης (categorical seduction), β) σε εσωτερική, η οποία διεξάγεται εντός ενός συστήματος προσωπικών δεδομένων και εξωτερική, η οποία υφίσταται π.χ. όταν η σχέση ενός ατόμου με έναν οργανισμό βρίσκεται σε άμεση σχέση με κάποιο άλλο οργανισμό, όπως π.χ. είναι τα δεδομένα εργασίας των υπαλλήλων που τηρούνται τόσο από τους εργοδότες όσο και από τους ασφαλιστικούς φορείς, γ) προγενέστερη και ύστερη που αφορά δεδομένα που τηρούνται π.χ. πριν και μετά από τη λήψη επιδόματος ασθενείας, όπως η κατάσταση της υγείας, δ) μονοπαραγοντική όταν αφορά μόνο έναν παράγοντα όπως π.χ. η αίτηση για αναπηρική σύνταξη και πολυπαραγοντική και τέλος, ε) θετική, όταν η διασταύρωση των δεδομένων γίνεται π.χ. για να βρεθεί ποια άτομα είναι κατάλληλα για να συμμετάσχουν σε κρατικά προγράμματα (π.χ. επιδόματα), και αρνητική η οποία αναφέρεται στις αρνητικές επιπτώσεις που μπορεί να έχει για το άτομο, με την έννοια ότι μπορεί να έχουν καταγραφεί ανακριβή και ελλιπή δεδομένα με αποτέλεσμα την απόρριψη αιτήματος για καταβολή επιδόματος, σε άδικες συλλήψεις κτλ. Μέσω αυτής διακινδυνεύονται αρκετά ατομικά δικαιώματα και ελευθερίες καθώς μπορεί να οδηγήσει στη δημιουργία διακρίσεων έναντι συγκεκριμένων κατηγοριών ανθρώπων (Lyon, 1996: 237 - 246).

Ανάλογη λειτουργία επιτελούν και τα συστήματα ταυτοποίησης που χρησιμοποιούν βιομετρικά δεδομένα τόσο σε διαβατήρια, όσο και σε ταυτότητες αφού θεωρείται ότι το ανθρώπινο σώμα παρέχει μεγαλύτερη ακρίβεια εξαιτίας του γεγονότος ότι αποτελεί ένα μόνιμο και άμεσο σύνδεσμο ανάμεσα στο αρχείο και στο πρόσωπο στο οποίο αναφέρεται.

Έχοντας σαν εφαλτήριο τα γεγονότα της 11$^{ης}$ Σεπτεμβρίου διευρύνθηκε η χρήση των βάσεων προσωπικών δεδομένων με στόχο την ταυτοποίηση υπόπτων και ομάδων υπόπτων (categorical suspects). Οι πληροφορίες σε αυτές τις βάσεις

δεδομένων αναλύονται και κατηγοριοποιούνται από τα δυτικά κράτη προκειμένου να εντοπιστούν και να οριστούν ομάδες κινδύνου, όπως π.χ. των Μουσουλμάνων προκαλώντας διακρίσεις, ακόμα και συλλήψεις ως ύποπτων τρομοκρατίας με αποτέλεσμα να ευνοείται η δημιουργία αντιτρομοκρατικής πολιτικής χωρίς σεβασμό στα ανθρώπινα δικαιώματα και στις πολιτικές ελευθερίες (Ball & Murakami, 2006; 3 – 4; Lyon, 2003: 60 – 61).

Ιδίως μετά τα γεγονότα της 11ης Σεπτεμβρίου στις ΗΠΑ υπάρχουν ειδικές μονάδες πολιτών που συνεργάζονται με την αστυνομία, οι αποκαλούμενες C.A.T. EYES (Community Anti – Terrorism Training Initiative) ενώ αναπτύχθηκαν και προγράμματα που ενθαρρύνουν τους οδηγούς φορτηγών, τους εργαζόμενους στην καθαριότητα, τους οδηγούς ταξί και τους διανομείς να αναφέρουν κάθε ύποπτη δραστηριότητα. Στην κοινωνία του φόβου και της καχυποψίας καθένας δικαιούται και πρέπει να είναι ενήμερος, συνεργάτης με τις αρχές. Η υποκλοπή στα κινητά τηλέφωνα, σε οχήματα, σε πιστωτικές κάρτες ειδικών RFID chip (Radio Frequency Identification) τα οποία μπορούν να «διαβαστούν» από 30 πόδια μακριά μέσω αόρατων αισθητήρων νομιμοποιείται (Marx, 2005).

Συνοπτικά η νέα παρακολούθηση περιλαμβάνει όχι μόνο φυσική κατόπτευση αλλά και μέσω των νέων τεχνολογιών ηλεκτρονική συλλογή, επεξεργασία και μετάδοση δεδομένων, αρχειοπαρακολούθηση, σύγκριση δεδομένων, κατασκευή προφίλ, αλλά και κοινωνική κατηγοριοποίηση και ταξινόμηση με διάφορα κριτήρια. Έτσι η κοινωνία μας καθίσταται «διάφανη», μια κοινωνία όπου οι πάντες πρέπει να γνωρίζουν τα πάντα. Η παρακολούθηση υπερβαίνει το ανθρώπινο σώμα καθιστώντας το πηγή άντλησης δεδομένων. Εισχωρεί δηλαδή στην ιδιωτικότητα του ατόμου με τη συλλογή και επεξεργασία τόσο των προσωπικών όσο και των ευαίσθητων προσωπικών πληροφοριών του ατόμου (Marx, 1998: 172).

### 1.8: <u>Συμπερασματικές παρατηρήσεις</u>

Έπειτα από την ανασκόπηση των παραπάνω κοινωνιολογικών προσεγγίσεων του φαινομένου της παρακολούθησης συμπεραίνουμε ότι ζούμε σε «κοινωνίες παρακολούθησης» όπου η επιτήρηση – παρακολούθηση με τη χρήση των νέων τεχνολογιών αποτελεί καθημερινή πραγματικότητα.

Με τη δημιουργία των εθνών – κρατών δημιουργήθηκε η ανάγκη συστηματικής συλλογής και επεξεργασίας των προσωπικών πληροφοριών για

διοικητικούς, εξουσιαστικούς αλλά και δημοσιονομικούς σκοπούς. Στην ύστερη νεωτερικότητα υπάρχει πλέον μετάβαση από το στάδιο παραγωγής υλικών αγαθών στην κοινωνία ης πληροφορίας και του Πληροφοριακού Καπιταλισμού (Informational Capitalism) όπου η πληροφορία κατέχει κεντρικό ρόλο. Με άλλα λόγια περάσαμε από τη βιομηχανική κοινωνία στη μεταβιομηχανική «δικτυακή κοινωνία» όπου η πληροφορία αποτελεί ταυτόχρονα την πρώτη ύλη αλλά και το εμπόρευμα (Καστέλς, 2005; Giddens, 2001).

Ταυτόχρονα η «Κοινωνία των Πληροφοριών» είναι και «Κοινωνία της Παρακολούθησης», με τη χρήση των νέων τεχνολογιών για διάφορους σκοπούς ασφάλειας, ελέγχου, φροντίδας, κέρδους, κτλ. Η όλη οργάνωση της σύγχρονης κοινωνίας βασίζεται στη χρήση των νέων τεχνολογιών για τη συλλογή και την επεξεργασία των πληροφοριών. Οι νέες ψηφιακές τεχνολογίες από απόσταση, με ταχύτητα και ευελιξία συντελούν στην παγκοσμιοποίηση της οικονομίας, στο πέρασμα από τις συγκεντρωτικές μεγάλες επιχειρήσεις στα αποκεντρωμένα δίκτυα κτλ. Απόρροια αυτών αποτελεί η εξέλιξη της παρακολούθησης ως διαδικασία συλλογής και επεξεργασίας δεδομένων με την επέκταση της σχεδόν σε όλες τις δραστηριότητες της καθημερινής ζωής. Στη διαδικασία αυτή οι προσωπικές πληροφορίες αποτελούν πολύτιμα αλλά εμπορεύσιμα αγαθά και ιδιαίτερα όταν αυτές είναι ευαίσθητες (Lyon, 2001). Συλλέγονται δηλαδή προσωπικά δεδομένα από διάφορες καθημερινές δραστηριότητες τα οποία με τη βοήθεια των νέων τεχνολογιών μπορεί να κατηγοριοποιηθούν, να συγκριθούν, να συσχετιστούν και να οδηγήσουν στη δημιουργία προφίλ (ψηφιδωτό παρακολούθησης). Αυτό έχει ως αποτέλεσμα την ένταξη ή τον αποκλεισμό του ατόμου, τη δημιουργία διακρίσεων και τη συρρίκνωση του ιδιωτικού χώρου, ιδιαίτερα με βάση το πρόταγμα της ασφάλειας μετά τα γεγονότα της 11$^{ης}$ Σεπτεμβρίου, όπου η ασφάλεια υπερτερεί των ατομικών και των θεμελιωδών ελευθεριών. Ταυτόχρονα παρατηρείται το παράδοξο της ιδιωτικότητας όπου το άτομο πρέπει να προστατεύει το σκληρό πυρήνα της ιδιωτικότητας του, ενώ ταυτόχρονα είναι αναγκασμένο να εκχωρεί ολοένα και περισσότερες προσωπικές πληροφορίες για την παροχή βασικών υπηρεσιών (Giddens, 2001).

Θεωρούμε ότι οι απόψεις των κοινωνιολόγων που αναφέραμε και ιδιαίτερα αυτές των Haggerty και Ericson αλλά και του Lyon μας βοηθούν ώστε να κατανοήσουμε τη λειτουργία της νέας παρακολούθησης και να ερμηνεύσουμε τις επιπτώσεις του γενικά, και τη σκοπιμότητα της συλλογής και επεξεργασίας των

ευαίσθητων προσωπικών δεδομένων ειδικότερα (μείωση των ευκαιριών ζωής, τη δημιουργία διακρίσεων, ένταξη ή αποκλεισμό).

Η συμβολή των νέων τεχνολογιών δεν αξιολογείται «τεχνοκεντρικά», με βάση δηλαδή τον «τεχνολογικό ντετερμινισμό» αλλά ιστορικά, κοινωνικά και πολιτισμικά (Ρόμπινς & Ουέμπστερ, 2002). Η νέα παρακολούθηση μέσω των νέων τεχνολογιών κατανοείται ως βασικός μηχανισμός ανασυγκρότησης του κράτους και της παγκοσμιοποιημένης οικονομίας στο πλαίσιο του νεοφιλελευθερισμού και νεοσυντηρητισμού.

# ΚΕΦΑΛΑΙΟ 2$^{Ο}$
# ΟΙ ΝΕΕΣ ΤΕΧΝΟΛΟΓΙΕΣ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ ΚΑΙ ΠΑΡΑΒΙΑΣΗΣ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΚΑΙ ΤΩΝ ΕΥΑΙΣΘΗΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

## 2.1: Οι νέες τεχνολογίες παρακολούθησης

Οι βασικές μέθοδοι παραβίασης της ιδιωτικότητας είναι α) η αυθαίρετη εισβολή, η παράνομη δηλαδή είσοδος, κατοχή ή απόκτηση περιουσίας που ανήκει σε άλλον μέσω επέκτασης και παραβίασης της ιδιωτικότητας, β) η κακοδιαχείριση των πληροφοριών, δηλαδή η παράνομη χρήση πληροφοριών για μη εξουσιοδοτημένους σκοπούς, γ) η παρεμπόδιση πληροφοριών που αφορά τη μη εξουσιοδοτημένη πρόσβαση σε προσωπικές πληροφορίες π.χ. μέσω παρακολούθησης των επικοινωνιών, δ) το data matching (συσχέτιση δεδομένων) που αναφέρεται στο συνδυασμό, στη σύνδεση και τη σύγκριση δεδομένων από δύο ή περισσότερες βάσεις δεδομένων για την παραγωγή νέων πληροφοριών. Βασικός στόχος της διαδικασίας αυτής είναι η εξαγωγή στατιστικών πληροφοριών ή η δημιουργία προφίλ χρηστών Η/Υ, συνδυάζοντας διάφορα δεδομένα για χρήστες διαμορφώνοντας έτσι τις προτιμήσεις ή/και τις συμπεριφορές τους και ε) το data mining (ανάσυρση δεδομένων) που αναφέρεται στη συλλογή όγκου πληροφοριών ή εξειδικευμένων στοιχείων από μία ή περισσότερες βάσεις δεδομένων για την εξαγωγή νέων πληροφοριών και γνώσεων που ήταν κρυμμένες ή/και μη αναγνωρισμένες (Wel, L. & Royakkers, L., 2004).

Κοινό χαρακτηριστικό των παραπάνω κατηγοριών αποτελεί ο κεντρικός ρόλος των νέων τεχνολογιών, των βάσεων δεδομένων και των δικτύων γενικότερα και αυτό επειδή τα προσωπικά δεδομένα συλλέγονται και αποθηκεύονται σε βάσεις δεδομένων των υπολογιστών ενώ χρησιμοποιούνται δίκτυα για τη μεταφορά, την επεξεργασία και τη συγχώνευση των πληροφοριών αυτών (Stamatellos, xx: 29 – 30).

Ουσιαστικά όμως δεν είναι οι τεχνολογίες αυτές καθ' αυτές που ευθύνονται για τις αλλαγές που επέρχονται στην κοινωνία. Απλά αποτελούν το μέσο για την επίτευξη των κοινωνικών αλλαγών. Δεν αποτελούν έναν παράγοντα που είναι αδύνατο να παρεμποδιστεί και «επιφέρει μαζικές αλλαγές στις κοινωνικές διευθετήσεις» αλλά και κοινωνικούς μετασχηματισμούς (Ρόμπινς & Ουέμπστερ, 2002). Αντίθετα αποτελούν μέσο για την επίτευξη των κοινωνικών αλλαγών πίσω

από τις οποίες κρύβεται η ίδια η κοινωνία (Ball & Webster, 2003: 113). Έτσι, στο επίκεντρο των σκέψεων και του συλλογισμού μας πρέπει να βρίσκονται ερωτήματα όπως α) ποιες είναι οι συνθήκες, τα κίνητρα δημιουργίας των νέων αυτών τεχνολογιών, β) ποιος είναι ο σκοπός της δημιουργίας τους, γ) ποιοι είναι εκείνοι που τις δημιούργησαν, δ) ποιοι τις χρησιμοποιούν και για ποιο σκοπό, ε) ποιες είναι οι επιπτώσεις της χρήσης τους για τον άνθρωπο και την ιδιωτική του ζωή και στ) ποιος ωφελείται από τη χρήση τους και ποιος χάνει. Και όλα αυτά στο πλαίσιο του πληροφοριακού δικτυακού καπιταλισμού όπου οι νέες τεχνολογίες είναι στη διάθεση του κράτους και διεθνών οργανισμών όπως είναι για παράδειγμα το SIS, η Europol, η Interpol κτλ αλλά και της αγοράς με σκοπό τον έλεγχο, την εξουσία, τη φροντίδα, την ασφάλεια αλλά και το κέρδος. Παρατηρούμε λοιπόν ότι οι νέες αυτές τεχνολογίες εφαρμόσθηκαν έπειτα από τα γεγονότα της 11$^{ης}$ Σεπτεμβρίου και αποτελούν το μέσο για τη διατήρηση της ασφάλειας και της πάταξης της διεθνούς τρομοκρατίας (Καστέλς, 2005: 37 - 45; Lyon, 2003b)

Ακολουθεί λοιπόν μια συνοπτική παράθεση και εξέταση των τεχνολογιών και των μεθόδων παρακολούθησης των προσωπικών και των ευαίσθητων προσωπικών δεδομένων, ώστε να γίνουν αντιληπτοί οι κίνδυνοι που επιφέρουν για τα προσωπικά δεδομένα.

### 2.2: <u>Παρακολούθηση μέσω βάσεων δεδομένων</u>

Οι βάσεις δεδομένων στις μέρες μας είναι κεντρικής σημασίας αφού δίνουν τη δυνατότητα στους χρήστες να συλλέγουν, να κατηγοριοποιούν, να οργανώνουν, να επιδεικνύουν και να εκτυπώνουν πληροφορίες με ένα τρόπο γρήγορο και ευέλικτο. Τέτοιες βάσεις δεδομένων χρησιμοποιούνται από διάφορους φορείς με τους οποίους συναλλασσόμαστε καθημερινά όπως τα σούπερ μάρκετ, οι τράπεζες, τα νοσοκομεία, τα καταστήματα, οι επιχειρήσεις, οι εταιρείες κινητής τηλεφωνίας, οι ΟΤΑ κτλ. Μάλιστα υπάρχει η δυνατότητα διασύνδεσης των βάσεων αυτών δίνοντας μεγαλύτερη ευελιξία, επιτρέποντας τις συσχετίσεις μεταξύ αρχείων και καθιστώντας έτσι ευκολότερη την έκδοση και τη διατήρηση των δεδομένων στοχεύοντας πάντα στη δημιουργία του πληροφοριακού προφίλ, το οποίο θα χρησιμοποιηθεί για την επίτευξη στόχων όπως ο έλεγχος, η ασφάλεια, το κέρδος κτλ. Έτσι η λεγόμενη «αρχειοπαρακολούθηση» αποτελεί αναπόσπαστο μέρος της καθημερινότητας του ατόμου καθώς διεξάγεται σχεδόν σε κάθε δραστηριότητα του. Πλέον δεν

παρακολουθείται το ίδιο το άτομο ως φυσικό πρόσωπο αλλά τα δεδομένα του (Haggerty, K. & Ericson, R., 2000: 606).

Ένας από τους τομείς στους οποίους έχει αναπτυχθεί η πληροφορική είναι και αυτός της εργασίας όπου χρησιμοποιούνται ηλεκτρονικά αρχεία προσωπικού που περιλαμβάνουν τα ημερομίσθια των εργαζομένων, τα ένσημα, τις άδειες τους κτλ, συστήματα καταγραφής τηλεφωνικών κλήσεων, της χρήσης του διαδικτύου, της μετακίνησης των εργαζομένων μέσα στους χώρους της επιχείρησης κτλ (Ιγγλεζάκης, 2004). Αυτά χρησιμοποιούνται από την εκάστοτε επιχείρηση για τη δημιουργία των προϋποθέσεων άσκησης εντατικού ελέγχου επιτήρησης της συμπεριφοράς και της απόδοσης των εργαζόμενων προσβάλλοντας έτσι την προσωπικότητα τους και παραβιάζοντας την ιδιωτική τους σφαίρα.

Μέσω της χρήσης των βάσεων δεδομένων παρέχεται ευκολότερη πρόσβαση σε πληροφορίες ενώ υπάρχει δυνατότητα ταχύτατης διαβίβασης των δεδομένων ανεξάρτητα από το χώρο και το χρόνο, χωρίς όμως αυτό να σημαίνει ότι δεν υπάρχουν και μειονεκτήματα καθώς δίνεται η δυνατότητα επεξεργασίας των υπαρχουσών αλλά και νέων πληροφοριών ώστε να δημιουργούνται προφίλ υπόπτων για κοινωνικό αποκλεισμό και κοινωνικές διακρίσεις.

Χαρακτηριστικό είναι το παράδειγμα του διατραπεζικού συστήματος «ΤΕΙΡΕΣΙΑΣ» που λειτουργεί από το 1997 και περιέχει στοιχεία για τους πολίτες που έχουν οφειλές από ακάλυπτες επιταγές, απλήρωτες συναλλαγματικές, έχουν πτωχεύσει, έχει εκδοθεί εναντίον τους διαταγή πληρωμής ή πρόγραμμα πλειστηριασμού, τους έχει επιβληθεί κατάσχεση, υποσημείωση κτλ. Υπάρχει πιθανότητα να χρησιμοποιηθούν – δημοσιοποιηθούν αρνητικές για το άτομο πληροφορίες που θα αποτελέσουν τροχοπέδη για την οικονομική και κοινωνική ανάπτυξη του ατόμου αφού κατηγοριοποιούνται σε μαύρες και λευκές λίστες (Ιγγλεζάκης, 2004).

Όμως ποιοι είναι αυτοί που έχουν πρόσβαση στις πληροφορίες που τους αφορούν προσωπικά; Για την άσκηση ελέγχου αναφορικά με την προστασία των προσωπικών και των ευαίσθητων προσωπικών δεδομένων έχει δημιουργηθεί όπως αναφέρουμε και παρακάτω αναλυτικά η ΑΠΔΠΧ (www.dpa.gr; Κανονιστική πράξη 1/1999). Πολλές φορές γίνεται κατηγοριοποίηση των ατόμων – χρηστών βάσει διαφόρων κριτηρίων όπως π.χ. οι πολιτικές τους πεποιθήσεις, οι κοινωνικές και οικονομικές τους δραστηριότητες, οι συμπεριφορές τους, κτλ με αποτέλεσμα να απειλείται η ιδιωτικότητα τους και οι ευκαιρίες ζωής τους από α) τις μαύρες λίστες

στις οποίες έχουν ενταχθεί τα άτομα βάσει του ιστορικού τους, β) τις βάσεις δεδομένων εξαιτίας κακομεταχείρισης, αμέλειας ή τη μη διατήρησης - ενημέρωσης των υπαρχόντων δεδομένων και γ) από την παράνομη αντιγραφή και πώληση των προσωπικών δεδομένων, κτλ (Abelson & Lessig, 1998; Stamatellos, xx: 30 – 31).

Έτσι, όσον αφορά το διατραπεζικό σύστημα ΤΕΙΡΕΣΙΑΣ Α.Ε., για τους παραπάνω λόγους η ΑΠΔΠΧ ορίζει ότι η επεξεργασία των προσωπικών δεδομένων είναι «απολύτως αναγκαία» από τη στιγμή που ο σκοπός της επεξεργασίας είναι «η ελαχιστοποίηση των κινδύνων από τη σύναψη πιστωτικών συμβάσεων με αφερέγγυους πελάτες … για την προστασία της εμπορικής πίστης και την εξυγίανση των οικονομικών συναλλαγών». Όμως πρέπει να συλλέγονται και να επεξεργάζονται μόνο όσα δεδομένα είναι απαραίτητα για την επίτευξη του σκοπού αυτού ενώ τα υποκείμενα τους πρέπει να ενημερώνονται για οποιαδήποτε γνωστοποίηση ή διαβίβαση τους (Απόφαση 24/2004) [11].

### 2.3: <u>Η παρακολούθηση μέσω και μέσα στο διαδίκτυο (Internet)</u>

Το διαδίκτυο δίνει τη δυνατότητα στους χρήστες του να έχουν άμεση πρόσβαση σε προσωπικά δεδομένα και πληροφορίες. Αν και αρχικά δημιουργήθηκε για στρατιωτικούς σκοπούς κατέληξε να αλλάξει τον κόσμο μέσω της δικτύωσης μεταξύ των υπολογιστών (Καστέλς, 2005: 37 – 38, 47). Όμως σε πολλές ιστοσελίδες εγκυμονεί ο κίνδυνος συλλογής και διαβίβασης προσωπικών πληροφοριών σε άλλες πηγές και βάσεις δεδομένων χωρίς να το γνωρίζει ο χρήστης ή χωρίς τη συγκατάθεση του. Επιπλέον, χρησιμοποιούνται «cookies» τα οποία είναι αρχεία που αποστέλλονται από τους παροχείς υπηρεσιών διαδικτύου προς τον υπολογιστή του χρήστη και αποθηκεύονται στο σκληρό του δίσκο για τον προσδιορισμό της ταυτότητας του χρήστη, παρέχοντάς στο διακομιστή διάφορες πληροφορίες σχετικά με τις προτιμήσεις, τις δραστηριότητες και τις καταναλωτικές συνήθειες του χρήστη. Οι χρήστες δεν ενημερώνονται για την αποθήκευση των cookies στο σκληρό τους δίσκο με αποτέλεσμα η όλη αυτή διαδικασία να θεωρείται ως απειλή για την ιδιωτικότητα και την ελευθερία της επιλογής τους (Ιγγλεζάκης, 2002; Stamatellos, xx: 32).

Όμως τα προσωπικά αυτά δεδομένα μπορούν να χρησιμοποιηθούν και από άλλες ιστοσελίδες δημιουργώντας έτσι το προφίλ του χρήστη όπου βάσει της

[11] Η αρχή της αναλογικότητας και του σκοπού αναλύεται παρακάτω στις σ. 51 – 52.

συμπεριφοράς του κατηγοριοποιείται σε βάσεις δεδομένων και πολλές φορές αποστέλλεται σε αυτόν ανεπιθύμητη ηλεκτρονική αλληλογραφία παραβιάζοντας έτσι όχι μόνο την ιδιωτικότητα τους αλλά φτάνοντας και στα όρια της κακόβουλης παρενόχλησης και του ηλεκτρονικού εγκλήματος (Stamatellos, xx: 32).

Χαρακτηριστικό είναι το παράδειγμα του ηλεκτρονικού εμπορίου που πραγματοποιείται μέσω διαδικτύου το οποίο έχει αυξήσει τον αριθμό των προσωπικών πληροφοριών που συλλέγονται από επιχειρήσεις. Για την πραγματοποίηση των εμπορικών συναλλαγών μέσω του διαδικτύου απαραίτητη προϋπόθεση είναι η χρήση της ταυτότητας, εν προκειμένω της πληροφορικής μας ταυτότητας, η οποία αποτελείται από μία σειρά δεδομένων όπως το όνομα, ηλικία, τόπος γέννησης, επάγγελμα που διαμορφώνουν μία πλήρη εικόνα του ατόμου. Επιπλέον στοιχεία της μπορούν να αποτελέσουν το ποινικό μητρώο, η οικονομική κατάσταση, το ιατρικό ιστορικό κά. Κάποια από τα δεδομένα αυτά λειτουργούν ως φορείς ταυτοποίησης καθώς προσδιορίζουν την ταυτότητα του ατόμου χωρίς την παροχή όλων των πληροφοριών που την απαρτίζουν (Pato, 2003). Ο αριθμός της ταυτότητας, ο αριθμός φορολογικού μητρώου, ο αριθμός μητρώου ασφάλισης θεωρούνται φορείς αυθεντικοποίησης καθώς επιτρέπουν την πιστοποίηση της ταυτότητας του ατόμου κατά τις συναλλαγές του. Η επεξεργασία τους γίνεται σε ελάχιστο χρόνο με ελάχιστο κόστος με αποτέλεσμα να υπάρχει η δυνατότητα αποσύνδεσης μίας πληροφορίας από το αρχικό της πλαίσιο αναφοράς, της ανασύνθεσης και της συσχέτισης της με άλλες πληροφορίες με αποτέλεσμα να δημιουργηθεί εκ νέου μία άλλη πληροφορία που πιθανόν να εξυπηρετεί κάποιους σκοπούς (Γιαννούλη, 1988; Ιγγλεζάκης, 2004).

Κατά τη διάρκεια των on-line συναλλαγών, οι καταναλωτές αφήνουν πίσω τους ψηφιακά ίχνη αλλά και προσωπικά τους δεδομένα χωρίς να έχουν επίγνωση ότι αυτό συμβαίνει. Όμως οι επιχειρήσεις παρακολουθούν τις δραστηριότητες – αγορές των καταναλωτών με αποτέλεσμα οι προσωπικές τους πληροφορίες, από την πιο ασήμαντη μέχρι την πιο ευαίσθητη, να μην προστατεύονται επαρκώς ώστε να μπορούν να χρησιμοποιηθούν για λόγους marketing. Υπάρχουν όμως και εταιρείες που συλλέγουν προσωπικά δεδομένα των επισκεπτών μέσω της προσφοράς εξατομικευμένων υπηρεσιών όπως αναζητήσεις, δωρεάν e-mail κτλ, τα οποία στη συνέχεια πωλούν και διαβιβάζουν σε τρίτους χωρίς οι καταναλωτές να το γνωρίζουν και να έχουν δώσει τη συγκατάθεση τους. Τέτοιου είδους λοιπόν δραστηριότητες συλλογής προσωπικών δεδομένων είναι συνήθεις στην οικονομία της πληροφορίας.

Επίσης, οι διαφημιστές για τους σκοπούς του μάρκετινγκ, συλλέγουν κρυφά προσωπικές πληροφορίες των χρηστών του διαδικτύου για την αποτελεσματικότητα των διαφημιστικών μηνυμάτων αφού παρέχεται στοχευμένη διαφήμιση γεγονός ιδιαίτερα ενοχλητικό για την ιδιωτική ζωή του ατόμου αφού με τον τρόπο αυτό γίνεται προσπάθεια χειραγώγησης του. Κάτι ανάλογο συμβαίνει και με την πραγματοποίηση τραπεζικών συναλλαγών μέσω του διαδικτύου με κίνδυνο την υποκλοπή των προσωπικών δεδομένων έχει σαν απόρροια την κλοπή των χρημάτων των καταθετών (www.privacyinternational.org).

Υπάρχουν όμως κάποιοι γενικοί κίνδυνοι που προκύπτουν κατά τη χρήση του διαδικτύου όπως π.χ. οι απάτες, η κλοπή κωδικών, ηλεκτρονικών υπογραφών, πιστωτικών καρτών, οι καταχρηστικές χρεώσεις για προϊόντα που ποτέ δεν παραγγέλθηκαν, η παράνομη χρήση e-mail για δήθεν χρηματικές παροχές, η λήψη αυθαίρετων e-mails για δήθεν χρηματικές παροχές, η παιδική πορνογραφία, οι παράνομες και καταχρηστικές χρεώσεις, οι διαφημίσεις επικίνδυνων προϊόντων, η διακίνηση – πειρατεία λογισμικού, η διακίνηση πορνογραφικού υλικού, προβλήματα ηλεκτρονικού εμπορίου όπως η μη αποστολή προϊόντος, η μη επιστροφή χρημάτων, το ηλεκτρονικό έγκλημα κτλ (Καστανάς, 2004).

Μία άλλη μορφή παραβίασης των προσωπικών και των ευαίσθητων δεδομένων με τη χρήση των νέων τεχνολογιών και του διαδικτύου είναι το «hacking» δηλαδή η μη εξουσιοδοτημένη πρόσβαση στο σύστημα των υπολογιστών και στα αρχεία κάποιου, την κλοπή προσωπικών πληροφοριών, ακόμα και οικειοποίησης της ταυτότητας μας π.χ. με την παραγγελία πιστωτικών καρτών στο όνομα μας, την αγορά ή την ενοικίαση στο όνομα μας, αφήνοντας όλους τους λογαριασμούς και τους φόρους εισοδήματος στο όνομα μας για να τους πληρώσουμε, κτλ (Καστέλς, 2005: 69).

Το phising είναι μία μέθοδος εξαπάτησης των καταναλωτών ενός οργανισμού, συνήθως κερδοσκοπικού χαρακτήρα, και συνίσταται στην απατηλή υφαρπαγή εμπιστευτικών πληροφοριών των καταναλωτών, όπως προσωπικά ή ευαίσθητα δεδομένα, οικονομικά δεδομένα κτλ με σκοπό την παράνομη χρήση τους για την πρόκληση βλάβης ξένης περιουσίας ή της χρήσης τους προς ιδίον όφελος (Chou et al,; Ollmann, 2004; USA Department of Justice, 2004).

Τα παραπάνω προβλήματα δεν προήλθαν με την εμφάνιση του διαδικτύου. Αντίθετα υπήρχαν ανέκαθεν. Όμως με την εμφάνιση του διαδικτύου και την αλλαγή στον τρόπο επικοινωνίας επιδεινώθηκαν. Έτσι, καθένας μας οφείλει να αναρωτηθεί

και να προβληματιστεί για το σκοπό της συλλογής των προσωπικών μας δεδομένων στο διαδίκτυο, ποιος τα ζητά, ποιοι κρύβονται πίσω από τους παροχείς των υπηρεσιών αυτών, ποιοι έχουν πρόσβαση σε αυτά, που θα χρησιμοποιηθούν, αν είναι ασφαλής η χρήση του διαδικτύου και η γνωστοποίηση των δεδομένων μας για την παροχή δικτυακών υπηρεσιών, αν τελικά το διαδίκτυο είναι απλά ένα πεδίο ελεύθερης επικοινωνίας ή ένα απλό, προσιτό και «αθώο» μέσο παρακολούθησης μας;

### 2.4: Βιντεο – παρακολούθηση με Κλειστά Κυκλώματα Τηλεόρασης (CCTV)

Η βιντεο – παρακολούθηση είναι η πιο συχνή μέθοδος παρακολούθησης αφού σχεδόν σε κάθε δημόσιο αλλά και ιδιωτικό χώρο ιδιαίτερα στη Μεγάλη Βρετανία όλοι οι πολίτες παρακολουθούνται μέσω των CCTV και αυτό με βάση το πρόταγμα της ασφάλειας για τον εντοπισμό ατόμων για την πρόληψη της εγκληματικότητας και της τρομοκρατίας. Τα CCTV χρησιμοποιούνται στους χώρους εργασίας για την παρακολούθηση των εργαζόμενων, στα σχολεία ακόμη και στις εκκλησίες. Η χρήση των καμερών έχει ενταθεί έπειτα από τα γεγονότα της 11$^{ης}$ Σεπτεμβρίου και θεωρείται ως πανάκεια για όλα τα προβλήματα. Η μαζική εγκατάσταση τους σε πολλούς δημόσιους χώρους στη χώρα μας πραγματοποιήθηκε για πρώτη φορά το πρώτο εξάμηνο του 2003 για τη σύνοδο κορυφής του Ευρωπαϊκού Συμβουλίου τον Ιούνιο του 2003 και κυρίως για την ασφάλεια των Ολυμπιακών Αγώνων το 2004 (Σαματάς, 2005: 493).

Οι κάμερες παρακολούθησης ουσιαστικά εστιάζουν σε κάποιο άτομο που θεωρείται ύποπτο, συνήθως βάσει της εμφάνισης του που ταιριάζει με το ψηφιακό προφίλ του υπόπτου που έχει προγραμματιστεί. Εκτός από την καταγραφή ήχου και εικόνας υπάρχει δυνατότητα διαβίβασης των εικόνων και ήχων έπειτα από την αλγοριθνική κωδικοποίηση και τη συσχέτιση τους με πολλαπλές βάσεις δεδομένων προγραμματισμένα με συγκεκριμένα προφίλ ατόμων και συμπεριφορών. Με τον τρόπο αυτό ο πανοπτισμός μετατρέπεται σε «υπέρ – πανοπτισμό» (Lyon, 2001: 114 – 118; Norris & Armstrong, 1999: 222; Poster, 1996: 189; Samatas, 2004: 121 – 122).

Από τη στιγμή που η χρήση των CCTV αποτελεί σύνηθες μέσο κατόπτευσης των δημόσιων χώρων για τον έλεγχο της εγκληματικότητας τίθεται ουσιαστικό ζήτημα αναφορικά με την προστασία της ιδιωτικότητας του ατόμου, των ανθρώπινων δικαιωμάτων και των δημοκρατικών ελευθεριών. Ποια είναι τα χαρακτηριστικά

εκείνα που κάνουν κάποιον να θεωρείται ύποπτος; Ποιος είναι αυτός που τα ορίζει; Ποιος παρακολουθεί τους παρακολουθούντες; Ενώ η πρόληψη και η καταστολή του εγκλήματος αποτελούν σημαντικό στόχο κάθε κοινωνίας, ολόκληρες κατηγορίες ατόμων μπορεί να θεωρηθούν ως πιθανοί εγκληματίες και να παρακολουθούνται ως τέτοιοι λόγω του ότι π.χ. ανήκουν σε «ορατές μειονότητες» λόγω εμφάνισης, προτιμήσεων, ιδεών κτλ (Stamatellos).

Ιδιαίτερα μετά την 11η Σεπτεμβρίου τα κριτήρια σύμφωνα με τα οποία θεωρείται κάποιος ύποπτος δεν αφορούν την εμπλοκή του υποκειμένου σε κάποια αντικοινωνική ή εγκληματική συμπεριφορά. Αντίθετα, όλα τα άτομα, ιδίως όμως των μειονοτήτων γίνονται στόχοι παρακολούθησης βάσει φυλής, κοινωνικής τάξης ή ακόμη και εμφάνισης με αποτέλεσμα τη δημιουργία κοινωνικά στιγματισμένων ομάδων. Ουσιαστικά μέσω της αντιτρομοκρατικής παρακολούθησης υποβοηθείται η δημιουργία και συντήρηση των κοινωνικών διακρίσεων στο πρόταγμα της ασφάλειας και της δημιουργίας μιας «πειθαρχημένης κοινωνίας» αναπαράγοντας το φόβο, τη δυσπιστία και την ανασφάλεια. Ο μόνος που ωφελείται είναι η βιομηχανία της τεχνολογίας της παρακολούθησης και η όλη «βιομηχανία» ασφάλειας – securities, κτλ που προωθούν την εφαρμογή των νέων τεχνολογιών επιτήρησης για το κέρδος, καθώς και το κράτος με τη νομιμοποίηση των πολιτικών αποκλεισμού των «οιωνεί ύποπτων» κατηγοριών για λόγους ασφάλειας (Samatas, 2004: 122 – 124; Σαματάς, 2005: 494 – 497; Lyon, 2007: 185 – 187).

### 2.5: <u>Δορυφορική παρακολούθηση</u>

Αρχικά οι δορυφόροι χρησιμοποιούνταν για καθαρά επιστημονικούς σκοπούς βγάζοντας φωτογραφίες της γης. Σήμερα μπορούν να λάβουν εικόνες της προσωπικής μας ζωής με τη χρήση του γνωστού σε όλους μας GPS[12] που βασίζεται στη μέθοδο που χρησιμοποιούσαν οι ναυτικοί προκειμένου να εντοπίσουν τη θέση τους στη θάλασσα (Stamatellos, xx: 33).

Το GPS αρχικά ήταν ένα στρατιωτικό σύστημα παρακολούθησης καταγράφοντας τα πάντα πάνω στη γη ενώ χρησιμοποιούνταν και για τις

[12] Η πιο διαδεδομένη τεχνολογία εντοπισμού θέσης είναι το GPS που λειτουργεί με τη βοήθεια δορυφόρου. Μάλιστα θεωρείται ότι μπορεί να έχει θετικά αποτελέσματα όταν χρησιμοποιούνται π.χ για τον κατ' οίκον περιορισμό παραβατών, για τον εντοπισμό παράνομων μεταναστών, τον εντοπισμό ζώων ή Ατόμων Με Ειδικές Ανάγκες (ΑΜΕΑ) (Stammatellos, xx:33).

τηλεπικοινωνίες, την πλοήγηση σε θάλασσα και αέρα, την πρόβλεψη των καιρικών φαινομένων κτλ.

Σήμερα χρησιμοποιείται σε μεγάλη κλίμακα τόσο από το ευρύ κοινό όσο και από ιδιωτικές εταιρείες φύλαξης (security) για τον εντοπισμό της γεωγραφικής μας θέσης αλλά και για την προστασία έναντι της εγκληματικότητας και της τρομοκρατίας. Χρησιμοποιείται επίσης και από την αστυνομία, το εμπορικό ναυτικό, το Υπουργείο Γεωργίας, το ΣΔΟΕ κτλ για την παρακολούθηση ανθρώπων και οχημάτων.

Συγκεκριμένα, ο δορυφόρος είναι αυτός που εντοπίζει τη θέση μας και στέλνει τα δεδομένα σε μια συσκευή βάσης και σ' αυτή που φέρουμε μαζί μας. Μάλιστα με τη νέα τεχνολογία στην κινητή τηλεφωνία που μπορεί να υποστηρίζει τη λειτουργία GPS, μπορεί άμεσα να εντοπιστεί η ακριβής θέση του χρήστη. Η νέα αυτή ανάγκη της εγκατάστασης μηχανισμών παρακολούθησης για την προσωπική προστασία και ασφάλεια που χρησιμοποιείται κυρίως από την οικονομική και κοινωνική ελίτ χαρακτηρίζεται ως «αυτοπτισμός» (Samatas, 2004: 124 – 125; Σαματάς, 2005: 497 - 499).

### 2.6: <u>Παρακολούθηση μέσω κινητής τηλεφωνίας</u>

Ο τομέας των τηλεπικοινωνιών παρουσιάζει διαρκή εξέλιξη. Έχουμε πλέον περάσει στην τεχνολογία 3G όπου τα κινητά τηλέφωνα είναι πλέον εξοπλισμένα με βιντεοκάμερες, internet, παιχνίδια, ατζέντες και διάφορες εφαρμογές οργάνωσης ενώ έχουν τη δυνατότητα αναπαραγωγής βίντεο, ήχου, εικόνας, MP3 κτλ.

Βασικότερα από τα μειονεκτήματα της κινητής τηλεφωνίας είναι το αυξημένο κόστος, ο κίνδυνος για την υγεία από την παρατεταμένη χρήση τους, το γεγονός ότι οι κοινωνικές σχέσεις παύουν πλέον να είναι προσωπικές ενώ παράλληλα με τη χρήση τους ενδεχομένως βρισκόμαστε υπό συνεχή παρακολούθηση αφού παρακρατώνται τα επικοινωνιακά δεδομένα (data retention) (Ιγγλεζάκης, 2004; Stamatellos, xx: 33). Ο φόβος υποκλοπής υπάρχει επειδή εξ ορισμού όλες οι ασύρματες επικοινωνίες διαβιβάζουν πληροφορίες στα αεροκύματα (airwaves) οι οποίες μπορεί να αποτελούνται από δεδομένα δρομολόγησης ή περιεχομένου όπου μπορούν να καταγραφούν και σε ορισμένες περιπτώσεις να διαχειριστούν χωρίς τη γνώση και τη συγκατάθεση μας (http://webhome.idirect.com/~dakk/presitations/delzotto/Slide1.html).

Όσον αφορά τον τομέα των τηλεπικοινωνιών, η ΕΕ θέσπισε την οδηγία 2006/24/ΕΚ για την παρακράτηση – διατήρηση των δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών που τροποποίησε την οδηγία 2002/58/ΕΚ. Η έννοια της «διατήρησης δεδομένων» (data retention) αναφέρεται γενικά στην αποθήκευση των αρχείων τηλεφωνικών κλήσεων, της κίνησης στο διαδίκτυο και της συναλλαγής δεδομένων τόσο από κυβερνήσεις όσο και από οικονομικούς οργανισμούς. Έτσι μέσω αυτής επιδιώκεται η άσκηση μαζικού ελέγχου και παρακολούθησης των διατηρηθέντων δεδομένων από τις κυβερνήσεις όσο και των συναλλαγών και της επισκεψιμότητας των ιστοσελίδων για εμπορικούς σκοπούς.

Η οδηγία αυτή απαιτεί από τα κράτη μέλη να διασφαλίσουν ότι οι πάροχοι των επικοινωνιών διατηρούν μόνο τα απαραίτητα στοιχεία που ορίζονται σε αυτήν για περίοδο μεταξύ έξι (6) μηνών και δύο (2) ετών για α) την ανίχνευση και τον εντοπισμό της πηγής της επικοινωνίας, β) την ανίχνευση και τον προσδιορισμό του προορισμού της επικοινωνίας, γ) τον προσδιορισμό της ημερομηνίας, ώρας και διάρκειας μιας επικοινωνίας, δ) τον προσδιορισμό του είδους της επικοινωνίας, ε) την ανακοίνωση για τον εντοπισμό της συσκευής και στ) τον προσδιορισμό της θέσης του εξοπλισμού κινητής επικοινωνίας. Τα δεδομένα αυτά πρέπει να είναι στη διάθεση των εκάστοτε κρατικών αρχών για τους σκοπούς της έρευνας, του εντοπισμού και τη δίωξη κάθε σοβαρού εγκλήματος όπως ορίζει το εθνικό δίκαιο κάθε κράτους μέλους (www.statewatch.org, www.digitalrights.gr/tiki/tiki-index.php?page=DataRetention).

### 2.7: Παρακολούθηση μέσω ηλεκτρονικών ταυτοτήτων – το νέο ηλεκτρονικό φακέλωμα

Η γνησιότητα και η ταυτοποίηση στις μέρες μας είναι ιδιαίτερης σημασίας και αυτό φαίνεται από την εισαγωγή των καρτών αναγνώρισης – ταυτοτήτων που πλέον περιλαμβάνουν μικροτσίπ με προσωπικά και βιομετρικά δεδομένα για την ταυτοποίηση του χρήστη. Χαρακτηριστικό είναι το παράδειγμα των συστημάτων smart card και e-pass που έχουν οι οδηγοί στις εθνικές οδούς αλλά και στην Αττική οδό όπου υπάρχουν αισθητήρες που χρεώνουν αυτόματα τον οδηγό κάθε φορά που περνά από διόδια (Stamatellos, xx: 33 – 34).

Υπάρχουν όμως και συστήματα ελέγχου πρόσβασης με βιομετρικά στοιχεία όπως η ίριδα του ματιού, το δακτυλικό αποτύπωμα, κτλ που στοχεύουν στην εξακρίβωση της ταυτότητας ενός ατόμου όταν μπαίνει σε ασφαλείς περιοχές ή όταν χρησιμοποιεί ορισμένους τομείς ορίζοντας ως ασφαλιστικές δικλείδες φυσικά ή γενετικά στοιχεία που είναι μοναδικά για κάθε άτομο (www.arcanesecurity.net/content/view/6/9/1/4/). Οι λόγοι χρήσης τους ποικίλουν από τη σύλληψη εγκληματιών μέχρι και την προστασία των πληροφοριών ενός υπολογιστή, είτε μέσω ηλεκτρονικού αποτυπώματος είτε μέσω σάρωσης της ίριδας του ματιού. Προκύπτουν όμως ζητήματα όπως ποιος, πως και για ποιο σκοπό θα τα χρησιμοποιήσει και ποια θα είναι τα όρια της χρήσης τους.

Ώθηση στη συγκεκριμένη εξέλιξη δόθηκε από κυβερνήσεις και κυβερνητικές υπηρεσίες για την αντιμετώπιση προβλημάτων ασφαλείας που συνδέονται με την αυξημένη κινητικότητα των ανθρώπων με αποτέλεσμα να αυξάνεται η συλλογή και επεξεργασία των «βιοσωματικών δεδομένων» σε διάφορους κοινωνικούς τομείς και κοινωνικές δραστηριότητες όπως η εργασία, η κοινωνική ασφάλιση, η επιβολή του νόμου, ο καταναλωτισμός, τα ταξίδια και η ψυχαγωγία.

Η χρήση των βιομετρικών χαρακτηριστικών και η «αρχειοθέτηση» τους αποτελεί υλικό για την παραγωγή νέων και περισσότερων πληροφοριών για άτομα, ομάδες, πληθυσμούς αναφορικά με το ιστορικό τους και το μέλλον τους διευκολύνοντας κατ' αυτό τον τρόπο η σκιαγράφηση και την κατηγοριοποίηση τους σε διάφορες ομάδες «κινδύνου». Οι δυνατότητες κατηγοριοποίησης των ανθρώπων μοιάζουν απεριόριστες. Η αποθήκευση, η ανάκτηση, η επεξεργασία των δεδομένων για αρκετά μεγάλη περίοδο μπορεί να αποτελέσει τμήμα της επεξεργασίας των γενικότερων προσωπικών πληροφοριών του ατόμου με τρόπους που μέχρι τώρα δεν ήταν εφικτοί.

Όμως θα αποτελέσει και την αφορμή για τη δημιουργία νέων και όχι αθώων μορφών παρακολούθησης. Η τεχνολογική εξέλιξη π.χ. στον ιατρικό τομέα έχει σαν αποτέλεσμα το ανθρώπινο σώμα να αποκτήσει νέα οντότητα και να επανακαθορισθεί ως πληροφορία. Έτσι, το σώμα ερμηνεύεται ως ροή πληροφοριών και επικοινωνιακό πλάνο (Lyon, 2003: 58 - 63).

Αν τα βιομετρικά συστήματα χρησιμοποιηθούν σωστά μπορεί να κάνουν τη ζωή μας ευκολότερη. Αν όχι, μπορεί να υπονομεύσουν τις πολιτικές μας ελευθερίες (http://www.greektechforum.com/forums/showthread.php?p=10445). Συχνά όμως δίνεται ιδιαίτερη σημασία στη σωματική ακεραιότητα αφού εξετάζεται μόνο ως

τμήμα για εισαγωγή δεδομένων (input) στο σύστημα. Στις περισσότερες χώρες εφαρμόζονται συγκεκριμένοι νόμοι και κανόνες όσον αφορά έρευνες που σχετίζονται με το σώμα για την προστασία των δικαιωμάτων του ατόμου. Όμως, προκύπτει ένας μεγάλος αριθμός θεμάτων που αφορούν τη σωματική ακεραιότητα όταν διακινδυνεύονται ή παραβιάζονται τα όρια. Έτσι, πρέπει να ξεκαθαριστεί από νομικής άποψης τι είναι αποδεκτό και τι όχι (Lyon, 2003: 66 – 69).

### 2.8: Παιχνίδια reality τύπου Big Brother και AGB

Το 2001 είχαμε την είσοδο του τηλεοπτικού παιχνιδιού «Big Brother» στην ελληνική τηλεόραση που είχε σαν αντικείμενο την παρακολούθηση της ρουτίνας απλών καθημερινών ανθρώπων από το ευρύ κοινό, γνωστό και ως «μαζοπτισμός» το οποίο είχε μεγάλη ακροαματικότητα. Στο παιχνίδι αυτό συμμετείχαν ενήλικες που είχαν δώσει τη συγκατάθεση τους να αποτελέσουν αντικείμενο παρακολούθησης 23 ώρες το 24ωρο από το διαδίκτυο, να διασκεδάζουν τους τηλεθεατές προκειμένου να αποκτήσουν ένα χρηματικό έπαθλο και προσωρινή φήμη – δημοσιότητα.

Αυτό είχε ως αποτέλεσμα την εκούσια παραβίαση της ιδιωτικότητας των παικτών η οποία αποτελούσε βορά στα ΜΜΕ[13], αλλά και εμπόρευμα για τους τηλεοπτικούς παραγωγούς και τις εταιρείες κινητής τηλεφωνίας που κερδοσκοπούσαν προσκαλώντας τους απλούς θεατές να συμμετέχουν στο παιχνίδι. Οι συμμετέχοντες όμως γενικά αδιαφορούν για τις επιπτώσεις της παραβίασης της ιδιωτικότητας τους και του πιθανού εξευτελισμού τους προκειμένου να αποκομίσουν πρόσκαιρη δημοσιότητα αλλά και κάποιο χρηματικό όφελος.

Έπειτα από την είσοδο της ιδιωτικής τηλεόρασης δημιουργήθηκε η ανάγκη μέτρησης της ακροαματικότητας των καναλιών για τους σκοπούς του ανταγωνισμού. Έτσι δημιουργήθηκε η AGB που ασχολείται με τη μέτρηση της τηλεθέασης. Δείγμα[14] της αποτελούν 1300 νοικοκυριά από διάφορες περιοχές της Ελλάδας στα οποία εγκαθίστανται ειδικές συσκευές που καταγράφουν την κατάσταση της τηλεόρασης, αν είναι ανοικτή ή κλειστή, την επιλογή των τηλεοπτικών καναλιών, ποιος είναι αυτός που παρακολουθεί και ποιο πρόγραμμα μέσω ενός ειδικού τηλεχειριστηρίου όπου κάθε μέλος του νοικοκυριού (ηλικίας 4+) δηλώνει την παρουσία του πατώντας

[13] Η παρακολούθηση των διάσημων και ισχυρών ατόμων από τις μάζες μέσω του κίτρινου τύπου έντυπου και ηλεκτρονικού χαρακτηρίζεται ως «συνοπτισμός» (Σαματάς, 2004).
[14] Το δείγμα της θεωρείται αντιπροσωπευτικό αφού αποτελείται από αστικά, ημι-αστικά, αγροτικά νοικοκυριά (www.agb.gr).

το αντίστοιχο κουμπί. Βάσει των αποτελεσμάτων της AGB τα τηλεοπτικά κανάλια διαμορφώνουν το τηλεοπτικό τους πρόγραμμα προκειμένου να προσελκύσουν τηλεθεατές και διαφημιστικά έσοδα αδιαφορώντας για την ποιότητα των προγραμμάτων[15] που θυσιάζεται στο βωμό της τηλεθέασης (Samatas, 2004: 125 – 128; www.Agb.gr).

### 2.9: Παράνομα καταναλωτικά προφίλ και λαθρεμπόριο προσωπικών δεδομένων

Όπως έχει ήδη αναφερθεί, τόσο ο δημόσιος όσο και ο ιδιωτικός τομέας χρησιμοποιούν τις νέες τεχνολογίες για τη συλλογή και επεξεργασία προσωπικών πληροφοριών τις οποίες αποθηκεύουν σε βάσεις δεδομένων. Οι ιδιώτες τις χρησιμοποιούν για την παραγωγή λιστών με προφίλ καταναλωτών, τα οποία και διαθέτουν προς πώληση πράγμα που αποτελεί παράνομη πράξη. Πράγματι, η νόμιμη ή παράνομη διάθεση προσωπικών πληροφοριών για την παραγωγή προφίλ είναι σχετικά εύκολο εγχείρημα στην Ελλάδα. Σύμφωνα με την ΑΠΔΠΧ τα ιατρικά δεδομένα δεν γίνονται σεβαστά από συγκεκριμένα νοσοκομεία και ιδιαίτερα στις μαιευτικές κλινικές που παρέχουν τα προσωπικά δεδομένα των νεογνών για καταναλωτικούς σκοπούς (Απόφαση 150/ 12 Δεκεμβρίου, 2001). Κάτι ανάλογο συνέβη και με τα στρατολογικά γραφεία που παρείχαν σε ιδιωτικές ψυχιατρικές κλινικές αρχεία πασχόντων από ψυχολογικά προβλήματα που εξαιρέθηκαν από τη στρατιωτική θητεία.

Μάλιστα, ο πρώτος πρόεδρος της ΑΠΔΠΧ παραδέχθηκε την ύπαρξη του λαθρεμπορίου των προσωπικών δεδομένων στη χώρα μας και την ανικανότητα της ΑΠΔΠΧ να το σταματήσει δηλώνοντας ότι «σαν κοινωνία βρισκόμαστε μπροστά σε μια χαοτική κατάσταση και σαν πολίτες είμαστε απροστάτευτοι… από όλων των ειδών τις ιδιωτικές πρωτοβουλίες που παρακολουθούν την ιδιωτική μας ζωή και καταγράφουν τα προσωπικά μας δεδομένα» (Samatas, 2004: 128 – 130).

Έτσι, τα προσωπικά δεδομένα συλλέγονται για τη δημιουργία του προφίλ του χρήστη το οποίο μπορεί να χρησιμοποιηθεί για διάφορους σκοπούς, από την αποστολή διαφημιστικών μηνυμάτων μέχρι και την αποκάλυψη της ταυτότητας αλλά

[15] Το ρόλο του ελέγχου της ποιότητας των ραδιοτηλεοπτικών προγραμμάτων έχει αναλάβει το Εθνικό Συμβούλιο Ραδιοτηλεόρασης (ΕΣΡ) που παρά τις ποινές που έχει επιβάλλει δεν μπορεί να λάβει δραστικά μέτρα έναντια στα τηλεοπτικά κανάλια τα περισσότερα από τα οποία λειτουργούν παράνομα χωρίς κρατική άδεια.

και την «κατηγοριοποίηση» του χρήστη ή ακόμη και το στιγματισμό του για τις επιλογές του όταν π.χ. κάποιος είναι ομοφυλόφιλος. Σε μερικές από αυτές τις περιπτώσεις μπορεί να χρησιμοποιηθούν – να δημοσιοποιηθούν αρνητικές για το άτομο πληροφορίες που θα αποτελέσουν τροχοπέδη για την ανάπτυξη της προσωπικότητας του. Σημαντικό είναι και το γεγονός ότι η επεξεργασία των δεδομένων αυτών γίνεται σε ελάχιστο χρόνο με ελάχιστο κόστος με αποτέλεσμα να υπάρχει η δυνατότητα αποσύνδεσης μίας πληροφορίας από το αρχικό της πλαίσιο αναφοράς, της ανασύνθεσης και της συσχέτισης της με άλλες πληροφορίες με αποτέλεσμα να δημιουργηθεί εκ νέου μία άλλη πληροφορία που πιθανόν να εξυπηρετεί κάποιους σκοπούς (Γιαννούλη, 1988; Ιγγλεζάκης, 2004; Stadler, 2000).

### 2.10: <u>Συμπερασματικές παρατηρήσεις</u>

Στις μέρες μας η χρήση των νέων τεχνολογιών παρακολούθησης είναι ιδιαίτερα διαδεδομένη. Η χρήση των βάσεων δεδομένων, των CCTV αλλά και του διαδικτύου από διάφορους φορείς με τους οποίους συναλλασσόμαστε αποτελεί καθημερινή πρακτική. Όλοι αποτελούμε στόχους παρακολούθησης σε διάφορες πτυχές της καθημερινότητας μας, από τα ψώνια στο super market και τις συναλλαγές μας με τράπεζες, νοσοκομεία κτλ, μέχρι και μία απλή διέλευση στην Αττική οδό, τη χρήση του GPS ή και του κινητού μας τηλεφώνου που πλέον είναι εξοπλισμένο με την τεχνολογία 3G.

Η συλλογή τόσο των προσωπικών όσο και των ευαίσθητων προσωπικών δεδομένων είναι κεντρικής σημασίας και πραγματοποιείται σχεδόν σε κάθε μας δραστηριότητα. Όσο πιο ευαίσθητη είναι μία πληροφορία τόσο πιο μεγάλη αξία έχει. Πλέον μέσω των νέων τεχνολογιών υπάρχει η δυνατότητα πέραν της συλλογής τεράστιου όγκου πληροφοριών και αυτή του συνδυασμού και της συσχέτισης τους για τη δημιουργία προφίλ που μπορεί να σημαίνει την ένταξη ή τον αποκλεισμό, τη δημιουργία διακρίσεων, κτλ. Χαρακτηριστικό είναι το παράδειγμα του διατραπεζικού συστήματος ΤΕΙΡΕΣΙΑΣ ΑΕ για την πιστοληπτική ικανότητα. Η συλλογή και η επεξεργασία των προσωπικών πληροφοριών άλλοτε γίνεται με τη συγκατάθεση των υποκειμένων τους και άλλοτε χωρίς καν αυτά να το γνωρίζουν, όπως συμβαίνει π.χ. με την αποστολή «cookies» από τους διακομιστές στους χρήστες του διαδικτύου. Μετά τα γεγονότα της 11$^{ης}$ Σεπτεμβρίου, η συλλογή και η επεξεργασία προσωπικών

πληροφοριών νομιμοποιείται στο πρόταγμα της ασφάλειας και της προστασίας ενάντια στη διεθνή τρομοκρατία.

Από τη στιγμή που αποτελούμε στόχο παρακολούθησης σχεδόν σε όλες τις εκφάνσεις της καθημερινότητας μας, συμφωνούμε με όσους μιλούν για το τέλος της ιδιωτικότητας (Gormley, 1997, Sykes, 1999). Για το λόγο αυτό θεωρούμε ότι πρέπει να ασκείται εντατικός έλεγχος αναφορικά με τη χρήση των τεχνολογιών παρακολούθησης, και να εφαρμόζεται πιστά το εθνικό και το ευρωπαϊκό δίκαιο για την προστασία των προσωπικών και των ευαίσθητων προσωπικών δεδομένων.

# ΚΕΦΑΛΑΙΟ 3$^{Ο}$
# Η ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΚΑΙ ΕΥΑΙΣΘΗΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΗΝ ΕΥΡΩΠΑΙΚΗ ΕΝΩΣΗ

## 3.1: Το πρόβλημα της προστασίας των προσωπικών και των ευαίσθητων προσωπικών δεδομένων και οι πολιτικές της ΕΕ

Η προστασία των προσωπικών μας δεδομένων έχει εκτός από την κοινωνική και νομική διάσταση. Για το λόγο αυτό κρίνεται αναγκαία η εξέταση των πολιτικών της ΕΕ για τη νομιμότητα της διαδικασίας επεξεργασίας των προσωπικών δεδομένων και την αναγνώριση δικαιωμάτων στα υποκείμενα των δεδομένων και των νομοθετικών ρυθμίσεων και Οδηγιών για την προστασία τους, που κάθε κράτος – μέλος της καλείται να ενσωματώσει στο εθνικό του δίκαιο και να προσαρμόσει στην κουλτούρα του.

## 3.2: Η Ευρωπαϊκή διάσταση στην προστασία των προσωπικών δεδομένων

Η εξάπλωση της χρήσης των ηλεκτρονικών υπολογιστών – και γενικότερα των νέων τεχνολογιών – στις διάφορες πτυχές της καθημερινότητας αλλά και στην οργάνωση της κοινωνίας μας αποτέλεσαν το έναυσμα στην ΕΕ για τη δημιουργία διαφόρων σχετικών ρυθμίσεων που στοχεύουν στην προστασία της ιδιωτικής ζωής. Έτσι, καθορίζουν τις προϋποθέσεις νόμιμης επεξεργασίας των δεδομένων και φροντίζουν ώστε να ελαχιστοποιούνται οι κίνδυνοι παραβίασης της ιδιωτικότητας με τη λήψη μέτρων ασφαλείας αλλά και τον έλεγχο που ασκείται από την ΑΠΔΠΧ. Διότι η αυτοματοποιημένη επεξεργασία και η χρήση των προσωπικών δεδομένων εγκυμονούν κινδύνους για τον άνθρωπο και την προστασία των θεμελιωδών δικαιωμάτων του από τη συλλογή, την καταχώρηση και τη διαβίβαση των δεδομένων του. Οι κίνδυνοι αυτοί αφορούν α) την προστασία της προσωπικότητας του ατόμου, β) το δικαίωμα της προστασίας της ιδιωτικής ζωής, γ) τη σφαίρα του απορρήτου, δ) το δικαίωμα ανάπτυξης της προσωπικότητας και ε) γενικότερα την άσκηση των θεμελιωδών δικαιωμάτων (Δόνος, 2004: 24 – 26).

Βασική θέση της ΕΕ είναι ότι η προστασία των προσωπικών και ιδιαίτερα των ευαίσθητων προσωπικών δεδομένων και της ιδιωτικής ζωής του ατόμου, αποτελεί

βασική προτεραιότητα αλλά και υποχρέωση κάθε κράτους – μέλους λαμβάνοντας πάντα υπόψη το πολιτισμικό και κοινωνικό του πλαίσιο αλλά και τις ιδιαιτερότητες του. Έτσι, το 1995 θέσπισε την οδηγία για την προστασία των προσωπικών δεδομένων για την εναρμόνιση των νομοθεσιών των κρατών – μελών όσον αφορά την παροχή αξιόπιστου επίπεδου προστασίας για τους πολίτες και την εξασφάλιση της ελεύθερης ροής των δεδομένων προσωπικού χαρακτήρα εντός των συνόρων της. Με την οδηγία αυτή καθορίζεται ένα βασικό επίπεδο προστασίας της ιδιωτικής ζωής ενισχύοντας την ήδη ισχύουσα νομοθεσία για την προστασία των δεδομένων αλλά και καθιερώνοντας ταυτόχρονα μία σειρά νέων δικαιωμάτων (www.privacyinternational.org).

Έτσι, η πρώτη χώρα η οποία θέσπισε νόμο για την προστασία των προσωπικών δεδομένων ήταν το κρατίδιο της Έσσης της Γερμανίας το 1970. Το παράδειγμα του κρατιδίου αυτού ακολούθησαν η Σουηδία το 1973, η Ομοσπονδιακή Δημοκρατία της Γερμανίας το 1977, η Αυστρία, η Γαλλία, η Δανία και η Νορβηγία το 1978, το Λουξεμβούργο το 1979, η Ισλανδία το 1981 κτλ. Τα νομοθετήματα αυτά είναι μέρος της «πρώτης γενιάς» νομοθετημάτων (Ιγγλεζάκης, 2004: 23; Αλεξανδροπούλου – Αιγυπτιάδου, 2007: 123).

Αρχικά η Ευρωπαϊκή Σύμβαση για την Προστασία των Ανθρώπινων Δικαιωμάτων και Θεμελιωδών Ελευθεριών όριζε α) το δικαίωμα του σεβασμού της ιδιωτικής και οικογενειακής ζωής του ατόμου, του χώρου κατοικίας και της αλληλογραφίας του και β) τη μη παρέμβαση κάθε κρατικής αρχής εξαιτίας της εφαρμογής του δικαιώματος αυτού εκτός εάν σύμφωνα με το νόμο είναι απαραίτητο για σκοπούς εθνικής και δημόσιας ασφάλειας ή για λόγους οικονομικής ευημερίας, για την πρόληψη της εγκληματικότητας, για την προστασία των δικαιωμάτων και των ελευθεριών άλλων κτλ (Stamatellos: 34 – 35).

### 3.2.1: <u>Πεδίο εφαρμογής και ορισμοί</u>

Η αντίληψη της ΕΕ για την προστασία των προσωπικών και των ευαίσθητων προσωπικών δεδομένων συνοψίζεται στη θέσπιση και στην εφαρμογή ειδικής νομοθεσίας που αποτελεί και την κατευθυντήρια γραμμή για όλες τις χώρες που ανήκουν σ' αυτήν (Gormley, 1997: 36; Gurau, Ranchhod & Gauzente, 2003: 652).

Έτσι, δίνεται ένας ευρύς ορισμός της έννοιας της «επεξεργασίας των προσωπικών δεδομένων» όπου ως τέτοια ορίζεται «κάθε λειτουργία ή ομάδα

λειτουργιών, αυτοματοποιημένων ή μη, που περιλαμβάνει χωρίς όμως να περιορίζεται στη συλλογή, καταγραφή, οργάνωση, αποθήκευση, προσαρμογή ή μεταβολή, ανάκτηση, διαβούλευση, χρήση, αποκάλυψη μέσω μεταβίβασης, διάδοσης των προσωπικών δεδομένων ή διαφορετικά καθιστώντας διαθέσιμη την παράταξη ή το συνδυασμό, την παρεμπόδιση, τη διαγραφή ή την καταστροφή τους» (Αλεξανδροπούλου – Αιγυπτιάδου, 2007: 33).

Ως «προσωπικά δεδομένα» ορίζεται «κάθε πληροφορία που αναφέρεται σε συγκεκριμένο φυσικό πρόσωπο», η οποία μπορεί να περιλαμβάνει εκτός από γραπτές πληροφορίες, φωτογραφίες, βιντεοσκοπήσεις, ηχογραφήσεις που αφορούν συγκεκριμένο φυσικό πρόσωπο. Ο ορισμός αυτός είναι ιδιαίτερα ευρύς με αποτέλεσμα ως προσωπικά δεδομένα να θεωρείται κάθε στοιχείο που μας προσδιορίζει άμεσα ή έμμεσα σαν προσωπικότητες αλλά και οποιοδήποτε στοιχείο μπορεί να χρησιμοποιηθεί για τον προσδιορισμό της ταυτότητας ενός προσώπου είτε αυτό είναι ο αριθμός της αστυνομικής του ταυτότητας, ο αριθμός κοινωνικής ασφάλισης, ένας κωδικός πρόσβασης ή ακόμη και ο αριθμός PIN. Έτσι, κάποιο δεδομένο δεν θεωρείται προσωπικό αν δεν συνδέεται με κάποιο φυσικό πρόσωπο ενώ υφίσταται όταν γίνεται η σύνδεση αυτή (Αλεξανδροπούλου – Αιγυπτιάδου, 2007: 33; Gormley, 1997: 36).

Ως «ευαίσθητα προσωπικά δεδομένα» θεωρούνται όλα τα δεδομένα και οι πληροφορίες που «ενδιαφέρουν» τους τρίτους και αυτός που τον αφορούν δεν επιθυμεί την κοινοποίηση τους. Συγκεκριμένα, ως τέτοια θεωρούνται τα δεδομένα που αφορούν ζητήματα υγείας, κοινωνικής πρόνοιας, φυλετικής και εθνικής προέλευσης, ερωτικής ζωής, πολιτικά φρονήματα, θρησκευτικές και φιλοσοφικές πεποιθήσεις, συμμετοχή σε συνδικαλιστικές οργανώσεις, ποινικές διώξεις ή καταδίκες, γενετικά δεδομένα, δηλώσεις για τα στοιχεία του αιτούντος άσυλο, τα δεδομένα των ληπτών και δωρητών οργάνων και ιστών κτλ. Δηλαδή ως τέτοια ορίζονται τα δεδομένα που σχετίζονται με την προσωπικότητα και την αυστηρή ιδιωτική ζωή του ατόμου (Χαλαζωνίτης, 1995: 303 – 318).

Ο διαχωρισμός των εννοιών «προσωπικά δεδομένα» και «ευαίσθητα προσωπικά δεδομένα» εξαρτάται από το πολιτιστικό και κοινωνικό πλαίσιο στο οποίο αναφέρονται. Στη χώρα μας δεδομένου του προηγούμενου αυταρχικού κράτους στην περίοδο της δικτατορίας, ευαίσθητα θεωρούνται τα δεδομένα που αφορούν αποκλειστικά την ιδιωτική ζωή του ατόμου αλλά και τις κοινωνικοπολιτικές του αντιλήψεις (Σαματάς, 2005). Η διαφορά μεταξύ απλών και ευαίσθητων προσωπικών

δεδομένων έγκειται στο ότι τα ευαίσθητα προσωπικά δεδομένα αναφέρονται κατά κόρον στο σκληρό πυρήνα της ιδιωτικής ζωής του ατόμου με αποτέλεσμα να τυγχάνουν ιδιαίτερης και αυστηρότερης νομικής προστασίας αναφορικά με την επεξεργασία τους και τις προϋποθέσεις της, όπου γι' αυτήν απαιτείται η γραπτή συγκατάθεση του προσώπου το οποίο αφορούν τα δεδομένα αυτά, σε αντιδιαστολή με τα απλά, όπου η προφορική συγκατάθεση είναι αρκετή. Επιπλέον, για να είναι νόμιμη η επεξεργασία των ευαίσθητων προσωπικών δεδομένων πρέπει να ληφθεί σχετική απόφαση από την ΑΠΔΠΧ, ενώ για τα απλά προσωπικά δεδομένα πρέπει να γίνει απλά γνωστοποίηση σε αυτήν (Αλεξανδροπούλου – Αιγυπτιάδου, 2007: 37).

### 3.2.2: Βασικές εγγυήσεις

Όσον αφορά την παροχή των βασικών εγγυήσεων για την προστασία των προσωπικών δεδομένων έχουν θεσπιστεί κάποιες αρχές οι οποίες πρέπει να τηρούνται κατά τη συλλογή και την επεξεργασία των προσωπικών και των ευαίσθητων προσωπικών δεδομένων ώστε οι διαδικασίες αυτές είναι νόμιμες.

#### 3.2.2.1: Η αρχή της νομιμότητας του σκοπού και του τρόπου επεξεργασίας

Σύμφωνα με την αρχή της νομιμότητας του σκοπού και του τρόπου επεξεργασίας, η επεξεργασία των δεδομένων πρέπει να γίνεται με νόμιμο τρόπο ενώ οι σκοποί για τους οποίους πραγματοποιείται πρέπει να είναι αφενός καθορισμένοι και σαφείς, και αφετέρου νόμιμοι. Αυτό σημαίνει πως για την επεξεργασία των δεδομένων αυτών απαιτείται η ύπαρξη κάποιου νόμιμου και συγκεκριμένου σκοπού. Σύμφωνα με την ΑΠΔΠΧ, κάποιοι από τους σκοπούς επεξεργασίας προσωπικών δεδομένων μπορεί να είναι «η διοίκηση προσωπικού, η διαχείριση πελατολόγιου, η προώθηση προϊόντων και υπηρεσιών, η προώθηση δημόσιων σχέσεων, η διαχείριση μετοχολογίου, το εμπόριο προσωπικών δεδομένων, η διαχείριση εκλογικών καταλόγων, η παροχή κοινωνικών υπηρεσιών, η παροχή δικαστικών υπηρεσιών, η δημόσια υγεία κτλ» (Αλεξανδροπούλου – Αιγυπτιάδου, 2007: 45 – 46; www.dpa.gr/gnostop.htm).

Για να είναι νόμιμη η επεξεργασία των δεδομένων πρέπει να έχει γνωστοποιηθεί από τον υπεύθυνο επεξεργασίας ο σκοπός της επεξεργασίας τους τόσο στο υποκείμενο των δεδομένων με κατανοητό και εύληπτο τρόπο όσο και στην

ΑΠΔΠΧ. Στην περίπτωση αλλαγής του σκοπού της επεξεργασίας των δεδομένων, αυτός πρέπει να γνωστοποιηθεί στην ΑΠΔΠΧ. Τέλος, «η μέθοδος επεξεργασίας των δεδομένων πρέπει να είναι νόμιμη, δηλαδή να μην παραβιάζει τις ελευθερίες και τα δικαιώματα του υποκειμένου τους και να γίνεται με προσήλωση στο συγκεκριμένο σκοπό που εξυπηρετεί», ενώ η επεξεργασία στο σύνολο της δεν πρέπει να υπερβαίνει το σκοπό της (Αλεξανδροπούλου – Αιγυπτιάδου, 2007: 46 – 47).

#### 3.2.2.2: <u>Η αρχή της αναλογικότητας</u>

Η αρχή της αναλογικότητας επιβάλλει να συλλέγονται και να επεξεργάζονται μόνο τόσα δεδομένα όσα είναι απαραίτητο να επεξεργαστούν προκειμένου να επιτευχθεί ο σκοπός για τον οποίο τα επεξεργάζονται. Δηλαδή, κατά το στάδιο της επιλογής τόσο του τρόπου της επεξεργασίας των δεδομένων όσο και κατά την επιλογή των δεδομένων που πρόκειται να επεξεργαστούν πρέπει να τηρείται ένα μέτρο, να συλλέγονται δηλαδή τα δεδομένα που θεωρείται ότι είναι χρήσιμα για το σκοπό διεξαγωγής της επεξεργασίας. Χαρακτηριστικό είναι το παράδειγμα των προσωπικών δεδομένων των ατόμων που δηλώνουν υποψηφιότητα για κάποια θέση εργασίας (π.χ. ιατρικές εξετάσεις εργαζόμενων στο χώρο της υγείας, των εστιατορίων, των ξενοδοχείων κτλ). Τέλος, τα προσωπικά δεδομένα που συλλέγονται και επεξεργάζονται πρέπει να είναι όσο το δυνατόν λιγότερα ανάλογα και με το σκοπό της επεξεργασίας τους (Αλεξανδροπούλου – Αιγυπτιάδου, 2007: 47 – 50).

#### 3.2.2.3: <u>Η αρχή της ακρίβειας</u>

Η αρχή της ακρίβειας για την επεξεργασία των προσωπικών δεδομένων υπαγορεύει ότι τα δεδομένα τα οποία συλλέγονται και επεξεργάζονται «πρέπει να ανταποκρίνονται στην πραγματικότητα, να είναι ακριβή, επίκαιρα και να υποβάλλονται σε ενημέρωση» (Αλεξανδροπούλου – Αιγυπτιάδου, 2007: 50). Δηλαδή, ο υπεύθυνος της επεξεργασίας πρέπει να είναι πολύ προσεκτικός και συνεπής, να λαμβάνει όλα τα απαραίτητα μέτρα κατά τη διάρκεια της επεξεργασίας των δεδομένων αυτών. Και αυτό για να αποφεύγει παραδρομές, τη σύγχυση λόγω συνωνυμίας ή εξαιτίας του γεγονότος ότι παρουσιάζονται ελλείψεις στα στοιχεία που συλλέχθηκαν (Γέροντας, 2002: 196; Αλεξανδροπούλου – Αιγυπτιάδου, 2002: 28; Αλεξανδροπούλου – Αιγυπτιάδου, 2007: 50 – 51).

### 3.2.2.4: Η αρχή της χρονικής διάρκειας της τήρησης των δεδομένων

Όπως υποδηλώνει και ονομασία της συγκεκριμένης αρχής, τα δεδομένα που συλλέγονται για την επίτευξη κάποιου σκοπού, «πρέπει να τηρούνται σε μορφή που να επιτρέπει τον προσδιορισμό των υποκειμένων τους μόνο για το χρονικό διάστημα που έχει οριστεί από την ΑΠΔΠΧ και που θεωρείται απαραίτητο για την επίτευξη του στόχου – σκοπού της συλλογής και επεξεργασίας τους» (Αλεξανδροπούλου – Αιγυπτιάδου, 2007: 52). Η ΑΠΔΠΧ είναι εκείνη που αποφασίζει για το χρονικό διάστημα που πρέπει να τηρείται το αρχείο προσωπικών δεδομένων για την επίτευξη κάποιου σκοπού. Ο περιορισμός αυτός αφορά καθαρά και μόνο τα προσωπικά δεδομένα[16].

Συνήθως, μετά την έλευση του χρονικού διαστήματος που χρειάζεται για την επεξεργασία των προσωπικών δεδομένων για την επίτευξη κάποιου σκοπού, ο υπεύθυνος της επεξεργασίας τους υποχρεούται να καταστρέψει το αρχείο. Όμως η ΑΠΔΠΧ έχει το δικαίωμα, αιτιολογημένα πάντα, «να επιτρέψει τη διατήρηση του αρχείου αυτού για λόγους ιστορικούς, επιστημονικούς ή στατιστικούς αρκεί να μη θίγονται τα δικαιώματα των υποκειμένων τους αλλά και τα δικαιώματα τρίτων».

Στην περίπτωση που οι προαναφερθείσες αρχές επεξεργασίας των δεδομένων δεν τηρούνται, ο υπεύθυνος της επεξεργασίας είναι υποχρεωμένος να τα καταστρέψει. Όσον αφορά την ΑΠΔΠΧ, στην περίπτωση που διαπιστώσει είτε αυτεπάγγελτα είτε έπειτα από καταγγελία, την ύπαρξη ανάλογης παράβασης υποχρεούται να επιβάλλει παύση της επεξεργασίας τους αλλά και την καταστροφή των δεδομένων που έχουν υποστεί επεξεργασία (Αλεξανδροπούλου – Αιγυπτιάδου, 2007: 52 – 55).

### 3.2.2.5: Διασύνδεση αρχείων

Όσον αφορά τη διασύνδεση των αρχείων (data matching) που περιέχουν ευαίσθητα προσωπικά δεδομένα ή που η διασύνδεση αυτή μπορεί να αποκαλύψει

[16] Όπως έχει ήδη αναφερθεί, τα δεδομένα δεν θεωρούνται προσωπικά όταν ο τρόπος με τον οποίο τηρούνται είναι τέτοιος που δεν επιτρέπει την ταυτοποίηση του υποκειμένου τους είτε άμεσα είτε έμμεσα.

τέτοιου είδους δεδομένα, πρέπει να γίνει σχετική γνωστοποίηση στην ΑΠΔΠΧ, η οποία εν τέλει θα εκδώσει την άδεια διασύνδεσης η οποία μπορεί να ανανεωθεί έπειτα από αίτηση των υπεύθυνων επεξεργασίας και πρέπει να περιλαμβάνει το σκοπό της αναγκαιότητας της διασύνδεσης, το είδος των προσωπικών δεδομένων που αφορά η διασύνδεση, το χρονικό διάστημα για το οποίο επιτρέπεται η διασύνδεση, τους όρους και τις προϋποθέσεις για την αποτελεσματικότερη προστασία των δικαιωμάτων και των ελευθεριών (Ιγγλεζάκης, 2004: 74 και 264; Γέροντας, 2002: 214; Αλεξανδροπούλου – Αιγυπτιάδου, 2002: 35).

Η διασύνδεση των αρχείων παρέχει τη δυνατότητα συσχέτισης των αρχείων αυτών μεταξύ των συμβαλλόμενων μερών ή και τρίτων χωρών έπειτα από σχετική άδεια. Αν δηλαδή δεν ακολουθηθούν οι απαραίτητες διαδικασίες για τη διασύνδεση των αρχείων αυτών και αν δεν ληφθούν τα απαραίτητα μέτρα προστασίας, υπάρχει κίνδυνος να εκτεθούν – γνωστοποιηθούν σε άτομα που δεν πρέπει όπως για παράδειγμα να γίνει παραβίαση των αρχείων που διαβιβάζονται από hackers.

### 3.2.2.6: <u>Η διασυνοριακή ροή δεδομένων προσωπικού χαρακτήρα</u>

Η διασυνοριακή ροή των δεδομένων προσωπικού χαρακτήρα είναι ελεύθερη μέσα στις χώρες της ΕΕ. Όταν χρειάζεται να γίνει διαβίβαση σε χώρες μη Ευρωπαϊκές, γίνεται έπειτα από απόφαση της ΑΠΔΠΧ. Τα στοιχεία που λαμβάνονται υπόψη για την έκδοση της άδειας διαβίβασης αφορούν τη φύση των δεδομένων που πρόκειται να διαβιβασθούν, το σκοπό και τη διάρκεια της επεξεργασίας τους, τους σχετικούς γενικούς και ειδικούς κανόνες δικαίου, τους κώδικες δεοντολογίας, τα μέτρα ασφαλείας για την προστασία των δεδομένων προσωπικού χαρακτήρα, το επίπεδο προστασίας της χώρας προέλευσης των δεδομένων αυτών και το επίπεδο προστασίας της χώρας προς την οποία γίνεται η διαβίβαση. Έτσι, τα μέτρα που λαμβάνονται είναι αυστηρά και η διαβίβαση επιτυγχάνεται μόνο εφόσον η ΑΠΔΠΧ κρίνει ότι η συγκεκριμένη χώρα διατηρεί ένα ικανοποιητικό επίπεδο προστασίας ανάλογο με αυτό της χώρας από την οποία γίνεται η εκάστοτε διαβίβαση (Ιγγλεζάκης, 2004: 75; Αλεξανδροπούλου – Αιγυπτιάδου, 2002: 36; Γέροντας, 2002: 217).

Στην περίπτωση που η διαβίβαση των δεδομένων γίνεται προς χώρα που δεν ανήκει στην ΕΕ ενώ θεωρείται ότι δεν εξασφαλίζει ικανοποιητικό επίπεδο προστασίας των προσωπικών δεδομένων, η χώρα αποστολής των δεδομένων υποχρεούται να ενημερώσει σχετικά την Ευρωπαϊκή Επιτροπή και τις ΑΠΔΠΧ των

άλλων κρατών – μελών. Έτσι στην περίπτωση αυτή η διαβίβαση επιτυγχάνεται έπειτα από άδεια της ΑΠΔΠΧ ενώ παράλληλα λαμβάνονται υπόψη α) αν το υποκείμενο των δεδομένων έχει δώσει τη συγκατάθεση του, εκτός αν η συγκατάθεση του αποσπάσθηκε παράνομα, β) αν η διαβίβαση είναι απαραίτητη για τη διασφάλιση ζωτικού συμφέροντος του υποκειμένου των δεδομένων αν αυτό αδυνατεί να δώσει τη συγκατάθεση του για φυσικούς ή νομικούς λόγους, γ) η επίτευξη συμφωνίας ανάμεσα στο υποκείμενο των δεδομένων και τον υπεύθυνο της επεξεργασίας ή μεταξύ του υπεύθυνου της επεξεργασίας και τρίτου προς το συμφέρον του υποκειμένου των δεδομένων, εφόσον αυτό αδυνατεί φυσικά ή νομικά να δώσει τη συγκατάθεση του, δ) η εκτέλεση προσυμβατικών μέτρων που έχουν ληφθεί έπειτα από αίτημα του υποκειμένου των δεδομένων.

Η διαβίβαση των δεδομένων επιτρέπεται επίσης και για τη διαφύλαξη του δημόσιου συμφέροντος (π.χ. συμβάσεις συνεργασίας με δημόσιες αρχές άλλων χωρών) εφόσον η χώρα προς την οποία γίνεται η διαβίβαση εξασφαλίζει ικανοποιητικό επίπεδο προστασίας των προσωπικών δεδομένων και ελευθεριών αλλά και της ιδιωτικής ζωής γενικότερα, την αναγνώριση, άσκηση ή υπεράσπιση κάποιου δικαιώματος ενώπιον δικαστηρίου και τέλος, όταν το μητρώο από το οποίο προέρχονται τα δεδομένα είναι δημόσιο το οποίο γνωστοποιείται στο κοινό υπό κάποιες προϋποθέσεις (Αλεξανδροπούλου – Αιγυπτιάδου, 2002: 37; Γέροντας, 2002: 217).

### 3.2.3: <u>Τα δικαιώματα των υποκειμένων των προσωπικών δεδομένων</u>

Μία από τις βασικότερες αν όχι η βασικότερη προϋπόθεση για την επεξεργασία των προσωπικών δεδομένων ενός υποκειμένου, είναι η συγκατάθεση του ίδιου του υποκειμένου. Δηλαδή, σε κάθε επεξεργασία των προσωπικών δεδομένων πρέπει να αναγνωρίζεται μία σειρά δικαιωμάτων που αφορούν α) τη συγκατάθεση του υποκειμένου, β) το δικαίωμα της ενημέρωσης, γ) το δικαίωμα της πρόσβασης[17], δ) το δικαίωμα της αντίρρησης, ε) το δικαίωμα προσωρινής δικαστικής προστασίας, στ) το δικαίωμα της αίτησης υποβολής κυρώσεων.

[17] Τόσο το δικαίωμα της πρόσβασης όσο και το δικαίωμα της αντίρρησης είναι από τα θεμελιώδη δικαιώματα της προστασίας των προσωπικών δεδομένων και ταυτόχρονα θεσμικά κατοχυρωμένα.

Γενικά, τα υποκείμενα οφείλουν να γνωρίζουν ότι έχουν δικαιώματα σχετικά με τα προσωπικά δεδομένα τους. Για το λόγο αυτό, παρακάτω ακολουθεί μία εκτενής αναφορά στα δικαιώματα που έχουν τα υποκείμενα αναφορικά με την επεξεργασία των προσωπικών τους δεδομένων και ιδιαίτερα των ευαίσθητων.

### 3.2.3.1: <u>Η συγκατάθεση του υποκειμένου</u>

Σύμφωνα με το άρθρο 2ια του ν. 2472/1997 την έννοια της συγκατάθεσης του υποκειμένου των δεδομένων αποτελεί «κάθε ελεύθερη, ρητή και ειδική δήλωση βουλήσεως, που εκφράζεται με τρόπο σαφή και με την οποία το υποκείμενο των δεδομένων, αφού προηγουμένως ενημερωθεί, δέχεται να αποτελέσουν αντικείμενο επεξεργασίας τα προσωπικά δεδομένα που το αφορούν». Για να μπορέσει κάποιος να δώσει τη συγκατάθεση του για την επεξεργασία των προσωπικών του δεδομένων, βασική προϋπόθεση είναι α) να έχει ενημερωθεί για το σκοπό της επεξεργασίας των δεδομένων του, β) ποια από τα δεδομένα του θα αποτελέσουν αντικείμενο επεξεργασίας, γ) ποιοι θα είναι οι αποδέκτες των δεδομένων του, δ) το όνομα, την επωνυμία και τη διεύθυνση του υπεύθυνου επεξεργασίας ή του εκπροσώπου του (Αλεξανδροπούλου – Αιγυπτιάδου, 2007: 61).

Η συγκατάθεση του υποκειμένου των προσωπικών δεδομένων διακρίνεται α) στην ελεύθερη δηλαδή σε αυτήν που δεν αποσπάσθηκε με χρήση πλάνης, απάτης, απειλής, ανάγκης ή σχέσης εξάρτησης του υποκειμένου από τον υπεύθυνο επεξεργασίας, β) τη ρητή η οποία δίνεται με τον προφορικό λόγο, ένα έγγραφο, νεύματα ή χειρονομίες αρκεί να είναι εμφανής η συγκατάθεση του ατόμου και γ) την ειδική συγκατάθεση που αφορά μία συγκεκριμένη επεξεργασία όπου και τη νομιμοποιεί και συνδέεται με την ενημέρωση του υποκειμένου των δεδομένων από τον υπεύθυνο της επεξεργασίας. Στην περίπτωση που ο υπεύθυνος επεξεργασίας θέλει να χρησιμοποιήσει – να επεξεργαστεί τα δεδομένα αυτά για κάποιο άλλο σκοπό πρέπει να ενημερώσει εκ νέου το υποκείμενο των δεδομένων και να αποσπάσει εκ νέου τη συγκατάθεση του (Αλεξανδροπούλου – Αιγυπτιάδου, 2007: 58 – 60; Γεωργιάδης, 2002: 372).

Αναφορικά με τη συγκατάθεση του υποκειμένου των δεδομένων, όταν αυτά είναι απλά δεδομένα αρκεί απλά και μόνο η προφορική – ρητή συγκατάθεση του ενώ για τα ευαίσθητα προσωπικά δεδομένα απαιτείται η γραπτή συγκατάθεση του υποκειμένου τους. Επιπλέον, το υποκείμενο των δεδομένων έχει το δικαίωμα να

ανακαλέσει τη συγκατάθεση του όποτε το θελήσει ανεξάρτητα με το βαθμό επεξεργασίας που έχουν υποστεί. Όσον αφορά την επεξεργασία δεδομένων που αποκαλύπτουν «φυλετική ή εθνική καταγωγή, πολιτικές απόψεις, θρησκευτικές πεποιθήσεις, φιλοσοφικές ή ηθικές αντιλήψεις … (ή) αφορούν την υγεία ή τη σεξουαλική ζωή» περιορίζεται αυστηρά και τις περισσότερες φορές απαγορεύεται χωρίς τη γραπτή άδεια του υποκειμένου των δεδομένων (Αλεξανδροπούλου – Αιγυπτιάδου, 2007: 37; Gormley, 1997: 37; Stamatellos: 35).

Υπάρχουν όμως και περιπτώσεις όπου για την επεξεργασία τόσο των απλών όσο και των ευαίσθητων προσωπικών δεδομένων δεν είναι απαραίτητη η συγκατάθεση του υποκειμένου των δεδομένων αυτών όπως π.χ. α) όταν η επεξεργασία είναι απαραίτητη «για την εκτέλεση σύμβασης μέλος της οποίας είναι το υποκείμενο των δεδομένων (π.χ. το μισθοδοτικό σύστημα των εργαζομένων, το διαχειριστικό σύστημα των ιδιοκτητών διαμερισμάτων μιας πολυκατοικίας)…, β) την εκπλήρωση υποχρέωσης του υπεύθυνου επεξεργασίας που επιβάλλεται από το νόμο (π.χ. η επεξεργασία δεδομένων πελατών από έμπορο για έκδοση ΦΠΑ στη ΔΟΥ)…, γ) τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου ή αν αδυνατεί να δώσει τη συγκατάθεση του για φυσικούς ή νομικούς λόγους…, δ) την εκτέλεση έργου δημόσιου συμφέροντος (π.χ. φόρος εισοδήματος ακινήτων) ή έργου σχετικού με την άσκηση της δημόσιας εξουσίας…, ε) την επίτευξη του σκοπού του υπεύθυνου επεξεργασίας υπό την προϋπόθεση ότι αυτός υπερέχει των δικαιωμάτων και συμφερόντων των προσώπων στα οποία αναφέρονται τα δεδομένα χωρίς να θίγονται οι θεμελιώδεις ελευθερίες τους» (Αλεξανδροπούλου – Αιγυπτιάδου, 2007: 63 – 65).

Όσον για την επεξεργασία των ευαίσθητων προσωπικών δεδομένων όπου απαιτείται η γραπτή συγκατάθεση του υποκειμένου τους, υπάρχουν κάποιες εξαιρέσεις που εφαρμόζονται όταν η επεξεργασία είναι απαραίτητη για τη διαφύλαξη του ζωτικού συμφέροντος του υποκειμένου ή αν το υποκείμενο αδυνατεί να δώσει τη συγκατάθεση του όπως π.χ. η επεξεργασία των δεδομένων ενός τραυματία. Το ίδιο συμβαίνει και όταν αυτή αφορά δεδομένα που δημοσιοποιεί το ίδιο το υποκείμενο τους ή είναι αναγκαία για την αναγνώριση, άσκηση ή υπεράσπιση δικαιώματος ενώπιον δικαστηρίου ή πειθαρχικού οργάνου αρκεί η επεξεργασία να μη διεξήχθη παράνομα, όταν αφορά θέματα υγείας και εκτελείται από επαγγελματία στην παροχή υπηρεσιών υγείας που δεσμεύεται από το ιατρικό απόρρητο και άλλους κώδικες δεοντολογίας ενώ κρίνεται αναγκαία για την ιατρική πρόληψη, διάγνωση, περίθαλψη ή διαχείριση των υπηρεσιών υγείας.

Επίσης και όταν αυτή εκτελείται από δημόσια αρχή και είναι απαραίτητη για λόγους εθνικής ασφάλειας, την εξυπηρέτηση αναγκών εγκληματολογικής ή σωφρονιστικής πολιτικής σχετικά με τη διακρίβωση εγκλημάτων, ποινικές καταδίκες ή μέτρα ασφαλείας, για λόγους προστασίας της δημόσιας υγείας, την άσκηση δημόσιου φορολογικού ελέγχου ή δημόσιου ελέγχου κοινωνικών παροχών, ή όταν διεξάγεται για ερευνητικούς και επιστημονικούς σκοπούς, τηρείται η ανωνυμία και όλα τα μέτρα για την προστασία των προσώπων στα οποία αναφέρονται. Τέλος, συμβαίνει και με δεδομένα δημόσιων προσώπων που ασκούν δημόσιο λειτούργημα ή τη διαχείριση συμφερόντων τρίτων και πραγματοποιείται αποκλειστικά για την άσκηση του δημοσιογραφικού επαγγέλματος (Γέροντας, 2002: 204; Αλεξανδροπούλου – Αιγυπτιάδου, 2007: 66 – 68).

#### 3.2.3.2: <u>Το δικαίωμα της ενημέρωσης</u>

Το υποκείμενο των προσωπικών δεδομένων έχει το δικαίωμα να ενημερώνεται για θέματα που αφορούν την επεξεργασία των δεδομένων του. Συγκεκριμένα, πρέπει να ενημερώνεται για το σκοπό της συλλογής και επεξεργασίας των δεδομένων που το αφορούν, ποιος ή ποιοι θα είναι οι αποδέκτες των δεδομένων αυτών, αν θα γνωστοποιηθούν σε άλλο φορέα κτλ. Η ενημέρωση αυτή γίνεται ταυτόχρονα με τη συλλογή των δεδομένων στην περίπτωση που διεξάγεται άμεσα από το υποκείμενο των δεδομένων ενώ στην περίπτωση που γίνεται από άλλες πηγές, πραγματοποιείται μετά την καταχώρηση τους και πριν από την οποιαδήποτε άλλη χρήση ή επεξεργασία. Ένας τρόπος ενημέρωσης είναι η δημοσίευση σε δύο από τις εφημερίδες ευρείας κυκλοφορίας της πρωτεύουσας η μία εκ των οποίων είναι καθημερινής κυκλοφορίας και η άλλη κυριακάτικη. Όταν για την επεξεργασία των δεδομένων ενός υποκειμένου δεν απαιτείται η συγκατάθεση του, «η ενημέρωση μπορεί να γίνει με ανάρτηση προειδοποιητικής πινακίδας στο χώρο της συναλλαγής, διάθεσης έντυπου υλικού, αναγραφής σε λογαριασμούς ή τιμολόγια, αναγραφής σε έντυπο αιτήσεων ή ερωτηματολόγιο όπου το υποκείμενο καλείται να το συμπληρώσει ενώ υπάρχει σχετική ευδιάκριτη και σαφής σήμανση, στο διαδίκτυο με ευδιάκριτη σήμανση στην αρχική σελίδα της ιστοσελίδας» (Γέροντας, 2002: 223 – 225).

Στην περίπτωση που το υποκείμενο διαφωνεί σχετικά με την επεξεργασία των δεδομένων του ή προβάλλει κάποια αντίρρηση σχετικά με αυτήν, έχει τη δυνατότητα να υποβάλει σχετικό αίτημα στην ΑΠΔΠΧ όπου θα ζητά τη διόρθωση, την

προσωρινή παύση της χρήσης τους, τη δέσμευση, τη μη διαβίβαση ή ακόμη και τη διαγραφή τους. Εντός δεκαπέντε ημερών λαμβάνει απάντηση από τον υπεύθυνο της επεξεργασίας όπου το υποκείμενο των δεδομένων ενημερώνεται για τις ενέργειες στις οποίες προέβη ή για τους λόγους που δεν ικανοποίησε το αίτημα του. Αν απορριφθούν οι αντιρρήσεις του υποκειμένου, ο υπεύθυνος επεξεργασίας πρέπει να κάνει και την ανάλογη γνωστοποίηση στην ΑΠΔΠΧ.

Ακόμη, το υποκείμενο των δεδομένων μπορεί να προσφύγει στην ΑΠΔΠΧ αν η απάντηση του υπεύθυνου επεξεργασίας δεν είναι εμπρόθεσμη ή ικανοποιητική για να εξεταστεί αν οι αντιρρήσεις του ευσταθούν. Αν η ΑΠΔΠΧ[18] κρίνει ότι οι αντιρρήσεις του ευσταθούν, έχει το δικαίωμα να διατάξει άμεση αναστολή της επεξεργασίας των δεδομένων μέχρι να ληφθεί οριστική απόφαση (Ιγγλεζάκης, 2004: 79; Αλεξανδροπούλου – Αιγυπτιάδου, 2002: 38; Γέροντας, 2002: 222).

#### 3.2.3.3: <u>Το δικαίωμα της πρόσβασης</u>

Στο άρθρο 12 του ν. 2472/1997 κατοχυρώνεται το δικαίωμα τη πρόσβασης του υποκειμένου στα δεδομένα που το αφορούν. Αν το υποκείμενο των δεδομένων το ζητήσει, ο υπεύθυνος της επεξεργασίας πρέπει να το ενημερώσει γραπτά με σαφή και εύληπτο τρόπο για όλα τα δεδομένα που το αφορούν, την προέλευση τους, τους σκοπούς της επεξεργασίας τους, ποιοι είναι οι αποδέκτες τους, αν έχουν υποστεί επεξεργασία και μέχρι ποιο στάδιο έχει φτάσει κτλ (Γέροντας, 2002: 232; Ιγγλεζάκης, 2004: 80; Αλεξανδροπούλου – Αιγυπτιάδου, 2002: 38).

Το αίτημα αυτό υποβάλλεται στον υπεύθυνο της επεξεργασίας και καταβάλλεται κάποιο χρηματικό ποσό που ορίζεται από την ΑΠΔΠΧ το οποίο επιστρέφεται στο υποκείμενο είτε από τον υπεύθυνο της επεξεργασίας είτε από την ΑΠΔΠΧ στην περίπτωση που αυτό είχε προσφύγει σε αυτή αν κριθεί ότι το αίτημα διόρθωσης ή διαγραφής είναι βάσιμο. Αν ο υπεύθυνος της επεξεργασίας δεν δώσει έγκαιρα την απάντηση του (εντός δεκαπέντε ημερών) ή αν η απάντηση του δεν είναι

[18] Ανάμεσα στα μητρώα που τηρεί η ΑΠΔΠΧ, είναι και το μητρώο όπου καταγράφονται όλα τα υποκείμενα που δήλωσαν σε αυτή την αντίρρηση σχετικά με την επεξεργασία των δεδομένων τους για διαφημιστικούς λόγους, λόγους προώθησης πωλήσεων αγαθών ή παροχών υπηρεσιών εξ αποστάσεων. Το μητρώο αυτό πρέπει να συμβουλεύονται οι υπεύθυνοι επεξεργασίας για να μην επεξεργάζονται τα δεδομένα των συγκεκριμένων προσώπων και να διαγράφουν όσα στοιχεία τους αφορούν (www.dpa.gr).

ικανοποιητική, το υποκείμενο των δεδομένων μπορεί να προσφύγει στην ΑΠΔΠΧ. Αν πάλι για κάποιο λόγο ο υπεύθυνος της επεξεργασίας αρνηθεί να ανταποκριθεί στο αίτημα του υποκειμένου των δεδομένων, είναι υποχρεωμένος να κάνει την ανάλογη γνωστοποίηση στην ΑΠΔΠΧ ενημερώνοντας το ότι πρέπει να προσφύγει σε αυτήν. Στην περίπτωση της αίτησης της διόρθωσης των δεδομένων του υποκειμένου, ο υπεύθυνος της επεξεργασίας είναι υποχρεωμένος αφού προβεί στη σχετική διόρθωση, να δώσει σχετικό αντίγραφο στο υποκείμενο αυτό (Αλεξανδροπούλου – Αιγυπτιάδου, 2002: 39; Ιγγλεζάκης, 2004: 80; Γέροντας, 2002: 232).

#### 3.2.3.4: <u>Το δικαίωμα της αντίρρησης</u>

Σύμφωνα με το άρθρο 13 του ν. 2472/1997 το υποκείμενο των δεδομένων έχει το «δικαίωμα να προβάλλει αντιρρήσεις σε σχέση με τα δεδομένα που το αφορούν και την επεξεργασία τους». Έτσι, αρχικά υποβάλλει γραπτή αίτηση στον υπεύθυνο επεξεργασίας για διόρθωση, προσωρινή μη χρησιμοποίηση, δέσμευση, μη διαβίβαση ή διαγραφή των δεδομένων. Ο υπεύθυνος επεξεργασίας μέσα σε δεκαπέντε μέρες οφείλει να ενημερώσει το υποκείμενο για τις ενέργειες στις οποίες έχει προβεί και αν αρνηθεί να ικανοποιήσει το αίτημα του, τους λόγους μη ικανοποίησης του ενώ ταυτόχρονα πρέπει να υποβάλλει γνωστοποίηση στην ΑΠΔΠΧ. Μετά το πέρας των δεκαπέντε ημερών και εφόσον δεν έχει δοθεί απάντηση στο υποκείμενο των δεδομένων, αυτό έχει το δικαίωμα να προσφύγει στην ΑΠΔΠΧ για να εξεταστούν οι αντιρρήσεις του που αν ευσταθούν, διατάσσει την παύση της επεξεργασίας τους μέχρι την έκδοση οριστικής απόφασης (Ιγγλεζάκης, 2004: 80; Γέροντας, 2002: 232; Αλεξανδροπούλου – Αιγυπτιάδου, 2002: 39).

#### 3.2.3.5: <u>Το δικαίωμα της προσωρινής δικαστικής προστασίας</u>

Στο άρθρο 13 του ν. 2472/1997 περιγράφεται το δικαίωμα του ατόμου για προσωρινή δικαστική προστασία. Έτσι, «καθένας έχει το δικαίωμα να ζητήσει από το αρμόδιο δικαστήριο την άμεση αναστολή, μη εφαρμογή πράξης ή απόφασης που θεωρεί ότι τον θίγει και έχει εκδοθεί από δημόσια αρχή, νομικό πρόσωπο δημοσίου ή ιδιωτικού δικαίου, ένωση προσώπων ή φυσικό πρόσωπο…» (Αλεξανδροπούλου – Αιγυπτιάδου, 2007: 98).

Αυτό αναφέρεται κυρίως σε αποφάσεις σχετικές με την αυτοματοποιημένη επεξεργασία στοιχείων που έχει σαν στόχο την αξιολόγηση της προσωπικότητας του, την αποδοτικότητα στην εργασία του, την οικονομική φερεγγυότητα, την αξιοπιστία και γενικά τη συμπεριφορά του (Γέροντας, 2002: 234; Αλεξανδροπούλου – Αιγυπτιάδου, 2002: 40; Ιγγλεζάκης, 2004: 81 και 272).

### 3.2.3.6: <u>Το δικαίωμα του πληροφοριακού αυτοκαθορισμού</u>

Το δικαίωμα του πληροφοριακού καθορισμού αναφέρεται στη δυνατότητα του ατόμου να αποφασίζει και να συμπροσδιορίζει πότε και υπό ποιες προϋποθέσεις είναι δυνατή η επεξεργασία των πληροφοριών που το αφορούν. Δηλαδή καθένας έχει το δικαίωμα να γνωρίζει ποιος, που, πότε και για ποιο σκοπό υποβάλλει σε επεξεργασία τα προσωπικά του δεδομένα. Το δικαίωμα αυτό βρίσκεται σε άμεση συνάρτηση με το συνταγματικά κατοχυρωμένο δικαίωμα της ελεύθερης ανάπτυξης της προσωπικότητας του ατόμου και με αυτό της προστασίας της ανθρώπινης αξιοπρέπειας (Δόνος, 2004: 26).

Επίσης, η έννοια του αυτοκαθορισμού προϋποθέτει ότι το άτομο είναι ελεύθερο να λαμβάνει αποφάσεις σχετικά με το τι θα κάνει, τι θα παραλείψει ενώ του δίνει το δικαίωμα να δρα με τρόπο σύμφωνο με την απόφαση του. Σύμφωνα με τον Ιγγλεζάκη, το δικαίωμα το πληροφοριακού αυτοκαθορισμού έχει μία έντονη κοινωνική διάσταση μιας και δεν περιορίζεται απλά και μόνο στην ύπαρξη και διασφάλιση ενός χώρου όπου το άτομο αναπτύσσει την προσωπικότητα του. Θεωρείται ότι πρέπει να ενισχύεται το συμμετοχικό δικαίωμα του πολίτη, η επικοινωνία του ατόμου με τους άλλους έτσι ώστε να μπορέσει να λειτουργήσει μια ελεύθερη και δημοκρατική κοινωνία με αποτέλεσμα το δικαίωμα για την προστασία των προσωπικών δεδομένων γίνεται επιτακτικότερο. Πρέπει να υπάρχει σεβασμός προς το δικαίωμα αυτό, και προστασία του ενώ συγχρόνως πρέπει να διασφαλίζεται η άσκηση του. Έτσι, το δικαίωμα του πληροφοριακού αυτοκαθορισμού μπορεί να περιορίζεται σε περιπτώσεις όπου το γενικό συμφέρον υπερτερεί του ιδιωτικού συμφέροντος (Ιγγλεζάκης, 2004: 51 – 54).

Η νομιμοποίηση της επεξεργασίας των προσωπικών και των ευαίσθητων προσωπικών δεδομένων μέσω της συγκατάθεσης του υποκειμένου τους και της άσκησης των λοιπών δικαιωμάτων του αποτελεί το περιεχόμενο του πληροφοριακού αυτοκαθορισμού, από τη στιγμή που το άτομο «καθορίζει το ίδιο το επιθυμητό

περιεχόμενο της προστατευόμενης ιδιωτικότητας του καθώς και τον τρόπο που προσδιορίζεται πληροφοριακά στις επικοινωνιακές του σχέσεις» (Δόνος, 2004: 27).

Όμως υπάρχει ένα πρόβλημα αναφορικά με τον πληροφοριακό αυτοκαθορισμό. Αφενός η ΕΕ ορίζει ότι είναι δικαίωμα του ατόμου να καθορίζει πότε, ποιες προσωπικές του πληροφορίες και για ποιο σκοπό θα γνωστοποιηθούν και για ποιο σκοπό θα χρησιμοποιηθούν. Αφετέρου, είναι δύσκολο από μέρους του ατόμου η διεκδίκηση του δικαιώματος αυτού αφού πολλές φορές είναι δύσκολο να έρθει σε αντιπαράθεση με τους θεσμούς και το κράτος.

### 3.3: Οι κατευθυντήριες γραμμές – οδηγίες της Ε.Ε

Σύμφωνα με τις οδηγίες της ΕΕ κάθε κράτος – μέλος έχει την υποχρέωση μέσω της εθνικής του νομοθεσίας να παρέχει προστασία ενάντια στην παράνομη επεξεργασία των δεδομένων επιβάλλοντας «αποτρεπτικές» ποινές για τη μη συμμόρφωση με τους εθνικούς νόμους που υιοθετήθηκαν σύμφωνα με τις οδηγίες της ΕΕ. Ορίζεται ακόμη η απαγόρευση της διαβίβασης σε κράτη μη μέλη της ΕΕ που δεν παρέχουν ικανοποιητικό επίπεδο προστασίας αντίστοιχο με εκείνο της Σύμβασης 108 του Συμβουλίου της Ευρώπης (Ιγγλεζάκης, 2004: 27; Αλεξανδροπούλου – Αιγυπτιάδου, 2007: 126 – 128; Gormley, 1997: 37 – 41).

Ακολουθούν συνοπτικά οι νομοθετικές ρυθμίσεις της ΕΕ αναφορικά με την προστασία των προσωπικών δεδομένων.

#### 3.3.1: Η Σύμβαση 108/1981 του Συμβουλίου της Ευρώπης

Η Σύμβαση 108/1981 του Συμβουλίου της Ευρώπης αποτελεί το πρώτο κείμενο που νομοθετήθηκε με αντικείμενο «την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα».

Στη σύμβαση αυτή α) τέθηκαν οι κατευθυντήριες γραμμές για την προστασία του ατόμου από την αθέμιτη επεξεργασία των προσωπικών δεδομένων από τη χρήση ηλεκτρονικών μέσων, β) θεσπίστηκαν κανόνες για την προστασία των δεδομένων αυτών στην περίπτωση της διασυνοριακής ροής πληροφοριών, γ) ορίστηκαν ειδικές κατηγορίες δεδομένων που δεν αποτελούν αντικείμενο αυτοματοποιημένης επεξεργασίας αν το εθνικό δίκαιο μιας χώρας δεν προσφέρει τις κατάλληλες

εγγυήσεις, δ) αποδίδονται δικαιώματα στα υποκείμενα των δεδομένων, ε) καθορίζεται η δημιουργία της Αρχής για τον έλεγχο της εφαρμογής της σύμβασης αυτής.

Η σύμβαση 108 κυρώθηκε από τη χώρα μας με το Ν. 2068/1992 (ΦΕΚ Α΄ 118/9.7.1992) «Κύρωση της Ευρωπαϊκής Σύμβασης για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα». Όμως μέχρι τη θέσπιση του Ν. 2472/1997 δεν υιοθετήθηκαν στο εσωτερικό δίκαιο ειδικές ρυθμίσεις για την προστασία των προσωπικών δεδομένων (Αλεξανδροπούλου – Αιγυπτιάδου, 2007: 125; Ιγγλεζάκης, 2004: 25; Μήτρου, 2004: 456).

### 3.3.2: Η Οδηγία 95/46/ΕΚ

Η Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας προσωπικών δεδομένων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών» ψηφίστηκε στις 24.10.1995 με βασικό στόχο την προσέγγιση και την εναρμόνιση του δικαίων των κρατών – μελών της ΕΕ για την προστασία των φυσικών προσώπων από την επεξεργασία των προσωπικών τους δεδομένων και την ελεύθερη κυκλοφορία των δεδομένων για την εγκαθίδρυση και λειτουργία της Εσωτερικής Αγοράς (Αλεξανδροπούλου – Αιγυπτιάδου, 2007: 129 – 130; Καλαντζής, 1996: 325).

Στόχος της Οδηγίας αυτής είναι η καλύτερη προστασία των προσωπικών δεδομένων των ατόμων με σεβασμό στις διαφορές και τις ιδιαιτερότητες καθενός από τα συμβαλλόμενα μέρη. Βάσει αυτής: α) οριοθετείται η νομιμότητα της επεξεργασίας (αρχή της νομιμότητας), β) τίθενται οι ποιοτικές προδιαγραφές επεξεργασίας των δεδομένων, γ) κατοχυρώνεται η αρχή του σκοπού της επεξεργασίας, η αρχή της διαφάνειας ως προς το βαθμό και τον τρόπο συλλογής και επεξεργασίας των δεδομένων και δ) ενδυναμώνεται η θέση των υποκειμένων των δεδομένων με δικαιώματα (Blume, 2003: 454).

### 3.3.3: Η Οδηγία 97/66/ΕΚ

Η Οδηγία 97/66/ΕΚ του Ευρωπαϊκού Κοινοβουλίου ψηφίστηκε στις 15.12.1997 και ορίζει τα περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τομέα των τηλεπικοινωνιών λόγω της χρήσης προηγμένης τεχνολογίας στα δημόσια τηλεπικοινωνιακά δίκτυα.

Στοχεύει στην «εναρμόνιση των διατάξεων των κρατών μελών οι οποίες απαιτούνται προκειμένου να διασφαλίζεται ισοδύναμο επίπεδο προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών, ιδίως δε το δικαίωμα στην ιδιωτική ζωή όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα, καθώς και στην ελεύθερη κυκλοφορία των δεδομένων αυτών και των τηλεπικοινωνιακών εξοπλισμών και υπηρεσιών στην Κοινότητα».

Η ανάγκη για τη θέσπιση και την εφαρμογή της οδηγίας αυτήν προέκυψε με την εμφάνιση των ψηφιακών δικτύων (ISDN) και των υπηρεσιών αναγνώρισης και προώθησης κλήσεων και ρυθμίζει ζητήματα όπως αυτά της ασφάλειας των δεδομένων, του απορρήτου των επικοινωνιών, των δεδομένων κίνησης και χρέωσης, της αναλυτικής χρέωσης, της αναγραφής της ταυτότητας της καλούσας/ συνδεδεμένης γραμμής, της αυτόματης προώθησης κλήσεων, των τηλεφωνικών καταλόγων των συνδρομητών καθώς και το πρόβλημα των αυτόματων συστημάτων κλήσης για εμπορικούς σκοπούς. Και αυτό για τα δημόσια τηλεπικοινωνιακά δίκτυα. Επίσης θέτει τις κατευθυντήριες γραμμές για την ίδρυση των ΑΠΔΠΧ (Μήτρου, 2006: 9 – 10).

Η ελληνική νομοθεσία προσαρμόστηκε στην Οδηγία αυτή με το Ν. 2774/1999 για την «Προστασία των δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα» (ΦΕΚ Α΄ 287/22.12.1999).

### 3.3.4: <u>Ο Κανονισμός 45/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 18.12.2000</u>

Ο κανονισμός 45/2001 του Ευρωπαϊκού Κοινοβουλίου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας προσωπικών δεδομένων από όργανα και οργανισμούς της Κοινότητας και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών ψηφίστηκε στις 18.12.2000 και αποτελεί απόρροια της Οδηγίας 95/46/ΕΚ.

Σκοπός του είναι «η τήρηση από τα όργανα και τους οργανισμούς της κοινότητας των κανόνων προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών των προσώπων, καθώς και η ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα μεταξύ των κρατών – μελών και των οργάνων και οργανισμών της Κοινότητας ή μεταξύ των οργάνων και οργανισμών της Κοινότητας στο πλαίσιο της άσκησης των αρμοδιοτήτων τους». Τέλος, μέσω κανονισμού αυτού εισάγεται η

ανεξάρτητη αρχή του Ευρωπαίου Επόπτη Προστασίας Δεδομένων που στοχεύει στην εποπτεία της νόμιμης επεξεργασίας των προσωπικών δεδομένων από τα όργανα και τους οργανισμούς της ΕΕ (Αλεξανδροπούλου – Αιγυπτιάδου, 2007: 130 – 131; Λουκέρης, 1997: 555).

### 3.3.5: Η Οδηγία 2002/58/ΕΚ

Η Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της Ευρώπης για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών ψηφίστηκε στις 12.7.2002 για να καταργήσει και να αντικαταστήσει την Οδηγία 97/66/ΕΚ εξαιτίας της αναγκαιότητας της προσαρμογής των υπηρεσιών ηλεκτρονικών επικοινωνιών στις νέες εξελίξεις των αγορών και των τεχνολογιών. Είναι συμπληρωματική ως προς την Οδηγία 95/46/ΕΚ αλλά και εξειδίκευση της ενώ παράλληλα παρέχει προστασία στα έννομα συμφέροντα των συνδρομητών που είναι νομικά πρόσωπα.

Στοχεύει στην «παροχή ισοδύναμου επιπέδου προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής σε όλους τους χρήστες των υπηρεσιών επικοινωνιών διαθέσιμων στο κοινό ανεξάρτητα από τις χρησιμοποιούμενες τεχνολογίες και ορίζει ότι η συλλογή δεδομένων μέσω λογισμικών παρακολούθησης, δικτυακών κοριών (web bugs) αποτελεί ενδεχόμενη παραβίαση της ιδιωτικής ζωής του ατόμου» (Αλεξανδροπούλου – Αιγυπτιάδου, 2007: 131 – 132).

### 3.3.6: Η Σύσταση R(99) 5 της Επιτροπής Υπουργών του Συμβουλίου της Ευρώπης

Η Σύσταση R (99) 5 της Επιτροπής των Υπουργών του Συμβουλίου της 12.7.2002 για την προστασία της ιδιωτικότητας στο διαδίκτυο θεωρεί ότι «η τεχνολογική ανάπτυξη και η γενίκευση της συλλογής και της επεξεργασίας των προσωπικών δεδομένων στις λεωφόρους επικοινωνίας εγκυμονεί κινδύνους για την ιδιωτικότητα του ατόμου ενώ αναγνωρίζει ότι οι επικοινωνίες που διεξάγονται μέσω των νέων τεχνολογιών οφείλουν να σέβονται τα ανθρώπινα δικαιώματα και τις θεμελιώδεις ελευθερίες και συγκεκριμένα το δικαίωμα στην ιδιωτικότητα και το απόρρητο της αλληλογραφίας, σύμφωνα με το άρθρο 8 της Ευρωπαϊκής Συνθήκης

για τα ανθρώπινα δικαιώματα και συστήνει την ευρεία διασπορά των κατευθυντήριων γραμμών που περιέχονται στο παράρτημα της». Οι κατευθυντήριες αυτές γραμμές αφορούν τους χρήστες αλλά και τους παροχείς υπηρεσιών διαδικτύου και περιγράφουν τις αρχές της ορθής πρακτικής σε σχέση με την ιδιωτικότητα και μπορούν να ενσωματωθούν ή να προσαρτηθούν σε κώδικες συμπεριφοράς (Καστανάς, 2001: 722; Αλεξανδροπούλου – Αιγυπτιάδου, 2007: 130).

Το σημαντικό στη συγκεκριμένη σύσταση είναι ότι εισάγει την εφαρμογή των βασικών αρχών προστασίας των προσωπικών δεδομένων στο χώρο του διαδικτύου με απώτερο στόχο την επέκταση της νομοθετικής ρύθμισης στις λεωφόρους των πληροφοριών (Καραγιάννης, 2000: 19; Κυριακόπουλος: 777; Αλεξανδροπούλου – Αιγυπτιάδου, 2007: 130).

### 3.3.7: Η Συνθήκη Σένγκεν

Η Συνθήκη του Σένγκεν (ΣΣ) υπεγράφη στις 14 Ιουνίου 1985 στην πόλη Σένγκεν του Λουξεμβούργου από τη Γαλλία, τη Γερμανία, το Βέλγιο, τις Κάτω χώρες και το Λουξεμβούργο[19]. Το 1990 υπεγράφη και από τα υπόλοιπα συμβαλλόμενα μέρη ενώ η Ελλάδα επικύρωσε τη συνθήκη αυτή και τη Σύμβαση Εφαρμογής της με το νόμο 2514/1997 (ΦΕΚ Α΄ 140/26 – 27.6.1997).

Αρχικός στόχος της ΣΣ ήταν η σταδιακή εξάλειψη των ελέγχων στα εσωτερικά σύνορα δηλαδή τα κοινά χερσαία σύνορα των χωρών – μελών καθώς επίσης και τα αεροδρόμια προκειμένου περί των εσωτερικών πτήσεων και τα θαλάσσια λιμάνια προκειμένου περί των κανονικών συνδέσεων πλοίων μεταφόρτωσης που προέρχονται ή κατευθύνονται αποκλειστικώς σε άλλο λιμάνι στο έδαφος των συμβαλλόμενων μερών χωρίς να προσεγγίζουν λιμάνια εκτός των εδαφών αυτών και κατ' επέκταση η εξασφάλιση της ελεύθερης διακίνησης προσώπων, κεφαλαίων, αγαθών και υπηρεσιών αλλά και η πάταξη του οργανωμένου εγκλήματος, μία συμφωνία που αργότερα ενστερνίστηκε και η ΕΕ.

[19] Η Σύμβαση Σένγκεν είναι μία συμφωνία που συνάφθηκε αρχικά μεταξύ Βελγίου, Γερμανίας, Γαλλίας, Λουξεμβούργου και Ολλανδίας για τη σταδιακή κατάργηση των ελέγχων στα μεταξύ τους σύνορα η οποία υπεγράφη από τα παραπάνω κράτη στις 14/6/1985 ενώ ενσωματώθηκε στη Συνθήκη για την Ενιαία Ευρωπαϊκή Πράξη της ΕΕ. Πήρε το όνομα της από την ομώνυμη πόλη Σένγκεν του Λουξεμβούργου. Στη συνέχεια επικυρώθηκε και από άλλες χώρες, την Ιταλία το 1990, την Ισπανία και την Πορτογαλία το 1991, την Ελλάδα το 1992, την Αυστρία το 1995, τη Σουηδία, τη Φιλανδία και τη Δανία το 1996, τη Νορβηγία και την Ισλανδία το 1999.

Έτσι, παράλληλα περιφρουρούνται τα εξωτερικά σύνορα των χωρών αυτών δηλαδή, τα χερσαία και θαλάσσια σύνορα καθώς επίσης και τα αεροδρόμια και τα θαλάσσια λιμάνια των συμβαλλόμενων μερών εφόσον δεν αποτελούν εσωτερικά σύνορα ή/και το άθροισμα των εξωτερικών συνόρων των κρατών – μελών προς τρίτες χώρες μη μέλη της ΕΕ με αποτέλεσμα να καθίσταται αδύνατο να προσπελαθούν.

Αυτό σημαίνει όλοι οι πολίτες των κρατών – μελών έχουν τη δυνατότητα να ταξιδεύουν στις χώρες αυτές χωρίς να έχουν κάποιο ταξιδιωτικό έντυπο – διαβατήριο επιδεικνύοντας μόνο την αστυνομική τους ταυτότητα. Για τους μη ευρωπαίους πολίτες που θέλουν να ταξιδέψουν σε κάποια από τις χώρες αυτές παράλληλα με το εισιτήριο τους εκδίδεται μία βίζα η οποία ισχύει για όλες τις χώρες για τρεις μήνες ενώ όσοι ζητούν άσυλο, υποβάλλουν σχετικό αίτημα σε κάποια χώρα όπου είτε το αίτημα γίνει αποδεκτό είτε όχι, η απόφαση είναι δεσμευτική για όλες τις χώρες της ζώνης Σένγκεν (Συνθήκη Σένγκεν, 1995: 9-11; Σαματάς, 2000: 2, 6-7; Samatas, 2004: 73; Wiener, 1999: 2).

Απόρροια της συμφωνίας αυτής ήταν η δημιουργία του Πληροφοριακού Συστήματος Σένγκεν Schenghen Information System (SIS)[20] βασικό αντικείμενο του οποίου είναι η προστασία της δημόσιας τάξης και ασφάλειας, συμπεριλαμβανομένης και της κρατικής ασφάλειας, αλλά και η εφαρμογή των διατάξεων της ΣΣ για την κυκλοφορία των προσώπων στην επικράτεια των συμβαλλόμενων μερών χρησιμοποιώντας πληροφορίες που διαβιβάζονται μέσω του συστήματος αυτού.

Το SIS είναι βασίζεται σ' ένα κεντρικό ηλεκτρονικό υπολογιστή εγκατεστημένο στο Στρασβούργο και ένα δίκτυο από εθνικά παραρτήματα σε κάθε χώρα – μέλος που αυτά σε συνδυασμό έχουν σαν αποτέλεσμα τη δημιουργία μιας βάσης δεδομένων καταγραφής δεδομένων. Τα κράτη – μέλη διαθέτουν ένα δίκτυο γραφείων (SIRENE) για την παροχή συμπληρωματικών πληροφοριών στα σημεία εθνικών εισόδων αλλά και το σύστημα VISION για την ανταλλαγή πληροφοριών για τη χορήγηση θεωρήσεων σε υπηκόους τρίτων χωρών στις οποίες τα κράτη Σένγκεν έχουν επιβάλλει καθεστώς διαβουλεύσεων (Παπακωνσταντής, 1998: 47-57, Περάκης, 2001: 396-397; Σαματάς, 2000: 9, Samatas, 2004: 77).

Ουσιαστικά, το SIS είναι το «φακέλωμα» σε ηλεκτρονική μορφή, η καταχώρηση σε βάσεις δεδομένων α) καταζητούμενων ατόμων έπειτα από αίτηση δικαστικής αρχής που μπορεί να συλληφθούν αν αυτό προβλέπεται στη νομοθεσία

[20] Ρυθμίζεται βάσει των άρθρων 92 – 101.

του κράτους που δέχεται την αίτηση, β) αλλοδαπών ατόμων στα οποία απαγορεύεται η είσοδος βάσει δικαστικής απόφασης, γ) εξαφανισμένων και αναζητούμενων προσώπων, δ) προσώπων που εμπλέκονται σε ποινικές υποθέσεις και κλητεύονται ως μάρτυρες ή κατηγορούμενοι και ε) ατόμων που παρακολουθούνται βάσει του άρθρου 99 (Αλεξανδροπούλου – Αιγυπτιάδου, 2007: 126 – 128; Ιγγλεζάκης, 2004: 27; Σαματάς, 2003: 9; Samatas, 2004: 78).

Οι πληροφορίες που συλλέγονται για τα άτομα αυτά είναι α) το ονοματεπώνυμο ενώ ενδεχόμενα συναφή στοιχεία καταγράφονται ξεχωριστά, β) τα ιδιαίτερα και αναλλοίωτα φυσικά χαρακτηριστικά, γ) το πρώτο γράμμα του δεύτερου ονόματος, δ) η ημερομηνία και ο τόπος γέννησης, ε) το φύλο, στ) η ιθαγένεια, ζ) η ένδειξη ότι τα υπόψη πρόσωπα είναι οπλισμένα, η) η ένδειξη ότι τα υπόψη πρόσωπα είναι βίαια, θ) ο λόγος της σήμανσης, ι) η στάση που ενδείκνυται να τηρηθεί.

Στο πλαίσιο της «διακριτικής παρακολούθησης» μπορούν να συλλεχθούν και να διαβιβαστούν πληροφορίες εν όλω ή εν μέρει στην αρχή που έχει προβεί στη σήμανση, μέσω μεθοριακών ή άλλων αστυνομικών και τελωνειακών ελέγχων που πραγματοποιούνται στο εσωτερικό της χώρας που αφορούν α) την εύρεση καταχωρημένου ατόμου ή οχήματος, β) ο τόπος, η ώρα ή ο λόγος ελέγχου, γ) το δρομολόγιο και ο προορισμός του ταξιδιού, δ) οι συνοδοί του ενδιαφερόμενου ή οι συνεπιβάτες του οχήματος, ε) το χρησιμοποιούμενο όχημα, στ) τα μεταφερόμενα αντικείμενα και ζ) οι συνθήκες εύρεσης του προσώπου ή του οχήματος (Συνθήκη Σένγκεν, 1995: 14-15; Samatas, 2004: 78-79).

Καταχωρούνται και οι αξιόποινες πράξεις για τις οποίες όχι μόνο υπάρχει «αμοιβαία συνδρομή» μεταξύ των αστυνομικών υπηρεσιών των συμβαλλόμενων, ενώ δίνεται και η δυνατότητα να παρακολουθηθεί και να κυνηγηθεί ο «ύποπτος» πέραν των συνόρων, με την προϋπόθεση ότι θα ανακοινωθεί στην ενδιαφερόμενη χώρα και θα υπάρξει αίτηση δικαστικής συνδρομής που θα «εκθέτει τους λόγους[21] που αιτιολογούν τη διέλευση των συνόρων χωρίς προηγούμενη εξουσιοδότηση» (Συνθήκη Σένγκεν, 1995: 14-15; Samatas, 2004: 78-79).

[21] Λόγοι όπως δολοφονία, φόνος, βιασμός, εμπρησμός, παραχάραξη, διακεκριμένη κλοπή και κλεπταποδοχή, εκβιασμός, απαγωγή και ομηρία, δουλεμπόριο, παράνομη διακίνηση ναρκωτικών και ψυχότροπων ουσιών, παράβαση των διατάξεων ως προς όλα τα όπλα και τα εκρηκτικά, καταστροφές δι' εκρηκτικών, παράνομη μεταφορά τοξικών και βλαβερών αποβλήτων, αδίκημα φυγής κατόπιν δυστυχήματος που προκάλεσε θάνατο ή σοβαρούς τραυματισμούς.

### 3.3.7.1: <u>Στόχοι – κοινωνικές επιπτώσεις του SIS</u>

Η λειτουργία και η οργάνωση του SIS βασίζεται στη δημιουργία ενιαίας αγοράς και την αντιμετώπιση του οργανωμένου εγκλήματος στο πλαίσιο της ΕΕ (Σαματάς, 2000: 8). Έτσι, η ΕΕ μετατρέπεται σε «φρούριο» για την προστασία κυρίως από μετανάστες και πρόσφυγες που προέρχονται από Τριτοκοσμικές χώρες (Samatas, 2004: 74 - 77). Δηλαδή, η παράνομη μετανάστευση θεωρείται ως απειλή για την ασφάλεια των χωρών – μελών της ΕΕ ώστε να δίνεται ιδιαίτερη έμφαση στη φύλαξη των συνόρων και την είσοδο μη Ευρωπαίων αλλοδαπών (Σαματάς, 2000: 8-9; Huysmans, 1995; Guerra, 1997: 7).

Ουσιαστικά ποινικοποιείται η παράνομη μετανάστευση αφού αποτελεί την κύρια αιτία από την οποία πλήττεται η ασφάλεια της Ευρωζώνης με αποτέλεσμα να αντιμετωπίζεται ως τέτοια και να μην αναζητούνται τρόποι εξάλειψης των αιτιών ύπαρξης της. Θεωρείται και αντιμετωπίζεται δηλαδή ως οργανωμένο έγκλημα όπως αυτό της εμπορίας και διακίνησης ναρκωτικών, όπλων και ανθρώπων (trafficking) ιδιαίτερα γυναικών.

Παράλληλα, εξαιτίας της φύσης της οργάνωσης του SIS, έρχονται στην επιφάνεια και προβλήματα που σχετίζονται με τη μαζική παρακολούθηση και την παραβίαση των ατομικών δικαιωμάτων και ελευθεριών αφού οι νόμοι για την προστασία της ιδιωτικότητας μπορούν να παραβιαστούν με τη χρήση της συγκεκριμένης βάσης δεδομένων[22].

Προκειμένου να μπορέσει να εισέλθει κάποιος μη Ευρωπαίος αλλοδαπός σε χώρα της ζώνης Σένγκεν πρέπει να διαθέτει τα απαραίτητα ταξιδιωτικά έγγραφα και την ειδική βίζα Σένγκεν. Τον έλεγχο των εγγράφων αυτών αναλαμβάνουν οι εκάστοτε αεροπορικές εταιρείες που υποχρεούται να έχουν προσωπικό που να ασχολείται αποκλειστικά με το συγκεκριμένο αντικείμενο.

Σύμφωνα μάλιστα με το άρθρο 27 της ΣΣ, στην περίπτωση που οι επισκέπτες των χωρών της ζώνης Σένγκεν δεν διαθέτουν τα απαραίτητα ταξιδιωτικά έγγραφα και τη βίζα, επιβάλλονται κυρώσεις π.χ. στις αεροπορικές εταιρείες οι οποίες υποχρεούται βάσει του νόμου να τους επιστρέψουν - απελάσουν στη χώρα προέλευσης τους ή σε «ασφαλείς τρίτες χώρες» πράγμα που πολλές φορές συνεπάγεται και την κακομεταχείριση τους κατά τη διάρκεια της απέλασης.

[22] Χαρακτηριστικό είναι το παράδειγμα της δράσης της EUROPOL.

Όταν απαγορεύεται σε κάποιον η είσοδος σε μία από τις χώρες της ζώνης Σένγκεν με την πρόφαση ότι υπάρχει κίνδυνος για τη δημόσια ή την εθνική ασφάλεια, αυτόματα κλείνουν οι πόρτες και για τις άλλες χώρες της ζώνης, καλλιεργώντας έτσι το συναίσθημα της ξενοφοβίας, τον κοινωνικό αποκλεισμό, το ρατσισμό και γενικότερα διακρίσεις σε διάφορα επίπεδα (Σαματάς, 2000: 20).

Απόρροια αυτού είναι η μείωση των αιτήσεων χορήγησης ασύλου από μη Ευρωπαίους πολίτες[23] ενώ ουσιαστικά καταργείται το δικαίωμα αίτησης πολιτικού ασύλου πολιτών της ΕΕ προς άλλες χώρες της Ευρωζώνης. Αυτά στη χώρα μας λαμβάνουν ακόμα μεγαλύτερες διαστάσεις εξαιτίας των κατάλοιπων που υπάρχουν από την περίοδο της δικτατορίας, της ξενοφοβίας, του αναπτυγμένου αισθήματος φόβου και καχυποψίας, του φακελώματος και του χαφιεδισμού αλλά και της ανάγκης προστασίας από κάποια εξωτερική απειλή (Σαματάς, 2003: 11 - 13; Samatas, 2004: 88 – 89).

Το SIS λειτουργεί βάσει του πατροπαράδοτου γραφειοκρατικού συστήματος που έχει εκσυγχρονιστεί με τη βοήθεια των νέων τεχνολογιών γενικά και των ηλεκτρονικών υπολογιστών και του διαδικτύου ειδικότερα. Όσοι έχουν συμφέροντα και χάνουν προνόμια με την εφαρμογή του και την κατάργηση των συνόρων και τη μείωση των εξουσιών του έθνους – κράτους, π.χ. συνοριακοί φύλακες, τελωνιακοί, αστυνομικοί, δικαστικοί κτλ, προσπαθούν με τη βοήθεια των νέων τεχνολογιών και της βιομηχανίας της ασφάλειας να ανακτήσουν δύναμη σε ευρωπαϊκό επίπεδο.

Ουσιαστικά το SIS αποτελεί μία νέα μορφή αστυνόμευσης σε πανευρωπαϊκό επίπεδο για την πάταξη της τρομοκρατίας και του διεθνούς οργανωμένου εγκλήματος μιας και τα άτομα και τα στοιχεία που εκχωρεί κάθε χώρα – μέλος στο Εθνικό Σύστημα Σένγκεν ελέγχονται και μπορούν να γνωστοποιηθούν τόσο στα άλλα Εθνικά Συστήματα όσο και στο Κεντρικό Σύστημα Σένγκεν στο Στρασβούργο.

Άλλωστε αυτό αποτελεί υποχρέωση κάθε χώρας – μέλους της ζώνης Σένγκεν καθώς «υποχρεούται να παρακολουθεί, να καταρτίζει και να κοινοποιεί με ηλεκτρονικό τρόπο τις λίστες με τα σχετικά ονόματα ή ψευδώνυμα ατόμων στις υπόλοιπες χώρες – μέλη, δεσμεύοντας έτσι τα άλλα μέλη να παρακολουθούν, να επιτηρούν ή να ελέγχουν τα συγκεκριμένα άτομα όταν βρεθούν στην επικράτεια τους». Όμως η νομιμοποίηση της εφαρμογής του συστήματος αυτού επέρχεται με την

[23] Στη χώρα μας η μείωση αυτή οφείλεται στην όλη διαδικασία αποθάρρυνσης και μη αποδοχής των αιτήσεων, στις κακές συνθήκες διαβίωσης στα κέντρα υποδοχής προσφύγων και στην ανυπαρξία πολιτικών για την ενσωμάτωση τους με αποτέλεσμα να αντιμετωπίζονται ως λαθρομετανάστες.

ενσωμάτωση του όχι μόνο στη νομοθεσία αλλά και στην αποδοχή των ευρωπαίων πολιτών της ζώνης Σένγκεν (Σαματάς, 2000: 19 - 21).

### 3.3.8: Η Συνθήκη Πρυμ (Σένγκεν ΙΙΙ)

Η συνθήκη Πρυμ είναι ουσιαστικά επέκταση της ΣΣ γι' αυτό θεωρείται ως Σένγκεν ΙΙΙ. Υπεγράφη στις 27.5.2005 στο Πρυμ της Γερμανίας απ' όπου και πήρε το όνομα της από τη Γερμανία, την Ισπανία, τη Γαλλία, το Λουξεμβούργο, την Ολλανδία, την Αυστρία και το Βέλγιο ενώ στις 15.2.2007 συμφωνήθηκε η ένταξη της στη νομοθεσία της ΕΕ στο Συμβούλιο των Υπουργών Δικαιοσύνης και Εσωτερικών Υποθέσεων της ΕΕ στις Βρυξέλλες.

Βασικός της στόχος είναι η ακόμα μεγαλύτερη ενδυνάμωση και η επιτάχυνση της ανταλλαγής πληροφοριών μεταξύ των επτά συμβαλλόμενων κρατών. Ουσιαστικά συμφωνήθηκε η ενσωμάτωση στη νομοθεσία της ΕΕ των άρθρων της Συνθήκης Πρυμ που σχετίζονται με την αστυνομική και δικαστική συνεργασία σε θέματα αντεγκληματικής πολιτικής (Τίτλος VI της ΣυνθΕΕ/ «τρίτος πυλώνας») με την εξαίρεση της διάταξης που αναφέρεται στην εκτός συνόρων αστυνομική παρέμβαση σε περίπτωση επικείμενου κινδύνου (άρθρο 18) καθώς και σε θέματα μεταναστευτικής πολιτικής.

Είναι σημαντική γιατί προβλέπει: α) τη δημιουργία από τα συμβαλλόμενα κράτη βάσεων δεδομένων γενετικών πληροφοριών (DNA) (βιοτραπεζών) και δακτυλικών αποτυπωμάτων, β) τη λήψη μέτρων για την πρόληψη τρομοκρατικών ενεργειών, γ) τη λήψη μέτρων για την καταπολέμηση της παράνομης μετανάστευσης, δ) την προστασία των δεδομένων και άλλες μορφές διακρατικής συνεργασίας.

Ουσιαστικά, με βάση το πρόταγμα της καταπολέμησης της τρομοκρατίας ιδίως μετά την 11$^{η}$ Σεπτεμβρίου αλλά και της παράνομης μετανάστευσης, καταπατώνται θεμελιώδη ανθρώπινα δικαιώματα καθώς α) αντιστρέφεται το τεκμήριο της αθωότητας καθιστώντας όλους τους ευρωπαίους πολίτες εν δυνάμει υπόπτους, β) τα ευαίσθητα προσωπικά δεδομένα και πληροφορίες (δακτυλικά αποτυπώματα, γενετικό υλικό) θα είναι προσβάσιμα από όλα τα συμβαλλόμενα κράτη – μέλη για την πρόληψη τρομοκρατικών ενεργειών και γ) νομιμοποιούνται «μαύρες λίστες» με στοιχεία διαδηλωτών και οι πληροφορίες διατίθενται σε όλα τα κράτη – μέλη με πρόφαση την πρόληψη κινδύνων που απειλούν τη δημόσια τάξη και ασφάλεια (www.mfhr.gr).

Έτσι το ηλεκτρονικό ευρωπαϊκό φακέλωμα λαμβάνει νέες διαστάσεις, καταγράφοντας ακόμη και τα ευαίσθητα βιογενετικά δεδομένα του ατόμου στα οποία μπορούν να έχουν πρόσβαση όλα τα κράτη – μέλη.

### 3.4: Συμπερασματικές παρατηρήσεις

Η νομοθεσία της ΕΕ που παρατέθηκε προηγουμένως δίνει τις κατευθυντήριες γραμμές σε όλα τα κράτη – μέλη για τη θέσπιση νομοθετικών ρυθμίσεων για την προστασία των προσωπικών και των ευαίσθητων προσωπικών δεδομένων.

Παρατηρούμε ότι κοινό χαρακτηριστικό των νόμων για την προστασία των προσωπικών δεδομένων αποτελεί το γεγονός ότι: α) εφαρμόζονται τόσο στον ιδιωτικό όσο και στο δημόσιο τομέα, β) εφαρμόζονται σε ένα μεγάλο εύρος δραστηριοτήτων συμπεριλαμβανομένης της συλλογής, της χρήσης και της διάδοσης των δεδομένων, γ) επιβάλλουν συγκεκριμένες υποχρεώσεις (υποχρεώσεις των φορέων συλλογής και επεξεργασίας δεδομένων και δικαιώματα των υποκειμένων των δεδομένων) σε οποιονδήποτε επιθυμεί να εμπλακεί σε οποιαδήποτε από τις προαναφερθείσες δραστηριότητες και δ) έχουν ελάχιστους περιορισμούς και εφαρμόζονται χωρίς να λαμβάνουν υπόψη το υποκείμενο των δεδομένων (Gormley, 1997: 32 – 33). Όμως υπάρχει πρόβλημα όσον αφορά την άσκηση του δικαιώματος του «πληροφοριακού αυτοκαθορισμού» αφού η ΕΕ το αναγνωρίζει ως δικαίωμα που εξαρτάται από τη βούληση του ατόμου ενώ υπάρχει πρόβλημα άσκησής του, αφού το άτομο τις περισσότερες φορές αδυνατεί να το εφαρμόσει ερχόμενο αντιμέτωπο με το κράτος, θεσμούς και άλλους ιδιωτικούς φορείς.

Παρόλα αυτά η ΕΕ θέτει τις κατευθυντήριες γραμμές προς τις οποίες πρέπει να κινηθεί η νομοθεσία κάθε κράτους – μέλους αφήνοντας σε καθεμιά από αυτές το περιθώριο να προσαρμόσει τη νομοθεσία για την προστασία των προσωπικών δεδομένων στην κουλτούρα της. Επίσης η ΕΕ επέβαλε τη δημιουργία ΑΠΔΠΧ στα κράτη – μέλη της. Όπως αναφέρουμε στο επόμενο κεφάλαιο, η χώρα μας έχει προσαρμόσει το εθνικό της δίκαιο σύμφωνα με τις επιταγές της ΕΕ. Το παραπάνω νομοθετικό πλαίσιο – τόσο το ευρωπαϊκό όσο και το ελληνικό – παρέχει επαρκείς εγγυήσεις για την προστασία των προσωπικών και των ευαίσθητων προσωπικών δεδομένων. Έτσι εξαρτάται από το πόσο σθεναρά κάθε κράτος – μέλος να επιβάλλει την εφαρμογή της σχετικής νομοθεσίας.

Τα ερωτήματα λοιπόν που πρέπει να μας απασχολούν σχετικά με τη συλλογή και την επεξεργασία των προσωπικών μας δεδομένων είναι (www.dpa.gr; Stamatellos, xx: 34):

- Ποιος είναι ο υπεύθυνος για τη συλλογή των δεδομένων; Με ποια μέθοδο συλλέχθηκαν; Χαρακτηρίζεται η μέθοδος αυτή από διαφάνεια και νομιμότητα σε σχέση με το δικαίωμα του ατόμου στην ιδιωτικότητα;
- Είναι ακριβής και επαληθευμένη η αποθήκευση των δεδομένων; Πόσο συχνά εκσυγχρονίζονται, ελέγχονται και διορθώνονται τα δεδομένα;
- Μπορούν τα άτομα να έχουν πρόσβαση στα προσωπικά τους δεδομένα; Μπορούν να αλλάζουν και να διορθώνουν τα δεδομένα τους; Τα δεδομένα γνωστοποιούνται σε άλλες ομάδες ή άτομα, όπως ιδιώτες ή μη κυβερνητικές οργανώσεις; Πληροφορούνται τα άτομα για τη χρήση των δεδομένων τους; Ποιος ελέγχει την πρόσβαση στα προσωπικά δεδομένα;
- Είναι ασφαλή τα δεδομένα έναντι μη εξουσιοδοτημένης πρόσβασης και χρήσης; Πόσο ασφαλείς είναι οι διαδικασίες ασφάλειας των δεδομένων; Ενημερώνονται τα άτομα για τις διαδικασίες αυτές; Προστατεύονται τα δικαιώματα των ατόμων σύμφωνα με το νόμο; Ποια είναι τα δικαιώματα των ατόμων στην περίπτωση παραβίασης της ασφάλειας;

Ο ρόλος της κάθε εθνικής ΑΠΔΠΧ είναι καθοριστικός για τα παραπάνω και γι' αυτό αναφερόμαστε εκτενώς σε αυτό παρακάτω.

# ΚΕΦΑΛΑΙΟ 4$^{Ο}$
# Η ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΚΑΙ ΤΩΝ ΕΥΑΙΣΘΗΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΗΝ ΕΛΛΑΔΑ

## 4.1: Η παρακολούθηση στην Ελλάδα

Η παρακολούθηση στην Ελλάδα καθ' όλη τη μετ' εμφυλιοπολεμική περίοδο αποτελούσε αποκλειστικό προνόμιο του αστυνομικού κράτους για την άσκηση του κοινωνικοπολιτικού ελέγχου και βασίζονταν κυρίως στην άμεση ανθρώπινη παρακολούθηση και τη συνεργασία της αστυνομίας και των κρατικών υπηρεσιών με πληροφοριοδότες ανά τη χώρα και στη γραφειοκρατική καταγραφή σε φακέλους των προσωπικών πληροφοριών. Βασικός σκοπός του φακελώματος ήταν η καταγραφή της πολιτικής ιδεολογίας και συμπεριφοράς όλων των Ελλήνων πολιτών και η συμμόρφωση τους στο αυταρχικό αντικομμουνιστικό καθεστώς, καθορίζοντας δρώντας καταλυτικά τον αποκλεισμό ή την ένταξη τους στις ευκαιρίες ζωής και στη διανομή των δημόσιων αγαθών (Samatas, 2004).

Όμως μεταδικτατορικά και ιδίως τώρα στις αρχές του 21$^{ου}$ αιώνα τόσο στην Ελλάδα όσο και σε άλλες χώρες εκσυγχρονίστηκαν στο πλαίσιο του πληροφοριακού καπιταλισμού και του ηλεκτρονικού πανοπτισμού όπου οι άνθρωποι αποτελούν αντικείμενο παρακολούθησης σε διάφορες πτυχές της καθημερινότητας τους. Πλέον το «φακέλωμα» είναι ηλεκτρονικό και όχι μόνο από το κράτος, δηλαδή η παρακολούθηση και η αρχειοπαρακολούθηση ειδικότερα επιτυγχάνεται μέσω ηλεκτρονικών βάσεων δεδομένων ενώ δεν αποτελεί πια κρατικό μονοπώλιο, αφού σε αυτήν εμπλέκονται υπερκρατικοί οργανισμοί, ιδιώτες και επιχειρήσεις για διάφορους σκοπούς, π.χ. μάρκετινγκ, κ.ά.

Χαρακτηριστικό είναι το παράδειγμα της βάσης δεδομένων δακτυλικών αποτυπωμάτων της ελληνικής αστυνομίας, δηλαδή το Αυτόματο Σύστημα Αναγνώρισης Δακτυλικών Αποτυπωμάτων (ΑΣΑΔΑ) το οποίο είναι συνδεδεμένο με το Εθνικό Σύστημα Πληροφοριών Σένγκεν (Senghen Information System – SIS), την EUROPOL κτλ, όπου συλλέγονται βιομετρικά και γενετικά δεδομένα ύποπτων πολιτών, αλλά και μεταναστών, χούλιγκανς, αναρχικών, κτλ. Το σύστημα αυτό νομιμοποιήθηκε έπειτα από το γεγονότα της 11$^{ης}$ Σεπτεμβρίου και την πάταξη της τοπικής τρομοκρατίας, δηλαδή τη σύλληψη των μελών της 17 Νοέμβρη το 2003, όταν ψηφίστηκε ο αποκαλούμενος «τρομονόμος» προτάσσοντας την ασφάλεια έναντι

των ατομικών ελευθεριών, ενθαρρύνοντας την κατασκοπεία των πολιτών, δίνοντας χρηματικά κίνητρα στους πληροφοριοδότες της αστυνομίας ενώ προωθείται η διεξαγωγή δικών χωρίς ενόρκους, θέτοντας δρακόντιες ποινές σε μέλη εγκληματικών συμμοριών κτλ. Επιπλέον η λήψη DNA και οι τράπεζες DNA για την ενδυνάμωση και την επιτάχυνση της ανταλλαγής πληροφοριών και ταυτοποίησης υπόπτων μεταξύ των συμβαλλόμενων χωρών της ζώνης Σένγκεν είναι πλέον γεγονός έπειτα από την υπογραφή της αποκαλούμενης Συνθήκης Πρύμ (Σένγκεν ΙΙΙ) (Samatas, 2004: 109 – 114, 149; Σαματάς, 2005: 499 - 502).

Η ελληνική νομοθεσία αναφορικά με τη συλλογή, την επεξεργασία και την προστασία των δεδομένων προσωπικού χαρακτήρα εκτός από όσα όριζε εξ αρχής βάσει του ελληνικού Συντάγματος έχει προσαρμοστεί σύμφωνα με τις επιταγές της ΕΕ. Έτσι για την προστασία των προσωπικών δεδομένων εφαρμόζονται α) το άρθρο $9^{A}$ του Συντάγματος 1975/86/2001, β) ο Ν. 2472/1997[24] (ΦΕΚ Α΄ 50, 1997) «για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα», γ) τα άρθρα 57 – 59 του Αστικού Κώδικα (ΑΚ) και δ) τα άρθρα 248 και $370^{A}$ του Ποινικού Κώδικα (ΠΚ) (Μήτρου, 2004: 470).

Ακολουθούν οι προβλέψεις του ελληνικού δικαίου για την προστασία των προσωπικών δεδομένων.

### 4.2: <u>Το Σύνταγμα της Ελλάδας</u>

Στην Ελλάδα η προστασία των προσωπικών δεδομένων είναι συνταγματικά κατοχυρωμένη. Έτσι, στην προστασία τους αναφέρονται (Κασιμάτης, 1995: 153):

- Το άρθρο 2 παράγραφος 1 του Συντάγματος που αφορά στο σεβασμό και την προστασία της αξίας του ανθρώπου ως πρωταρχική υποχρέωση της πολιτείας ενώ θεμελιώνεται η έννοια της προσωπικότητας και η προστασία της απέναντι σε κράτος και ιδιώτες (Δαγτόγλου, 1991: 1138). Ακόμη αξιώνει ο άνθρωπος να μην καθίσταται πληροφοριακό αντικείμενο και μέσο για την επίτευξη κάποιου σκοπού με αποτέλεσμα η καταγραφή των προσωπικών πληροφοριών για τον έλεγχο και τη χειραγώγηση του ανθρώπου αποτελεί προσβολή της

[24] Ο Ν. 2472/1997 τροποποιήθηκε με τους νόμους α) 2819/2000 (ΦΕΚ Α΄ 84), β) 2915.2001 (ΦΕΚ Α΄ 109), γ) 3051/2002 (ΦΕΚ Α΄ 220), δ) 3156/2003 (ΦΕΚ Α΄ 157), ε) 2774/99 και στ) επιμέρους οδηγίες της ΑΠΔΠΧ.

αξίας του ανθρώπου αλλά και της ελευθερίας του να μην προσδιορίζεται από άλλους (Μήτρου, 2001: 85).

- Το άρθρο 5 παράγραφος 1 του Συντάγματος που κατοχυρώνει το δικαίωμα ελεύθερης ανάπτυξης της προσωπικότητας του ατόμου και συμμετοχής του στην κοινωνική, οικονομική και πολιτική ζωή της χώρας ενώ περιλαμβάνει και το δικαίωμα της πληροφοριακής του αυτοδιάθεσης (Μάνεσης, 1982: 118; Μήτρου, 2001: 86; Δαγτόγλου, 1991: 1144).
- Το άρθρο $5^{A}$ που κατοχυρώνει το δικαίωμα στην πληροφόρηση[25] και τη συμμετοχή στην Κοινωνία της Πληροφορίας[26] (Δαγτόγλου, 1991: 405 και 432).
- Το άρθρο 9 παράγραφος 1 εδάφιο β΄ για την προστασία της ιδιωτικής[27] και οικογενειακής ζωής του ατόμου το οποίο αποτελεί προέκταση του δικαιώματος της ελεύθερης ανάπτυξης της προσωπικότητας και παρέχει προστασία στο άτομο ως ιδιώτη και όχι ως πολίτη (Χρυσογόνος, 2002: 236).
- Το άρθρο $9^{A}$ για την προστασία των προσωπικών δεδομένων πράγμα που δηλώνει την επίγνωση των κινδύνων που επιφέρουν οι νέες τεχνολογίες ενώ παράλληλα αναγνωρίζεται το δικαίωμα του ανθρώπου να περιορίζει τη χρήση των δεδομένων που τον αφορούν ως προϋπόθεση για την ελεύθερη ανάπτυξη και δράση του μέσα σε μια κοινωνία βασικό χαρακτηριστικό της οποίας αποτελεί η ραγδαία τεχνολογική εξέλιξη. Προστατεύεται ο ιδιωτικός βίος τόσο ως κοινωνική ιδιότητα όσο και ως μέρος για την άσκηση των πολιτικών και κοινωνικών δικαιωμάτων του ατόμου (Γέροντας, 2002: 93; Μήτρου, 2001: 85 και 90).
- Το άρθρο 13 παράγραφος 1 εδάφιο α΄ για την προστασία της ελευθερίας της θρησκευτικής συνείδησης και της ελευθερίας της λατρείας που αποτελούν βασικό στοιχείο της προσωπικότητας του ατόμου και επιδέχεται προστασίας ως ευαίσθητο προσωπικό δεδομένο (Κοτζάμπασης, 2000: 256).

---

[25] Αυτό συνδέεται και με το δικαίωμα της ελεύθερης έκφρασης βασική προϋπόθεση του οποίου αποτελεί η συλλογή πληροφοριών. Στο άρθρο αυτό δηλαδή κατοχυρώνεται η ελευθερία του «πληροφορείν» και του «πληροφορείσθαι».

[26] Στην εποχή μας με την ανάπτυξη των νέων τεχνολογιών, η κατοχύρωση του δικαιώματος στην πληροφόρηση αποτελεί απαραίτητη προϋπόθεση για τη διαμόρφωση της έκφρασης και της γνώμης αλλά και για τη συμμετοχή στα κοινωνικά, πολιτικά και οικονομικά δρώμενα της χώρας μας (Χρυσογόνος, 2002: 196).

[27] Η έννοια της ιδιωτικής ζωής ποικίλει ανάλογα με το πολιτιστικό και κοινωνικό πλαίσιο στο οποίο αναφέρεται.

- Το άρθρο 19 για την προστασία του απορρήτου των επικοινωνιών και της ελεύθερης ανταπόκρισης και επικοινωνίας[28] που συνδέεται με το δικαίωμα του ατόμου να μην αποκαλύπτει στοιχεία της προσωπικότητας του (Χρυσογόνος, 2002: 238).
- Το άρθρο 25 που κατοχυρώνει την προστασία των ατομικών και κοινωνικών δικαιωμάτων και απαγορεύει την καταχρηστική τους άσκηση ενώ παράλληλα κατοχυρώνεται συνταγματικά η ανεξάρτητη Αρχή για τη διασφάλιση του δικαιώματος αυτού (Μήτρου, 2001: 98).
- Το άρθρο $101^{A}$ για τη θέσπιση της ΑΠΔΠΧ, του τρόπου συγκρότησης και λειτουργίας τους εισάγοντας νέες εγγυήσεις για την προστασία των δικαιωμάτων σκοπός των οποίων είναι η προστασία των προσωπικών δεδομένων. Η ΑΠΔΠΧ χαρακτηρίζεται ως ανεξάρτητη αφού οι περιορισμοί στις αρμοδιότητες της θα σήμαιναν μειωμένη αποτελεσματικότητα στην προστασία των δικαιωμάτων αυτών (Μήτρου, 2001: 101).

### 4.3: <u>Ο Ν. 2472/1997</u>

Ο Ν. 2472/1997 αφορά την προστασία του ατόμου από την επεξεργασία των προσωπικών δεδομένων ενσωματώνοντας την Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου η θέσπιση του οποίου αποτελούσε βασική προϋπόθεση για την ένταξη της χώρας μας στο SIS. Σκοπός του είναι η παροχή προστασίας των δικαιωμάτων και των ελευθεριών του ατόμου και της ιδιωτικής του ζωής από την επεξεργασία δεδομένων προσωπικού χαρακτήρα ρυθμίζοντας τις προϋποθέσεις της και η προστασία του δικαιώματος του πληροφοριακού αυτοκαθορισμού (Αλεξανδροπούλου – Αιγυπτιάδου, 2002: 24; Γέροντας, Α., 2002: 178; Μίττλετον, 2001: 751; Νούσκαλης, 2007: 71).

Βάσει αυτού διαμορφώνονται, στηρίζονται και κατοχυρώνονται α) οι ουσιαστικές και τυπικές προϋποθέσεις για την επεξεργασία των προσωπικών δεδομένων, β) τα δικαιώματα του υποκειμένου των δεδομένων, γ) οι εγγυήσεις για την προστασία του υποκειμένου των δεδομένων και δ) ο έλεγχος της επεξεργασίας των δεδομένων αυτών με την ίδρυση της ΑΠΔΠΧ.

[28] Η ανάγκη για την προστασία του δικαιώματος αυτού γίνεται επιτακτικότερη εξαιτίας του γεγονότος της τεχνολογικής εξέλιξης στον τομέα των τηλεπικοινωνιών. Έτσι, απόρροια της αναγκαιότητας αυτής ήταν η θέσπιση του ν. 2774/1999 (ΦΕΚ Α΄ 287/22.12.1999).

Δίνεται ένας ευρύς ορισμός της έννοιας των προσωπικών δεδομένων, της επεξεργασίας των δεδομένων αυτών και της έννοιας του αρχείου περιλαμβάνοντας όλα τα είδη επεξεργασίας (δημόσια ή μη, αυτοματοποιημένη ή μη) ενώ ταυτόχρονα τα προσωπικά δεδομένα διακρίνονται σε απλά και ευαίσθητα προσωπικά δεδομένα.

Βασικός σκοπός του είναι η προστασία του ατόμου από την αθέμιτη συλλογή και επεξεργασία των προσωπικών του δεδομένων και η διασφάλιση της χρήσης της πληροφορικής «τόσο από το δημόσιο όσο και από ιδιώτες» για την επιδίωξη των σκοπών που η έννομη τάξη προστατεύει και σε ορισμένες περιπτώσεις ευνοεί (Κριάρη – Κατράνη, 1999: 55).

Έτσι, πρέπει να γνωστοποιείται κάθε επεξεργασία ή αρχείο[29] που τηρείται για ορισμένες επεξεργασίες και ιδιαίτερα τα αρχεία που περιλαμβάνουν ευαίσθητα προσωπικά δεδομένα επιβάλλοντας κυρώσεις (διοικητικές, ποινικές, αστικές κυρώσεις) κατά περίπτωση ενώ είναι οδηγός για την ίδρυση της ΑΠΔΠΧ (Αλεξανδροπούλου – Αιγυπτιάδου, 2002: 25; Γέροντας, 2002: 177).

### 4.4: <u>Ο Αστικός κώδικας</u>

Επιπλέον αναφορά για την προστασία των προσωπικών και των ευαίσθητων προσωπικών δεδομένων γίνεται και στον ΑΚ και ειδικότερα στο άρθρο 57 που προστατεύει την προσωπικότητα του ατόμου από κάθε είδους προσβολές. Με τον όρο «προσωπικότητα» εννοεί όλα τα αγαθά που τη συγκροτούν και την προσδιορίζουν και αποτελούν εκδηλώσεις της αναπόσπαστα συνδεδεμένες με το πρόσωπο στο οποίο ανήκουν ως οντότητα φυσική, βιολογική, ψυχική, οικονομική, πολιτισμική, πολιτική, πνευματική και κοινωνική. Παρατηρούμε λοιπόν ότι η έννοια της προσωπικότητας βάσει του άρθρου αυτού είναι ιδιαίτερα ευρεία με αποτέλεσμα να προσφέρει κάλυψη και ενάντια στις προσβολές που μπορεί να προκύψουν εξαιτίας της ραγδαίας εξέλιξης της τεχνολογίας (Αγγελόπουλος, 2003: 56; Γέροντας, 2002: 98).

[29] Σύμφωνα με το Ν. 2472/1997 ως αρχείο δεδομένων προσωπικού χαρακτήρα ορίζεται το σύνολο των δεδομένων προσωπικού χαρακτήρα τα οποία αποτελούν ή μπορεί να αποτελέσουν αντικείμενο επεξεργασίας και τα οποία τηρούνται από το Δημόσιο ή από νομικό πρόσωπο δημοσίου ή ιδιωτικού δικαίου ή ένωση προσώπων ή φυσικό πρόσωπο. Έπειτα από τροποποίηση του παραπάνω ορισμού με το Ν. 3471/2006, ως αρχείο θεωρείται κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα τα οποία είναι προσιτά με γνώμονα συγκεκριμένα κριτήρια (Νούσκαλης, 2007: 59). Σύμφωνα μάλιστα με το Νούσκαλη (2007: 73) το αρχείο προσωπικών δεδομένων φαίνεται να λειτουργεί «ως το υλικό αντικείμενο των περιγραφόμενων πράξεων και η μονάδα μέτρησης του προσβαλλόμενου έννομου αγαθού του πληροφοριακού αυτοκαθορισμού ή του ιδιωτικού βίου».

Επιπλέον εισάγονται και προστατεύονται οι έννοιες α) του πληροφοριακού αυτοκαθορισμού, β) της προσβολής της προσωπικότητας, γ) της αξίωσης για άρση της προσβολής, δ) της αξίωσης για παράλειψη της προσβολής στο μέλλον, ε) της αξίωσης για αποζημίωση, στ) της αξίωσης για ικανοποίηση για ηθική βλάβη κτλ.

### 4.5: Συμπερασματικές παρατηρήσεις

Η παραπάνω παράθεση της ελληνικής νομοθεσίας για την προστασία των προσωπικών και των ευαίσθητων προσωπικών δεδομένων, δείχνει ότι το ελληνικό δίκαιο έχει ενσωματώσει τις σχετικές οδηγίες της ΕΕ προσαρμόζοντας τις στην κουλτούρα της χώρας μας, παρέχοντας επαρκείς εγγυήσεις για την προστασία τους. Παρόλα αυτά όμως υπάρχουν δυσκολίες στην εφαρμογή της. Προς την κατεύθυνση αυτή είναι που δουλεύει η ΑΠΔΠΧ με τον ανεξάρτητο χαρακτήρα της ασκώντας έλεγχο στους φορείς συλλογής και επεξεργασίας προσωπικών δεδομένων και επιβάλλοντας κυρώσεις κάθε φορά που διαπιστωθεί παραβίαση των δικαιωμάτων και προσωπικών δεδομένων.

Με βάση το ικανοποιητικό θεσμικό και νομοθετικό πλαίσιο αλλά και τη δράση της ΑΠΔΠΧ η Ελλάδα κατέλαβε την πρώτη θέση ως προς την προστασία των προσωπικών δεδομένων το 2007 σε συγκριτική έρευνα της EPIC και Privacy International (www.epic.org).

# ΚΕΦΑΛΑΙΟ 5$^{Ο}$
# ΟΙ ΑΠΟΦΑΣΕΙΣ ΤΗΣ ΕΛΛΗΝΙΚΗΣ ΑΡΧΗΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

## 5.1: Συνοπτικό προφίλ της Ελληνικής Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) (www.dpa.gr)

Η ΑΠΔΠΧ είναι μια συνταγματικά κατοχυρωμένη ανεξάρτητη Αρχή που αποτελεί απόρροια της λειτουργίας της ΣΣ και έχει σαν στόχο την προστασία των δικαιωμάτων της προσωπικότητας και της ιδιωτικής ζωής του ατόμου. Ρόλος της είναι η φροντίδα για την προστασία των προσωπικών δεδομένων και τη διασφάλιση της μη συλλογής και επεξεργασίας των ευαίσθητων προσωπικών δεδομένων (Cate, 1997: 408; Σαματάς, 2003: 18). Παρόλα αυτά, σύμφωνα με τη ΣΣ και το Ν. 2472/1997, επιτρέπεται η συλλογή και επεξεργασία ευαίσθητων προσωπικών δεδομένων για λόγους εθνικής ασφάλειας, άμυνας και δημόσιας τάξης.

Πρωταρχικός της στόχος είναι η προστασία του πολίτη από την παράνομη επεξεργασία των προσωπικών του δεδομένων αλλά και η συνδρομή προς αυτόν σε κάθε περίπτωση που διαπιστώνεται παραβίαση των σχετικών δικαιωμάτων του σε κάθε επιχειρησιακό τομέα (χρηματοπιστωτικά, υγεία, ασφάλιση, εκπαίδευση, δημόσια διοίκηση, μεταφορές, ΜΜΕ κτλ).

Μία από τις βασικές αρμοδιότητες της ΑΠΔΠΧ αποτελεί η έκδοση άδειας συλλογής και επεξεργασίας των ευαίσθητων δεδομένων και η έκδοση άδειας λειτουργίας σχετικού αρχείου έπειτα από αίτηση του υπεύθυνου επεξεργασίας. Ακόμη, για την επίτευξη του στόχου της που δεν είναι άλλος από την προστασία του δικαιώματος της προστασίας της ιδιωτικής ζωής, έχει τη δυνατότητα να επιβάλλει επιπλέον όρους και προϋποθέσεις (Κριάρη – Κατράνη, 1999: 57).

Τέλος, υποστηρίζει και καθοδηγεί τους υπεύθυνους επεξεργασίας στην εκπλήρωση των υποχρεώσεων τους απέναντι στο νόμο, λαμβάνοντας υπόψη τις νέες ανάγκες των υπηρεσιών της ελληνικής κοινωνίας, καθώς και την διείσδυση των σύγχρονων ψηφιακών επικοινωνιών και δικτύων στρέφοντας την προσοχή και στην παρατήρηση και αντιμετώπιση ζητημάτων που προκύπτουν με την εξέλιξη των νέων τεχνολογιών και εφαρμογών (www.dpa.gr).

### 5.2: Ενδεικτικές αποφάσεις της ΑΠΔΠΧ για την προστασία των ευαίσθητων προσωπικών δεδομένων

Η ΑΠΔΠΧ κατά καιρούς έχει εκδώσει αρκετές αποφάσεις για την προστασία των προσωπικών δεδομένων των ατόμων. Έπειτα από ανασκόπηση στις αποφάσεις της ΑΠΔΠΧ, επιλέχθηκαν κάποιες από αυτές που αφορούν τα ευαίσθητα προσωπικά δεδομένα (www.dpa.gr):

Με την απόφαση της ***15/5/2000*** η ΑΠΔΠΧ καλεί το Υπουργείο Δημόσιας Τάξης να αφαιρέσει από το νέο έντυπο των αστυνομικών ταυτοτήτων τα εξής στοιχεία: το δακτυλικό αποτύπωμα, το ονοματεπώνυμο συζύγου, το γένος, το επάγγελμα, τη διεύθυνση κατοικίας, την υπηκοότητα και το θρήσκευμα. Ιδιαίτερα η απόφαση για τη μη αναγραφή του θρησκεύματος είχε προκαλέσει την έντονη αντίδραση της Εκκλησίας. Παρόλα αυτά η μη αναγραφή του κρίθηκε σκόπιμη καθώς αυτό αναφέρεται στον εσωτερικό κόσμο του ατόμου με αποτέλεσμα να θεωρηθεί απρόσφορο και μη αναγκαίο για την εξατομίκευση της ταυτότητας του ατόμου. Κάτι ανάλογο συμβαίνει και με τη λήψη δακτυλικού αποτυπώματος που θεωρείται ότι υπερβαίνει το μέτρο και προσβάλλει την προστατευόμενη από το Σύνταγμα αξία του ανθρώπου. Αντί αυτού υπάρχει η φωτογραφία για την ταυτοποίηση του ατόμου.

Η απόφαση της ***26/9/2000*** αφορά την επεξεργασία προσωπικών δεδομένων μέσω CCTV όπου καταγράφονται οι προϋποθέσεις νομιμότητας της επεξεργασίας των προσωπικών δεδομένων μέσω κλειστών κυκλωμάτων CCTV αλλά και οι υποχρεώσεις του εκάστοτε υπεύθυνου επεξεργασίας τους.

Η απόφαση της ***13/11/2000*** αφορά καταγγελίες πολιτών σχετικά με τη διαδικασία αίτησης σύνδεσης σε δίκτυα κινητής τηλεφωνίας όπου οι εταιρείες απαιτούν την προσκόμιση φωτοαντιγράφων του εκκαθαριστικού της εφορίας, λογαριασμό ΔΕΗ – ΟΤΕ, πιστωτική κάρτα και ταυτότητα τα οποία παραμένουν στην κατοχή του φορέα παροχής τηλεπικοινωνιακών υπηρεσιών. Η ΑΠΔΠΧ αποφάνθηκε ότι η συλλογή των στοιχείων αυτών είναι αναγκαία και νόμιμη αφού η συλλογή, η τήρηση και η επεξεργασία τους γίνεται σύμφωνα με το ν. 2472/1997.

Η απόφαση της ***29/11/2000*** αναφέρεται στο στρατολογικό πιστοποιητικό τύπου Α΄ όπου η ΑΠΔΠΧ αποφάνθηκε ότι σε αυτό πρέπει να αναγράφονται μόνο η επιτυχής εκπλήρωσης των στρατιωτικών υποχρεώσεων κάποιου και σε περίπτωση απαλλαγής του, ότι απαλλάχθηκε νόμιμα χωρίς να αναγράφεται ο λόγος απαλλαγής. Έτσι αποφεύγεται ο στιγματισμός του ατόμου στην περίπτωση που αντιμετωπίζει

προβλήματα ψυχικής υγείας, εξαρτήσεων από αλκοόλ και ναρκωτικά, λόγω θρησκευτικών πεποιθήσεων, ομοφυλοφιλίας, των αντιρρησιών συνείδησης κτλ, με την έννοια ότι η αναγραφή τέτοιου είδους στοιχείων στο συγκεκριμένο πιστοποιητικό θα αποτελούσε ανασταλτικό παράγοντα σε διάφορες πτυχές της ζωής του όπως π.χ. για την ανεύρεση εργασίας καθώς κανένας δεν θα ήταν διατεθειμένος να προσλάβει στην επιχείρηση του κάποιο στιγματισμένο.

Στην απόφαση ***100/2000*** γίνεται αναφορά στη χρήση δεδομένων για την ερωτική ζωή του κ. Κορκολή και του κ. Ασλάνη μέσω βίντεο αλλά και προσωπικού ημερολογίου που παρουσιάστηκαν στις εκπομπές «Κίτρινος τύπος» και «Ζούγκλα» του κ. Τριανταφυλλόπουλου μέσω της τηλεόρασης του ALPHA. Η ΑΠΔΠΧ έκρινε παράνομη την κατοχή, καταχώρηση σε αρχείο και τηλεοπτική χρήση των ευαίσθητων προσωπικών δεδομένων των παραπάνω ατόμων. Διέταξε τη διακοπή της επεξεργασίας και την καταστροφή των δεδομένων των ατόμων αυτών τόσο από τον ALPHA όσο και από την εταιρεία «Ε. ΤΡΙΑΝΤΑΦΥΛΛΟΠΟΥΛΟΣ και ΣΙΑ Ε.Ε.» αλλά και την επιστροφή στον κο Ασλάνη του προσωπικού ημερολογίου του και την καταστροφή οποιουδήποτε αντιγράφου του. Τέλος, επέβαλλε πρόστιμο είκοσι πέντε εκατομμύρια δραχμές (25.000.000) στην εταιρεία «Ε. ΤΡΙΑΝΤΑΦΥΛΛΟΠΟΥΛΟΣ και ΣΙΑ Ε.Ε.» και δέκα εκατομμύρια δραχμές (10.000.000) στον ALPHA για παράνομη επεξεργασία και τηλεοπτική χρήση ευαίσθητων δεδομένων στις παραπάνω εκπομπές.

Σύμφωνα με την οδηγία ***1122/2000*** της ΑΠΔΠΧ σε συνδυασμό με την προηγούμενη απόφαση 26/9/2000, η επεξεργασία των προσωπικών δεδομένων που καταγράφονται από CCTV είναι νόμιμη όταν αφορά την προστασία προσώπων ή αγαθών ή τη ρύθμιση της κυκλοφορίας σύμφωνα με την αρχή της αναγκαιότητας και της αναλογικότητας. Δηλαδή οι κάμερες πρέπει να εγκαθίστανται και να κάνουν λήψεις από τέτοια σημεία ώστε να συλλέγονται μόνο τα απαραίτητα δεδομένα τα οποία πρέπει να είναι απόλυτα ακριβή και να μην τηρούνται πάνω από δεκαπέντε (15) μέρες. Όσον αφορά τους ανοικτούς χώρους δεν πρέπει να κάνουν λήψη εικόνων της εισόδου ή του εσωτερικού των κατοικιών. Ο εκάστοτε υπεύθυνος επεξεργασίας του CCTV οφείλει να γνωστοποιεί στην ΑΠΔΠΧ την ύπαρξη του κυκλώματος και να ζητήσει την άδεια της για ειδικές περιπτώσεις κυκλωμάτων. Ακόμη, οφείλει να ενημερώνει με διάφορα μέσα ότι ο χώρος βιντεοσκοπείται και να λαμβάνει τα απαραίτητα μέτρα ασφαλείας για την ασφάλεια της επεξεργασίας. Με βάση την

οδηγία αυτή η ΑΠΔΠΧ είναι σε συνεχή ρήξη με την Ελληνική Αστυνομία (ΕΛΑΣ) και το Υπουργείο Δημόσιας Τάξης.

Σύμφωνα με την απόφαση ***58/2001*** σε συνδυασμό με την απόφαση 29/1/2000 απαγορεύεται η δημοσίευση των ευαίσθητων προσωπικών δεδομένων των στρατεύσιμων που αφορούν την ψυχική τους υγεία και την τυχόν εξάρτηση τους από ουσίες.

Με την απόφαση ***115/2001*** η ΑΠΔΠΧ εξετάζει ζητήματα που αφορούν την επεξεργασία των προσωπικών δεδομένων των εργαζομένων μέσω της παρακολούθησης των επικοινωνιών τους, της επιτήρησης των χώρων εργασίας, της διαβίβασης των δεδομένων τους σε τρίτους αλλά και τη χρήση βιομετρικών μεθόδων για τον έλεγχο της πρόσβασης στο χώρο εργασίας με τη χρήση των νέων τεχνολογιών όπου διαπιστώθηκε η ανάγκη και η δυσκολία εξειδίκευσης των δικαιωμάτων εξαιτίας της ανισότητας που υπάρχει στην εργασιακή σχέση. Έτσι, ερμηνεύει και εξειδικεύει το ν. 2472/1997 ορίζοντας τις προϋποθέσεις και τις αρχές νόμιμης επεξεργασίας των προσωπικών δεδομένων των εργαζομένων για τους σκοπούς της απασχόλησης γενικότερα (π.χ. ανεύρεση εργασίας μέσω ΟΑΕΔ). Ορίζει ότι τα ευαίσθητα προσωπικά δεδομένα πρέπει να καταχωρίζονται και να διατηρούνται χωριστά από τα άλλα δεδομένα ενώ πρόσβαση σε αυτά πρέπει να έχει μόνο ο υπεύθυνος επεξεργασίας ή εξουσιοδοτημένα πρόσωπα ενώ αναφέρεται και στα δικαιώματα του εργαζόμενου αναφορικά με τα δεδομένα που τηρεί ο εργοδότης για το άτομο του. Κάθε παράβαση των παραπάνω επιφέρει διοικητικές κυρώσεις όπως η προειδοποίηση με αποκλειστική προθεσμία για άρση της παραβίασης, πρόστιμο τριακοσίων ως πεντακοσίων χιλιάδων δραχμών (300.000 – 50.000.000), προσωρινή ανάκληση της άδειας, καταστροφή του αρχείου ή διακοπή της επεξεργασίας και καταστροφή των σχετικών δεδομένων – αλλά και ποινικές κυρώσεις που ξεκινούν από φυλάκιση και χρηματική ποινή ενός ως πέντε εκατομμυρίων δραχμών (1 – 5.000.000) ως και κάθειρξη πέντε ως είκοσι ετών (5 – 20) και χρηματική ποινή μέχρι δέκα εκατομμυρίων δραχμών (10.000.000).

Η απόφαση ***147/2001*** αφορά τη συλλογή και τη χρήση προσωπικών και ευαίσθητων προσωπικών δεδομένων ενώπιον δικαστηρίου. Η ΑΠΔΠΧ αποφάσισε ότι επιτρέπεται κατ' εξαίρεση η συλλογή και η επεξεργασία ευαίσθητων και μη ευαίσθητων προσωπικών δεδομένων και η ίδρυση και λειτουργία σχετικού αρχείου, ύστερα από άδεια της ΑΠΔΠΧ, όταν η επεξεργασία είναι αναγκαία για την

αναγνώριση, άσκηση ή υπεράσπιση δικαιώματος ενώπιον δικαστηρίου ή πειθαρχικού οργάνου.

Σύμφωνα με την απόφαση ***150/2001*** επιβάλλεται πρόστιμο της τάξης των πέντε εκατομμυρίων δραχμών (5.000.000) σε ασφαλιστική εταιρεία για την επεξεργασία προσωπικών δεδομένων κυρίας που γέννησε σε κάποιο μαιευτήριο που χρησιμοποιήθηκαν για τη διαφήμιση ασφαλιστικών προγραμμάτων για το νεογέννητο και πρόστιμο ενός εκατομμυρίου δραχμών (1.000.000) στο μαιευτήριο για την παράλειψη της λήψης τεχνικών και οργανωτικών μέτρων που είχε σαν αποτέλεσμα τη διαρροή προσωπικών δεδομένων κάποιων.

Με την απόφαση ***51/2002*** απαγορεύεται η κοινοποίηση ιατρικής συνταγής από το φαρμακείο προς φαρμακαποθήκη για την προμήθεια φαρμάκων καθώς αυτή περιέχει ευαίσθητα προσωπικά δεδομένα για την κατάσταση της υγείας του εργαζόμενου και το είδος των φαρμάκων που λαμβάνει. Δεν τίθεται όμως θέμα τόσο για το γιατρό που τη συνταγογράφησε και για τον φαρμακοποιό που την εκτελεί καθώς δεσμεύονται από το ιατρικό απόρρητο.

Κάτι ανάλογο συμβαίνει και με την απόφαση ***99/2002*** όπου ψυχίατρος προκειμένου να του καταβληθεί το αντίτιμο της ιατρικής επίσκεψης κάποιου μέσω της ασφάλειας του απαιτούνταν η κατάθεση της πραγματογνωμοσύνης του ιατρού, πράγμα που αντίκειται στο ν. 2472/1997 και είναι παράνομο μιας και αποτελεί ευαίσθητο προσωπικό δεδομένο.

Η απόφαση ***61/2003*** αναφέρεται στην αίτηση του δικηγόρου κάποιου γιατρού για να λάβει τα στοιχεία νοσηλείας του ή επίσκεψης στα εξωτερικά ιατρεία κάποιου ασθενούς νοσοκομείου για χρήση ενώπιον δικαστηρίου. Η ΑΠΔΠΧ αποφάνθηκε ότι το νοσοκομείο υποχρεούται να ανακοινώσει τα στοιχεία αυτά αρκεί να ενημερώσει το υποκείμενο τους.

Η απόφαση ***12/2004*** αφορά την αίτηση κάποιου προς εταιρεία κινητής τηλεφωνίας για να λάβει κάποια στοιχεία κλήσεων που έγιναν προς συγκεκριμένο αριθμό που ανήκει σε συγκεκριμένο άτομο για χρήση τους ενώπιον δικαστηρίου. Η ΑΠΔΠΧ έκρινε ότι δεν υπάρχει κώλυμα σύμφωνα με το ν. 2472/1997 αρκεί το συγκεκριμένο άτομο να έχει ενημερωθεί για την ανακοίνωση αυτή.

Η απόφαση ***21/2004*** απαγορεύει στην Αστυνομική Διεύθυνση Προσωπικού την αναγραφή του είδους της πειθαρχικής ποινής στην προσωρινή βεβαίωση στοιχείων ταυτότητας και την αντικατάσταση της με την αναφορά ότι ο αστυνομικός αυτός δεν είναι σε θέση να τελέσει τα υπηρεσιακά του καθήκοντα αφού η επιβολή

διοικητικών κυρώσεων δεν εμπίπτει στις αρμοδιότητες της ΑΠΔΠΧ, ενώ δίδει ανάλογη σύσταση στο Υπουργείο Δημόσιας Τάξης για αυτού του είδους βεβαιώσεις που θα εκδοθούν εφεξής.

Η απόφαση ***26/2004*** αφορά την έκθεση των όρων νομιμότητας της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα για τους σκοπούς της άμεσης εμπορίας ή διαφήμισης και της διαπίστωσης πιστοληπτικής ικανότητας.

Η απόφαση ***43/2004*** στρέφεται ενάντια σε ασφαλιστική εταιρεία που ζήτησε από ασφαλισμένο να προσκομίσει βιντεοκασέτα λαπαροσκόπησης και αποτελέσματα ιστολογικής εξέτασης για να του καταβληθεί το 80% του κόστους των εξετάσεων αυτών. Μάλιστα διέταξε την καταστροφή των συγκεκριμένων ευαίσθητων δεδομένων ενώ επέβαλλε πρόστιμο είκοσι χιλιάδων ευρώ στην εταιρεία αυτή για παράνομη επεξεργασία ευαίσθητων προσωπικών δεδομένων.

Η απόφαση ***47/2004*** αποτελεί απάντηση στην αίτηση διευθυντή καρδιολογικής κλινικής κάποιου νοσοκομείου για χρήση στοιχείων νοσηλείας που βρίσκονται στο αρχείο για ερευνητικούς σκοπούς. Η ΑΠΔΠΧ χορήγησε τη συγκεκριμένη άδεια υπό τους όρους ότι η πρόσβαση στα στοιχεία των φακέλων των ασθενών θα γίνει στο χώρο του αρχείου του νοσοκομείου, ότι ο αιτών και οι βοηθοί του θα πάρουν μόνο όσα στοιχεία θεωρούν απαραίτητα για την εκπλήρωση του επιστημονικού τους στόχου και ότι δεν επιτρέπεται να καταγραφούν και να συνδεθούν τα στοιχεία που ταυτοποιούν τους ασθενείς με τα ιατρικά δεδομένα.

Η απόφαση ***51/2004*** αφορά την έκδοση διαβατηρίων σε ανυπότακτους και λιποτάκτες σύμφωνα με την οποία τους απαγορεύεται η χορήγηση ή θεώρηση διαβατηρίων για μετάβαση σε άλλη χώρα εφόσον βρίσκονται στο εξωτερικό, ενώ η απαγόρευση αυτή δεν ισχύει για τους ανυπότακτους του εξωτερικού για ταξίδια σε χώρες του εξωτερικού και για την είσοδο τους στην Ελλάδα για την εκπλήρωση των στρατιωτικών τους υποχρεώσεων. Αποφάνθηκε ότι πρέπει να αναγράφεται στα διαβατήρια των ανυπότακτων του εξωτερικού η φράση: «ισχύει για ταξίδια σε χώρες του εξωτερικού (πλην Ελλάδος) και για την είσοδο στην Ελλάδα για την εκπλήρωση των στρατιωτικών του υποχρεώσεων». Έτσι περιορίζεται η ελευθερία διακίνησης του ατόμου στο πρόταγμα της εθνικής άμυνας της χώρας.

Η απόφαση ***61/2004*** εξετάζει τη νομιμότητα της πρόσβασης του εργοδότη στους προσωπικού υπολογιστές των εργαζομένων όπου η ΑΠΔΠΧ αποφαίνεται ότι αν η εταιρεία θέλει να παρακολουθεί τους υπολογιστές των εργαζόμενων πρέπει να το γνωστοποιεί σε αυτούς με τρόπο σαφή και εύληπτο ενώ απαγορεύεται να

καταγράφει τις ιστοσελίδες που επισκέπτονται οι εργαζόμενοι για στατιστικούς λόγους αλλά μπορεί να περιορίζει τις ιστοσελίδες που μπορούν να επισκέπτονται. Απαγορεύει τη συλλογή και επεξεργασία δεδομένων των κλήσεων και επικοινωνιών στο χώρο εργασίας εκτός αν είναι απαραίτητο για την οργάνωση και την περάτωση μιας εργασίας ενώ πρέπει να είναι ανάλογα του σκοπού που επιτελούν.

Σύμφωνα με την απόφαση ***52/2005*** της ΑΠΔΠΧ απαγορεύεται η συλλογή απλών προσωπικών δεδομένων που αφορούν τρίτους - συγγενείς εργαζόμενων καθώς αυτό υπερβαίνει την αρχή του σκοπού της επεξεργασίας των δεδομένων με αποτέλεσμα να διατάξει την καταστροφή τους εντός 15 ημερών.

Στην απόφαση ***70/2005*** εξετάζεται η νομιμότητα της προβολής από τηλεοπτικό κανάλι της δραστηριότητας Μητροπολίτη όσον αφορά το αξίωμα του και στοιχεία της παιδικής του ηλικίας. Η ΑΠΔΠΧ αποφάνθηκε ότι επειδή οι Μητροπολίτες αποτελούν δημόσια πρόσωπα και συνδέονται με την άσκηση δημόσιου λειτουργήματος, το κοινό έχει το δικαίωμα του πληροφορείν και του πληροφορείσθαι με αποτέλεσμα να θεωρείται νόμιμη η προβολή δεδομένων που έχουν να κάνουν με το αξίωμα του. Όμως απαγορεύει την προβολή και την επανάληψη προβολής δεδομένων που έχουν να κάνουν με την παιδική ηλικία του Μητροπολίτη αφού αποτελούν ευαίσθητα προσωπικά δεδομένα και εμπίπτουν στη σφαίρα της ιδιωτικής του ζωής.

Με την απόφαση ***28/2006*** διαπιστώνεται ότι Υγειονομικές επιτροπές και η Υγειονομική επιτροπή του ασφαλιστικού φορέα καταχώρισαν ευαίσθητα προσωπικά δεδομένα στις ιατρικές γνωματεύσεις που εξέδωσαν και χορήγησαν στον ασθενή και κατά συνέπεια προέβησαν σε παράνομη επεξεργασία των δεδομένων του. Έτσι η ΑΠΔΠΧ επέβαλλε στο γενικό γραμματέα της περιφέρειας Χ που είναι υπεύθυνος επεξεργασίας για την επεξεργασία των επιτροπών αυτών αλλά και στη διεύθυνση αναπηρίας του ασφαλιστικού φορέα πρόστιμο τριών χιλιάδων ευρώ (3.000).

Σύμφωνα με τη γνωμοδότηση ***5/2007*** για τη συμφωνία για τη διαβίβαση καταστάσεων με ονόματα των επιβατών από την ΕΕ στις ΗΠΑ, το επίπεδο προστασίας των προσωπικών δεδομένων έχει μειωθεί αισθητά καθώς α) τα στοιχεία που διαβιβάζονται είναι περισσότερα και περιλαμβάνουν πληροφορίες και για τρίτα πέραν του υποκειμένου πρόσωπα, β) η Υπηρεσία Τελωνείων και Προστασίας των Συνόρων των ΗΠΑ μπορεί σε εξαιρετικές περιπτώσεις να επεξεργάζεται και ευαίσθητα προσωπικά δεδομένα, γ) η διάρκεια διατήρησης των δεδομένων έχει

αυξηθεί στα δεκαπέντε τουλάχιστον έτη και δ) ο μηχανισμός ελέγχου του συστήματος διαβίβασης δεν προβλέπει τη συμμετοχή Ανεξάρτητων Αρχών.

Η απόφαση ***6/2007*** αφορά τη δημοσιοποίηση από το Υπουργείο Εθνικής Άμυνας των ονομάτων των ατόμων που α) απηλλάγησαν νόμιμα από την υποχρέωση στράτευσης για λόγους υγείας, β) κρίθηκαν κατάλληλα για στράτευση έπειτα από επανέλεγχο των δικαιολογητικών τους και γ) απαλλάχθηκαν παράνομα από την υποχρέωση στράτευσης για λόγους υγείας. Η ΑΠΔΠΧ διαφωνεί με τη δημοσιοποίηση των στοιχείων αυτών αφού «…δε συνάδει τις διατάξεις του ν. 2472/1997, εφόσον τα ως άνω δεδομένα δεν εμπίπτουν σε οποιαδήποτε από τις προβλεπόμενες εξαιρέσεις του νόμου, η τυχόν συνδρομή των οποίων θα επέτρεπε την επιδιωκόμενη επεξεργασία τους».

Η απόφαση ***34/2007*** εμπίπτει στην προσβολή των ευαίσθητων προσωπικών δεδομένων στους τομείς εργασίας και κοινωνικής ασφάλισης καθώς αφορά αίτηση της εταιρεία GOODYEAR για γνωστοποίηση δεδομένων τριακοσίων είκοσι δύο (322) πρώην εργαζόμενων στην εν λόγω εταιρεία από το ΙΚΑ, το ΟΑΕΕ – ΤΕΒΕ και τον ΟΑΕΔ. Εδώ, η διαβίβαση των δεδομένων των εργαζόμενων αυτών από το ΙΚΑ αλλά και το σχετικό αρχείο που τηρήθηκε στην εταιρεία αυτή ήταν παράνομα αφού δεν υπήρχε άδεια της ΑΠΔΠΧ με αποτέλεσμα να διαταχθεί η προσωρινή διακοπή της επεξεργασίας του σχετικού αρχείου στην εταιρεία ενώ το ΙΚΑ κλήθηκε εντός δεκαπέντε (15) ημερών να δώσει διευκρινήσεις για την παράνομη διαβίβαση τους υποβάλλοντας αντίγραφα των εγγράφων που δόθηκαν στην παραπάνω εταιρεία. Τέλος, κλήθηκε η διοίκηση του ΟΑΕΕ – ΤΕΒΕ να απαντήσει εντός δεκαπέντε (15) ημερών για το αν διαβιβάσθηκαν προσωπικά δεδομένα των εργαζόμενων στην παραπάνω εταιρεία.

Η απόφαση ***50/2007*** αναφέρεται στην εγκατάσταση βιομετρικού συστήματος σε εταιρεία για τον έλεγχο της εισόδου και εξόδου των εργαζόμενων σε αυτήν. Η ΑΠΔΠΧ αποφάνθηκε ότι η εταιρεία πρέπει να σταματήσει άμεσα την επεξεργασία των δεδομένων που έχει συλλέξει, να απεγκαταστήσει το βιομετρικό αυτό σύστημα και να καταστρέψει το αρχείο που έχει δημιουργηθεί ενώ της επιβάλλει πρόστιμο χιλίων πεντακοσίων ευρώ (1500) και την προειδοποιεί ότι πρέπει να ενημερώνει τα υποκείμενα των δεδομένων αλλά και να γνωστοποιεί τη σύσταση, λειτουργία ή έναρξη επεξεργασίας ενός τέτοιου αρχείου στην ΑΠΔΠΧ.

Παρόμοια περίπτωση είναι αυτή της απόφασης ***62/2007*** όπου εργαζόμενοι σε εταιρεία κατήγγειλαν την ύπαρξη βιομετρικού συστήματος για τον έλεγχο εισόδου –

εξόδου των εργαζόμενων με τη διαφορά ότι η ΑΠΔΠΧ επέβαλε εκτός από την αναστολή της επεξεργασίας των δεδομένων, την απεγκατάσταση του συστήματος αυτού και την καταστροφή του αρχείου, την αφαίρεση των καμερών πρόστιμο οκτώ χιλιάδων ευρώ (8000) για την εγκατάσταση του βιομετρικού συστήματος και έξι χιλιάδων ευρώ (6000) για την παράνομη λειτουργία CCTV στο χώρο εργασίας και την απεγκατάσταση του λογισμικού παρακολούθησης από τα PC του ιδιοκτήτη και του διευθυντή της εταιρείας.

Με την απόφαση ***3/2008*** επιβάλλεται πρόστιμο εξήντα χιλιάδων ευρώ (60.000) στην ΕΘΝΙΚΗ ΑΣΦΑΛΙΣΤΙΚΗ η οποία χρησιμοποίησε ευαίσθητα προσωπικά δεδομένα του πελάτη της που αναγράφονται στο απολυτήριο του στρατού του και αφορούν το σεξουαλικό προσανατολισμό του προκειμένου να αξιολογήσουν το αίτημα του για σύναψη σύμβασης ασφάλειας ζωής.

Η απόφαση ***17/2008*** αναφέρεται στην περίπτωση δημοσίευσης σε εφημερίδα τόσο σε έντυπη μορφή όσο και στην ιστοσελίδα της φωτογραφιών που αναδεικνύουν την ερωτική ζωή κάποιων ατόμων όπου η ΑΠΔΠΧ αποφάνθηκε ότι η επεξεργασία των δεδομένων αυτών, η σύσταση και η λειτουργία του αρχείου αυτού είναι παράνομη αφού αφορά ευαίσθητα προσωπικά δεδομένα και επέβαλλε στην εφημερίδα αυτή πρόστιμο εκατόν πενήντα χιλιάδων ευρώ (150.000) ενώ διέταξε την καταστροφή των δεδομένων αυτών.

Η απόφαση ***33/2008*** αφορά την αίτηση κάποιου πελάτη προς τράπεζα για την παροχή στοιχείων και εγγράφων που αφορούν το πρόσωπο του για να στηρίξει μήνυση κατά παντός υπευθύνου υπάλληλου της τράπεζας για παράνομη πρόσβαση στα δεδομένα οικονομικής του συμπεριφοράς, για παράνομη χορήγηση σε τρίτο μη εξουσιοδοτημένο πρόσωπο αντιγράφου της οικονομικής του κατάστασης το οποίο είχε προσαγάγει και επικαλεστεί ο τρίτος σε φάκελο εκκρεμούς δίκης σχετικά με αντιδικία μεταξύ τους. Η ΑΠΔΠΧ προειδοποίησε την τράπεζα να δώσει τα στοιχεία που ζητά ο αιτών εντός δέκα ημερών από τη λήψη της απόφασης αυτής.

Η απόφαση ***50/2008*** αποτελούσε απάντηση σε αίτηση υιοθετημένου ατόμου για πρόσβαση στα αρχεία του βρεφοκομείου όπου ήταν τρόφιμος για να ανακαλύψει την ταυτότητα των πραγματικών του γονέων. Η ΑΠΔΠΧ αποφάνθηκε ότι η Κοινωνική Υπηρεσία του βρεφοκομείου αυτού είναι υποχρεωμένη να γνωστοποιήσει τα στοιχεία του αρχείου που τηρεί θεωρώντας ότι υπερτερεί η διάθεση τους στον αιτούντα από τα δικαιώματα και το συμφέρον των φυσικών του γονέων. Για το λόγο αυτό δεν απαιτείται η συγκατάθεση των φυσικών του γονέων.

### 5.3: <u>Συμπερασματικές παρατηρήσεις</u>

Η θεσμοθέτηση των ΑΠΔΠΧ σε όλες τις ευρωπαϊκές χώρες και στη χώρα μας αποτελεί μία σημαντική προσπάθεια για την προστασία των προσωπικών και των ευαίσθητων προσωπικών δεδομένων ιδιαίτερα υπό τις απειλές των νέων τεχνολογιών.

Η λειτουργία της Ελληνικής ΑΠΔΠΧ βασίζεται τόσο στο ευρωπαϊκό δίκαιο όσο και στο ελληνικό που έχει προσαρμοστεί σε αυτό. Ιδιαίτερα θετικό είναι το γεγονός ότι αποτελεί ανεξάρτητη αρχή που της επιτρέπει να λειτουργεί αντικειμενικά και ανεπηρέαστα και αυτό φαίνεται από τις παραπάνω αποφάσεις που έχει εκδώσει επιβάλλοντας κυρώσεις τόσο σε υπουργεία όσο και στην ΕΛΑΣ.

Ο ανεξάρτητος αυτός χαρακτήρας της ΑΠΔΠΔΧ τονίζεται ιδιαίτερα από το γεγονός της αντιδικίας που είχε με το Υπουργείο Δημόσιας Τάξης και την ΕΛΑΣ μετά τους Ολυμπιακούς Αγώνες της Αθήνας το 2004 για την εγκατάσταση και λειτουργία των ολυμπιακών καμερών στο οδικό δίκτυο της Αττικής όπου και τους επέβαλε πρόστιμο τριών χιλιάδων ευρώ (3.000) επειδή σε κάποιες από αυτές δεν είχε εγκατασταθεί το ειδικό λογισμικό απόκρυψης εικόνων, κάποιες από αυτές δεν έπρεπε να λειτουργούν και ο χρόνος τήρησης των αρχείων τους υπερέβαινε τις επτά ημέρες (Απόφαση 57/2006). Αξίζει δε να σημειωθεί το γεγονός ότι είχε επιτραπεί με προηγούμενη απόφαση η λειτουργία των καμερών αυτών για το σκοπό της διαχείρισης της κυκλοφορίας των οχημάτων (Απόφαση 39/2006) κι όχι για λόγους ασφάλειας. Επίσης το Μάρτιο του 2008 ήρθε ξανά σε αντιπαράθεση με το Υπουργείο Δημόσιας Τάξης για χρήση των CCTV για σκοπούς πέραν της διαχείρισης της κυκλοφορίας, επιβάλλοντας πρόστιμο πέντε χιλιάδων ευρώ (5000) (Απόφαση7/2008). Αργότερα το Νοέμβριο, η διαμάχη αυτή οδήγησε στην παραίτηση της ΑΠΔΠΧ που αντιτάχθηκε στην κατόπτευση των διαδηλώσεων για την επέτειο της εξέγερσης του Πολυτεχνείου δηλώνοντας με τον τρόπο αυτό τον ανεξάρτητο χαρακτήρα της και το γεγονός ότι τόσο οι κρατικοί φορείς όσο και οι ιδιωτικοί φορείς πρέπει να αντιμετωπίζονται ισότιμα για την προστασία των προσωπικών και των ευαίσθητων προσωπικών δεδομένων και πολιτικών ελευθεριών των πολιτών. Έτσι θεώρησε ότι δεν έχει λόγο ύπαρξης αν δεν μπορεί να περιορίζει τις αντισυνταγματικές αυθαιρεσίες του κράτους.

Παρόλα αυτά η ΑΠΔΠΧ δεν είναι ιδιαίτερα αποτελεσματική στην ελληνική πραγματικότητα παρά τις χρήσιμες παρεμβάσεις της και αυτό φαίνεται και από τις ίδιες τις δηλώσεις του πρώτου προέδρου της κ. Β. Δαφέρμου, ο οποίος επισήμανε ότι

η ΑΠΔΠΧ χωρίς επαρκή υποδομή και στελέχωση «δεν μπορεί να είναι αποτελεσματική στο να προστατεύσει την προσωπική ζωή των Ελλήνων πολιτών παρά τις προσπάθειες που καταβάλει». Επιπλέον τόνισε ότι «το πιο σημαντικό είναι ότι ο κόσμος δε γνωρίζει από τι απειλούνται και με ποιους τρόπους προστατεύονται τα (προσωπικά του) δεδομένα» και υπογράμμισε ότι «Ενώ έχουμε καταφέρει να ελέγχουμε λίγο πολύ τις κρατικές υπηρεσίες μας, είναι εντελώς αδύνατον να ελέγξουμε ποιες εταιρείες κρατάνε σε βάσεις δεδομένων προσωπικά μας αρχεία και πως τα χρησιμοποιούν… Οι νόμοι (προστασίας προσωπικών δεδομένων) είναι σχεδόν ανενεργοί, κυρίως επειδή ως πολίτες ελάχιστα ενδιαφερόμαστε για την προστασία αυτών των πληροφοριών» (Σαματάς, 2005: 523 – 514). Δηλαδή θεωρεί ότι υπάρχει άγνοια και αμέλεια από μέρους των πολιτών για τη διεκδίκηση της προστασίας των δεδομένων τους, εκχωρώντας τα χωρίς να ενδιαφέρονται για το ποιος, πότε και για ποιο σκοπό θα χρησιμοποιήσει αυτά τα δεδομένα.

Συνολικά όμως, η δράση της ελληνικής ΑΠΔΠΧ θεωρείται θετική γεγονός που έχει εκτιμηθεί και από την EPIC και την Privacy International αλλά και από ελληνικές μη κυβερνητικές οργανώσεις όπως το Παρατηρητήριο Ανθρωπίνων Δικαιωμάτων, κά.

# ΚΕΦΑΛΑΙΟ 6$^{Ο}$
# ΕΜΠΕΙΡΙΚΗ ΔΙΕΡΕΥΝΗΣΗ ΤΗΣ ΠΡΟΣΤΑΣΙΑΣ ΤΩΝ ΕΥΑΙΣΘΗΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΕ ΤΟΠΙΚΟ ΕΠΙΠΕΔΟ

## 6.1: Εμπειρική έρευνα σε φορείς συλλογής και επεξεργασίας ευαίσθητων προσωπικών δεδομένων

### 6.1.1: Αντικείμενο και στόχοι της έρευνας σε φορείς

Αντικείμενο της παρούσας εμπειρικής έρευνας είναι να διαπιστωθεί ο βαθμός προστασίας των ευαίσθητων προσωπικών δεδομένων από διάφορους φορείς των οποίων η λειτουργία βασίζεται κυρίως στη συλλογή των δεδομένων αυτών σε τοπικό επίπεδο της πόλης του Ρεθύμνου.

Για την πληρέστερη κατανόηση των συνθηκών και των προϋποθέσεων νόμιμης καταγραφής και επεξεργασίας των προσωπικών και των ευαίσθητων προσωπικών δεδομένων έγινε βιβλιογραφική έρευνα και μελέτη της σχετικής νομοθεσίας, των γνωμοδοτήσεων και αποφάσεων της ΑΠΔΠΧ.

Έτσι, πραγματοποιήθηκε επίσκεψη σε φορείς του Ρεθύμνου όπως μία ασφαλιστική εταιρεία, το στρατολογικό γραφείο, το νοσοκομείο και μία αλυσίδα super market που τηρούν αρχείο προσωπικών και ευαίσθητων προσωπικών δεδομένων προκειμένου να διαπιστωθεί αν η τήρηση των αρχείων αυτών είναι σύμφωνη με τις οδηγίες και τις επιταγές της ΑΠΔΠΧ. Σε καθέναν λοιπόν από τους παραπάνω φορείς έγινε άτυπη συνέντευξη με τους υπεύθυνους – διευθυντές όπου διερευνήθηκε η διαδικασία συλλογής και επεξεργασίας των δεδομένων των υποκειμένων προκειμένου να διαπιστωθεί η νομιμότητα ή μη της διαδικασίας αρχειοθέτησης και επεξεργασίας των προσωπικών πληροφοριών και ιδιαίτερα των ευαίσθητων στο σύνολο της.

Ο στόχος της έρευνας μας είναι να αποδειχθεί αν η ελληνική νομοθεσία για την προστασία των προσωπικών και των ευαίσθητων προσωπικών δεδομένων εφαρμόζεται επαρκώς, αν ακολουθούνται οι οδηγίες της ΕΕ για την προστασία τους, και αν η ΑΠΔΠΧ λειτουργεί ανασταλτικά για την παράνομη συλλογή και επεξεργασία των προσωπικών δεδομένων από διάφορους φορείς. Και όλα αυτά με δεδομένη τη ραγδαία εξέλιξη της τεχνολογίας όπου η παράνομη πρόσβαση, η παραβίαση και η εμπορία των προσωπικών μας δεδομένων και ιδιαίτερα των

ευαίσθητων γίνεται ολοένα και ευκολότερη επειδή αποτελούν κυρίως εμπορεύσιμο αγαθό.

### 6.1.2: Μεθοδολογία και στάδια της έρευνας σε φορείς

Προκειμένου να διαπιστωθεί ο βαθμός προστασίας των προσωπικών και των ευαίσθητων προσωπικών μας δεδομένων από διάφορους δημόσιους και ιδιωτικούς φορείς, χρησιμοποιήθηκε η μέθοδος της ημι – δομημένης και άτυπης συνέντευξης επειδή με τη χρήση της προωθείται η ελεύθερη έκφραση των ερωτώμενων[30].

Κατά τη διεξαγωγή της έρευνας στο σύνολο της ακολουθήθηκαν κάποια στάδια βάσει εκείνων που χρησιμοποιήθηκαν σε άλλες έρευνες. Για την οργάνωση και την πραγματοποίηση των άτυπων συνεντεύξεων με τους υπεύθυνους των παραπάνω φορέων λάβαμε υπόψη μας κάποιες γενικές θεματικές ενότητες ανάλογα με το αντικείμενο τους, και σχετικά με τις υποθέσεις που έχουμε εξαρχής θέσει.

Στη συνέχεια, επιλέχθηκαν τα πρόσωπα, δηλαδή οι υπάλληλοι του νοσοκομείου, ο αντιπρόσωπος ασφαλιστικής εταιρείας, ο διευθυντής αλυσίδας super market και ο διευθυντής του στρατολογικού γραφείου, οι οποίοι αρχικά ενημερώθηκαν για το σκοπό της έρευνας. Το στάδιο αυτό είναι ιδιαίτερα σημαντικό αφού εδώ κερδίζεται το ενδιαφέρον κάθε μέλους της έρευνας ξεχωριστά προκειμένου να διασφαλιστεί η συνεργασία τους. Ακολούθησε η διεξαγωγή της έρευνας με τη χρήση των μεθόδων της ημι – δομημένης και άτυπης συνέντευξης. Τόσο κατά την έναρξη όσο και κατά τη διάρκεια των συνεντεύξεων αυτών έγινε προσπάθεια να κεντριστεί το ενδιαφέρον των συνεντευξιαζόμενων για τη σπουδαιότητα του θέματος. Στην πορεία των συνεντεύξεων μερικές φορές κρίθηκε αναγκαίο να τεθούν διευκρινιστικές ερωτήσεις για την πληρέστερη κατανόηση και την εις βάθος ανάλυση και μελέτη του ερευνώμενου θέματος.

Τέλος, αναλύθηκαν τα δεδομένα που συλλέχθηκαν μέσω της καταγραφής και της έκθεσης των αποτελεσμάτων των συνεντεύξεων.

[30] Με τη μέθοδο αυτή οι ερωτώμενοι δίνουν απαντήσεις θέτοντας τα δικά τους όρια δίνοντας παράλληλα έμφαση στο σημείο που αυτοί πιστεύουν ότι είναι σημαντικό αναφορικά με το ερευνώμενο θέμα (Κυριαζή, 2001).

### 6.1.3: Μεθοδολογικές δυσχέρειες

Για την αποδοχή της συνέντευξης δεν είχαμε πρόβλημα. Κατά την εκπόνηση της παραπάνω έρευνας όμως αντιμετωπίστηκαν κάποιες δυσκολίες εξαιτίας της φύσης του ερευνώμενου θέματος, τα ευαίσθητα προσωπικά δεδομένα. Για παράδειγμα, κάποιοι από τους υπεύθυνους των φορέων δήλωναν άγνοια σε σχέση με το τι προβλέπεται από τη νομοθεσία για τη χρήση των ευαίσθητων προσωπικών δεδομένων και μάλιστα στην περίπτωση των ασφαλισμένων τι είδους επεξεργασία γίνεται από τα κεντρικά γραφεία της ασφαλιστικής εταιρείας στην Αθήνα. Θεωρούσαν δηλαδή τον εαυτό τους και τη θέση τους ως ανεύθυνο κρίκο μιας αλυσίδας της επεξεργασίας των προσωπικών και των ευαίσθητων προσωπικών δεδομένων των πολιτών στο πλαίσιο της εταιρείας τους, ότι αποτελούσαν ένα απλό εργαλείο που περιορίζεται απλά και μόνο στη συλλογή των δεδομένων αυτών, αγνοώντας ή γνωρίζοντας πολύ επιγραμματικά τι συμβαίνει μετά, και πως αυτά τα δεδομένα θα επεξεργαστούν και για ποιο ακριβώς σκοπό.

### 6.1.4: Τα αποτελέσματα της έρευνας σε φορείς

#### 6.1.4.1: Στρατολογικό γραφείο

Η εκπλήρωση της στρατιωτικής θητείας σύμφωνα με το Σύνταγμα της Ελλάδας αποτελεί βασική υποχρέωση κάθε άρρενα πολίτη. Συγκεκριμένα «κάθε Έλληνας που μπορεί να φέρει όπλα είναι υποχρεωμένος να συντελεί στην άμυνα της πατρίδας, σύμφωνα με τις επιτεγές των νόμων» (Άρθρο 4 Συντάγματος; Λυκοβάρδη, 2004: 142). Αυτό αιτιολογείται αν λάβουμε υπόψη την ιστορία του ελληνικού κράτους, ως έθνος – κράτος, τη σημαντικότητα της γεωπολιτικής του θέσης, τη διαρκή αντιπαλότητα με τους γείτονες και την αναγκαιότητα για την Εθνική Άμυνα. Ο συνδυασμός των παραπάνω ενισχύει την ανάγκη ύπαρξης και συντήρησης του στρατού και της άμυνας του και ιδιαίτερα εξαιτίας του γεγονότος της σύνδεσης του στρατού με τα εθνικά ιδεώδη και αξίες που είναι βαθιά ριζωμένες στη συνείδηση των Ελλήνων ανά τους αιώνες (Λυκοβάρδη, 2004: 140).

Αφού η εκπλήρωση της στρατιωτικής θητείας αποτελεί καθολική υποχρέωση των Ελλήνων ανδρών, σχεδόν κανένας δεν απαλλάσσεται από αυτήν παρά μόνο αν συντρέχουν σοβαροί λόγοι. Επιπλέον, υποχρεούται σε στρατιωτική θητεία και οι

Έλληνες που γεννήθηκαν και διέμεναν έκτοτε στο εξωτερικό, από τη στιγμή που αποφάσισαν να ζήσουν μόνιμα στην Ελλάδα. Το σκεπτικό αυτό πηγάζει τόσο από την ανάγκη ενίσχυσης της άμυνας της χώρας μας όσο και από τη λογική ότι για να μπορέσει κάποιος να γίνει φορέας των δικαιωμάτων που έχει κάθε Έλληνας πολίτης πρέπει να αποδεχθεί και τις ανάλογες υποχρεώσεις.

Σήμερα η στρατιωτική θητεία είναι διάρκειας δώδεκα (12) μήνων ενώ υπάρχουν και περιπτώσεις υπαγωγής σε εννεάμηνη (9) και εξάμηνη (6) μειωμένη θητεία κυρίως για λόγους οικογενειακούς, ενώ στην κατηγορία αυτή εμπίπτουν και οι ομογενείς.

Ανάλογη μεταχείριση έχουν και οι αιτούντες απαλλαγή με τη διαφορά ότι εδώ υπάγονται και όσοι επικαλούνται οικογενειακούς λόγους, οι αλλοδαποί που μονάζουν στο Άγιο Όρος, όσοι κρίνονται ακατάλληλοι για στράτευση από τις υγειονομικές επιτροπές των ενόπλων δυνάμεων κι εκείνοι που έχουν καταδικαστεί αμετάκλητα σε κάθειρξη ή σε ποινή που για τους στρατιωτικούς συνεπάγεται καθαίρεση και δεν επακολούθησε αμνηστία, χάρη ή παραγραφή της ποινής με άρση των συνεπειών της καταδίκης (www.stratologia.gr). Όσο για τις περιπτώσεις αναβολής κατάταξης στο στρατό περιορίζονται στις σπουδές και λόγω θεραπευτικής αγωγής σε Κέντρα Θεραπείας Εξαρτημένων Ατόμων (ΚΕΘΕΑ) από ουσίες.

Ακόμη υπάρχουν κι εκείνοι που συνειδητά δεν επιθυμούν, δηλαδή φέρνουν αντίρρηση στην εκπλήρωση της στρατιωτικής τους θητείας, οι αποκαλούμενοι «αντιρρησίες συνείδησης» οι οποίοι έχουν συγκεκριμένες ιδεολογικές, πολιτικές, φιλοσοφικές ή θεολογικές αντιλήψεις εξαιτίας των οποίων αντιστέκονται στη χρήση βίας, και κατά συνέπεια αντιστέκονται σε στρατοκεντρικές ιδεολογικές αντιλήψεις και πρότυπα (Λυκοβάρδη, 2004: 139). Αυτοί είτε εκπληρώνουν άοπλη στρατεύσιμη στρατιωτική θητεία σε υπηρεσίες και μονάδες των ενόπλων δυνάμεων, είτε υποχρεώνονται σε εναλλακτική υπηρεσία σε φορείς του δημόσιου τομέα, αφού το δηλώσουν στο Υπουργείο Εθνικής Άμυνας.

Έπειτα από προσεκτική μελέτη της απόφασης 3/2008 της ΑΠΔΠΧ προκύπτει ότι πριν την έκδοση της απόφασης η οποία απαγορεύει την αναγραφή του κριτηρίου απόλυσης από το στρατό, οι ομοφυλόφιλοι δεν υπηρετούσαν καν τη στρατιωτική τους θητεία. Χαρακτηρίζονταν ως ακατάλληλοι για στράτευση και έπαιρναν απολυτήριο στρατού Ι5 ως πάσχοντες από «αναφερόμενη διαταραχή σεξουαλικής ταυτότητας σε άτομο με χαρακτηρολογική εκτροπή». Δηλαδή, αντιμετωπίζονταν ως ψυχικά διαταραγμένοι.

Το ζήτημα που προκύπτει είναι τι συμβαίνει με τα δεδομένα των στρατεύσιμων ή ακόμη καλύτερα των υποψήφιων στρατεύσιμων ειδικών κατηγοριών και αυτών που απαλλάσσονται, πώς αυτά επεξεργάζονται, πού φυλάσσονται, σε ποιούς γνωστοποιούνται, ποιοί έχουν πρόσβαση σε αυτά;

Σύμφωνα με το διευθυντή του στρατολογικού γραφείου, ακολουθούνται αποκλειστικά και μόνο οι απαραίτητες διαδικασίες που ορίζει ο νόμος. Προκειμένου να διαπιστωθεί αν κάποιος εμπίπτει σε μειωμένη θητεία, για να δοθεί αναβολή στράτευσης ή ακόμη και για την εκπλήρωση στρατιωτικής θητείας συλλέγονται προσωπικά δεδομένα των στρατεύσιμων από το εκάστοτε στρατολογικό γραφείο, τα οποία γνωστοποιούνται στη Μονάδα στην οποία καλείται ο εκάστοτε στρατεύσιμος να υπηρετήσει.

Η περίπτωση των αντιρρησιών συνείδησης όμως είναι ιδιαίτερη εξαιτίας του γεγονότος ότι οι αντιλήψεις τους, οι λόγοι άρνησης εκπλήρωσης ένοπλης θητείας και η περίπτωση των εξαρτημένων από ουσίες ατόμων αποτελούν ευαίσθητα προσωπικά δεδομένα σύμφωνα με το ν.2472/1997 και επιδέχονται της ανάλογης προστασίας από το νόμο. Οι αντιρρησίες συνείδησης ουσιαστικά τίθενται ενάντια στη νομική υποχρέωση για στράτευση συγκρουόμενοι με τη δικαιοσύνη και την έννομη τάξη. Για τη διαπίστωση της ειλικρίνειας του υποψήφιου στρατεύσιμου συστήνεται επιτροπή που απαρτίζεται από επιστήμονες ανάλογα με τους λόγους για τους οποίους προβάλλονται αντιρρήσεις αναφορικά με τη διεκπεραίωση ένοπλης θητείας.

Όταν κάποιος καλείται να υπηρετήσει εναλλακτική θητεία, τοποθετείται σε δημόσιες υπηρεσίες με απόφαση του Υπουργείου Εθνικής Άμυνας έπειτα από αίτηση των υπηρεσιών αυτών στο παραπάνω υπουργείο όπου δηλώνουν εγγράφως ότι έχουν ανάγκη από προσωπικό. Δηλαδή, εκτός από το ότι θεωρούνται ως αντιρρησίες συνείδησης, δεν υπάρχουν κριτήρια τοποθέτησης τους στις δημόσιες υπηρεσίες, και η τοποθέτηση τους μπορεί να μην σχετίζεται με το αντικείμενο των σπουδών τους.

Έτσι ο στρατεύσιμος έπειτα από την τοποθέτηση του στον εκάστοτε δημόσιο φορέα υπόκεινται στο εργασιακό καθεστώς. Δηλαδή υπάγεται στη σχέση εργοδότη – εργαζόμενου, ακολουθεί το ωράριο εργασίας του φορέα, έχει συγκεκριμένο αριθμό αδειών, δεν έχει τη στρατιωτική ιδιότητα και εν ολίγοις εξομοιώνεται με τους υπαλλήλους του φορέα. Ο φορέας αυτός βρίσκεται σε διαρκή επικοινωνία με το στρατολογικό γραφείο παρέχοντας του ενημέρωση αναφορικά με τη συμπεριφορά του στρατεύσιμου. Όμως η θητεία τους είναι μεγαλύτερη των δώδεκα (12) μηνών.

Όμως εκτός από τον τρόπο συλλογής και επεξεργασίας των προσωπικών δεδομένων των ατόμων αυτών προκύπτει και το ζήτημα της αντιμετώπισης τους από τον εκάστοτε φορέα και τους εργαζόμενους σε αυτόν, ως προς το πρόσωπο του. Όλοι γνωρίζουν ότι το συγκεκριμένο άτομο εργάζεται στο φορέα για συγκεκριμένο χρονικό διάστημα υπηρετώντας εναλλακτική θητεία γεγονός που πιθανόν οδηγεί στο στιγματισμό του από τους συναδέλφους ή και από την τοπική κοινωνία στην οποία βρίσκεται η υπηρεσία αυτή.

Όσο για την προσαύξηση στη θητεία τους, δίνεται η αίσθηση ότι έχει τιμωρητικό χαρακτήρα λόγω της άρνησης εκπλήρωσης «κανονικής» θητείας. Αφού παρεκκλίνουν από το «κανονικό», τιμωρούνται με προσαύξηση της εναλλακτικής θητείας. Όμως ο διευθυντής του στρατολογικού γραφείου δεν έχει την ίδια άποψη μιας και θεωρεί ότι η προσαύξηση αυτή αποτελεί προσπάθεια εξομοίωσης της εναλλακτικής με την «κανονική» - ένοπλη θητεία. Κατά τον τρόπο αυτό εξισώνονται οι παραπάνω μορφές θητείας αφού όσοι υπηρετούν εναλλακτική θητεία δεν τυγχάνουν των κακουχιών και των ταλαιπωριών εκείνων που υπηρετούν ένοπλη θητεία με ότι αυτό συνεπάγεται.

Όσον αφορά τώρα τους ανυπότακτους και λιποτάκτες, λαμβάνονται μία σειρά μέτρων όπως: α) η μη χορήγηση πιστοποιητικού στρατολογικής κατάστασης ενώ χάνουν το δικαίωμα του εκλέγειν και εκλέγεσθαι, β) αν έχουν καταδικαστεί αμετάκλητα για εγκλήματα ανυποταξίας ή λιποταξίας, στερούνται του δικαιώματος άσκησης επαγγέλματος, γ) αν πριν από την τέλεση του «εγκλήματος» αυτού έχει εκδοθεί άδεια ασκήσεως επαγγέλματος, θεωρείται άκυρη και ανακαλείται από την ημέρα που η καταδίκη έγινε αμετάκλητη.

Ακόμη, δεν έχουν δικαίωμα διορισμού σε δημόσια θέση, δεν μπορούν να αποδημήσουν σε χώρα του εξωτερικού ή να ναυτολογηθούν σε πλοία γραμμής του εξωτερικού ενώ παράλληλα δεν επιτρέπεται η χορήγηση ή θεώρηση των διαβατηρίων τους εκτός από την περίπτωση των ανυπότακτων εξωτερικού που διαμένουν σε χώρα του εξωτερικού.

Μέσα από την έρευνα τόσο στο στρατολογικό γραφείο όσο και από τη μελέτη της ηλεκτρονικής διεύθυνσης www.stratologia.gr παρατηρούμε ότι η λειτουργία του συστήματος αυτού απαιτεί τη συλλογή προσωπικών και ευαίσθητων προσωπικών δεδομένων των στρατεύσιμων ανδρών που σύμφωνα με το διευθυντή του στρατολογικού γραφείου χρησιμοποιούνται καθαρά για υπηρεσιακούς σκοπούς.

Τα πάντα πρέπει να είναι εις γνώση του στρατού και να ελέγχονται από αυτόν για την εξυπηρέτηση των αναγκών της εθνικής άμυνας. Μπορεί με σχετική απόφαση της ΑΠΔΠΧ να μην αναγράφεται το κριτήριο απόλυσης[31] στο πιστοποιητικό στρατολογικής κατάστασης, όμως ο στρατός εξακολουθεί να συλλέγει και να επεξεργάζεται ευαίσθητα προσωπικά δεδομένα των στρατεύσιμων ανδρών, αλλά και των εφέδρων αξιωματικών. Επίσης η ΑΠΔΠΧ έχει λάβει μία σειρά αποφάσεων για την πρόληψη του αποκλεισμού και του στιγματισμού όσων δεν υπηρετούν τη στρατιωτική θητεία τους, όπως η απαγόρευση της γνωστοποίησης προσωπικών δεδομένων των στρατεύσιμων ανδρών που αφορούν την ψυχική υγεία και την εξάρτηση από ουσίες χωρίς τη συγκατάθεση τους (Απόφαση 58/2001), η διαγραφή της φράσης «Ισχύει για ταξίδια σε χώρες εξωτερικού (πλην Ελλάδος) και για είσοδο στην Ελλάδα για την εκπλήρωση των στρατιωτικών του υποχρεώσεων» από τα διαβατήρια (Απόφαση 51/2004), η διαγραφή ανυποταξίας κάποιου τόσο από τη στρατολογική μερίδα όσο και από το στρατιωτικό πιστοποιητικό τύπου Α΄ (Απόφαση 34/2006), η απαγόρευση της δημοσιοποίησης από το Υπουργείο Εθνικής Άμυνας των ονομάτων όσων απηλλάγησαν νόμιμα ή μη, για λόγους υγείας, από τη στράτευση και όσων κρίθηκαν κατάλληλοι για στράτευση έπειτα από επανέλεγχο (Απόφαση 6/2007). Σ' αυτούς περιλαμβάνεται και η κατηγορία των ομοφυλόφιλων και των αρνητών στράτευσης για λόγους συνέπειας.

Η προστασία του αρχείου τους είναι καλύτερη συγκριτικά με παλαιότερα. Όμως οι κυρώσεις για όσους αρνούνται να εκπληρώσουν τη στρατιωτική τους θητεία είναι «βαριές» αφού στερούνται του δικαιώματος άδειας άσκησης επαγγέλματος, του δικαιώματος του εκλέγειν και του εκλέγεσθαι, του δικαιώματος διορισμού σε δημόσια θέση, του δικαιώματος ελεύθερης διακίνησης και εξόδου προς το εξωτερικό. Επικρατεί ένα αυταρχικό και σχεδόν απόλυτο καθεστώς που επιβάλλει την καθολική στράτευση των Ελλήνων ανδρών όπου τάσσεται ως υπέρτατο αγαθό η προστασία και η άμυνα της πατρίδας, δηλαδή η ασφάλεια της χώρας. Όταν κάποιος αρνείται για οποιοδήποτε λόγο να εκπληρώσει τις στρατιωτικές του υποχρεώσεις, αντιμετωπίζεται με στιγματισμό και αποκλείεται από πολλές δραστηριότητες ακόμη και της καθημερινής ζωής και του αγώνα για επιβίωση ενώ στερείται και το δικαίωμα του εκλέγειν και του εκλέγεσθαι που αποτελεί ένα από τα θεμελιώδη ανθρώπινα δικαιώματα.

[31] Παλαιότερα αναγράφονταν η ένδειξη Ι1, Ι2, Ι3, Ι4 και Ι5.

Όμως το ουσιαστικό πρόβλημα στην περίπτωση της απαλλαγής από την υποχρέωση στράτευσης των ανδρών αποτελεί ο ενδεχόμενος κοινωνικός αποκλεισμός που υφίστανται με βάση την πιθανή δημοσιοποίηση των προσωπικών τους δεδομένων και της μη υπηρέτησης ή απόλυσης λόγω διαφόρων «ευαίσθητων δεδομένων» (Απόφαση 6/2007).

Καταληκτικά, έπειτα από την άτυπη αυτή συνέντευξη με το διευθυντή του στρατολογικού γραφείου, θεωρούμε ότι τα ευαίσθητα προσωπικά δεδομένα των στρατεύσιμων προστατεύονται επαρκώς σύμφωνα με τις επιταγές της σχετικής νομοθεσίας.

#### 6.1.4.2: <u>Ασφαλιστική εταιρεία</u>

Στις μέρες μας αρκετοί εργαζόμενοι εκτός από την ασφάλιση τους σε δημόσιο ασφαλιστικό φορέα από την εργασία τους, αναζητούν ασφάλιση σε ιδιωτικές ασφαλιστικές εταιρίες, πρόσθετη ιατροφαρμακευτική περίθαλψη, ασφάλιση ζωής και συνταξιοδοτικά προγράμματα μέχρι και την ασφάλιση της επιχείρησης τους, του σπιτιού τους, του οχήματος τους και γενικότερα της περιουσίας τους για την προστασία τους π.χ. από φυσικές καταστροφές, εμπρησμούς κτλ.

Τα δεδομένα της κοινωνικής ασφάλισης αποτελούν ευαίσθητα προσωπικά δεδομένα σύμφωνα με το ν.2472/1997. Έτσι κρίθηκε αναγκαία η διερεύνηση της διαδικασίας συλλογής και της επεξεργασίας των δεδομένων αυτών από ασφαλιστικές εταιρείες. Για το λόγο αυτό επισκεφθήκαμε ένα τοπικό παράρτημα κάποιας ασφαλιστικής εταιρείας.

Από τη συνέντευξη με το διευθυντή της εταιρείας αυτής προέκυψε ότι τα δεδομένα που συνήθως συλλέγουν από τον υποψήφιο πελάτη τους είναι το ονοματεπώνυμο, η διεύθυνση, η ηλικία, το επάγγελμα, η οικογενειακή κατάσταση, ο Αριθμός Φορολογικού Μητρώου, ο αριθμός δελτίου ταυτότητας, το εκκαθαριστικό σημείωμα και το ιατρικό ιστορικό ανάλογα με το είδος ασφάλισης για το οποίο ενδιαφέρεται ο πελάτης.

Σκοπός της συλλογής τους είναι η εκτίμηση της ανάληψης κινδύνου από μέρους της εταιρείας για την ασφάλιση του εκάστοτε πελάτη. Έτσι η ηλικία και η κατάσταση της υγείας παίζουν σημαντικό ρόλο για το αν η εταιρεία θα προβεί στην ασφάλιση του ατόμου. Δηλαδή υπάρχουν περιπτώσεις όπου το αίτημα για ασφάλιση απορρίπτεται π.χ. για λόγους υγείας, όταν κάποιος είναι παχύσαρκος γεγονός που τον

καθιστά ευάλωτο σε πολλές ασθένειες ή όταν πάσχει από κάποια σοβαρή ή χρόνια ασθένεια.

Η απόφαση για την ασφάλιση κάποιου δε λαμβάνεται από το τοπικό παράρτημα αλλά από το κεντρικό αρμόδιο τμήμα στην Αθήνα. Δηλαδή τα ευαίσθητα προσωπικά δεδομένα των πελατών κοινοποιούνται στα κεντρικά γραφεία της εταιρείας. Το ερώτημα είναι πως γίνεται αυτή η κοινοποίηση; Ο διευθυντής μας είπε ότι γίνεται μέσω του διαδικτύου και με συστημένη αποστολή τους εκεί. Έτσι, γεννιέται το ερώτημα του κατά πόσο ασφαλής είναι η διαδικασία αυτή, αν χρησιμοποιούνται όλα τα απαραίτητα μέτρα προστασίας τους όπως π.χ. η χρήση προστατευτικού υλικού στους υπολογιστές κτλ. Επίσης μας είπε ότι λαμβάνονται όλα τα απαραίτητα μέτρα χωρίς όμως να θελήσουν να μας δώσουν περεταίρω διευκρινήσεις. Τα στοιχεία αυτά αποθηκεύονται τόσο σε ηλεκτρονική όσο και σε έντυπη μορφή εντός της εταιρείας σε ειδικά ντουλάπια που κλειδώνουν στα οποία έχει πρόσβαση μόνο ορισμένοι υπάλληλοι μέσα στο παράρτημα. Επιπλέον μας ανέφερε ότι τα δεδομένα των πελατών χρησιμοποιούνται μόνο για τους σκοπούς που οι ίδιοι οι πελάτες έχουν συμφωνήσει. Αυτό όμως έρχεται σε αντίθεση με το γεγονός ότι όταν π.χ. κάποιος πελάτης πάθει κάποιο ατύχημα, η εταιρεία τον «ενημερώνει» και για άλλες πρόσθετες ασφαλιστικές καλύψεις που θα μπορούσε να είχε. Δηλαδή η εταιρεία εκμεταλλεύεται το συμβάν αυτό προς όφελος της «διαφημίζοντας» και τις άλλες ασφαλιστικές καλύψεις της εταιρείας.

Με βάση την παραπάνω συνέντευξη πιστεύουμε ότι η εταιρεία αυτή θέλει να δηλώνει ότι τη χαρακτηρίζει σοβαρότητα, υπευθυνότητα και συνέπεια προς τους πελάτες της. Όμως θεωρούμε ότι πρέπει να διατηρούνται κάποιες επιφυλάξεις αναφορικά με την προστασία των ευαίσθητων προσωπικών μας δεδομένων, οι οποίες αφορούν τη διαδικασία κοινοποίησης τους στα κεντρικά γραφεία και την ασφάλεια των δεδομένων αυτών.

Βασικότερο όμως όλων είναι το γεγονός ότι ο ασφαλισμένος θεωρείται ως ένα σύνολο προσωπικών πληροφοριών, και πολλά από τα προσωπικά του δεδομένα μπορούν να αποτελέσουν ανασταλτικό παράγοντα για την ασφάλιση του διότι το κίνητρο της εταιρείας είναι τελικά το κέρδος.

### 6.1.4.3: <u>Νοσοκομείο</u>

Στο νοσοκομείο Ρεθύμνου έγινε συνέντευξη με τους υπεύθυνους σε διάφορα γραφεία όπως στο γραφείο κίνησης, στις γραμματείες των κλινικών, στο γραφείο των ραντεβού αλλά και στην κοινωνική υπηρεσία.

Το γραφείο κίνησης συλλέγει προσωπικά και ευαίσθητα προσωπικά δεδομένα των ασθενών που νοσηλεύθηκαν στο νοσοκομείο που αφορούν το ονοματεπώνυμο του ασθενούς, το πατρώνυμο, την ημερομηνία γέννησης τους, την οικογενειακή τους κατάσταση, το φορέα κοινωνικής ασφάλισης, την ημερομηνία εισόδου και εξόδου από το νοσοκομείο, την κλινική όπου νοσηλεύθηκαν και το λόγο νοσηλείας τους.

Τα δεδομένα των ασθενών επεξεργάζονται και χρησιμοποιούνται για την έκδοση εξιτηρίων, την είσπραξη των νοσηλίων και για την έκδοση πιστοποιητικών που οι ίδιοι οι ασθενείς πιθανόν να ζητήσουν για κάθε νόμιμη χρήση.

Μας ειπώθηκε ότι οι ασθενείς γνωρίζουν και ενημερώνονται για το λόγο συλλογής και επεξεργασίας των δεδομένων τους, ενώ γνωρίζουν και το δικαίωμα τους να έχουν πρόσβαση σε αυτά ανά πάσα στιγμή. Σύμφωνα με τον υπάλληλο του συγκεκριμένου γραφείου, οι συνηθέστεροι λόγοι για τους οποίους οι ασθενείς ζητούν να έχουν πρόσβαση στα δεδομένα τους και για την έκδοση ανάλογων πιστοποιητικών είναι για δικαστική χρήση, για χρήση σε επιτροπές των ασφαλιστικών τους ταμείων και για την ιδιωτική τους ασφάλιση, αν διαθέτουν.

Τα ευαίσθητα προσωπικά δεδομένα των ασθενών αποθηκεύονται τόσο σε έντυπη όσο και σε ηλεκτρονική – μηχανογραφημένη μορφή σε αρχεία σε ειδικά ντουλάπια μέσα στο γραφείο κίνησης που κλειδώνουν ενώ όσον αφορά τους υπολογιστές, για να μπορέσει να έχει κάποιος πρόσβαση σε αυτούς πρέπει να γνωρίζει τους κωδικούς. Σε αυτά έχουν πρόσβαση μόνο οι εξουσιοδοτημένοι υπάλληλοι του γραφείου κίνησης και ένα άτομο από το τμήμα διοίκησης του νοσοκομείου, οι οποίοι γνωρίζουν τους κωδικούς πρόσβασης. Ρωτήθηκαν αν αλλάζουν τακτικά τους κωδικούς πρόσβασης και ανέφεραν ότι αυτό γίνεται σχεδόν σε μηνιαία βάση. Τα στοιχεία αυτά τηρούνται για χρονικό διάστημα σύμφωνα με αυτό που ορίζει ο νόμος.

Όσον αφορά τις γραμματείες των κλινικών τα στοιχεία που συλλέγουν είναι το ονοματεπώνυμο των ασθενών, το πατρώνυμο, η ημερομηνία γέννησης, η οικογενειακή κατάσταση στην περίπτωση ανάγκης για επικοινωνία των γιατρών με το

συγγενικό – οικογενειακό περιβάλλον, η διεύθυνση, ο ασφαλιστικός φορέας, η ημερομηνία εισόδου και εξόδου από το νοσοκομείο και η διάγνωση – πάθηση τους.

Σύμφωνα με την υπάλληλο, τα στοιχεία αυτά τηρούνται προς ενημέρωση του γραφείου κινήσεως, για την τοποθέτηση των ασθενών σε δωμάτια, για την ενημέρωση των γιατρών σχετικά με τον αριθμό των ασθενών που νοσηλεύονται, την πάθηση τους κτλ αλλά και για την ενημέρωση του τηλεφωνικού κέντρου για την καλύτερη εξυπηρέτηση εκείνων που καλούν για να μάθουν σε ποιο δωμάτιο νοσηλεύεται κάποιος γνωστός ή οικείος τους. Στα δεδομένα αυτά έχουν πρόσβαση μόνο οι γιατροί και οι ασθενείς ή οι συγγενείς τους ενώ παράλληλα γνωστοποιούνται στο γραφείο κίνησης και στο τηλεφωνικό κέντρο για την καλύτερη λειτουργία του νοσοκομείου αλλά και για την καλύτερη εξυπηρέτηση των ίδιων των ασθενών. Τέλος, φυλάσσονται σε ντουλάπια που κλειδώνουν μέσα στο δωμάτιο της γραμματείας στο οποίο πρόσβαση έχει μόνο η συγκεκριμένη υπάλληλος και για χρονικό διάστημα που ορίζει ο νόμος.

Όταν καλείται το γραφείο των ραντεβού προκειμένου να κανονιστεί κάποιο ραντεβού για γιατρό ζητούνται το ονοματεπώνυμο, το πατρώνυμο, η διεύθυνση, τηλέφωνο επικοινωνίας και ο ασφαλιστικός φορέας στον οποίο ανήκει ο εξυπηρετούμενος. Σύμφωνα με τον υπάλληλο του γραφείου αυτού, τα στοιχεία αυτά συλλέγονται αποκλειστικά και μόνο για την καλύτερη εξυπηρέτηση των ασθενών. Χρησιμοποιούνται δηλαδή για την οργάνωση των ραντεβού ανά ημέρα και ανά ιατρείο, για την ειδοποίηση των ασθενών στην περίπτωση που δεν είναι εφικτή η υλοποίηση των ραντεβού για διάφορους λόγους αλλά και για τη δημιουργία φακέλου για κάθε ασθενή προκειμένου να γνωρίζουν την κίνηση καθενός από αυτούς στο νοσοκομείο, με την έννοια ότι παρακολουθούν ποιες επισκέψεις και πόσες έχουν πραγματοποιήσει ανά ιατρείο κτλ. Μάλιστα, τον τελευταίο καιρό τα οργανώνουν με τη χρήση υπολογιστών στους οποίους υπάρχουν κωδικοί πρόσβασης τους οποίους γνωρίζουν οι εξουσιοδοτημένοι υπάλληλοι του γραφείου αλλά και ένα άτομο της διοίκησης και τους οποίους φροντίζουν να αλλάζουν ανά δύο με τρεις μήνες. Τα στοιχεία αυτά υπάρχουν και σε έντυπη μορφή και φυλάσσονται στο συγκεκριμένο γραφείο σε ειδικά ντουλάπια που κλειδώνουν.

Με βάση την άτυπη συνέντευξη μας πιστεύουμε ότι κάποιοι από τους υπεύθυνους έχουν επίγνωση του ότι χειρίζονται ευαίσθητα προσωπικά δεδομένα, ενώ κάποιοι άλλοι θεωρούν την επεξεργασία τους ως μία διαδικασία ρουτίνας.

Όσο για την κοινωνική υπηρεσία, υπάρχει αρχείο που τηρείται σε έντυπη μορφή όπου καταγράφονται τα περιστατικά και το κοινωνικό ιστορικό των ατόμων που έχουν επισκεφθεί την κοινωνική λειτουργό. Τα συνηθέστερα στοιχεία που συλλέγονται είναι το ονοματεπώνυμο, το πατρώνυμο, η ημερομηνία γέννησης, η οικογενειακή κατάσταση και όνομα και τηλέφωνο πλησιέστερου συγγενούς στην περίπτωση που χρειάζεται να γίνει επικοινωνία με το οικείο οικογενειακό – συγγενικό περιβάλλον, η διεύθυνση, ο ασφαλιστικός τους φορέας, η κατάσταση της σωματικής και ψυχικής τους υγείας.

Ο σκοπός της συλλογής τους είναι η πληρέστερη κατανόηση της κατάστασης του ασθενούς και η επικοινωνία με το συγγενικό του περιβάλλον αν αυτό κριθεί αναγκαίο. Έτσι δημιουργείται ένα αρχείο που αναφέρεται στην πορείας της υγείας και της γενικότερης κοινωνικής και ψυχολογικής κατάστασης του ασθενούς. Τα δεδομένα αυτά μπορούν να κοινοποιηθούν μόνο στην περίπτωση ανάγκης συνεργασίας με άλλους φορείς όπως η Διεύθυνση Κοινωνικής Πρόνοιας, τα ΚΑΠΗ, τα προγράμματα «Βοήθεια στο σπίτι», οι δικαστικές αρχές, υπηρεσίες οι οποίες με τη σειρά τους δεσμεύονται για την τήρηση του απορρήτου η οποία αποτελεί βασική αρχή δεοντολογίας του επαγγέλματος τους.

#### 6.1.4.4: <u>Αλυσίδα super market</u>

Βασική τακτική των περισσότερων αλυσίδων super market στις μέρες μας είναι η προσέλκυση πελατών και η διατήρηση τους με την έκδοση «bonus cards» και «loyalty cards» οι οποίες προσφέρουν εκπτώσεις ή δώρα στους καταναλωτές σε κάθε τους συναλλαγή – αγορά από το εκάστοτε super market της αλυσίδας. Πάνω στις κάρτες αυτές υπάρχει ένα barcode στο οποίο καταγράφονται τα στοιχεία και οι αγορές μας κάθε φορά που τη χρησιμοποιούμε.

Η έκδοση τους γίνεται στα ταμεία όπου ο καταναλωτής καλείται να συμπληρώσει μία φόρμα με προσωπικά του δεδομένα όπως το ονοματεπώνυμο, ηλικία, επάγγελμα, οικογενειακή κατάσταση, διεύθυνση, αριθμό ατόμων στο νοικοκυριό, ηλικία πρώτου, δεύτερου και τρίτου παιδιού κτλ.

Ο υπάλληλος που εκδίδει την κάρτα αυτή ενημερώνει τους καταναλωτές ότι χρησιμοποιείται είτε για τη συλλογή πόντων με τις αγορές όπου τελικά δίνεται δωροεπιταγή, είτε επειδή χρησιμοποιώντας τις μπορούν να έχουν έκπτωση σε κάποια προϊόντα. Όμως ακόμη και οι ίδιοι οι υπάλληλοι που έχουν αναλάβει και είναι

υπεύθυνοι τη συλλογή των προσωπικών δεδομένων των πελατών αλλά και για τη σωστή ενημέρωση τους αγνοούν όπως διαπιστώσαμε το σκοπό και τον τρόπο επεξεργασίας των δεδομένων που συλλέγουν.

Σημαντικό επίσης είναι το ότι κανένας υπάλληλος δεν παρακινεί τον πελάτη να διαβάσει τους όρους «εμπιστευτικότητας» που αναγράφονται με πολύ μικρά γράμματα στο τέλος της φόρμας αυτής. Κανένας καταναλωτής δε γνωρίζει τελικά για ποιο λόγο πραγματικά συμπληρώνει τη συγκεκριμένη φόρμα, ποιος χρησιμοποιεί τα προσωπικά του δεδομένα, πως και για ποιους σκοπούς. Όλοι τους φαίνεται να αγνοούν, ακόμη και οι υπάλληλοι, τον «όρο εμπιστευτικότητας» που αναφέρει ότι «ο κάτοχος της κάρτας αυτής επιτρέπει στην εταιρεία να συγκεντρώνει, διατηρεί και επεξεργάζεται τα στοιχεία που αναφέρονται σε αυτήν… ότι η εταιρεία εγγυάται την προστασία των στοιχείων αυτών από οποιαδήποτε παράνομη πρόσβαση και αθέμιτη επεξεργασία καθώς και τη χρήση τους αποκλειστικά και μόνο για εμπορικούς και επικοινωνιακούς σκοπούς» (Έντυπο αίτησης).

Έπειτα από συνέντευξη με το διευθυντή του πολυκαταστήματος διαπιστώσαμε ότι τα στοιχεία αυτά χρησιμοποιούνται για στατιστικούς λόγους και για λόγους πιστότητας των πελατών, δηλαδή του ελέγχου της επισκεψιμότητας των πελατών στο κατάστημα. Χρησιμοποιούνται δηλαδή από το τμήμα μάρκετινγκ και το τμήμα πωλήσεων προκειμένου να διαπιστώσουν ποιοι είναι οι πελάτες τους, από ποιο κοινωνικοοικονομικό στρώμα προέρχονται, ποια είναι η σχέση οικονομικού στρώματος και προϊόντων που αγοράζουν, ποια είναι η σχέση κοινωνικού στρώματος και προϊόντων που αγοράζουν, ποια προϊόντα παρουσιάζουν αυξημένη ή μειωμένη κατανάλωση κτλ.

Επίσης χρησιμοποιούνται για να διαπιστωθεί αν υπάρχει σχέση ανάμεσα στην αυξημένη ή μειωμένη κατανάλωση των προϊόντων με την τιμή των προϊόντων, με την οικονομική κατάσταση των καταναλωτών, με τον αριθμό των ατόμων στο νοικοκυριό, τον τόπο κατοικίας, την ηλικία, την οικογενειακή κατάσταση του καταναλωτή.

Έτσι δημιουργούν το προφίλ των καταναλωτών που λειτουργεί βοηθητικά προς την επιχείρηση δίνοντας της τη δυνατότητα να αναπροσαρμόσει το μάρκετινγκ της, να βελτιώσει την προώθηση των πωλήσεων αλλά και να κάνει τις ανάλογες προσφορές σε διάφορα προϊόντα πρώτης ανάγκης αλλά και σε νέα προϊόντα που θέλουν να προωθήσουν, είτε σε προϊόντα των οποίων την πώληση θέλουν να αυξήσουν.

### 6.1.5: Συμπεράσματα από την έρευνα σε φορείς

Μέσα από τις συνεντεύξεις στους παραπάνω φορείς επαληθεύτηκε η αρχική μας υπόθεση ότι οι φορείς αυτοί σε τοπικό επίπεδο δεν εφαρμόζουν αυστηρά την προστασία των προσωπικών δεδομένων ιδίως των ευαίσθητων προσωπικών δεδομένων που είναι ζωτικής σημασίας. Αν και τα πάντα οργανώνονται και λειτουργούν γύρω από αυτά, τα δεδομένα άλλες φορές για την καλύτερη εξυπηρέτηση των «πελατών» και άλλες προς όφελος του ίδιου του φορέα, υπάρχει πρόβλημα για την ασφαλή προστασία τους.

Φαινομενικά τουλάχιστον τα πάντα λειτουργούν σύμφωνα με τις βασικές επιταγές του νόμου. Όμως σχεδόν ουδείς φορέας φροντίζει να ενημερώνει τα υποκείμενα των δεδομένων για τα δικαιώματα τους αναφορικά με την πρόσβαση σε αυτά, τη γνώση του σκοπού και του τρόπου επεξεργασίας τους, γεγονός που έρχεται σε αντίθεση με όσα ισχυρίστηκαν για τη νομιμότητα των διαδικασιών που ακολουθούν.

Για παράδειγμα οι εργαζόμενοι στην αλυσίδα super market παρακινούν τους πελάτες να γίνουν κάτοχοι των «smart και loyalty cards» χωρίς να γνωρίζουν τους πραγματικούς σκοπούς συλλογής των δεδομένων των πελατών με αποτέλεσμα να μην ενημερώνουν κατάλληλα και τους καταναλωτές. Όσο για τους ίδιους τους καταναλωτές, αγνοούν τους όρους απόκτησης των «smart cards» – κερδοκάρτας, αφού είναι γραμμένοι στο κάτω μέρος της φόρμας με πολύ μικρά γράμματα. Έτσι δίνουν τη συγκατάθεση τους για την επεξεργασία και διάδοση – πώληση των δεδομένων τους μη γνωρίζοντας αν και πως αυτά θα επεξεργαστούν αλλά και το πως και για ποιους σκοπούς θα χρησιμοποιηθούν.

Όσο για το στρατολογικό γραφείο, η εκχώρηση των προσωπικών και ευαίσθητων προσωπικών δεδομένων θεωρείται υποχρεωτική και αναπόφευκτη διαδικασία την οποία πρέπει να υποστούν όλοι οι άρρενες Έλληνες αφού αποτελεί γι' αυτούς καθολική υποχρέωση. Το σύστημα αυτό μπορεί να χαρακτηριστεί καθολικό και επιβάλλει διακρίσεις με διάφορους τρόπους, στιγματίζοντας και αποκλείοντας όσους παρεκκλίνουν από το «κανονικό», π.χ. από το δημόσιο τομέα κτλ.

Όσο για την ασφαλιστική εταιρεία αρκεί να σκεφτούμε ότι πρόκειται για ιδιωτική επιχείρηση και ως τέτοια έχει σαν σκοπό το κέρδος στου οποίου το βωμό μπορεί ενδεχομένως να θυσιάζεται το απόρρητο των προσωπικών πληροφοριών. Χαρακτηριστική είναι η απόφαση 42/2007 όπου επιβάλλεται στην

ΙΝΤΕΡΑΜΕΡΙΚΑΝ ΕΛΛΗΝΙΚΗ ΕΤΑΙΡΕΙΑ ΑΣΦΑΛΙΣΕΩΝ ΖΗΜΙΩΝ ΑΕ πρόστιμο ύψους σαράντα χιλιάδων ευρώ (40.000) για την παράλειψη της ικανοποίησης του δικαιώματος πρόσβασης κάποιου ασφαλισμένου στα ευαίσθητα προσωπικά δεδομένα που αφορούν το πρόσωπο του, αλλά και η απόφαση 3/2008 όπου επιβάλλει πρόστιμο εξήντα χιλιάδων ευρώ (60.000) στην ΕΘΝΙΚΗ ΑΣΦΑΛΙΣΤΙΚΗ για επεξεργασία των ευαίσθητων προσωπικών δεδομένων κάποιου τα οποία περιλαμβάνονται στο απολυτήριο του στρατού και αφορούν το σεξουαλικό του προσανατολισμό για την αξιολόγηση του αιτήματος του για σύναψη ασφάλειας ζωής (www.dpa.gr).

Το γενικότερο συμπέρασμα των παραπάνω άτυπων συνεντεύξεων μας είναι ότι παρά την ύπαρξη της αναγκαίας νομοθεσίας για την προστασία των προσωπικών και των ευαίσθητων προσωπικών δεδομένων, υπάρχει πρόβλημα στην εφαρμογή της και ιδιαίτερα στο επίπεδο της τοπικής κοινωνίας μιας επαρχιακής πόλης όπως το Ρέθυμνο. Τα αίτια μπορούν να αναζητηθούν α) στην έλλειψη ελέγχων στους φορείς συλλογής και επεξεργασίας προσωπικών δεδομένων, β) στην άγνοια ή αμέλεια των πολιτών για τη διεκδίκηση της άσκησης των δικαιωμάτων τους και γ) στην έλλειψη ενημέρωσης των πολιτών σε θέματα που αφορούν την προστασία των προσωπικών και ιδιαίτερα των ευαίσθητων προσωπικών τους δεδομένων.

## 6.2: Εμπειρική έρευνα με ερωτηματολόγιο

### 6.2.1: Αντικείμενο και στόχοι της έρευνας με ερωτηματολόγιο

Αντικείμενο της έρευνας με ερωτηματολόγιο αποτελεί η ανάδειξη των απόψεων – αντιλήψεων κατοίκων του Ρεθύμνου σχετικά με την προστασία ή μη των προσωπικών και των ευαίσθητων προσωπικών τους δεδομένων.

Επιμέρους στόχος της έρευνας αυτής είναι η διερεύνηση της πιθανής σχέσης ανάμεσα στη χρήση των υπηρεσιών που προσφέρουν διάφοροι φορείς οι οποίοι τηρούν προσωπικά δεδομένα με τις αντιλήψεις των κατοίκων του Ρεθύμνου για το βαθμό προστασίας των προσωπικών τους δεδομένων.

### 6.2.2: Μεθοδολογία και στάδια της έρευνας με ερωτηματολόγιο

Για την πραγματοποίηση της έρευνας με ερωτηματολόγιο, αρχικά πραγματοποιήθηκε βιβλιογραφική έρευνα και μελέτη. Στη συνέχεια, μέσω διαδικτύου βρήκαμε παρόμοιες έρευνες αναφορικά με τις αντιλήψεις πολιτών για την προστασία των προσωπικών τους δεδομένων. Από αυτές επιλέχθηκαν δύο: α) η έρευνα του Ευρωβαρομέτρου (Ιανουάριος, 2008) για τη μελέτη των αντιλήψεων πολιτών των χωρών της ΕΕ σχετικά με την προστασία των προσωπικών τους δεδομένων αλλά και β) η έρευνα της Σχολής Κοινωνικών Επιστημών του Πανεπιστημίου Κρήτης που είχε σαν στόχο τη διερεύνηση θεμάτων προστασίας της ιδιωτικής ζωής και των προσωπικών δεδομένων εντός της Πανεπιστημιακής Κοινότητας (2008) που είχε αναρτηθεί στην ιστοσελίδα της Σχολής Κοινωνικών Επιστημών www.soc.uoc.gr .

Για την πραγματοποίηση της έρευνας αυτής χρησιμοποιήθηκε η μέθοδος του ερωτηματολογίου, του οποίου η σύνταξη αποτελεί συνδυασμό των ερωτηματολογίων που χρησιμοποιήθηκαν στις προαναφερθείσες έρευνες. Έτσι, το δείγμα αποτέλεσαν σαράντα δύο (42) κάτοικοι της πόλης του Ρεθύμνου είκοσι επτά (27) γυναίκες και δεκαπέντε (15) άνδρες. Το δείγμα μας είναι τυχαίο και ενδεικτικό και δεν μπορεί να θεωρηθεί αντιπροσωπευτικό.

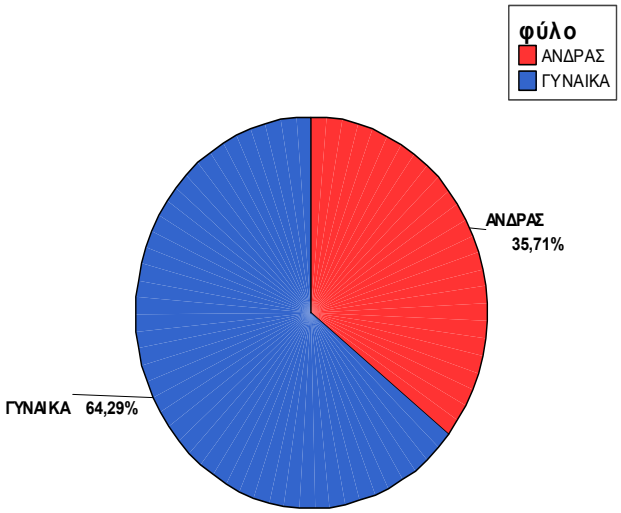
Η ανάλυση των ερωτηματολογίων πραγματοποιήθηκε με τη βοήθεια του στατιστικού προγράμματος SPSS 16.0. Ακολούθησε η ερμηνεία των αποτελεσμάτων που προέκυψαν από την ανάλυση αυτή.

### 6.2.3: Τα αποτελέσματα της έρευνας με ερωτηματολόγιο

#### 6.2.3.1: Γραφική απεικόνιση των αποτελεσμάτων της έρευνας με ερωτηματολόγιο

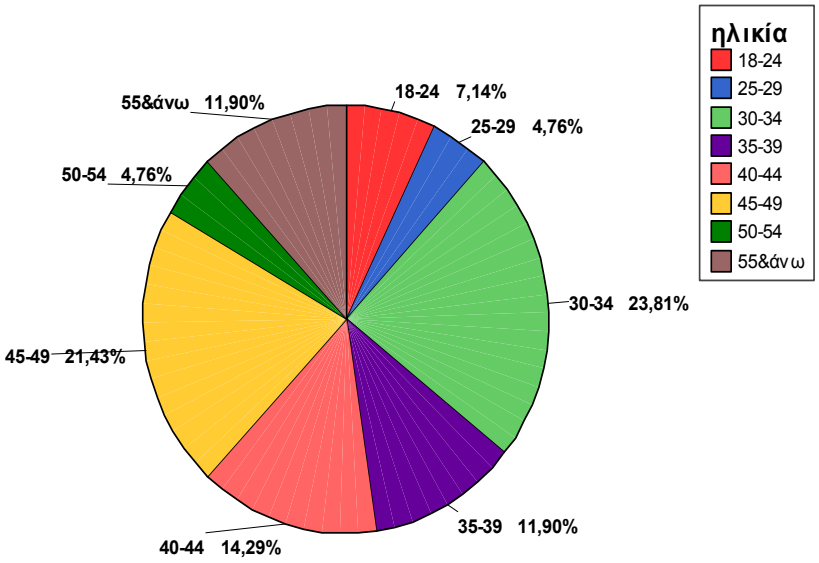
Ακολουθεί η γραφική απεικόνιση των αποτελεσμάτων της έρευνας ανά ερώτηση.

## ΦΥΛΟ



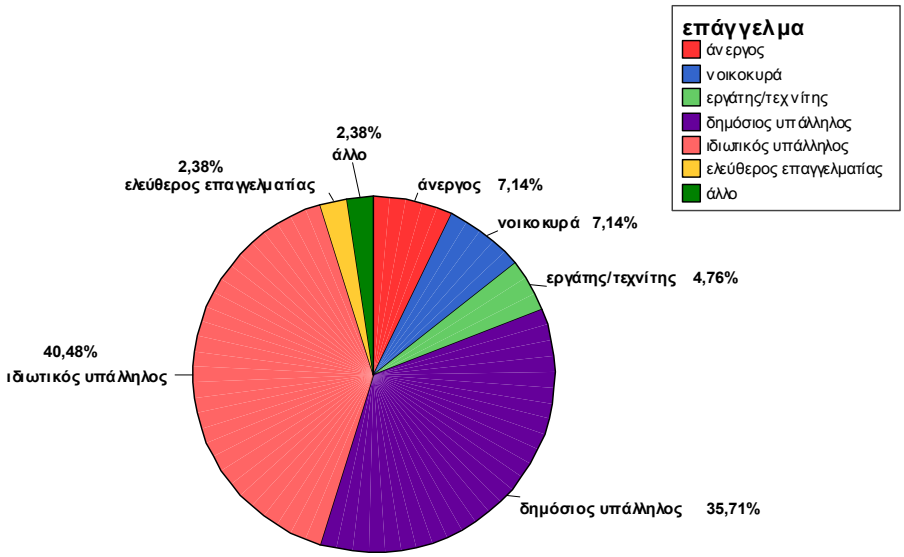

**ΔΙΑΓΡΑΜΜΑ 1**

## ΗΛΙΚΙΑ



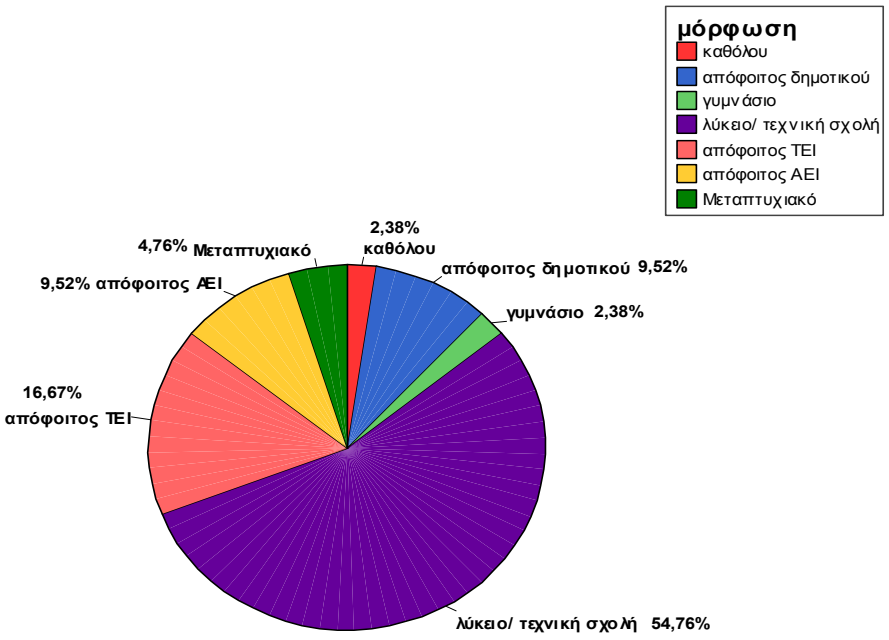

**ΔΙΑΓΡΑΜΜΑ 2**

## ΕΠΑΓΓΕΛΜΑ



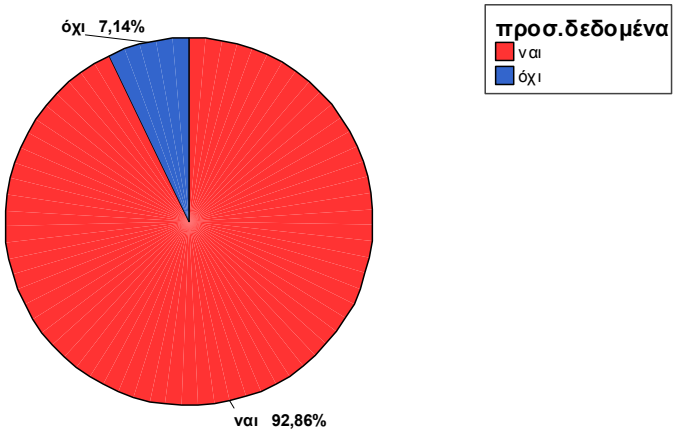

**ΔΙΑΓΡΑΜΜΑ 3**

## ΜΟΡΦΩΤΙΚΟ ΕΠΙΠΕΔΟ



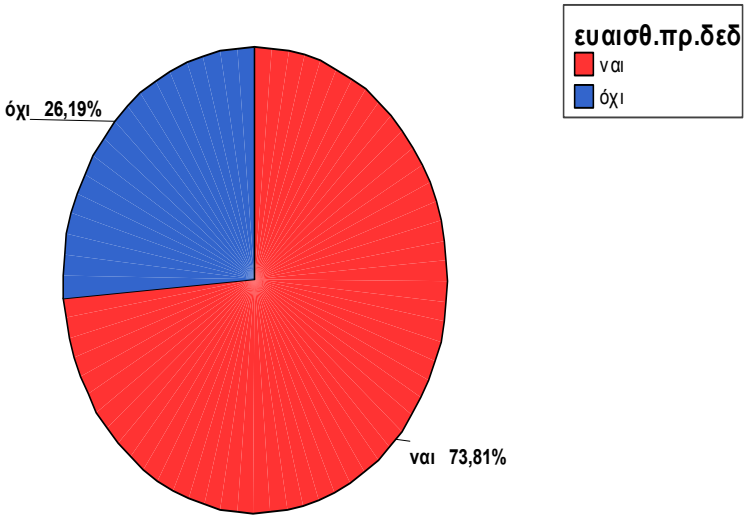

**ΔΙΑΓΡΑΜΜΑ 4**

**Γνωρίζετε τι είναι προσωπικά δεδομένα;**



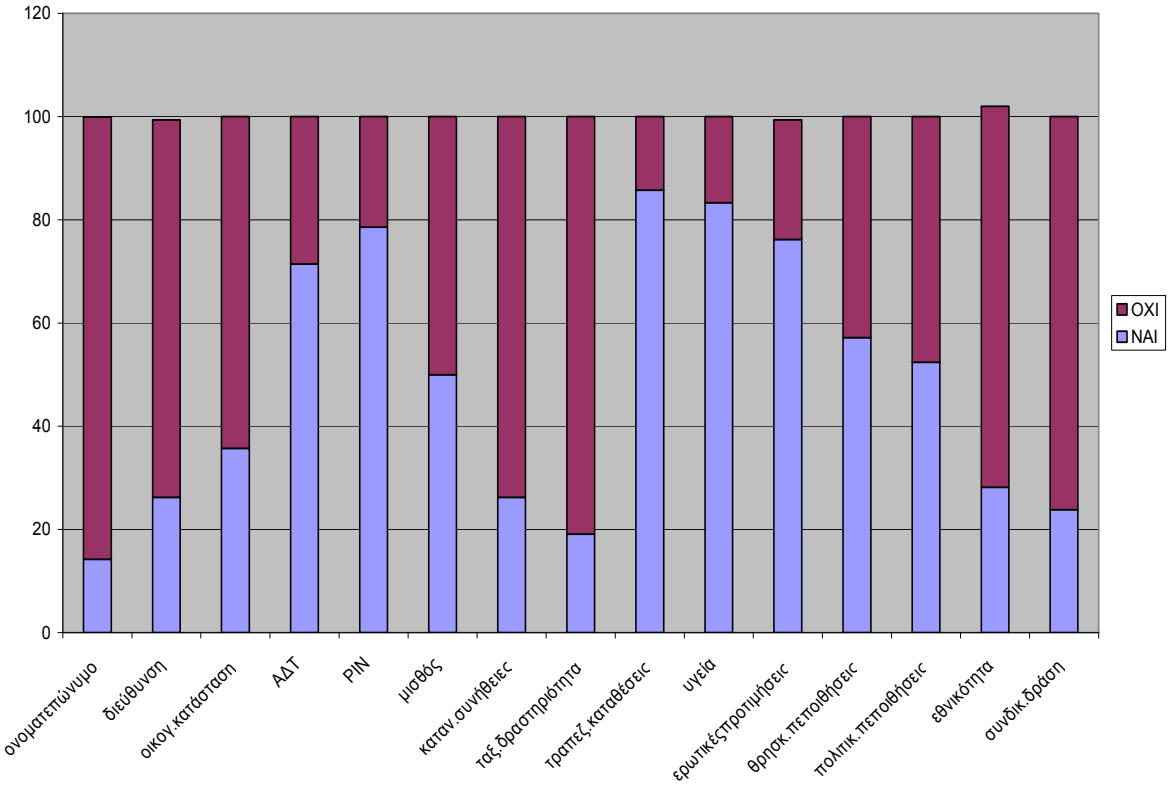

**ΔΙΑΓΡΑΜΜΑ 5**

**Γνωρίζετε τι είναι ευαίσθητα προσωπικά δεδομένα;**



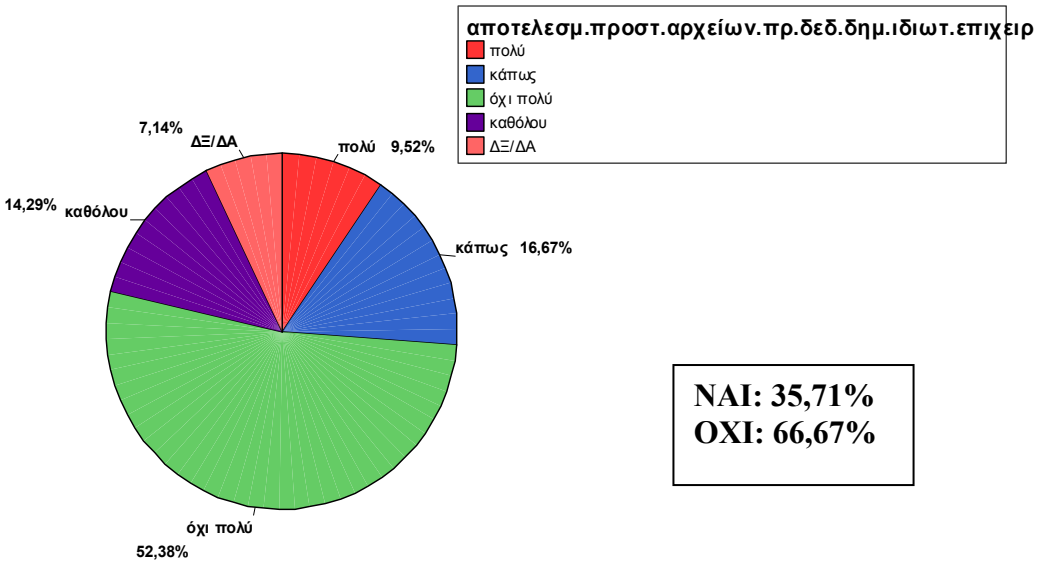

**ΔΙΑΓΡΑΜΜΑ 6**

**Ποια από τα παρακάτω δεδομένα θεωρείτε ότι είναι ευαίσθητα και ποια όχι;**



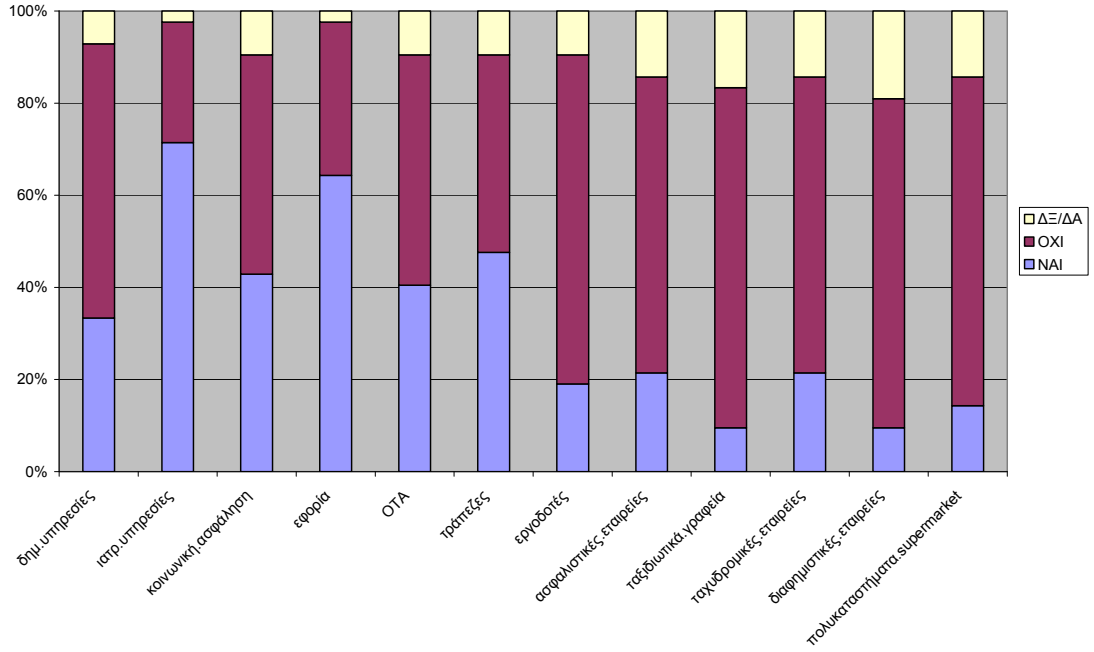

**ΔΙΑΓΡΑΜΜΑ 7**

**Σε ποιο βαθμό πιστεύετε ότι οι νόμοι στην Ελλάδα είναι αποτελεσματικοί για την προστασία των προσωπικών σας πληροφοριών – δεδομένων που διατηρούνται στα αρχεία των δημόσιων υπηρεσιών αλλά και των ιδιωτικών επιχειρήσεων;**



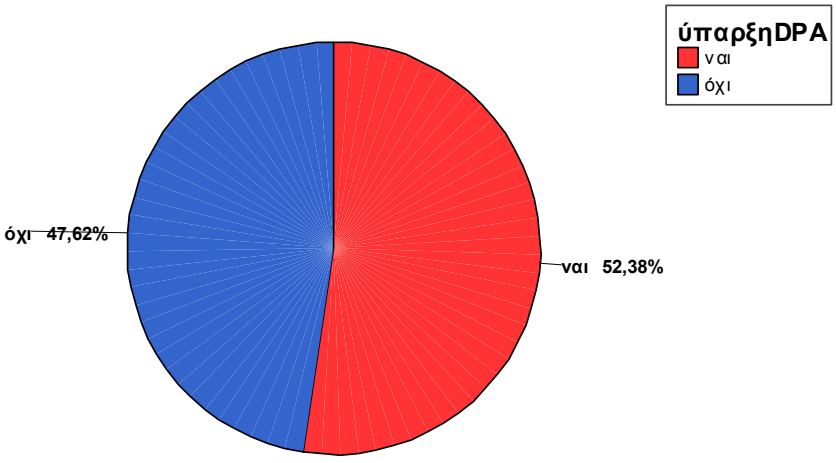

**ΔΙΑΓΡΑΜΜΑ 8**

**Ακολουθεί μία λίστα οργανισμών που πιθανόν να κρατούν κάποια προσωπικά σας δεδομένα. Ποιους από αυτούς εμπιστεύεστε ότι κάνουν σωστή χρήση των προσωπικών σας πληροφοριών.**



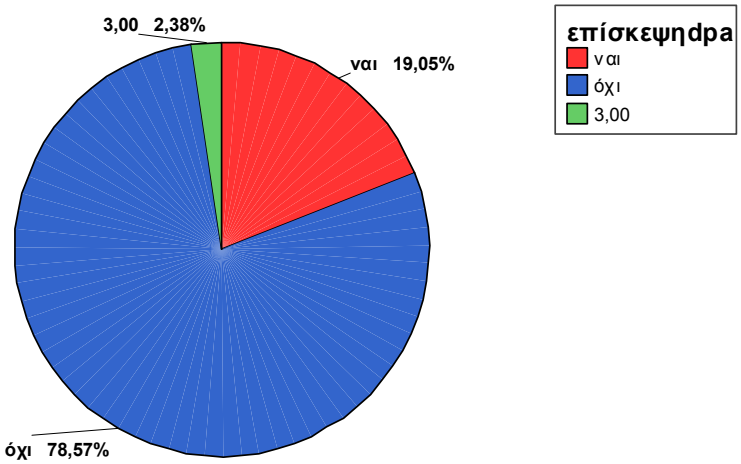

**ΔΙΑΓΡΑΜΜΑ 9**

**Γνωρίζετε για την ύπαρξη και λειτουργία της Ελληνικής ΑΠΔΠΧ που λειτουργεί στην Ελλάδα από το Νοέμβριο του 1997;**



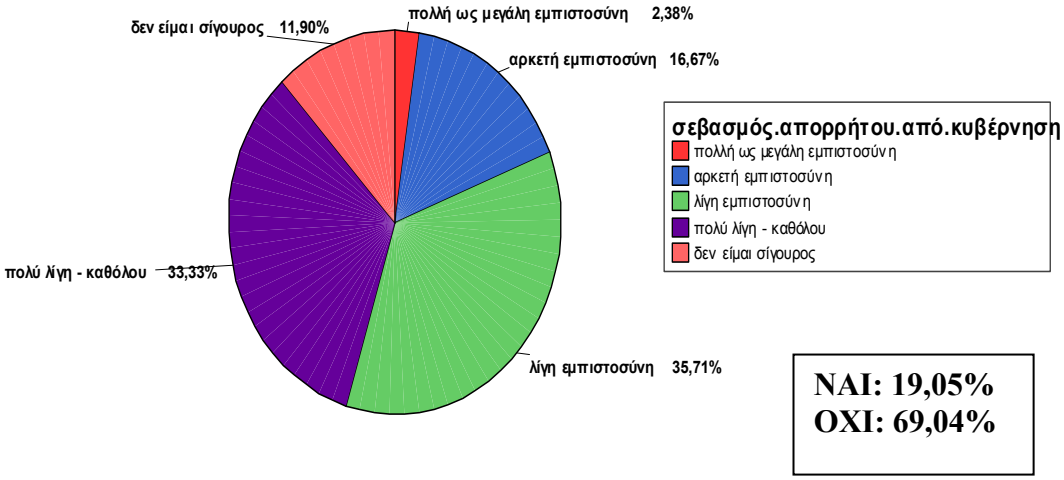

**ΔΙΑΓΡΑΜΜΑ 10**

**Αν ναι, έχετε επισκεφθεί την ιστοσελίδα (www.dpa.gr) της ΑΠΔΠΧ;**



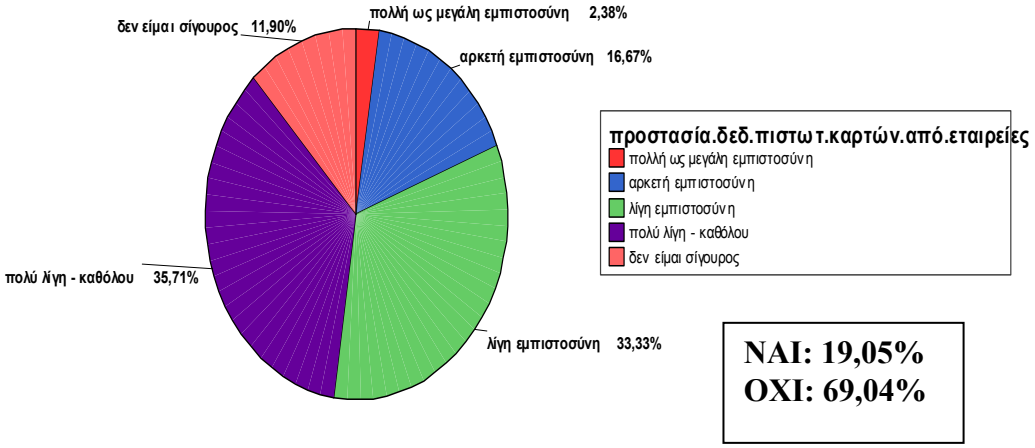

**ΔΙΑΓΡΑΜΜΑ 11**

**Πόση εμπιστοσύνη έχετε στην εκάστοτε Ελληνική Κυβέρνηση αν αυτή σέβεται το απόρρητο των προσωπικών πληροφοριών των πολιτών;**



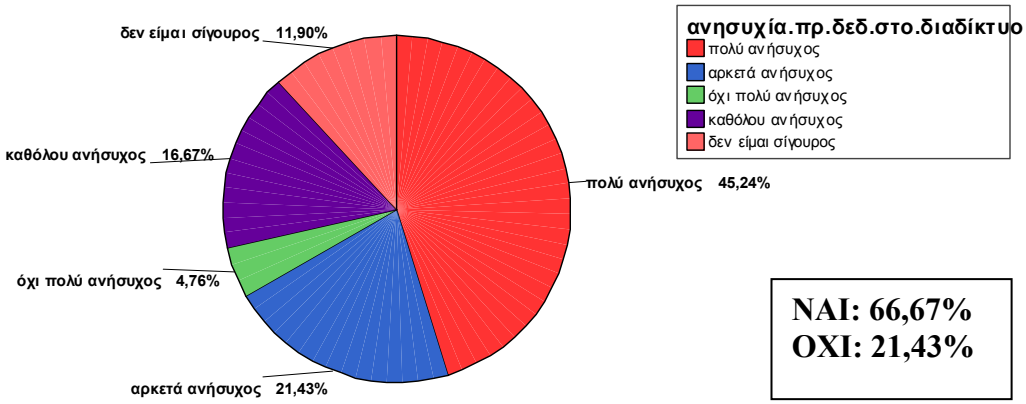

**ΔΙΑΓΡΑΜΜΑ 12**

**Πόση εμπιστοσύνη έχετε ότι οι ιδιωτικές εταιρείες, οι τράπεζες, τα σούπερ μάρκετ και όπου αλλού ψωνίζετε με πιστωτικές κάρτες, προστατεύουν τις προσωπικές σας πληροφορίες;**



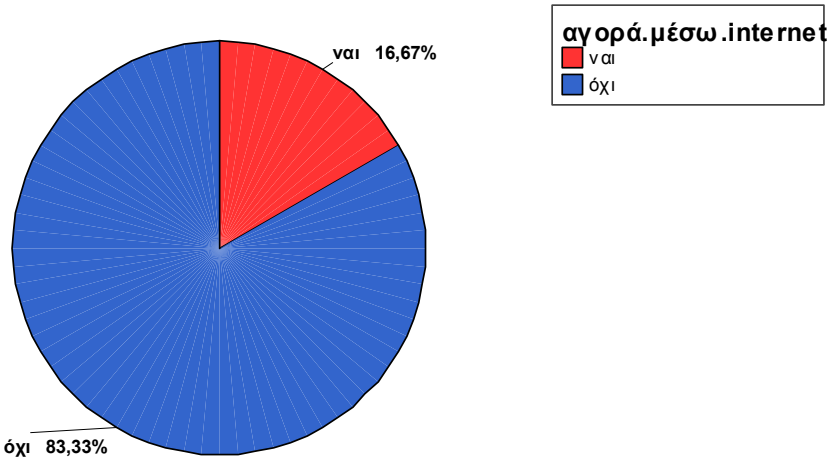

**ΔΙΑΓΡΑΜΜΑ 13**

**Στο θέμα της προστασίας της ιδιωτικής ζωής (ιδιωτικότητας) και των προσωπικών σας δεδομένων πόσο ανήσυχος-η είστε όταν δίνετε προσωπικές πληροφορίες στο διαδίκτυο (internet), όπως το όνομα σας, διεύθυνση, ημερομηνία γέννησης, φύλο, αριθμό πιστωτικής κάρτας κτλ;**



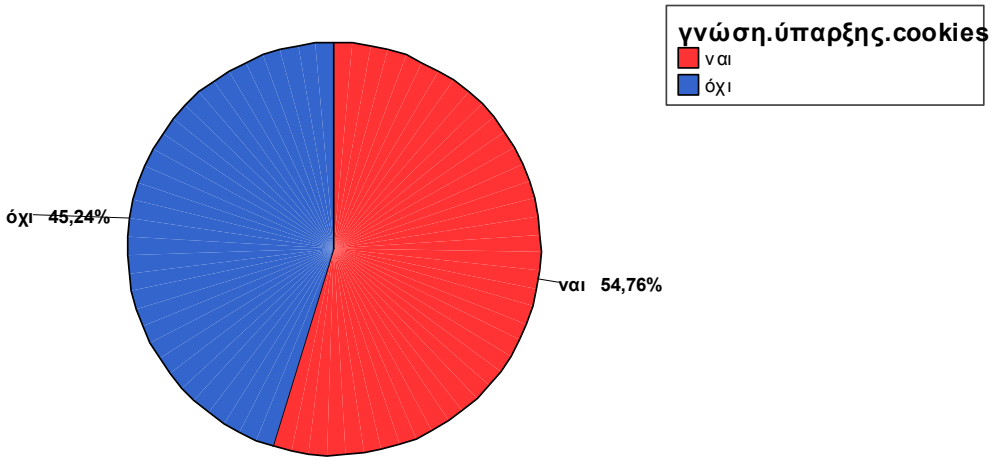

**ΔΙΑΓΡΑΜΜΑ 14**

**Έχετε αγοράσει ποτέ κάποιο προϊόν ή υπηρεσία μέσω του Internet;**



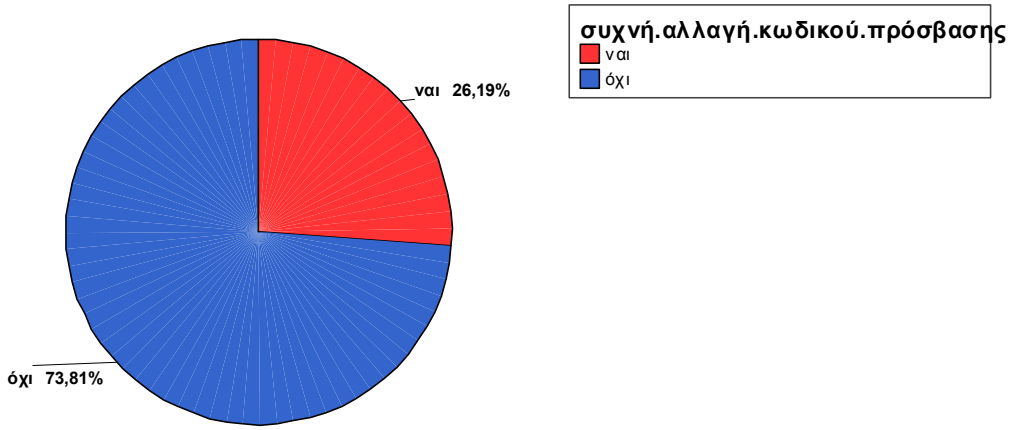

**ΔΙΑΓΡΑΜΜΑ 15**

**Γνωρίζετε ότι με διάφορα προγράμματα (cookies) μπορεί να παρακολουθούνται τα ψηφιακά ίχνη σας στο διαδίκτυο;**



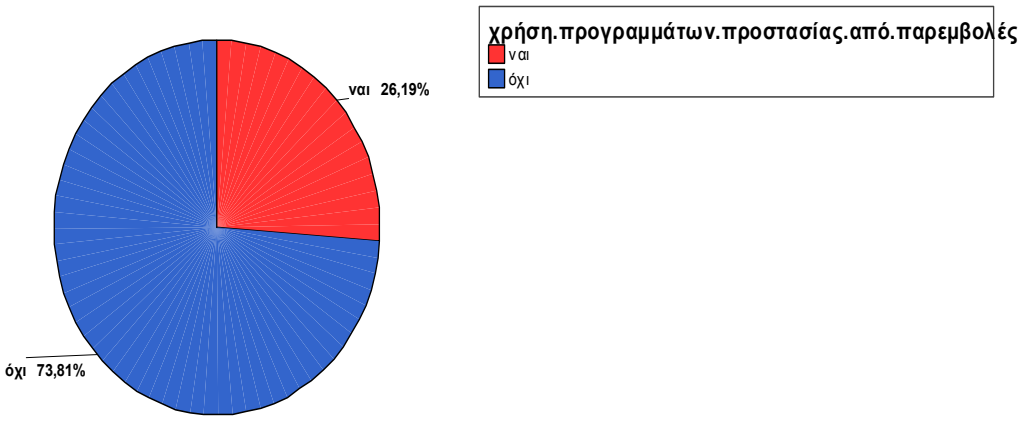

**ΔΙΑΓΡΑΜΜΑ 16**

**Αλλάζετε συχνά τον κωδικό πρόσβασης σας στο διαδίκτυο και στις πιστωτικές κάρτες σας;**



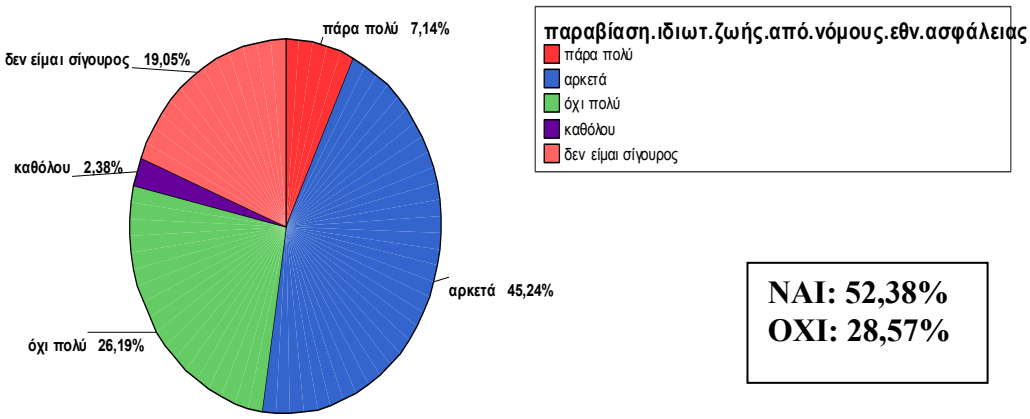

**ΔΙΑΓΡΑΜΜΑ 17**

**Χρησιμοποιείτε στον Η/Υ και στο κινητό σας τηλέφωνο κάποιο πρόγραμμα προστασίας από παρενοχλήσεις, εισβολείς – χάκερς κτλ;**



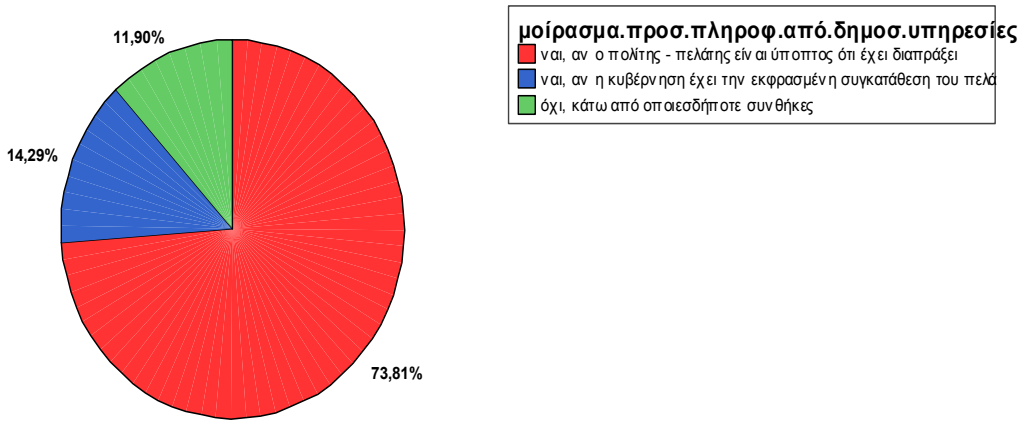

**ΔΙΑΓΡΑΜΜΑ 18**

**Οι ελληνικές κυβερνήσεις έχουν περάσει νόμους για την προστασία της εθνικής ασφάλειας. Σε ποιο βαθμό πιστεύετε ότι οι νόμοι αυτοί για την προστασία της εθνικής ασφάλειας παραβιάζουν την ιδιωτική ζωή των πολιτών;**



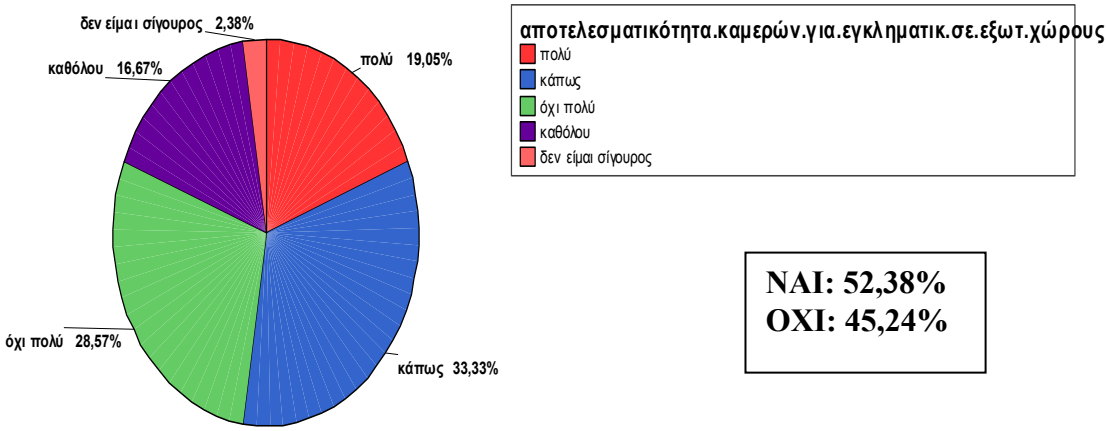

**ΔΙΑΓΡΑΜΜΑ 19**

**Σε ποιο βαθμό θεωρείτε ότι πρέπει μια κυβερνητική/ δημόσια υπηρεσία ή μια επιχείρηση να μοιράζεται τις προσωπικές πληροφορίες των πολιτών – πελατών: α. με άλλες υπηρεσίες, β. με ξένες κυβερνήσεις και γ. με ιδιωτικές επιχειρήσεις;**




**ΔΙΑΓΡΑΜΜΑ 20**

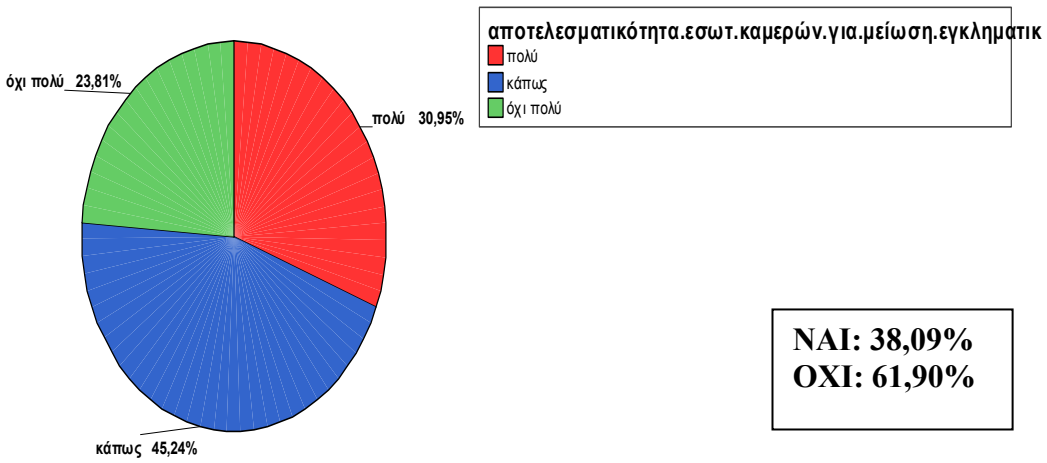
**Κατά τη γνώμη σας πόσο αποτελεσματικές στη μείωση της εγκληματικότητας είναι οι κάμερες σε εξωτερικούς δημόσιους χώρους;**




**ΝΑΙ: 52,38%**
**ΟΧΙ: 45,24%**

**ΔΙΑΓΡΑΜΜΑ 21**

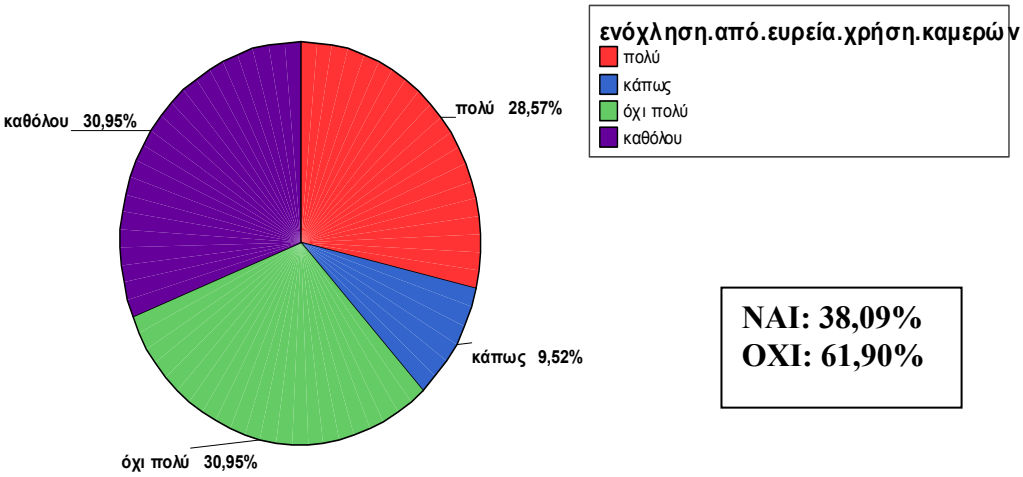
**Κατά τη γνώμη σας πόσο αποτελεσματικές στη μείωση της εγκληματικότητας είναι οι εσωτερικές κάμερες σε επιχειρήσεις, τράπεζες κτλ;**




**ΝΑΙ: 38,09%**
**ΟΧΙ: 61,90%**

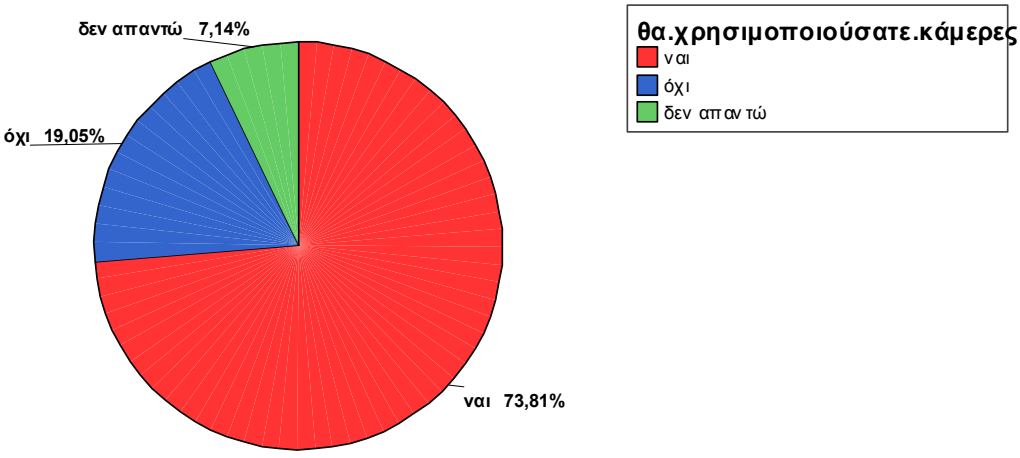
**ΔΙΑΓΡΑΜΜΑ 22**

**Σας ενοχλεί ή όχι το γεγονός της ευρείας χρήσης καμερών ασφαλείας σε πάρα πολλούς χώρους όπως στα περίπτερα, ακόμα και σε εκκλησίες;**



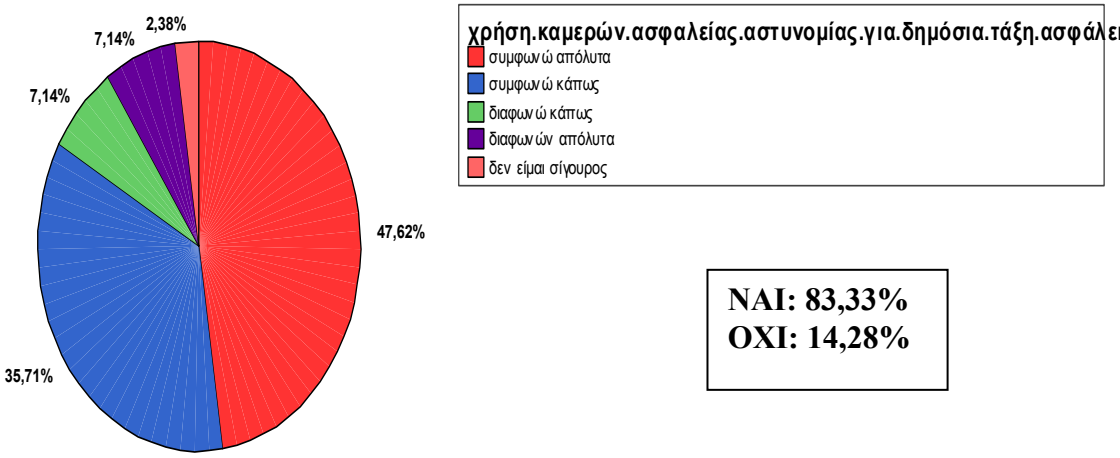

**ΔΙΑΓΡΑΜΜΑ 23**

**Εσείς θα χρησιμοποιούσατε κάμερες ασφαλείας για τη φύλαξη και ασφάλεια της κατοικίας ή της επιχείρησης σας;**



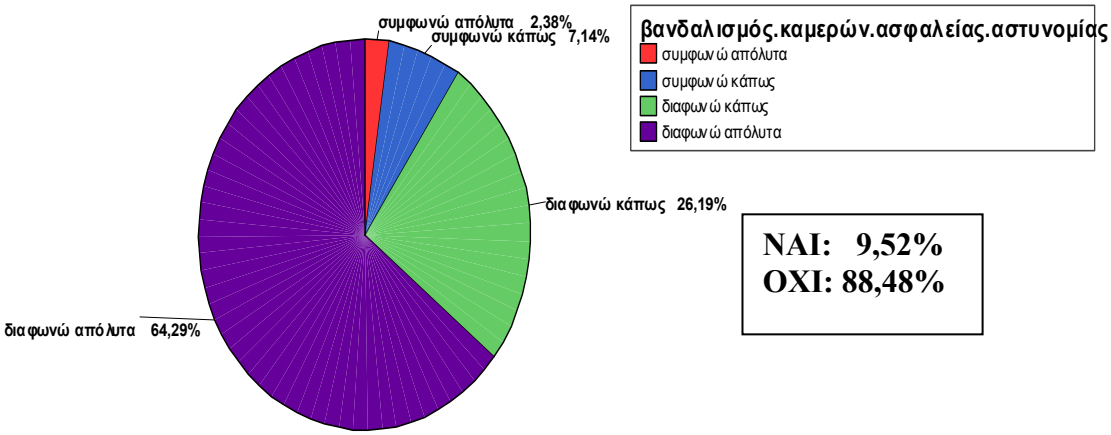

**ΔΙΑΓΡΑΜΜΑ 24**

**Συμφωνείτε ή διαφωνείτε οι κάμερες της αστυνομίας για τη διαχείριση της κυκλοφορίας να χρησιμοποιούνται και για λόγους ασφαλείας και δημόσιας τάξης;**



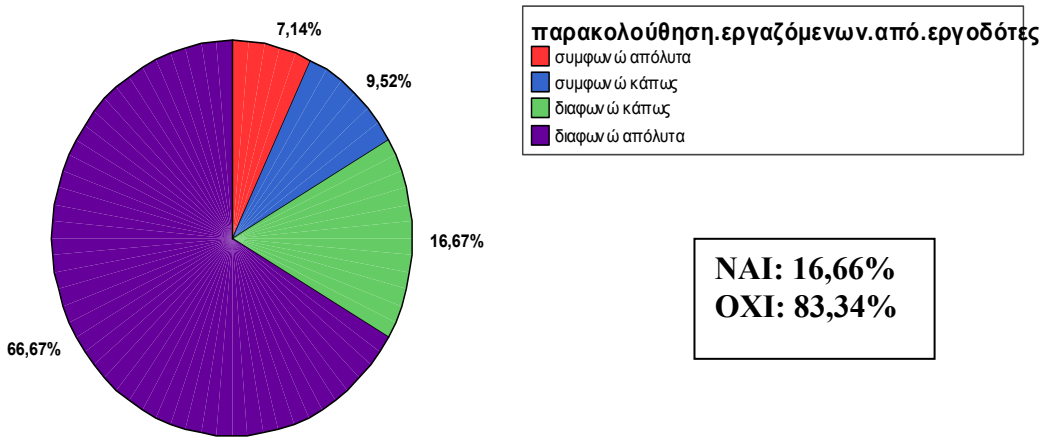

**ΔΙΑΓΡΑΜΜΑ 25**

**Συμφωνείτε ή διαφωνείτε με το βανδαλισμό – καταστροφή των καμερών ασφαλείας της αστυνομίας;**



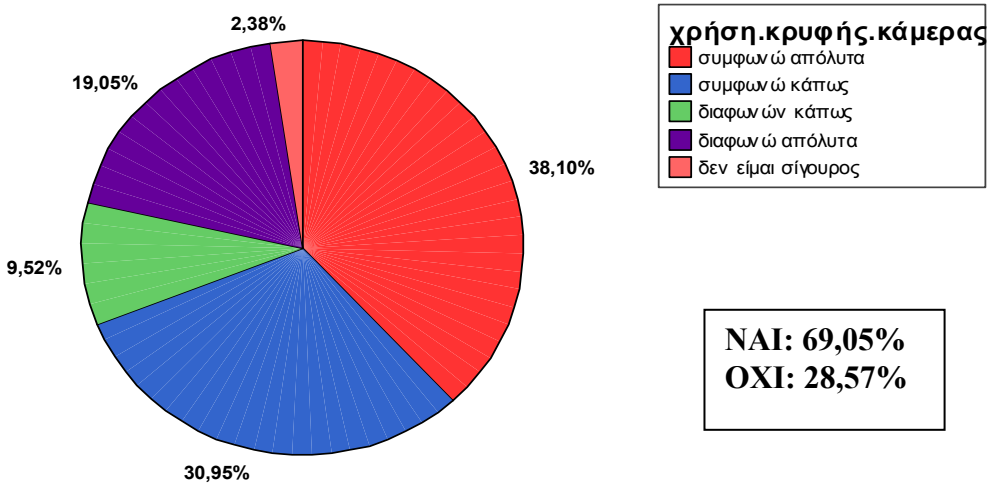

**ΔΙΑΓΡΑΜΜΑ 26**

**Σε ποιο βαθμό συμφωνείτε ή διαφωνείτε ότι θα πρέπει να επιτρέπεται στους εργοδότες να παρακολουθούν με κάμερες ή και άλλα ηλεκτρονικά μέσα τους εργαζόμενους τους και να διαβάζουν το ηλεκτρονικό ταχυδρομείο τους;**



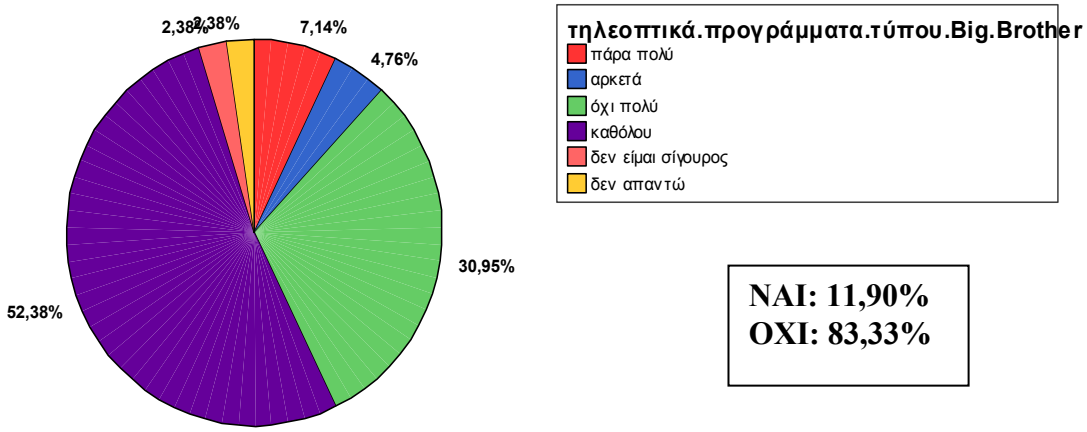

**ΔΙΑΓΡΑΜΜΑ 27**

**Σε ποιο βαθμό συμφωνείτε ή διαφωνείτε με τη χρήση κρυφής κάμερας για την απόδειξη μιας παράνομης πράξης;**



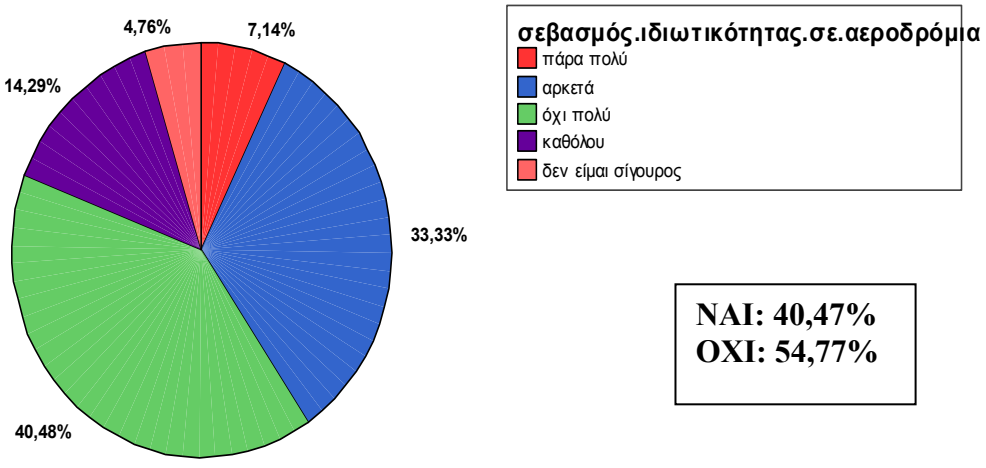

**ΔΙΑΓΡΑΜΜΑ 28**

**Σας αρέσουν τα τηλεοπτικά προγράμματα τύπου Big Brother που χρησιμοποιούν κάμερες παρακολούθησης;**



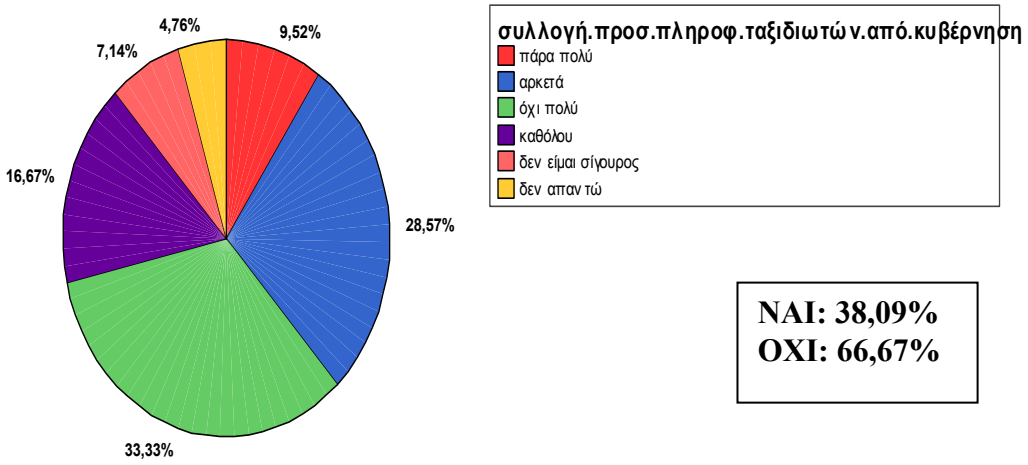

**ΔΙΑΓΡΑΜΜΑ 29**

**Σε ποιο βαθμό θεωρείτε ότι η ιδιωτικότητας σας (η προσωπικότητα και τα προσωπικά σας δεδομένα) γίνεται σεβαστή στα αεροδρόμια όταν ταξιδεύετε αεροπορικώς;**




**ΔΙΑΓΡΑΜΜΑ 30**

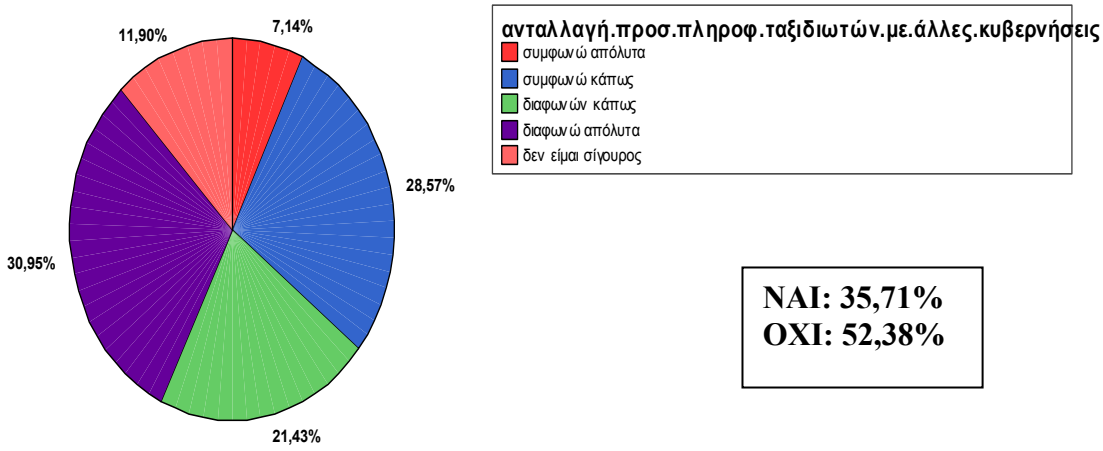
**Συμφωνείτε ή διαφωνείτε στο ότι η Ελληνική κυβέρνηση να έχει το δικαίωμα να συλλέγει προσωπικές πληροφορίες για τους ταξιδιώτες;**




**ΝΑΙ: 38,09%**
**ΟΧΙ: 66,67%**

**ΔΙΑΓΡΑΜΜΑ 31**

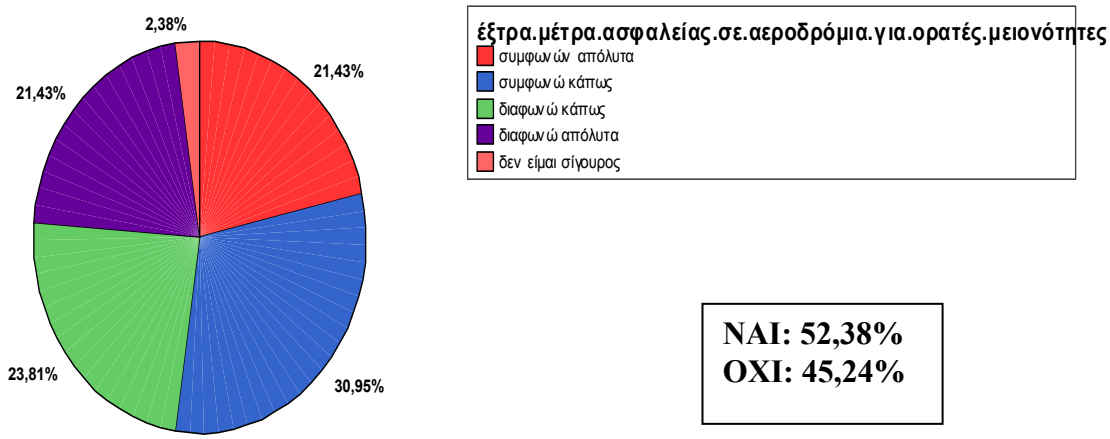
**Συμφωνείτε ή διαφωνείτε στο ότι η Ελληνική κυβέρνηση θα πρέπει να μπορεί να μοιράζεται τις προσωπικές πληροφορίες για τους ταξιδιώτες με άλλες κυβερνήσεις;**




**ΝΑΙ: 35,71%**
**ΟΧΙ: 52,38%**

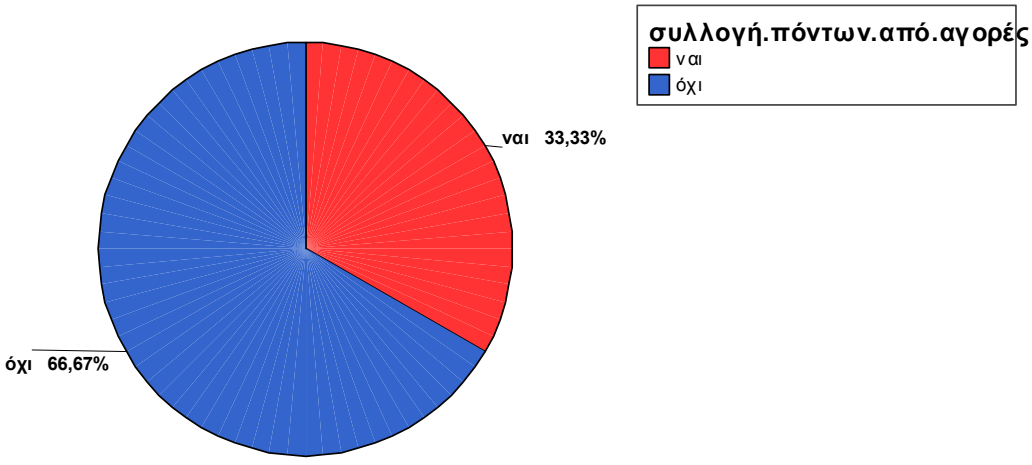
**ΔΙΑΓΡΑΜΜΑ 32**

**Σε ποιο βαθμό συμφωνείτε οι αξιωματούχοι ασφαλείας στα αεροδρόμια θα πρέπει να παίρνουν έξτρα μέτρα ασφαλείας για τα ταξιδεύοντα μέλη ορατών μειονοτήτων (έγχρωμοι, μουσουλμάνοι κτλ);**



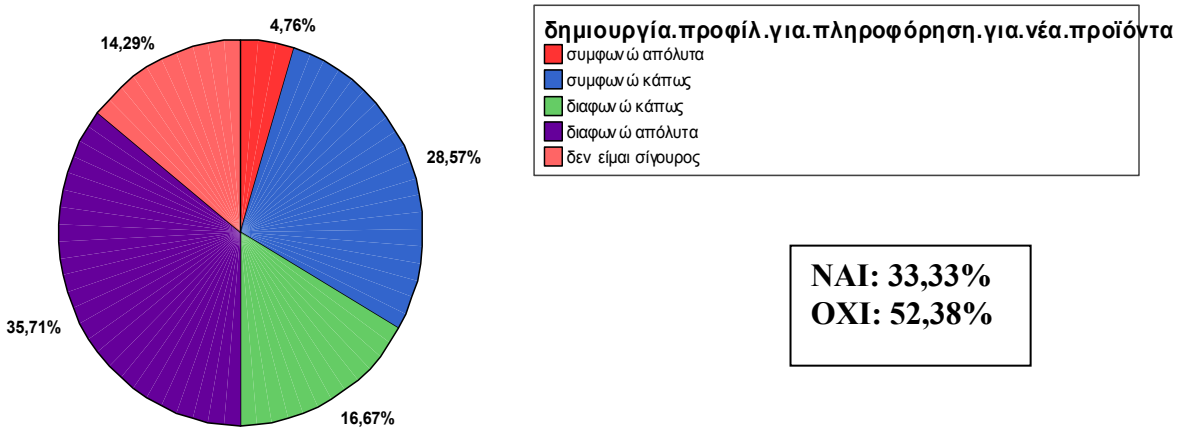

**ΔΙΑΓΡΑΜΜΑ 33**

**Μερικές αεροπορικές και άλλες εταιρείες προσφέρουν στους πελάτες τους διάφορα προνόμια – μπόνους με βάση τη συλλογή πόντων από τις αγορές τους απ' αυτές. Εσείς σαν καταναλωτής μαζεύετε τέτοιους πόντους;**




**ΔΙΑΓΡΑΜΜΑ 34**

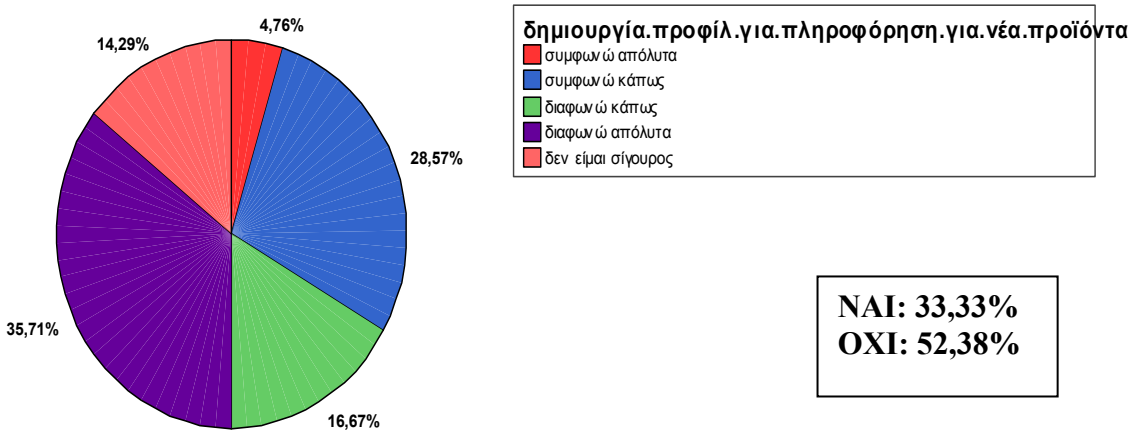
**Πόσο αποδεκτό ή όχι είναι για σας μια επιχείρηση να δημιουργεί το προφίλ σας ως πελάτη της, χρησιμοποιώντας πληροφορίες για τις καταναλωτικές σας προτιμήσεις, ώστε να σας πληροφορεί για προϊόντα και υπηρεσίες που ενδεχομένως σας ενδιαφέρουν;**




**ΝΑΙ: 33,33%**
**ΟΧΙ: 52,38%**

**ΔΙΑΓΡΑΜΜΑ 35**

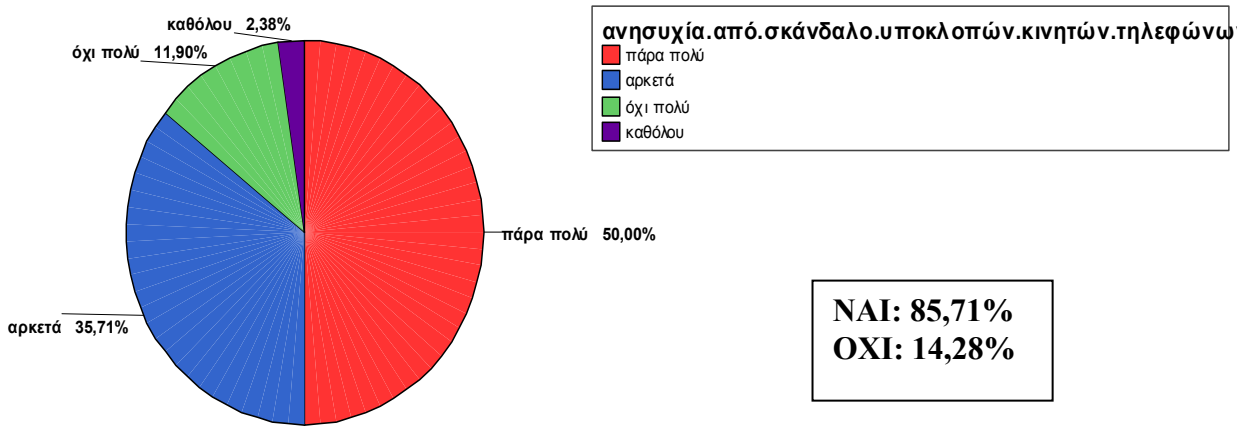
**Θα σας ενοχλούσε ή όχι αν η επιχείρηση αυτή διέθετε ή πωλούσε το καταναλωτικό σας προφίλ σε άλλους χωρίς την άδειά σας;**




**ΝΑΙ: 33,33%**
**ΟΧΙ: 52,38%**

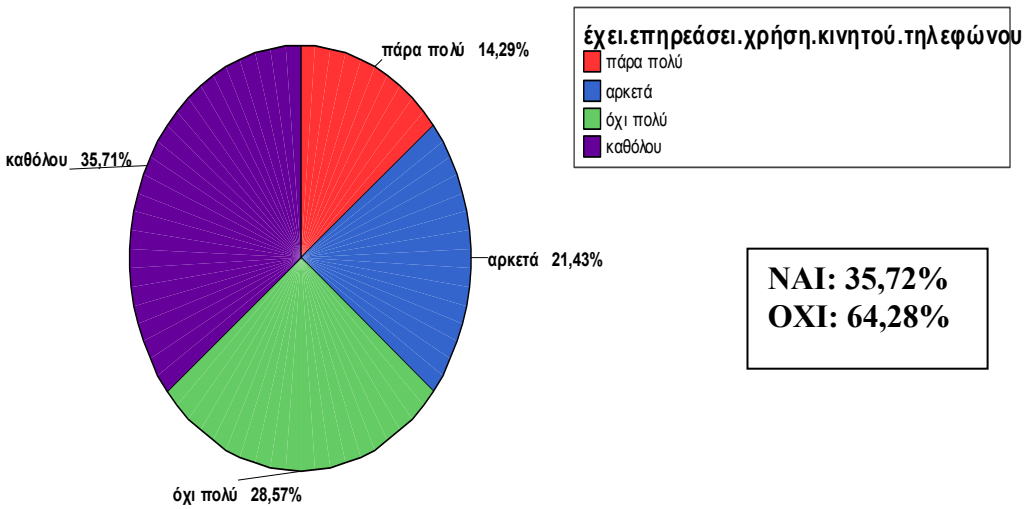
**ΔΙΑΓΡΑΜΜΑ 36**

**Σας έχει ανησυχήσει ή όχι το πρόσφατο σκάνδαλο των υποκλοπών των κινητών τηλεφώνων στην Ελλάδα;**



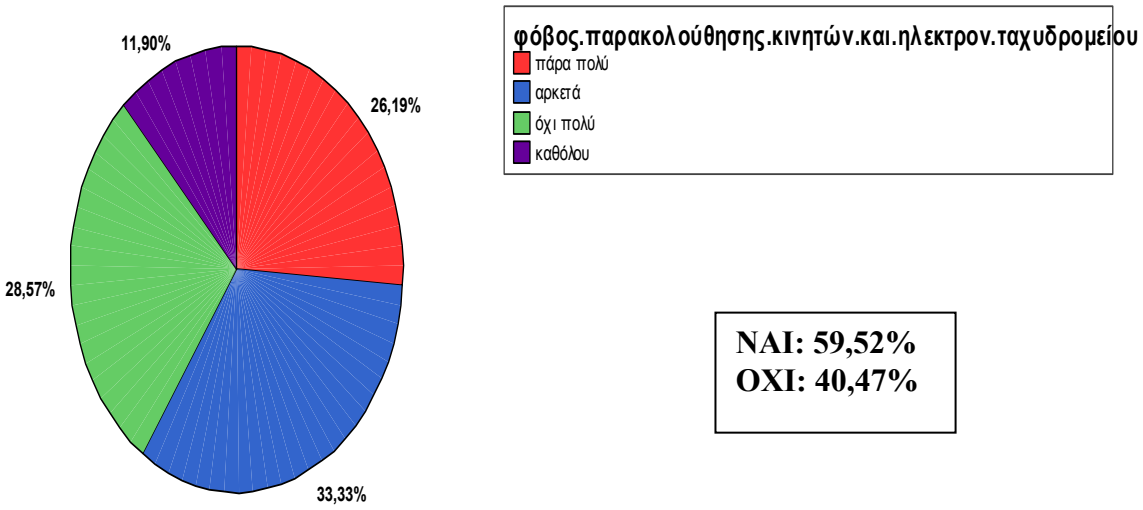

**ΔΙΑΓΡΑΜΜΑ 37**

**Αν ναι, πόσο σας έχει επηρεάσει στη χρήση του κινητού σας τηλεφώνου;**



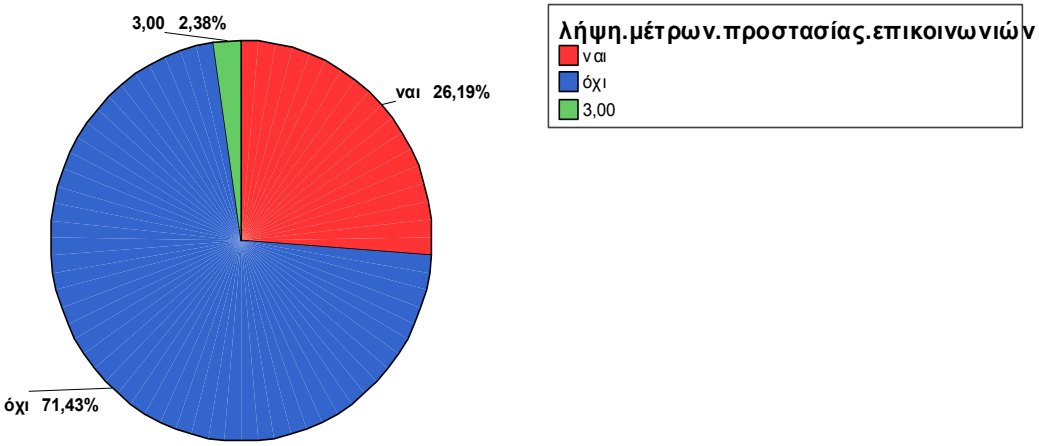

**ΔΙΑΓΡΑΜΜΑ 38**

**Φοβάστε ότι οι τηλεφωνικές σας συνομιλίες ιδιαίτερα στο κινητό τηλέφωνο αλλά και το ηλεκτρονικό σας ταχυδρομείο μπορεί να παρακολουθούνται;**



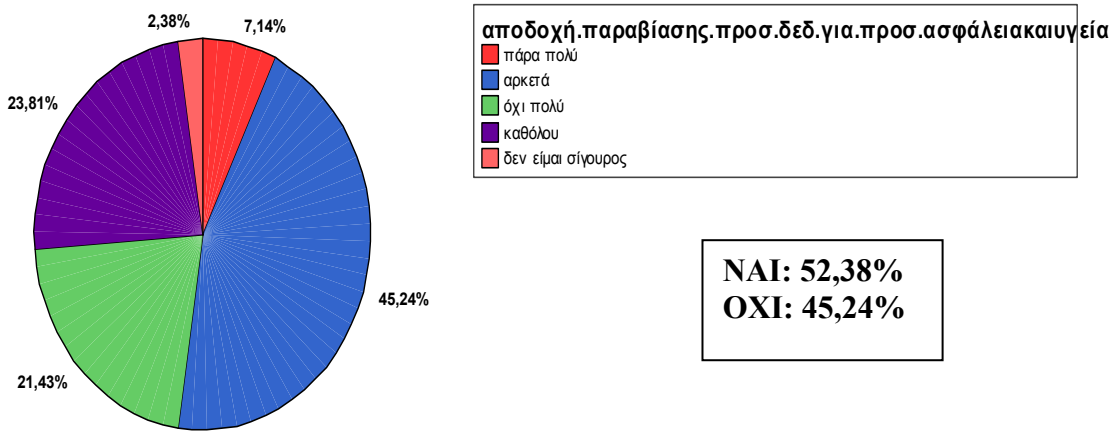

**ΔΙΑΓΡΑΜΜΑ 39**

**Παίρνετε ή όχι κάποια μέτρα προστασίας των επικοινωνιών σας μέσω Η/Υ ή τηλεφώνου;**



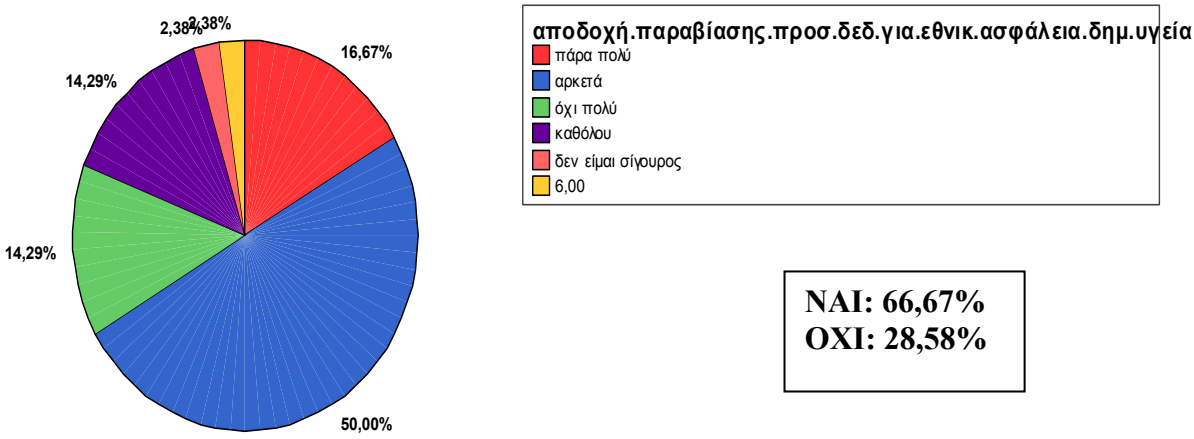

**ΔΙΑΓΡΑΜΜΑ 40**

**Τελικά, αποδέχεστε ή όχι την παραβίαση της ιδιωτικής σας ζωής και των προσωπικών σας δεδομένων για την προσωπική σας ασφάλεια και υγεία;**




**ΔΙΑΓΡΑΜΜΑ 41**

**Σε ποιο βαθμό αποδέχεστε ή όχι την παραβίαση της ιδιωτικής σας ζωής και των προσωπικών σας δεδομένων για λόγους εθνικής ασφάλειας και δημόσιας υγείας;**




**ΔΙΑΓΡΑΜΜΑ 42**

### 6.2.3.2: Ανάλυση των αποτελεσμάτων της έρευνας με ερωτηματολόγιο

Το δείγμα μας των σαράντα δύο (42) ατόμων στην πλειοψηφία του αποτελούνταν από γυναίκες (27 άτομα – 64,3%) και από δεκαπέντε (15) άνδρες (38,71%). Περίπου οι μισοί από τους ερωτώμενους ανήκουν στις ηλικιακές ομάδες των 30-34 (10 άτομα – 23,8%) και των 45-49 (9 άτομα – 21,4%), είναι απόφοιτοι λυκείου ή τεχνικής σχολής (23 άτομα – 54,8%) και απασχολούνται στον ιδιωτικό (17 άτομα – 40,5%) και το δημόσιο τομέα (15 άτομα – 35,7%). Έτσι δεν θεωρούμε το δείγμα μας αντιπροσωπευτικό της πόλης του Ρεθύμνου. Είναι απλά ενδεικτικό επειδή αποτελείται κυρίως από γυναίκες μορφωμένες, εργαζόμενες στο δημόσιο και τον ιδιωτικό τομέα και άρα μεσαίου εισοδήματος, οι οποίες έχουν μεγαλύτερη γνώση και πληροφόρηση.

Η συντριπτική πλειοψηφία των ερωτώμενων δηλώνει ότι έχει επίγνωση των όρων προσωπικά (92,9%) και ευαίσθητα προσωπικά δεδομένα (73,8%) και το τι αυτοί περιλαμβάνουν. Τα άτομα αυτά είναι κατά κύριο λόγο απόφοιτοι λυκείου ή τεχνικής σχολής και εργάζονται τόσο στον ιδιωτικό όσο και στο δημόσιο τομέα.

Στην προσπάθεια να διασταυρωθεί ο βαθμός γνώσης τους για το τι είναι τα ευαίσθητα προσωπικά δεδομένα, και τέθηκε ανάλογη ερώτηση, παρατηρούμε ότι γι' αυτούς η έννοια των ευαίσθητων προσωπικών δεδομένων επικεντρώνεται γύρω από οικονομικά θέματα όπως οι τραπεζικές καταθέσεις (85,7%), ο μισθός (50%) και ο προσωπικός κωδικός πρόσβασης (PIN) (78,6%). Όσον αφορά την καταγραφή της συνδικαλιστικής δράσης δηλώνουν σε ποσοστό 76,2% ότι δεν αποτελεί ευαίσθητο προσωπικό δεδομένο πράγμα που σύμφωνα με το Ν. 2472/1997 δεν ισχύει.

Σε ποσοστό 52,4% θεωρούν ότι οι νόμοι στην Ελλάδα για την προστασία των προσωπικών δεδομένων δεν είναι πολύ αποτελεσματικοί, και φαίνεται να επικρατεί μια γενική τάση δυσπιστίας ως προς τη σωστή χρήση των προσωπικών πληροφοριών από διάφορους φορείς (ΔΙΑΓΡΑΜΜΑ 7).

Οι περισσότεροι (52,4%) φαίνεται να γνωρίζουν την ύπαρξη της ΑΠΔΠΧ χωρίς όμως να έχουν επισκεφθεί την ιστοσελίδα της (78,6%). Ακόμη φαίνεται να έχουν λίγη (35,7%) ως καθόλου (33,3%) εμπιστοσύνη στις κυβερνήσεις αναφορικά με το σεβασμό που αυτές δείχνουν στο απόρρητο των προσωπικών πληροφοριών των πολιτών. Ανάλογη δυσπιστία δείχνουν και στις ιδιωτικές εταιρείες, τις τράπεζες, τα σούπερ μάρκετ και γενικά τα καταστήματα από τα οποία ψωνίζουν με τη χρήση

πιστωτικών καρτών (35,7%). Όμως αυτό δεν λειτουργεί αποτρεπτικά ως προς τη χρήση των καρτών αυτών. Ίσως εξαιτίας της παγκόσμιας οικονομικής κρίσης και της έλλειψης ρευστού τον τελευταίο καιρό.

Δείχνουν να ανησυχούν πολύ (45,2%) για την προστασία της ιδιωτικής τους ζωής και των προσωπικών τους δεδομένων όταν δίνουν προσωπικές τους πληροφορίες στο διαδίκτυο. Το γεγονός αυτό σε συνδυασμό με το ότι έχουν επίγνωση του ότι μπορεί να παρακολουθούνται τα ψηφιακά τους ίχνη μέσω των cookies στο διαδίκτυο (54,8%) λειτουργεί αποτρεπτικά στο να κάνουν αγορές μέσω του διαδικτύου (83,3%).

Παρόλο λοιπόν που έχουν επίγνωση των κινδύνων για την προστασία της ιδιωτικότητας τους που προκύπτουν από τη χρήση του διαδικτύου, δεν λαμβάνουν τα απαραίτητα μέτρα όπως η συχνή αλλαγή κωδικού πρόσβασης (73,8%) και η χρήση προγραμμάτων προστασίας από παρενοχλήσεις σε ηλεκτρονικούς υπολογιστές και κινητά τηλέφωνα (73,8%).

Επίσης παρατηρούμε ότι οι ερωτηθέντες σε ποσοστό 45,2% θεωρούν ότι οι νόμοι που έχουν θεσπιστεί για την προστασία της εθνικής άμυνας παραβιάζουν αρκετά την ιδιωτική τους ζωή. Παρά το γεγονός ότι θεωρούν ότι η παραβίαση της ιδιωτικότητας τους είναι ένα υπαρκτό φαινόμενο, αποδέχονται τη γνωστοποίηση των προσωπικών πληροφοριών των πολιτών – πελατών μιας υπηρεσίας/ επιχείρησης σε άλλες υπηρεσίες, κυβερνήσεις ή επιχειρήσεις στην περίπτωση που κάποιος πολίτης είναι ύποπτος ότι έχει διαπράξει παράνομη πράξη (73,8%). Αυτό μπορεί να σημαίνει ότι δεν έχουν επίγνωση του δικαιώματος της συγκατάθεσης ή ακόμη και των γενικότερων δικαιωμάτων τους όσον αφορά την επεξεργασία των προσωπικών τους δεδομένων.

Στις μέρες μας η χρήση των καμερών ασφαλείας και των CCTV τόσο σε ανοικτούς όσο και σε κλειστούς χώρους είναι ιδιαίτερα διαδεδομένη. Σύμφωνα με τις απαντήσεις των ερωτώμενων, θεωρούν ότι η χρήση τους σε εξωτερικούς δημόσιους χώρους (33,3%) και σε εσωτερικούς χώρους – επιχειρήσεις (45,2%) είναι κάπως αποτελεσματική για τη μείωση της εγκληματικότητας. Έτσι δεν φαίνεται να ενοχλούνται από την ευρεία χρήση τους (31%). Φαίνεται δηλαδή να έχουν αποδεχθεί τη χρήση τους και το καθεστώς της παρακολούθησης σε διάφορες πτυχές της καθημερινής τους ζωής ως κάτι το φυσιολογικό με αποτέλεσμα να επιθυμούν και τη χρήση των καμερών ασφαλείας για τη φύλαξη και την ασφάλεια της κατοικίας ή της επιχείρησης τους (73,8%). Έτσι, συμφωνούν απόλυτα με τη χρήση των καμερών της

αστυνομίας για τη δημόσια τάξη και ασφάλεια (47,6%), είναι ενάντια στην καταστροφή τους (64,3%) και συμφωνούν με τη χρήση κρυφών καμερών για την απόδειξη μιας παράνομης πράξης (38,1%). Ενώ όμως αποδέχονται την παρακολούθηση σε διάφορες πτυχές της καθημερινότητας τους, εναντιώνονται στη χρήση των καμερών ή άλλων μέσων παρακολούθησης από τους εργοδότες τους (66,7%) και δεν τους αρέσουν τηλεοπτικά προγράμματα τύπου Big Brother (52,4%).

Για την πολιτική της ασφάλειας στα αεροδρόμια όλων των χωρών και κατά συνέπεια και στη χώρα μας είναι ο έλεγχος διαβατηρίων, η τοποθέτηση microchip στα διαβατήρια, ο έλεγχος των αποσκευών, οι σαρωτές σώματος κτλ δεν θεωρούν ότι η ιδιωτικότητα τους παραβιάζεται ιδιαίτερα όταν ταξιδεύουν αεροπορικώς (40,5%). Έτσι, συμφωνούν αρκετά όσον αφορά το δικαίωμα της κυβέρνησης να συλλέγει προσωπικές πληροφορίες για τους ταξιδιώτες (33,3%). Αν και στα αεροδρόμια βλέπουμε ότι υπάρχουν ιδιωτικές εταιρείες security που έχουν αναλάβει τόσο τον έλεγχο των αποσκευών όσο και το σωματικό έλεγχο των ταξιδιωτών, αυτό γίνεται αποδεκτό λόγω του φόβου και της ανάγκης πάταξης της τρομοκρατίας, ιδιαίτερα μετά τα γεγονότα της 11$^{ης}$ Σεπτεμβρίου.

Ακόμη, κάποιοι φαίνεται να διαφωνούν απόλυτα (31%) με το γεγονός της ύπαρξης του δικαιώματος της εκάστοτε κυβέρνησης να μοιράζεται προσωπικές πληροφορίες των ταξιδιωτών με άλλες κυβερνήσεις και φορείς όπως το SIS, η Ιντερπόλ και άλλους οργανισμούς με παρόμοιους σκοπούς για την πάταξη της τρομοκρατίας, την μείωση της παράνομης μετανάστευσης κτλ.

Αντίθετα, δείχνουν να συμφωνούν κάπως (31%) με τη λήψη επιπρόσθετων μέτρων ασφαλείας στα αεροδρόμια για ταξιδιώτες που ανήκουν σε ορατές μειονότητες όπως είναι οι έγχρωμοι, οι μουσουλμάνοι κτλ. Αυτό δείχνει αφενός μία τάση ρατσιστικής αντιμετώπισης αλλά και ξενοφοβίας έναντι των μειονοτήτων αυτών και αφετέρου μια τάση άμυνας και αντιμετώπισης της τρομοκρατίας.

Όσον αφορά τη συλλογή των προσωπικών δεδομένων των καταναλωτών, αρκετές είναι οι εταιρείες που χρησιμοποιούν κάρτες bonus προκειμένου να προσελκύσουν και να δελεάσουν τους υποψήφιους πελάτες. Σε ποσοστό 66,7% οι ερωτηθέντες του δείγματος απάντησαν ότι δεν συλλέγουν τέτοιου είδους πόντους. Ακόμη, φαίνεται να διαφωνούν απόλυτα (35,7%) με το γεγονός της δημιουργίας του προσωπικού τους προφίλ βάσει των καταναλωτικών τους συνηθειών από εταιρείες marketing προκειμένου να τους παρέχεται πληροφόρηση για προϊόντα και υπηρεσίες που αυτές προσφέρουν, ενώ ενοχλούνται πολύ (35,7%) με την ιδέα της διάθεσης ή

πώλησης του καταναλωτικού τους προφίλ σε άλλους χωρίς να έχουν δώσει τη συγκατάθεση τους.

Επίσης τον τελευταίο καιρό όλοι μας σχεδόν έχουμε πληροφορηθεί για το σκάνδαλο των υποκλοπών των κινητών τηλεφώνων το 2004 - 2005. Έτσι, οι μισοί από τους ερωτηθέντες του δείγματος μας (50%) έχουν θορυβηθεί πάρα πολύ από το συγκεκριμένο σκάνδαλο, φοβούνται αρκετά (33,3%) ότι οι επικοινωνίες τους μέσω κινητού τηλεφώνου ή ηλεκτρονικού ταχυδρομείου μπορεί να παρακολουθούνται χωρίς όμως να έχουν επηρεαστεί ιδιαίτερα στη χρήση του κινητού τους τηλεφώνου (28,6%). Αυτό συμβαίνει είτε από άγνοια, αμέλεια ή ανάγκη επειδή οι νέες τεχνολογίες έχουν εισβάλει για τα καλά στην καθημερινότητα μας με αποτέλεσμα η χρήση τους να είναι αναγκαία παρά τους κινδύνους που εγκυμονεί. Αν και ο φόβος για την παρακολούθηση των επικοινωνιών τους είναι έκδηλος, η συντριπτική πλειοψηφία (71,4%) δηλώνει ότι δεν παίρνει κάποια μέτρα προστασίας για τις επικοινωνίες τους είτε μέσω του ηλεκτρονικού υπολογιστή είτε μέσω τηλεφώνου.

Εν τέλει, δηλώνουν ότι αποδέχονται την παραβίαση της ιδιωτικής τους ζωής και των προσωπικών τους δεδομένων για την προσωπική τους ασφάλεια και υγεία (45,2%) και ιδιαίτερα για λόγους εθνικής ασφάλειας και δημόσιας υγείας (50%).

#### 6.2.3.3: <u>Συμπερασματικές παρατηρήσεις</u>

Παρατηρούμε λοιπόν ότι η πλειοψηφία του δείγματος μας, αν και μεσαίας τάξης λόγω ανώτερης εκπαίδευσης και επαγγελματικής θέσης, είναι άτομα απληροφόρητα αναφορικά με την προστασία των προσωπικών τους δεδομένων. Μάλιστα για λόγους άγνοιας ή αμέλειας δεν διεκδικούν την άσκηση των δικαιωμάτων τους αναφορικά με την προστασία των δεδομένων τους. Έτσι αποδέχονται την κρατική και αστυνομική παρακολούθηση για λόγους ασφάλειας και υγείας.

Επειδή το δείγμα μας είναι ενδεικτικό και αποτελείται κυρίως από γυναίκες μορφωμένες, εργαζόμενες τόσο στο δημόσιο όσο και στον ιδιωτικό τομέα και άρα μεσαίου εισοδήματος, και είναι απληροφόρητες σε θέματα προστασίας των προσωπικών τους δεδομένων, η άγνοια θα είναι πολύ μεγαλύτερη σε άτομα κατώτερου μορφωτικού και οικονομικού επιπέδου. Όμως αυτό δε σημαίνει απαραίτητα ότι άτομα υψηλότερου μορφωτικού και οικονομικού επιπέδου που μπορεί να έχουν μεγαλύτερη πληροφόρηση, παίρνουν και περισσότερα μέτρα

προστασίας. Έτσι χρειάζεται περεταίρω διερεύνηση προκειμένου να διαπιστωθεί ο βαθμός πληροφόρησης ή μη και ευαισθητοποίησης ή μη τόσο των οικονομικά ασθενέστερων όσο και των οικονομικά ανώτερων στρωμάτων.

### 6.3: Άλλα σχετικά αποτελέσματα ερευνών του Ευρωβαρομέτρου και της Σχολής Κοινωνικών Επιστημών του Πανεπιστημίου Κρήτης

#### 6.3.1: Τα αποτελέσματα της έρευνας του Ευρωβαρομέτρου

Η έρευνα του Ευρωβαρομέτρου που διεξήχθη τον Ιανουάριο του 2008 είχε σαν στόχο την καταγραφή των αντιλήψεων και των στάσεων των ευρωπαίων πολιτών αναφορικά με θέματα που αφορούν την προστασία των προσωπικών τους δεδομένων σε διάφορους τομείς.

Στην έρευνα αυτή βρέθηκε ότι η πλειοψηφία των ευρωπαίων πολιτών δείχνει μεγάλο ενδιαφέρον για θέματα που αφορούν την προστασία των προσωπικών τους δεδομένων καθώς τα 2/3 των συμμετεχόντων ενδιαφέρονταν για το αν τα προσωπικά τους δεδομένα προστατεύονται και διαχειρίζονται σωστά (64%). Επίσης δείχνουν να εμπιστεύονται τις ιατρικές υπηρεσίες, τους γιατρούς αλλά και την αστυνομία ότι προστατεύουν πληρέστερα τα δεδομένα τους, ενώ θεωρούν ότι το επίπεδο της προστασίας τους στην χώρα τους δεν είναι επαρκές (48%).

Πιστεύουν ότι η εθνική τους νομοθεσία δεν μπορεί να προστατεύσει τον ολοένα αυξανόμενο αριθμό των ατόμων που αφήνουν προσωπικά δεδομένα στο διαδίκτυο (54%). Μάλιστα θεωρούν ότι οι συμπολίτες τους έχουν χαμηλό επίπεδο γνώσεων για την προστασία των δεδομένων τους (77%). Παρόλο που αρκετοί από αυτούς είναι ενημερωμένοι για τους υπάρχοντες νόμους για την προστασία των δεδομένων τους, μόνο το 29% γνώριζε ότι τα ευαίσθητα προσωπικά δεδομένα τυγχάνουν ειδικής νομικής προστασίας, ενώ μόλις το 17% γνώριζε ότι τα προσωπικά δεδομένα μπορούν να διαβιβαστούν εκτός ΕΕ αν στη χώρα προς την οποία γίνεται η διαβίβαση υπάρχει ένα ικανοποιητικό επίπεδο προστασίας.

Οι περισσότεροι από αυτούς δεν γνώριζαν για την ύπαρξη των ΑΠΔΠΧ (72%) ενώ η Ελλάδα και η Ουγγαρία είχαν τα υψηλότερα επίπεδα γνώσης (51% και 46% αντίστοιχα). Οι περισσότεροι από τους χρήστες του διαδικτύου 82% θεωρούν ότι η διαβίβαση δεδομένων μέσω αυτού δεν είναι ασφαλής ενώ μόλις το 22%

χρησιμοποιεί εργαλεία και τεχνολογίες για την ενίσχυση της ασφάλειας των δεδομένων τους.

Επίσης θεωρούν ότι η προστασία ενάντια στην τρομοκρατία αποτελεί ένα επαρκή λόγο – κίνητρο για τον περιορισμό της προστασίας των προσωπικών δεδομένων καθώς το 82% θεωρεί ότι μπορεί να καταστεί δυνατή η καταγραφή των λεπτομερειών των επιβατών κατά την πτήση, των τηλεφωνικών επικοινωνιών (72%) αλλά και της χρήσης των πιστωτικών καρτών (75%) και του διαδικτύου (69%). Μάλιστα το 1/3 των ερωτώμενων θεωρούσε ότι πρέπει να καταγράφονται μόνο οι ύποπτοι (27% - 35%) ενώ περίπου το 1/5 επιθυμούσε τη λήψη αυστηρότερων μέτρων (14% - 21%).

Στην ίδια έρευνα όσον αφορά την περίπτωση των Ελλήνων, δεν εμπιστεύονται διάφορους οργανισμούς ότι τηρούν και σέβονται το απόρρητο των προσωπικών τους δεδομένων. Η συντριπτική πλειοψηφία αυτών (93%) δηλώνει ότι δεν είναι ενήμεροι για θέματα που αφορούν την προστασία των προσωπικών τους δεδομένων ενώ θεωρούν ότι τα προσωπικά τους δεδομένα δεν προστατεύονται επαρκώς (71%) αν και δηλώνουν ενήμεροι για τις υποχρεώσεις των φορέων επεξεργασίας απέναντι στα υποκείμενα των δεδομένων (66%). Δηλώνουν άγνοια (73%) σχετικά με το γεγονός ότι για να διαβιβαστούν δεδομένα σε χώρα που δεν ανήκει στην ΕΕ πρέπει αυτή να έχει επαρκές επίπεδο προστασίας τους και θεωρούν μη ασφαλή τη διαβίβαση τους (92%). Μάλιστα το 56% των Ελλήνων δηλώνει ότι δεν γνωρίζει για την ύπαρξη και εφαρμογή αυστηρότερων νόμων για την προστασία των ευαίσθητων προσωπικών δεδομένων.

Όσον αφορά τη χρήση του διαδικτύου, δηλώνουν ανήσυχοι αναφορικά με το γεγονός ότι αφήνουν προσωπικά ίχνη κατά τη χρήση του καθώς θεωρούν ότι η ισχύουσα νομοθεσία δεν είναι σε θέση να αντιμετωπίσει αλλά και να παράσχει προστασία ενάντια στους κινδύνους που προκύπτουν από τη χρήση του (63%). Ακόμη, το 51% αυτών αγνοούν την ύπαρξη μέσων και τεχνολογιών που ενισχύουν την προστασία των προσωπικών τους δεδομένων. Όμως, δεν τις χρησιμοποιούν και για διάφορους άλλους λόγους όπως π.χ. το υψηλό κόστος. Τέλος, φαίνεται να ενισχύεται ο βαθμός αποδοχής της παρακολούθησης της χρήσης του διαδικτύου και αυτό εξαιτίας του φόβου της τρομοκρατίας.

### 6.3.2: Τα αποτελέσματα της έρευνας της Σχολής Κοινωνικών Επιστημών του Πανεπιστημίου Κρήτης

Η Σχολή Κοινωνικών Επιστημών του Πανεπιστημίου Κρήτης με επιστημονικό υπεύθυνο τον αναπληρωτή καθηγητή του τμήματος Κοινωνιολογίας κο Σαματά, στα τέλη του 2008 διεξήγαγε έρευνα με θέμα «Προστασία των προσωπικών δεδομένων» σε φοιτητές του Πανεπιστημίου Κρήτης οι οποίοι απάντησαν σε ηλεκτρονικό ερωτηματολόγιο μέσω της ιστοσελίδας της Σχολής Κοινωνικών Επιστημών (www.soc.uoc.gr).

Από τα αποτελέσματα της έρευνας φάνηκε ότι το 80% των φοιτητών έχει λίγη ως καθόλου εμπιστοσύνη στην εκάστοτε Ελληνική κυβέρνηση και στις δημόσιες Αρχές αναφορικά με το σεβασμό που δείχνουν στο απόρρητο των προσωπικών πληροφοριών. Το 74% αυτών δεν αποδέχεται την παραβίαση της ιδιωτικής τους ζωής και των προσωπικών τους δεδομένων για λόγους υγείας και ασφάλειας, το 68% ούτε για λόγους εθνικής ασφάλειας ενώ το 94% διαφωνεί σθεναρά με τη χρήση καμερών ή άλλων ηλεκτρονικών μέσων στον εργασιακό χώρο.

Επίσης τηρούν στάση δυσπιστίας όσον αφορά στη σχέση κράτους – κυβερνήσεων και των προσωπικών δεδομένων καθώς το 51% θεωρεί ότι η νομοθεσία για την προστασία των προσωπικών πληροφοριών που διατηρούνται στα αρχεία δημόσιων υπηρεσιών αλλά και των ιδιωτικών επιχειρήσεων είναι αναποτελεσματική. Ανάλογη στάση δυσπιστίας τηρούν και ως προς ιδιωτικές εταιρείες, τράπεζες και σούπερ μάρκετ και όπου αλλού ψωνίζουν με πιστωτικές κάρτες για την προστασία των προσωπικών τους δεδομένων (77%).

Το 67% θεωρεί ότι η νομοθεσία για την προστασία της εθνικής ασφάλειας παραβιάζει την ιδιωτική ζωή. Αυτό έχει σαν αποτέλεσμα να ενοχλούνται από την ευρεία διάδοση των καμερών ασφαλείας σε δημόσιους και ιδιωτικούς χώρους (85%) ενώ το 27% επικροτεί ακραίες λύσεις όπως η καταστροφή των καμερών ακόμη και με βανδαλισμούς. Επίσης είναι ενάντια στη χρήση των καμερών για τη φύλαξη της κατοικίας ή της επιχείρησης τους (55%).

Το 70% αυτών θεωρούν πως η ιδιωτικότητα, η προσωπικότητα και τα προσωπικά τους δεδομένα δεν γίνονται σεβαστά στα αεροδρόμια όταν ταξιδεύουν, και το 87% διαφωνεί με τη λήψη επιπλέον μέτρων ασφαλείας όταν ταξιδεύουν μέλη ορατών μειονοτήτων.

Όσον αφορά τη χρήση του διαδικτύου, το 99% δηλώνει ότι έχει αγοράσει προϊόντα μέσω αυτού, αν και το 85% αυτών έχουν επίγνωση των κινδύνων που υπάρχουν μέσω προγραμμάτων εντοπισμού των ψηφιακών τους ιχνών. Αυτή η αντιφατική τους συμπεριφορά χαρακτηρίζει και τις τηλεφωνικές επικοινωνίες τους, καθώς φαίνεται να φοβούνται αρκετά ως πάρα πολύ ότι οι τηλεφωνικές τους συνομιλίες, ιδίως στο κινητό τηλέφωνο και το ηλεκτρονικό ταχυδρομείο, ενδέχεται να παρακολουθούνται, παρόλα αυτά δεν παίρνουν ιδιαίτερα μέτρα προστασίας[32]. Αυτό γενικά λέγεται «παράδοξο της ιδιωτικότητας» (Samatas, 2003).

### 6.3.3: <u>Σύγκριση των αποτελεσμάτων των παραπάνω ερευνών</u>

Έπειτα από τη σύγκριση των αποτελεσμάτων των προαναφερθέντων ερευνών με τα αποτελέσματα της δικής μας έρευνας, παρατηρούμε ότι σε γενικές γραμμές οι απόψεις για την προστασία των προσωπικών δεδομένων τόσο των ευρωπαίων πολιτών όσο και των Ελλήνων πολιτών ταυτίζονται.

***ΠΙΝΑΚΑΣ 1***

| | **Ρεθυμνιώτες** | **Φοιτητές** | **Έλληνες** | **Ευρωπαίοι** |
|---|---|---|---|---|
| **Εμπιστοσύνη σε ιατρικές, κρατικές υπηρεσίες & αστυνομία για την προστασία των ΠΔ** | ΟΧΙ | ΟΧΙ | ΟΧΙ | ΝΑΙ |
| **Γνώση ύπαρξης ΑΠΔΠΧ** | ΝΑΙ | ΝΑΙ | ΝΑΙ | ΟΧΙ |
| **Αποδοχή παραβίασης της ιδιωτικότητας & ΠΔ για λόγους δημόσιας ασφάλειας & υγείας** | ΝΑΙ | ΟΧΙ | ΝΑΙ | ΝΑΙ |
| **Αποδοχή παραβίασης ιδιωτικότητας στα αεροδρόμια** | ΝΑΙ | ΟΧΙ | ΝΑΙ | ΝΑΙ |
| **Λήψη επιπρόσθετων μέτρων στα αεροδρόμια για ορατές μειονότητες** | ΝΑΙ | ΟΧΙ | ΝΑΙ | ΟΧΙ |
| **Αποδοχή CCTV** | ΝΑΙ | ΟΧΙ | | |

Από τον παραπάνω πίνακα συμπεραίνουμε ότι οι Έλληνες δείχνουν λιγότερη εμπιστοσύνη στις κρατικές και ιατρικές υπηρεσίες καθώς και στην αστυνομία

[32] Έρευνα Σχολής Κοινωνικών Επιστημών Πανεπιστημίου Κρήτης, 2008; Στεργίου, 2009.

αναφορικά με την προστασία των προσωπικών τους δεδομένων συγκριτικά με τους Ευρωπαίους ενώ το δείγμα μας των Ρεθεμνιωτών τις εμπιστεύεται. Παράλληλα είναι περισσότερο ενημερωμένοι για την ύπαρξη της ΑΠΔΠΧ. Οι Έλληνες και οι Ευρωπαίοι σε αντίθεση με τους φοιτητές αποδέχονται την παραβίαση των προσωπικών τους δεδομένων και της ιδιωτικότητας τους για λόγους δημόσιας ασφάλειας και υγείας γενικά, αλλά και όταν ταξιδεύουν με αεροπλάνο ειδικότερα. Επίσης οι Ρεθυμνιώτες και οι Έλληνες σε αντίθεση με τους φοιτητές και τους Ευρωπαίους συμφωνούν με τη λήψη επιπρόσθετων μέτρων στα αεροδρόμια για τις ορατές μειονότητες ενώ το δείγμα μας σε αντίθεση με τους φοιτητές αποδέχεται τη χρήση των CCTV αλλά και των καμερών ασφαλείας της αστυνομίας, όχι όμως και στην παρακολούθηση στο χώρο εργασίας από τους εργοδότες.

Οι παραπάνω διαφοροποιήσεις μπορεί να οφείλονται: α) στις μνήμες που έχει αφήσει το αυταρχικό καθεστώς της Χούντας, β) στην ανάγκη προστασίας από κάθε δυνητική εσωτερική ή εξωτερική απειλή και ιδιαίτερα έπειτα από το γεγονότα της 11$^{ης}$ Σεπτεμβρίου (τρομοκρατία, ξενοφοβία, ρατσισμός ως απόρροια του νεοσυντηρητισμού) και γ) στον αντιεξουσιαστικό τρόπο σκέψης των φοιτητών που αντιτίθενται σε κάθε μορφή εξουσίας και ελέγχου.

# ΓΕΝΙΚΑ ΣΥΜΠΕΡΑΣΜΑΤΑ

Στην εποχή μας το ζήτημα της σωστής διαχείρισης αλλά και της προστασίας των προσωπικών και ιδιαίτερα των ευαίσθητων προσωπικών δεδομένων έχει ιδιαίτερη σημασία. Διότι το φαινόμενο της παρακολούθησης με τη χρήση των νέων τεχνολογιών εξαιτίας των τεράστιων δυνατοτήτων τους, επεκτείνεται σε καθημερινές δραστηριότητες με τη μορφή της συλλογής και επεξεργασίας των προσωπικών πληροφοριών για διάφορους σκοπούς (ασφάλειας, ελέγχου, φροντίδας, κέρδους, κτλ) με ή χωρίς τη συγκατάθεση των ατόμων. Μάλιστα οι προσωπικές πληροφορίες και ιδιαίτερα οι ευαίσθητες αποτελούν τα καύσιμα του 21$^{ου}$ αιώνα. Έτσι η λεγόμενη «νέα παρακολούθηση» πέραν της δυνατότητας συλλογής τεράστιων ποσοστήτων πληροφοριών, έχει τη δυνατότητα κατηγοριοποίησης, σύγκρισης και συσχέτισης των δεδομένων, δημιουργώντας έτσι νέες διακρίσεις και αποκλεισμούς. Έπειτα από την παράθεση των κύριων κατά τη γνώμη μας κοινωνιολογικών προσεγγίσεων του φαινομένου της παρακολούθησης, συμπεραίνουμε ότι η νέα παρακολούθηση που βασίζεται στη χρήση των νέων τεχνολογιών μπορεί να κατανοηθεί ως βασικός μηχανισμός ανασυγκρότησης του κράτους και της παγκοσμιοποιημένης οικονομίας στο πλαίσιο του νεοφιλελευθερισμού και του νεοσυντηρητισμού.

Για την προστασία τόσο των προσωπικών όσο και των ευαίσθητων προσωπικών δεδομένων, η ΕΕ έχει θεσπίσει το απαραίτητο νομοθετικό πλαίσιο που πρέπει να ακολουθεί κάθε κράτος – μέλος. Τόσο το ελληνικό όσο και το ευρωπαϊκό δίκαιο παρέχει επαρκείς εγγυήσεις για την προστασία των προσωπικών και των ευαίσθητων προσωπικών δεδομένων. Έτσι εξαρτάται από το πόσο σθεναρά κάθε κράτος – μέλος επιβάλει την εφαρμογή της παραπάνω νομοθεσίας. Για το λόγο αυτό η ΕΕ επέβαλε τη δημιουργία των εθνικών ΑΠΔΠΧ των οποίων ρόλος είναι η άσκηση ελέγχου στους φορείς συλλογής και επεξεργασίας προσωπικών δεδομένων, επιβάλλοντας κυρώσεις κάθε φορά που διαπιστωθεί παραβίαση των δικαιωμάτων και προσωπικών δεδομένων. Η Ελληνική ΑΠΔΠΧ μέχρι σήμερα λειτουργεί αντικειμενικά και ανεπηρέαστα επιβάλλοντας κυρώσεις ακόμα και σε Υπουργεία και την ΕΛΑΣ. Μάλιστα η χώρα μας κατέλαβε την πρώτη θέση ως προς την προστασία των προσωπικών δεδομένων το 2007 σε συγκριτική έρευνα της EPIC και Privacy International.

Αν και με μικρό δείγμα έρευνας μπορούμε να συμπεράνουμε ότι στο τοπικό επίπεδο της πόλης του Ρεθύμνου υπάρχει μία γενικότερα στάση αποδοχής της

παρακολούθησης από κρατικούς και ιδιωτικούς φορείς. Αντίθετα στο γενικό Ελληνικό επίπεδο και το Ευρωπαϊκό φαίνεται να επικρατεί μία γενικότερη τάση δυσπιστίας όσον αφορά την προστασία των προσωπικών δεδομένων με αποτέλεσμα να δυσανασχετούν στην παρακολούθηση τους από διάφορους φορείς γενικά, να έχουν επίγνωση των κινδύνων που ελλοχεύουν με την χρήση του διαδικτύου και του ηλεκτρονικού εμπορίου και παρόλα αυτά να εξακολουθούν να το χρησιμοποιούν. Θεωρούν δε ότι οι ιατρικές υπηρεσίες, οι φορείς κοινωνικής ασφάλισης και η εφορία κάνουν σωστή διαχείριση των δεδομένων τους ενώ δυσπιστούν ως προς τη χρήση τους από τις διάφορες δημόσιες υπηρεσίες, τους εργοδότες και τα ταξιδιωτικά γραφεία.

Έτσι, συμπεραίνουμε ότι στην τοπική κοινωνία της επαρχιακής πόλης του Ρεθύμνου το αίσθημα του φόβου και της ασφάλειας είναι εντονότερο ώστε να αποδέχονται την κρατική παρακολούθηση. Παρά την ύπαρξη της νομοθεσίας για την προστασία των προσωπικών δεδομένων, δεν φαίνεται να υπάρχει συνειδητοποίηση από μέρους των φορέων συλλογής και επεξεργασίας των δεδομένων ότι διαχειρίζονται ευαίσθητα προσωπικά δεδομένα με αποτέλεσμα η εφαρμογή της νομοθεσίας, τουλάχιστον σε τοπικό επαρχιακό επίπεδο να ατονεί περισσότερο, αλλά και λόγω της άγνοιας ή αμέλειας των πολιτών.

Παρόλο που το δείγμα μας αποτελείται από γυναίκες μέσης και ανώτερης εκπαίδευσης, εργαζόμενες στο δημόσιο και ιδιωτικό τομέα και άρα μεσαίου εισοδήματος, είναι απληροφόρητες σε θέματα προστασίας των προσωπικών του δεδομένων. Υποθέτουμε λοιπόν ότι τα άτομα των οικονομικά ασθενέστερων τάξεων με κατώτερη εκπαίδευση είναι πολύ λιγότερο πληροφορημένα. Αυτό όμως δε σημαίνει απαραίτητα ότι τα άτομα των οικονομικά και μορφωτικά ανώτερων τάξεων είναι και περισσότερο πληροφορημένα, είτε παίρνουν μέτρα προστασίας τους. Για το λόγο αυτό θεωρούμε ότι χρειάζεται περεταίρω διερεύνηση του θέματος με περισσότερο αντιπροσωπευτικό δείγμα και σύγκριση με σχετικές έρευνες σε μεγάλα αστικά κέντρα.

Όμως η παρακολούθηση δεν είναι μόνο αρνητική. Αντίθετα αποτελεί ένα νόμισμα που έχει δύο όψεις και η θετική της όψη αφορά την επεξεργασία των ευαίσθητων προσωπικών δεδομένων για λόγους δημόσιας ασφάλειας και υγείας, για λόγους ελέγχου και φροντίδας κτλ, με όλους τους περιορισμούς, τις εγγυήσεις και την προστασία των νόμων. Στη χώρα μας η θετική όψη της παρακολούθησης δεν είναι αποδεκτή εξαιτίας του αυταρχικού παρελθόντος. Έτσι, με βάση τα παραπάνω

θεωρούμε ότι είναι αναγκαίο να πληροφορηθεί και να παιδαγωγηθεί περισσότερο ο πολίτης για τους κινδύνους που έχει η παραβίαση της ιδιωτικότητας του και της αθέμιτης επεξεργασίας των ευαίσθητων προσωπικών του δεδομένων.

## ΕΛΛΗΝΙΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ


- Αγγελόπουλος, Π. (2003). Βασικές έννοιες αστικού δικαίου. Αθήνα – Κομοτηνή: Σάκκουλας.
- Αλεξανδροπούλου – Αιγυπτιάδου, Ε. (2002). Ζητήματα από το δίκαιο της Πληροφορικής. Αθήνα – Κομοτηνή: Σάκκουλας.
- Αλεξανδροπούλου – Αιγυπτιάδου, Ε. (2007). Προσωπικά δεδομένα. Αθήνα – Κομοτηνή : Σάκκουλας.
- Allen, J. (2003): Μεταβιομηχανισμός και μεταφορντισμός. στο: Η νεωτερικότητα σήμερα. Αθήνα: Σαββάλας.
- Bell, D. (1999). Ο πολιτισμός της μεταβιομηχανικής δύσης. Αθήνα: Νεφέλη.
- Γέροντας, Α. (2002). Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία προσωπικών δεδομένων (Μια συμβολή στην ερμηνεία του Ν. 2472/1997 «Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα». Αθήνα – Κομοτηνή: Σάκκουλας.
- Γεωργιάδης, Α. (2002). Γενικές αρχές αστικού δικαίου. Αθήνα – Κομοτηνή: Σάκκουλας.
- Γιαννούλη, Χ. (1988), Ηλεκτρονική επεξεργασία προσωπικών πληροφοριών και συνταγματικά δικαιώματα. ΕφαρμΔημΔικ.
- Δαγτόγλου, Π. (1991). Ατομικά δικαιώματα Α΄. Αθήνα: Σάκκουλας.
- Δόνος, Π. (2004). «Τεχνολογική διακινδύνευση και προστασία προσωπικών δεδομένων». στο: Νέες τεχνολογίες και συνταγματικά δικαιώματα. Αθήνα – Θεσσαλονίκη: Σάκκουλας.
- Giddens, A. (2001). Οι συνέπειες της νεωτερικότητας, Αθήνα: Κριτική.
- Συνθήκη Σένγκεν, (1995). Αθήνα: Ποντίκι.
- Hall, St., Held, D. and McGrew, A. (2003). Η νεωτερικότητα σήμερα. Αθήνα: Σαββάλας.
- Ιγγλεζάκης, Ι. (2002). Η προστασία των προσωπικών δεδομένων στο διαδίκτυο (internet). Ρυθμίσεις εθνικού και κοινοτικού δικαίου. ΕπισκΕΔ.
- Ιγγλεζάκης, Ι. (2004). Ευαίσθητα προσωπικά δεδομένα: η επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων και οι συνέπειες της. Αθήνα; Θεσσαλονίκη: Σάκκουλας.

- Καλαντζής, Α. (1996). Η προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων. Νομικό Βήμα 44, σ. 317
- Καραγιάννης, Β. (2000). Η νομική προστασία της ηλεκτρονικής ανταλλαγής δεδομένων. Δίκαιο Επιχειρήσεων και Εταιρειών 6 σ. 19.
- Κασιμάτης, Γ. (1995). Σύνταγμα και κοινό δίκαιο. Σε: Τσάτσος, Δ. Η ερμηνεία του Συντάγματος. Αθήνα – Κομοτηνή: Σάκκουλας.
- Καστανάς, Η. (2001). Ίντερνετ και προστασία προσωπικών δεδομένων. Δικαιώματα του Ανθρώπου 11 σ. 711.
- Καστανάς, Η. (2004). «Το internet και η προστασία της ιδιωτικής ζωής και της ελεύθερης έκφρασης: σε αναζήτηση έξυπνων ρυθμίσεων», στο: Νέες τεχνολογίες και συνταγματικά δικαιώματα. Αθήνα: Σάκκουλας.
- Καστέλς, Μ. (2004). Η Κοινωνία του Διαδικτύου στο: Τάτσης, Ν. (2004): Νεωτερικότητα και Κοινωνική Αλλαγή. Αθήνα: Νήσος.
- Καστέλς, Μ. (2005). Ο γαλαξίας του διαδικτύου: Στοχασμοί για το διαδίκτυο, τις επιχειρήσεις και την κοινωνία. Αθήνα: Καστανιώτη.
- Κοτζάμπασης, Α. (2000). Η εθνική ή θρησκευτική συνείδηση ως στοιχείο της προσωπικότητας και η προστασία της στο πλαίσιο του ΑΚ 57. Κριτική Επιθεώρηση νομικής θεωρίας και πράξης.
- Κριάρη - Κατράνη, Ι. (1999). Γενετική τεχνολογία και θεμελιώδη δικαιώματα: η συνταγματική προστασία των γενετικών δεδομένων. Αθήνα: Σάκκουλας.
- Κυριαζή, Ν. (2001). Κοινωνιολογική έρευνα. Αθήνα: Ελληνικά Γράμματα.
- Κυριακόπουλος, Γ. (2001). Ασφάλεια και προστασία δεδομένων προσωπικού χαρακτήρα. Οι ρυθμίσεις του Συμβουλίου της Ευρώπης. Δικαιώματα του Ανθρώπου 11 σ. 763.
- Λυκοβάρδη, Κ. (2004). «Η αντίρρηση συνείδησης στη στρατιωτική θητεία: από τις ποινικές καταδίκες στη νομική ανοχή» στο: Τσαπόγας, Μ. και Χριστόπουλος, Δ. Τα δικαιώματα στην Ελλάδα 1953 – 2003. Από το τέλος του εμφυλίου στο τέλος της μεταπολίτευσης. Αθήνα: Καστανιώτη.
- Λουκέρης, Γ. (1997). Εναρμόνιση του δικαίου της προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα στην Ευρωπαϊκή Ένωση. Νομικό Βήμα 45, σ. 547.
- Μάνεσης, Α. (1982). Συνταγματικά δικαιώματα – α΄ ατομικές ελευθερίες. Θεσσαλονίκη: Πανεπιστημιακές εκδόσεις.

- Μήτρου, Λ. (2001). Προστασία προσωπικών δεδομένων: ένα νέο δικαίωμα; Σε: Τσάτσο, Δ.Θ., Βενιζέλο, Ε. και Κοντιάδη, Η. (2001). Το νέο Σύνταγμα, πρακτικά συνεδρίου για το αναθεωρημένο Σύνταγμα του 1975/1986/2001. Αθήνα.
- Μήτρου, Λ. (2004). Προστασία προσωπικών δεδομένων. Στο: Κάτσικας, Σ., Γκρίτζαλης, Δ., Γκρίτζαλης, (επιμ.) Ασφάλεια πληροφοριακών συστημάτων. Εκδόσεις Νέων Τεχνολογιών, σ. 443-524.
- Μήτρου, Λ. (2006). Προστασία προσωπικών δεδομένων στο πεδίο των ηλεκτρονικών επικοινωνιών: Παράδοση 11 – Επεξεργασία δεδομένων στο διαδίκτυο, διεθνείς κανονιστικές πρωτοβουλίες.
- Μίττλετον, Φ. (2001). Δικαίωμα στον πληροφοριακό αυτοκαθορισμό και δημόσια τάξη: Ο ρόλος της Αρχής στο: Δόνος, Π., Μήτρου, Λ., Μίττλετον, Φ. και Παπακωνσταντίνου Ευ. Η Αρχή Προστασίας Προσωπικών Δεδομένων και η επαύξηση της προστασίας των δικαιωμάτων, στον τόμο Δίκαιο και Κοινωνία στον 21$^{ο}$ αιώνα (Διεύθυνση: Γ. Παπαδημητρίου). Αθήνα – Θεσσαλονίκη:
- Νούσκαλης, Γ. (2007). Ποινική προστασία προσωπικών δεδομένων: Η νομολογιακή συμβολή στην ερμηνεία βασικών όρων. Αθήνα – Θεσσαλονίκη: Σάκκουλας.
- Παπακωνσταντής, Γ. (1998). Συμφωνίες Schengen, Γενική Επισκόπηση, Βασικά Κείμενα.
- Περάκης, Σ. (2001). Η ΕΕ & το πολιτικό άσυλο: Κλείνοντας τις πόρτες». ΕΠΟΧΗ, 20.5.
- Ρόμπινς, Κ. και Ούμπστερ, Φ. (2002). Η εποχή του τεχνοπολιτισμού: Από την κοινωνία της πληροφορίας στην εικονική ζωή. Αθήνα: Καστανιώτη.
- Σαματάς, Μ. (2003). «Ασφάλεια, ελευθερία και δημοκρατία υπό τη Σύμβαση Σένγκεν». Ελληνική Επιθεώρηση Πολιτικής Επιστήμης, τ. 22 Δεκ. 2003.
- Σαματάς, Μ. (2005). «Η εξέλιξη της παρακολούθησης των πολιτών στην Ελλάδα: Από την κρατική παρακολούθηση στις νέες μορφές υπερεθνικού και αγοραίου πανοπτισμού». Στο: Κονιόρδος, Σ., Μαράτου, Λ. και Παναγιωτοπούλου, (επιμ.). Κοινωνικές εξελίξεις στη σύγχρονη Ελλάδα. Αθήνα: Σάκκουλας.
- Στεργίου, Α. (2009). Απεταξάμην το e – φακέλωμα. Ελευθεροτυπία.

- ΦΕΚ Α΄ 50, 1997.
- ΦΕΚ Α΄ 140/26 – 27.6.1997.
- ΦΕΚ Α΄ 287/22.12.1999.
- Χαλαζωνίτης, Κ. (1995). «Οι ευαίσθητες πληροφορίες». Στο: Αλεξανδρής, Ν., Κιουντούζης, Ε., Τραπεζάνογλου, Β., (επιμ.) Ασφάλεια πληροφοριών: Τεχνικά, Νομικά και Κοινωνικά Θέματα. Εκδόσεις Ελληνικής Εταιρείας Επιστημόνων Η/Υ και Πληροφορικής (ΕΠΥ), σ. 303-318.
- Χάρβεϊ, Ν. (2007). Νεοφιλελευθερισμός: Ιστορία και παρόν. Αθήνα: Καστανιώτη.
- Χρυσογόνος, Κ. (2002). Ατομικά και κοινωνικά δικαιώματα. Αθήνα – Κομοτηνή: Σάκκουλας.

## ΞΕΝΟΓΛΩΣΣΗ ΒΙΒΛΙΟΓΡΑΦΙΑ


- Abelson, H. & Lessig, L. (1998). Digital Identity in cyberspace. In White Paper Submitted for 6.805/Law of Cyberspace: Social Protocols.
- Ball, K. and Webster, F. (2003). The Intensification of surveillance crime, terrorism and warfare in the information age. London: Sterling, VA, Pluto Press.
- Ball, K. and Murakami Wood, D. (2006). A report on the Surveillance Society. Surveillance Studies Network. Available at: www.ico.gov.uk/upload/documents/library/data_pretection/practical_application/surveillance_society_full_report_2006.pdf cited 16/10/2006.
- Blume, P. (2003). "Danish data protection with respect to law libraries". International Journal of Legal Information. 31 (4), pp. 452 – 461.
- Chou, N., Ledesma, R., Teraguchi, Y. and Mitchell, J.C., (xx). Client-side defense against web-based identity theft. Computer Science Department, Stanford University.
- Clarke, R. (1927). "Introduction to dataveillance…". Available at: www.anu.edu.au/people/Roger.Clarke/Dv/info.htm#Dv
- Flash Eurobarometer 225 – The gallup Organisation (2008). Data Protection in the European Union: Citizens' perceptions.
- Giddens, A. (1987). Nation state and Violence. University of California Press.
- Gormley, F.H. (1997). Privacy in the information age. Washington: Brookings Institution Press.
- Guerra, St. (1997). "International Migration in the Mediterranean", paper presented at Conference on "Non – military Aspects if Security in Southern Europe" Santorin, 19-21 Sept.
- Gurau, C., Ranchhod, A. and Gauzente, C. (2003). "To legislate or not to legislate: a comparative exploratory study of privacy/personalization factors affecting French, UK and US Web sites", Journal of consumer marketing, 20 (7) p.p. 652 – 664. Available at: http://hermia.emeraldinsight.com
- Haggerty, K. & Ericson, R. (2000). The surveillant assemblage. London School of Economics and Political Science 53(4): 605 – 622.

- Huysmans, J. (1995). "Migrants as a Security problem: Dangers of 'Securitizing' Societal Issues" in Miles, R. & Threnhardt, D. ed. Migration and European Intergration, Pinter, pp. 53-72.
- Lyon, D. (1994). The Electronic Eye: The Rise of Surveillance Society. Cambridge: Polity Press.
- Lyon, D. (1996). Computers, surveillance and privacy. Minneapolis – London: University of Minnesota Press.
- Lyon, D. (2001). Surveillance Society: Monitoring everyday life. Open University Press.
- Lyon, D. (2003). Surveillance as social sorting: computer codes and mobile bodies. London: Routledge.
- Lyon, D. (2003b). Surveillance after September 11, Cambridge, Polity.
- Lyon, D. (2007). Surveillance studies: an overview. Cambridge: Polity Press.
- Marx, G. (1998). "Ethics for the New Surveillance. The Information Society". 14 93), pp. 172 – 185. Available at www.informaworld.com/smpp/content~db=all-content=a713856357
- Marx, G. (2002). "What's new about the 'New surveillance'? Classifying for Change and Continuity". Surveillance & Society 1 (1): 9 – 29.
- Marx, G. (2005). Soft Surveillance: The Growth of Mandatory Volunteerism in Collecting Personal Information – "Hey Buddy Can You Spare DNA?". Στο Surveillance and Security: Technological Politics and Power in Everyday Life. Edited by T. Monahan. N.Y. Routledge.
- Mathieson, T., (1997). "The viewer society: Foucault's Panopticon revisited". Theoretical Criminology, 1, pp. 215 – 234.
- Norris, Cl. & Armstrong, G. (1999). The Maximum Surveillance Society: The rise of CCTV. Oxford & New York: Berg.
- Ollmann, G. (2004). The phising guide: Understanding and preventing ph
- Pato, J. (2003). Identity management: Setting context. Encyclopedia of Information Security (Summer/Fall).
- Patton, P. (1994). "MetamorphoLogic: Bodies and Powers in A Thousand Plateaus". Journal of the British Society of Phenomenology. 25 (2): 157 – 169.

- Samatas, M. (2003). “The privacy paradox for webusers”. In workshop on “Trust Management” September 2003. Imperial College, London. UK. Available at www.dse.doc.ic.ac.uk/events/itrust/slides/samatas.pfd
- Samatas, M. (2004). Surveillance in Greece: From Anticommunist to Consumer Surveillance. New York: Pella.
- Stadler, F. (2000). Informational identity: From analog to digital. Korunk
- Stamatellos, G. (xx). Computer ethics: A global perspective. Sudbury, Massachusetts: Jones and Bartlett publishers.
- Sykes, Ch. (1999). The end of privacy. St Martin Press, N.Y.
- USA Department of Justice, Criminal Division, Special Report on “phising”.
- Well, L. & Royakkers, L., (2004). Ethical issues in web data mining. Netherlands: Ethics and information technology (6), p.p. 129 – 140.
- Wiener, A. (1999). Situating Decisions. The Puzzle of the British ‘No’ to Schengen”.

## ΙΣΤΟΓΡΑΦΙΑ


- www.dpa.gr
- www.stratologia.gr
- www.mfhr.gr
- www.privacyinternational.org
- http://webhome.idirect.com/~dakk/presitations/delzotto/Slide1.html
- http://greektechforum.com/forums/showthread.php.?p=10445
- www.arcanesecurity.net/content/view/6/9/1/4/
- www.Agb.gr
- www.dpa.gr/gnostop.htm
- www.statewatch.org
- www.EPIC.org
- www.greylodge.org/occultreview/glor_012/Surveillance.pdf
- www.digitalrights.gr
- www.humanrightsfirst.org/us_law/after_911/PDF/9_11_3rd_anniversary.pdf
- www.urbaneye.net
- www.digitalrights.gr/tiki/tiki-index.php?page=DataRetention

`

# ΠΑΡΑΡΤΗΜΑ

**ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ**
**ΣΧΟΛΗ ΚΟΙΝΩΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ**
**ΤΜΗΜΑ ΚΟΙΝΩΝΙΟΛΟΓΙΑΣ**
**ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ «ΚΟΙΝΩΝΙΟΛΟΓΙΑ»**

# ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ ΕΡΕΥΝΑΣ
# Η ΑΝΤΙΛΗΨΗ ΚΑΤΟΙΚΩΝ ΤΟΥ ΡΕΘΥΜΝΟΥ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

**ΡΕΘΥΜΝΟ 2009**

## ΔΗΜΟΓΡΑΦΙΚΑ ΣΤΟΙΧΕΙΑ

1. **Φύλο** Άνδρας □ Γυναίκα □
2. **Ηλικία** 18 – 24 □ 25 – 29 □ 30 – 34 □ 35 – 39 □
   40 – 44 □ 45 – 49 □ 50 – 54 □ 55 & άνω□
3. **Επάγγελμα** Άνεργος □ Νοικοκυρά □ Εργάτης/ τεχνίτης □
   Δημόσιος υπάλληλος □ Ιδιωτικός υπάλληλος □
   Ελεύθερος επαγγελματίας □ Άλλο □
4. **Μορφωτικό επίπεδο** Καθόλου □ Λίγες τάξεις του δημοτικού □ Απόφοιτος δημοτικού □ Γυμνάσιο □ Λύκειο/τεχνική σχολή □ Απόφοιτος ΤΕΙ □ Απόφοιτος ΑΕΙ □ Μεταπτυχιακό □

## ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

5. Γνωρίζετε τι είναι προσωπικά δεδομένα;

| ΝΑΙ | ΟΧΙ |
|---|---|
| 1 | 2 |

6. Γνωρίζετε τι είναι ευαίσθητα προσωπικά δεδομένα;

| ΝΑΙ | ΟΧΙ |
|---|---|
| 1 | 2 |

7. Ποια από τα παρακάτω δεδομένα θεωρείτε ότι είναι ευαίσθητα και ποια όχι;

| Α/Α | ΔΕΔΟΜΕΝΑ | ΝΑΙ | ΟΧΙ |
|---|---|---|---|
| **7.1** | Ονοματεπώνυμο | 1 | 2 |
| **7.2** | Διεύθυνση | 1 | 2 |
| **7.3** | Οικογενειακή κατάσταση | 1 | 2 |
| **7.4** | Επάγγελμα | 1 | 2 |
| **7.5** | ΑΦΜ | 1 | 2 |
| **7.6** | Αριθμός αστυνομικής ταυτότητας | 1 | 2 |
| **7.7** | Αριθμός PIN | 1 | 2 |
| **7.8** | Μισθός | 1 | 2 |
| **7.9** | Καταναλωτικές συνήθειες | 1 | 2 |
| **7.10** | Ταξιδιωτική δραστηριότητα | 1 | 2 |
| **7.11** | Τραπεζικές καταθέσεις | 1 | 2 |
| **7.12** | Κατάσταση υγείας | 1 | 2 |
| **7.13** | Ερωτικές προτιμήσεις | 1 | 2 |
| **7.14** | Θρησκευτικές πεποιθήσεις | 1 | 2 |
| **7.15** | Πολιτικές πεποιθήσεις | 1 | 2 |
| **7.16** | Εθνικότητα | 1 | 2 |
| **7.17** | Συνδικαλιστική δράση | 1 | 2 |

8. Σε ποιο βαθμό πιστεύετε ότι οι νόμοι στην Ελλάδα είναι αποτελεσματικοί για την προστασία των προσωπικών σας πληροφοριών – δεδομένων που διατηρούνται στα αρχεία των δημόσιων υπηρεσιών αλλά και των ιδιωτικών επιχειρήσεων;

| ΠΟΛΥ | ΚΑΠΩΣ | ΟΧΙ ΠΟΛΥ | ΚΑΘΟΛΟΥ | ΔΞ/ΔΑ |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |

9. Ακολουθεί μία λίστα οργανισμών που πιθανόν να κρατούν κάποια προσωπικά σας δεδομένα. Ποιους από αυτούς εμπιστεύεστε ότι κάνουν σωστή χρήση των προσωπικών σας πληροφοριών.

| Α/Α | ΟΡΓΑΝΙΣΜΟΙ | ΝΑΙ | ΟΧΙ | ΔΞ/ΔΑ |
|---|---|---|---|---|
| **8.1** | Δημόσιες υπηρεσίες | 1 | 2 | 3 |
| **8.2** | Ιατρικές υπηρεσίες & γιατροί | 1 | 2 | 3 |
| **8.3** | Αστυνομία | 1 | 2 | 3 |
| **8.4** | Κοινωνική ασφάλιση | 1 | 2 | 3 |
| **8.5** | Εφορία | 1 | 2 | 3 |
| **8.6** | Τοπικές αρχές (ΟΤΑ) | 1 | 2 | 3 |
| **8.7** | Τράπεζες | 1 | 2 | 3 |
| **8.8** | Εργοδότες | 1 | 2 | 3 |
| **8.9** | Ασφαλιστικές εταιρείες | 1 | 2 | 3 |
| **8.10** | Ταξιδιωτικά γραφεία | 1 | 2 | 3 |
| **8.11** | Ταχυδρομικές εταιρείες | 1 | 2 | 3 |
| **8.12** | Μη κερδοσκοπικές οργανώσεις | 1 | 2 | 3 |
| **8.13** | Διαφημιστικές εταιρείες, εταιρείες έρευνας αγοράς | 1 | 2 | 3 |
| **8.14** | Πολυκαταστήματα – σούπερ μάρκετ | 1 | 2 | 3 |

10. Γνωρίζετε την ύπαρξη και λειτουργία της Ελληνικής «Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα» που λειτουργεί στην Ελλάδα από το Νοέμβριο του 1997;

| ΝΑΙ | ΟΧΙ |
|---|---|
| 1 | 2 |

11. Αν ναι, έχετε επισκεφθεί την ιστοσελίδα (www.dpa.gr) της Αρχής αυτής;

| ΝΑΙ | ΟΧΙ | ΔΕΝ ΑΠΑΝΤΩ |
|---|---|---|
| 1 | 2 | 3 |

12. Πόση εμπιστοσύνη έχετε στην εκάστοτε Ελληνική Κυβέρνηση αν αυτή σέβεται το απόρρητο των προσωπικών πληροφοριών των πολιτών;

| Πολλή ως μεγάλη εμπιστοσύνη | Αρκετή εμπιστοσύνη | Λίγη εμπιστοσύνη | Πολύ λίγη – καθόλου | Δεν είμαι σίγουρος |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |

13. Πόση εμπιστοσύνη έχετε ότι οι ιδιωτικές εταιρείες, οι τράπεζες, τα σούπερ μάρκετ και όπου αλλού ψωνίζετε με πιστωτικές κάρτες, προστατεύουν τις προσωπικές σας πληροφορίες;

| Πολλή ως μεγάλη εμπιστοσύνη | Αρκετή εμπιστοσύνη | Λίγη εμπιστοσύνη | Πολύ λίγη – καθόλου | Δεν είμαι σίγουρος |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |

## ΔΙΑΔΙΚΤΥΟ (INTERNET)

14. Στο θέμα της προστασίας της ιδιωτικής σας ζωής (ιδιωτικότητας) και των προσωπικών σας δεδομένων πόσο ανήσυχος-η είστε όταν δίνετε προσωπικές πληροφορίες στο διαδίκτυο (internet), όπως το όνομα σας, διεύθυνση, ημερομηνία γέννησης, φύλο, αριθμό πιστωτικής κάρτας κτλ;

| Πολύ ανήσυχος-η | Αρκετά ανήσυχος-η | Όχι πολύ ανήσυχος-η | Καθόλου ανήσυχος-η | Δεν είμαι σίγουρος |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |

15. Έχετε αγοράσει ποτέ κάποιο προϊόν ή υπηρεσία μέσω του Internet;

| ΝΑΙ | ΟΧΙ |
|---|---|
| 1 | 2 |

16. Γνωρίζετε ότι με διάφορα προγράμματα (cookies) μπορεί να παρακολουθούνται τα ψηφιακά ίχνη σας στο διαδίκτυο;

| ΝΑΙ | ΟΧΙ |
|---|---|
| 1 | 2 |

17. Αλλάζετε συχνά τον κωδικό πρόσβασης σας στο διαδίκτυο και στις πιστωτικές κάρτες σας;

| ΝΑΙ | ΟΧΙ |
|---|---|
| 1 | 2 |

18. Χρησιμοποιείτε στον Η/Υ και στο κινητό σας τηλέφωνο κάποιο πρόγραμμα προστασίας από παρενοχλήσεις, εισβολείς – χάκερς κτλ;

| ΝΑΙ | ΟΧΙ |
|---|---|
| 1 | 2 |

19. Οι ελληνικές κυβερνήσεις έχουν περάσει νόμους για την προστασία της εθνικής ασφάλειας. Σε ποιο βαθμό πιστεύετε ότι οι νόμοι αυτοί για την προστασία της εθνικής ασφάλειας παραβιάζουν την ιδιωτική ζωή των πολιτών;

| Πάρα πολύ | Αρκετά | Όχι πολύ | Καθόλου | Δεν είμαι σίγουρος-η |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |

20. Σε ποιο βαθμό θεωρείτε ότι πρέπει μια κυβερνητική/ δημόσια υπηρεσία ή μια επιχείρηση να μοιράζεται τις προσωπικές πληροφορίες των πολιτών – πελατών: α. με άλλες υπηρεσίες, β. με ξένες κυβερνήσεις και γ. με ιδιωτικές επιχειρήσεις;

□ Ναι, είναι δικαίωμα της κυβέρνησης ή της επιχείρησης κάτω απ' όλες τις συνθήκες
□ Ναι, αν ο πολίτης ή ο πελάτης είναι ύποπτος ότι έχει διαπράξει κάποια παράνομη πράξη

□ Ναι, αν η κυβέρνηση ή η επιχείρηση έχει την εκφρασμένη συγκατάθεση του πελάτη
□ Όχι, κάτω από οποιεσδήποτε συνθήκες
□ Δεν είμαι σίγουρος-η

## ΚΑΜΕΡΕΣ

21. Κατά τη γνώμη σας πόσο αποτελεσματικές στη μείωση της εγκληματικότητας είναι οι κάμερες σε εξωτερικούς δημόσιους χώρους;

| Πολύ | Κάπως | Όχι πολύ | Καθόλου | Δεν είμαι σίγουρος-η | Δεν απαντώ |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 |

22. Κατά τη γνώμη σας πόσο αποτελεσματικές στη μείωση της εγκληματικότητας είναι οι εσωτερικές κάμερες σε επιχειρήσεις, τράπεζες κτλ;

| Πολύ | Κάπως | Όχι πολύ | Καθόλου | Δεν είμαι σίγουρος-η | Δεν απαντώ |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 |

23. Σας ενοχλεί ή όχι το γεγονός της ευρείας χρήσης καμερών ασφαλείας σε πάρα πολλούς χώρους όπως στα περίπτερα, ακόμα και σε εκκλησίες;

| Πολύ | Κάπως | Όχι πολύ | Καθόλου | Δεν είμαι σίγουρος-η | Δεν απαντώ |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 |

24. Εσείς θα χρησιμοποιούσατε κάμερες ασφαλείας για τη φύλαξη και ασφάλεια της κατοικίας ή της επιχείρησης σας;

| ΝΑΙ | ΟΧΙ | ΔΕΝ ΑΠΑΝΤΩ |
|---|---|---|
| 1 | 2 | 3 |

25. Συμφωνείτε ή διαφωνείτε οι κάμερες της αστυνομίας για τη διαχείρηση της κυκλοφορίας να χρησιμοποιούνται και για λόγους ασφαλείας και δημόσιας τάξης;

| Συμφωνώ απόλυτα | Συμφωνώ κάπως | Διαφωνώ κάπως | Διαφωνώ απόλυτα | Δεν είμαι σίγουρος-η |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |

26. Συμφωνείτε ή διαφωνείτε με το βανδαλισμό – καταστροφή των καμερών ασφαλείας της αστυνομίας;

| Συμφωνώ απόλυτα | Συμφωνώ κάπως | Διαφωνώ κάπως | Διαφωνώ απόλυτα | Δεν είμαι σίγουρος-η |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |

27. Σε ποιο βαθμό συμφωνείτε ή διαφωνείτε ότι θα πρέπει να επιτρέπεται στους εργοδότες να παρακολουθούν με κάμερες ή και άλλα ηλεκτρονικά μέσα τους εργαζόμενους τους και να διαβάζουν το ηλεκτρονικό ταχυδρομείο τους;

| Συμφωνώ απόλυτα | Συμφωνώ κάπως | Διαφωνώ κάπως | Διαφωνώ απόλυτα | Δεν είμαι σίγουρος-η |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |

28. Σε ποιο βαθμό συμφωνείτε ή διαφωνείτε με τη χρήση κρυφής κάμερας για την απόδειξη μιας παράνομης πράξης;

| Συμφωνώ απόλυτα | Συμφωνώ κάπως | Διαφωνώ κάπως | Διαφωνώ απόλυτα | Δεν είμαι σίγουρος-η |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |

29. Σας αρέσουν τα τηλεοπτικά προγράμματα τύπου Big Brother που χρησιμοποιούν κάμερες παρακολούθησης;

| Πάρα πολύ | Αρκετά | Όχι πολύ | Καθόλου | Δεν είμαι σίγουρος-η | Δεν απαντώ |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 |

## ΤΑΞΙΔΕΥΟΝΤΑΣ

30. Σε ποιο βαθμό θεωρείτε ότι η ιδιωτικότητας σας (η προσωπικότητα και τα προσωπικά σας δεδομένα) γίνεται σεβαστή στα αεροδρόμια όταν ταξιδεύετε αεροπορικώς;

| Πάρα πολύ | Αρκετά | Όχι πολύ | Καθόλου | Δεν είμαι σίγουρος-η | Δεν απαντώ |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 |

31. Συμφωνείτε ή διαφωνείτε στο ότι η Ελληνική κυβέρνηση να έχει το δικαίωμα να συλλέγει προσωπικές πληροφορίες για τους ταξιδιώτες;

| Πάρα πολύ | Αρκετά | Όχι πολύ | Καθόλου | Δεν είμαι σίγουρος-η | Δεν απαντώ |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 |

32. Συμφωνείτε ή διαφωνείτε στο ότι η Ελληνική κυβέρνηση θα πρέπει να μπορεί να μοιράζεται τις προσωπικές πληροφορίες για τους ταξιδιώτες με άλλες κυβερνήσεις;

| Συμφωνώ απόλυτα | Συμφωνώ κάπως | Διαφωνώ κάπως | Διαφωνώ απόλυτα | Δεν είμαι σίγουρος-η |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |

33. Σε ποιο βαθμό συμφωνείτε οι αξιωματούχοι ασφαλείας στα αεροδρόμια θα πρέπει να παίρνουν έξτρα μέτρα ασφαλείας για τα ταξιδεύοντα μέλη ορατών μειονοτήτων (έγχρωμοι, μουσουλμάνοι κτλ);

| Συμφωνώ απόλυτα | Συμφωνώ κάπως | Διαφωνώ κάπως | Διαφωνώ απόλυτα | Δεν είμαι σίγουρος-η |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |

34. Μερικές αεροπορικές και άλλες εταιρείες προσφέρουν στους πελάτες τους διάφορα προνόμια – μπόνους με βάση τη συλλογή πόντων από τις αγορές τους απ' αυτές. Εσείς σαν καταναλωτής μαζεύετε τέτοιους πόντους;

| ΝΑΙ | ΟΧΙ |
|---|---|
| 1 | 2 |

35. Πόσο αποδεκτό ή όχι είναι για σας μια επιχείρηση να δημιουργεί το προφίλ σας ως πελάτη της, χρησιμοποιώντας πληροφορίες για τις καταναλωτικές σας

προτιμήσεις, ώστε να σας πληροφορεί για προϊόντα και υπηρεσίες που ενδεχομένως σας ενδιαφέρουν;

| Συμφωνώ απόλυτα | Συμφωνώ κάπως | Διαφωνώ κάπως | Διαφωνώ απόλυτα | Δεν είμαι σίγουρος-η |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |

36. Θα σας ενοχλούσε ή όχι αν η επιχείρηση αυτή διέθετε ή πωλούσε το καταναλωτικό σας προφίλ σε άλλους χωρίς την άδειά σας;

| Πάρα πολύ | Αρκετά | Όχι πολύ | Καθόλου | Δεν είμαι σίγουρος-η | Δεν απαντώ |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 |

## ΥΠΟΚΛΟΠΕΣ

37. Σας έχει ανησυχήσει ή όχι το πρόσφατο σκάνδαλο των υποκλοπών των κινητών τηλεφώνων στην Ελλάδα;

| Πάρα πολύ | Αρκετά | Όχι πολύ | Καθόλου | Δεν είμαι σίγουρος-η | Δεν απαντώ |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 |

38. Αν ναι, πόσο σας έχει επηρεάσει στη χρήση του κινητού σας τηλεφώνου;

| Πάρα πολύ | Αρκετά | Όχι πολύ | Καθόλου | Δεν είμαι σίγουρος-η |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |

39. Φοβάστε ότι οι τηλεφωνικές σας συνομιλίες ιδιαίτερα στο κινητό τηλέφωνο αλλά και το ηλεκτρονικό σας ταχυδρομείο μπορεί να παρακολουθούνται;

| Πάρα πολύ | Αρκετά | Όχι πολύ | Καθόλου | Δεν είμαι σίγουρος-η |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |

40. Παίρνετε ή όχι κάποια μέτρα προστασίας των επικοινωνιών σας μέσω Η/Υ ή τηλεφώνου;

| ΝΑΙ | ΟΧΙ |
|---|---|
| 1 | 2 |

41. Τελικά, αποδέχεστε ή όχι την παραβίαση της ιδιωτικής σας ζωής και των προσωπικών σας δεδομένων για την προσωπική σας ασφάλεια και υγεία;

| Πάρα πολύ | Αρκετά | Όχι πολύ | Καθόλου | Δεν είμαι σίγουρος-η |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |

42. Σε ποιο βαθμό αποδέχεστε ή όχι την παραβίαση της ιδιωτικής σας ζωής και των προσωπικών σας δεδομένων για λόγους εθνικής ασφάλειας και δημόσιας υγείας;

| Πάρα πολύ | Αρκετά | Όχι πολύ | Καθόλου | Δεν είμαι σίγουρος-η | Δεν απαντώ |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 |