Τεχνολογικό Εκπαιδευτικό Ίδρυμα Πάτρας

Σχολή Διοίκησης & Οικονομίας

Τμήμα Λογιστικής

Πτυχιακή εργασία: Ιδιωτικότητα στις Υπηρεσίες Διαδικτύου

Εκπόνηση από:

Παγκάκης Αθανάσιος
Λεμποτέσης Θοδωρής
Κατσιφέρης Κωνσταντίνος

Επιβλέπων καθηγητής:

Σταμάτης Κωνσταντίνος

Πάτρα, Μάιος 2013

Περιεχόμενα

Περίληψη

Στην συγκεκριμένη προσπάθεια θα προσπαθήσουμε να καλύψουμε σφαιρικά το ζήτημα της ιδιωτικότητας στις υπηρεσίες διαδικτύου, με τις οποίες αλληλεπιδρούμε καθημερινά.

Στο κεφάλαιο 1, αναφερόμαστε αναλυτικά στον ορισμό και την ιστορία της ιδιωτικότητας, προσπαθώντας να αποκτήσουμε ένα θεωρητικό υπόβαθρο σχετικά με την έννοια που αναλύουμε.

Στο κεφάλαιο 2, αναφερόμαστε στην ιδιωτικότητα και την ασφάλεια της πληροφορίας στο διαδίκτυο. Αναφερόμαστε αναλυτικά στην παραβίαση του απορρήτου και στην χρήση των cookies και την ασφάλεια την οποία παρέχουν.

Στο κεφάλαιο 3, φέρουμε εκτενή παραδείγματα υπηρεσιών διαδικτύου, και ειδικότερα στον κλάδο της λογιστικής. Αρχικά αναφέρουμε τον ορισμό και κάποια βασικά στοιχεία της αρχιτεκτονικής των υπηρεσιών διαδικτύου και εν συνεχεία αναλύουμε τις υπηρεσίες με τις οποίες αλληλεπιδρά καθημερινά ο κλάδος μας. Τέλος, εκτενής αναφορά γίνεται στην Δίωξη Ηλεκτρονικού Εγκλήματος, το οποίο αποτελεί το εκτελεστικό όργανο της κυβέρνησης για την προστασία της ιδιωτικότητας και όχι μόνο.

Στο κεφάλαιο 4 και στο κεφάλαιο 5, υπάρχει εκτενής αναφορά στο νομικό πλαίσιο που υφίσταται για να προστατεύει τους χρήστες, είτε σε διεθνές επίπεδο, είτε σε εθνικό, και στις κανονιστικές προσεγγίσεις της ιδιωτικότητας. Η νομική κατοχύρωση του χρήστη αποτελεί πλέον κύριο μέλημα της εκάστοτε κυβέρνησης.

Τέλος, στο κεφάλαιο 6 αναφέρονται τα συμπεράσματα μας, ύστερα από την ενδελεχή έρευνα την οποία πραγματοποιήσαμε.

Εισαγωγή

Η ιδιωτικότητα ως έννοια

Η εποχή στην οποία βρισκόμαστε χαρακτηρίζεται ως η εποχή της πληροφορίας. Η ανάπτυξη του διαδικτύου και γενικότερα η άνθηση του ηλεκτρονικού εμπορίου οδήγησαν σε νέες τάσεις και προκλήσεις τόσο για τους καταναλωτές όσο και για τις επιχειρήσεις. Πλέον κάθε σύγχρονη επιχείρηση είτε παραδοσιακή (offline) είτε εξολοκλήρου διαδικτυακή (online) έχει το δικό της ιστοχώρο που παρέχει τα προϊόντα της ή/και τις υπηρεσίες της καθώς και πλήθος πληροφοριών. Από την άλλη πλευρά ολοένα και μεγαλύτερο μέρος του πληθυσμού αρχίζει να υιοθετεί τη χρήση του διαδικτύου είτε για να αγοράσει κάποιο προϊόν είτε για να αναζητήσει συγκεκριμένες πληροφορίες είτε για να ενημερωθεί. Επίσης πολλές συναλλαγές μεταξύ των κρατικών υπηρεσιών και των πολιτών γίνονται πλέον ηλεκτρονικά. Ενδεικτικά αναφέρουμε κάποιες εφαρμογές όπως η ηλεκτρονική διακυβέρνηση (e-government) και η ηλεκτρονική εκπαίδευση (e-learning) καθώς εμφανίζονται ολοένα και περισσότερες (e-medicine, e-voting, e-commerce). Στο σύνολο των νέων αυτών ηλεκτρονικών δραστηριοτήτων η αξία της πληροφορίας που διακινείται μεγαλώνει συνεχώς. Μέρος αυτής της πληροφορίας προέρχεται από την καταγραφή, αποθήκευση και διαχείριση των ιδιωτικών δεδομένων των χρηστών και των κοινωνικών ομάδων που δραστηριοποιούνται στο διαδίκτυο. Έτσι το θέμα της ιδιωτικότητας έρχεται δυναμικά στην επιφάνεια και πλέον αποτελεί θέμα υψίστης

προτεραιότητας τόσο στις ανησυχίες των καταναλωτών όσο και των επιχειρήσεων.

Είναι όμως πράγματι τόσο σημαντικό το θέμα της ιδιωτικότητας όπως πράγματι

παρουσιάζεται και κατά πόσο ενδιαφέρει και τις επιχειρήσεις η υιοθέτηση μιας πελατοκεντρικής πολιτικής στο θέμα της ιδιωτικότητας; Τα παρακάτω στοιχεία είναι ενδεικτικά (http://www.privacyexchange.org/iss/surveys/surveys.html):

Οι παρούσες πρακτικές της συλλογής και επεξεργασίας δεδομένων σε εξατομικευμένους ιστότοπους φαίνεται ότι συγκρούονται με θέματα ιδιωτικότητας των χρηστών του διαδικτύου, που αναφέρουν χαρακτηριστικά ότι:

1) ανησυχούν πολύ σχετικά με απειλές της ιδιωτικότητάς τους όταν χρησιμοποιούν το διαδίκτυο σε ποσοστό 81%-87%,

2) είναι εξαιρετικά ή πολύ ανήσυχοι σχετικά με την αποκάλυψη ιδιωτικών τους πληροφοριών στο διαδίκτυο σε ποσοστό 67%-74%, και

3) είναι εξαιρετικά ανήσυχοι σχετικά με την παρακολούθησή τους στο διαδίκτυο σε ποσοστό 54%-77%.

Οι χρήστες του διαδικτύου δεν ανησυχούν μόνο αλλά ήδη αντιδρούν. Πιο συγκεκριμένα έχουν καταγραφεί οι εξής συμπεριφορές που πρέπει να προβληματίσουν ιδιαίτερα τα στελέχη των επιχειρήσεων:

1) 41% των χρηστών κατά μέσο όρο εγκαταλείπουν ιστοχώρους που απαιτούν καταχώρηση πληροφοριών

2) 40% στις ΗΠΑ, 27% στη Μεγάλη Βρετανία και 32% στη Γερμανία έχουν δώσει αναληθείς ή ψεύτικες πληροφορίες καταχώρησης και

3) 54% στις Η.Π.Α., 32% στη Μεγάλη Βρετανία και 35% στη Γερμανία έχουν αποφύγει να αγοράσουν κάτι από το διαδίκτυο λόγω θεμάτων ιδιωτικότητας, ή έχουν αγοράσει λιγότερα.

Οι χρηστές διαδικτύου που ανησυχούν σχετικά με την ιδιωτικότητά τους δεν είναι αφελείς αλλά έχουν πραγματιστικές ανάγκες:

1) θέλουν οι ιστοχώροι να ζητούν την άδειά τους για να χρησιμοποιούν ιδιωτικά τους δεδομένα σε ποσοστό 81% κατά μέσο όρο, και

2) 31% στις ΗΠΑ, 30% στη Μεγάλη Βρετανία και 51% στη Γερμανία είναι διατεθειμένοι να δίνουν ιδιωτικές πληροφορίες με αντάλλαγμα κάτι χρήσιμο.

Επίσης εάν η αντίληψη του πελάτη για τα θέματα ιδιωτικότητας του δεν αντιμετωπίζεται σοβαρά από την επιχείρηση, ο πελάτης δεν θα συναλλάσσεται πλέον με αυτή την επιχείρηση (Smith and Rupp 2004). Έρευνα των Freeman και Urbaczewski (2005) κατέληξε στο συμπέρασμα πως η ιδιωτικότητα έχει ιδιαίτερα μεγάλο ενδιαφέρον και αποτελεί σημαντικό θέμα για τους καταναλωτές. Επίσης έρευνα του Zhang (2005) έδειξε πως η γνώση των χρηστών διαδικτύου για τις παραβιάσεις της ιδιωτικότητάς τους στο διαδίκτυο είναι μικρότερη σε σύγκριση με θέματα ασφαλείας, προστασίας και ανανέωσης των τεχνολογιών ασφαλείας. Επομένως συμπεραίνει ότι οι ίδιοι οι χρήστες δεν έχουν τελείως συνειδητοποιήσει τους κινδύνους της παραβίασης της ιδιωτικότητάς τους. Από την παράθεση των παραπάνω στοιχείων συμπεραίνουνε τη σημαντικότητα του θέματος της ιδιωτικότητας τόσο για τους καταναλωτές όσο και για τις επιχειρήσεις.

Κεφάλαιο 1

1.1. Η έννοια της ιδιωτικότητας

Η ιδιωτικότητα ως έννοια από μόνη της είναι ιδιαίτερα ενδιαφέρουσα και μυστηριώδης, ίσως επειδή σχεδόν κανένας δεν συμφωνεί στο τι πραγματικά είναι. Όμως το «δικαίωμα στην ιδιωτικότητα» ενέπνευσε πλήθος συζητήσεων και αντιπαραθέσεων σε πολλά επιστημονικά πεδία όπως νομικό, φιλοσοφικό, κοινωνικό, πολιτικό και πιο πρόσφατα τεχνολογικό πεδίο. Χαρακτηριστικά αναφέρουμε τη δήλωση του Lyndon B. Johnson (προέδρου των Η.Π.Α. 1963-1969) πως «κάθε άνθρωπος πρέπει να γνωρίζει ότι οι συνομιλίες του, οι συναναστροφές του και η προσωπική του ζωή είναι ιδιωτικά».

Οι πρώτες σκέψεις για την έννοια της ιδιωτικότητας επικεντρώθηκαν στο να απαντήσουν στο ερώτημα γιατί είναι σημαντική η ιδιωτικότητα και τι αποτελέσματα έχει η διατήρησή της σε κάθε άτομο. Πολλοί θεωρητικοί υποστήριξαν ότι η ιδιωτικότητα είναι μία άκρως σημαντική ανθρώπινη αξία, απαραίτητη για πολλές εκφάνσεις της ηθικής και κοινωνικής πλευράς ενός ατόμου. Τέτοιες ενδεικτικές αναφορές είναι: η ιδιωτικότητα είναι μία απαραίτητη προϋπόθεση για την ανάπτυξη διαφορετικών και βαρυσήμαντων σχέσεων (Rachels 1975) η ιδιωτικότητα είναι ένα σημαντικό στοιχείο της προσωπικότητας και της ακεραιότητας(Fried 1968)˙ η ιδιωτικότητα αποτελεί προϋπόθεση για την ανθρώπινη αξιοπρέπεια και διατηρεί την ατομικότητα και την αυτονομία του ατόμου (Bloustein 1964) και τέλος η ιδιωτικότητα είναι μία αναγκαία συνθήκη για την επίτευξη οικειότητας(Gerstein 1978).

Οι προσπάθειες απόδοσης κάποιου αυστηρού ορισμού σχετικά με το τι είναι ιδιωτικότητα δεν απέδωσαν διότι η αντίληψη του τι είναι εξαρτάται και από την γενική αντίληψη του κοινωνικού συνόλου που εντάσσεται το άτομο και από τη σχετική εμπειρία κάθε ατόμου(Westin 1981 και1984). Όλοι όμως οι ορισμοί σύμφωνα με τον Shoemen (1984) συνοψίζονται στις εξής3 κύριες κατηγορίες:

I. Στο δικαίωμα του ατόμου να μπορεί ανά πάσα στιγμή να ελέγχει την πρόσβαση στην πληροφορία που πηγάζει από το άτομό του.

II. Στο εύρος ελέγχου που έχει ένα άτομο σχετικά με τις ιδιωτικές του πληροφορίες ή που έχει διαισθητική πρόσβαση σε αυτά.

III. Στο επίπεδο περιορισμένης πρόσβασης σε ένα άτομο και στις ιδιωτικές του πληροφορίες.

Λόγω όμως του γεγονότος ότι και οι τρεις παραπάνω κατηγορίες εμφανίζουν μερικά μειονεκτήματα, αρκετοί θεωρητικοί ανέκρουσαν ότι η ιδιωτικότητα είναι μία σύνθετη και πολύπλοκη έννοια για να αποδοθεί με έναν απλό ορισμό και πρότειναν ότι θα πρέπει να αντιμετωπιστεί σαν μία συλλογή από αλληλοσχετιζόμενες έννοιες. Έτσι οι Benn and Gaus (1983) πρότειναν ότι η ιδιωτικότητα είναι μία ευρεία κοινωνική έννοια που ορίζει πώς ένα άτομο αντιλαμβάνεται και αλληλεπιδρά με την κοινωνία.

Από την άλλη πλευρά εκδηλώθηκαν και αρκετές απόψεις θεωρητικών που αντιμετωπίζουν πιο κριτικά το θέμα της ιδιωτικότητας. Έτσι οι Prosser (1960) and Thomson (1975) δηλώνουν ότι δεν υπάρχει το δικαίωμα στην ιδιωτικότητα υποστηρίζοντας ότι αν και η ιδιωτικότητα αποτελεί μία σημαντική έννοια αντιμετωπίζοντάς την σαν κάτι το ξεχωριστό είναι αντιπαραγωγικό αφού υπάρχουν άλλες συνυφασμένες έννοιες που μπορούν να την διασφαλίσουν όπως το δικαίωμα της ιδιοκτησίας και της σωματικής ακεραιότητας. Ακόμα πιο επικριτικός είναι oWasserstrom (1984) που τονίζει ότι η

ιδιωτικότητα ως διαφύλαξη πληροφοριών για ένα άτομο μπορεί να αποτελέσει από ηθικής πλευράς συνώνυμο της υποκρισίας και της απάτης με αποτέλεσμα να μην είναι κοινωνικά αποδεκτή. Μία ακόμα έννοια της ιδιωτικότητας ίσως πιο ενδιαφέρουσα για το πεδίο του ηλεκτρονικού εμπορίου έχει εισαχθεί από τον Posner (1984) που υποστηρίζει ότι τα θέματα της ιδιωτικότητας δεν είναι διακριτά και μπορούν να εξηγηθούν καλύτερα με οικονομικούς όρους: πιστεύει ότι η πληροφορία έχει αξία και οι άνθρωποι θα πρέπει να πληρωθούν το ανάλογο αντίτιμο για να την αποκαλύψουν. Επομένως υπάρχουν δύο οικονομικά αγαθά: τα ιδιωτικά στοιχεία και η διαδικασία αγοράς/πώλησης αυτών. Δηλαδή σύμφωνα με τον Posner τα άτομα δεν επιθυμούν τη διαφύλαξη των ιδιωτικών τους στοιχείων για χάρη της

ιδιωτικότητας αλλά για τα οικονομικά ή κοινωνικά πλεονεκτήματα που τους προσφέρουν. Επομένως τα ιδιωτικά στοιχεία θα πρέπει να προστατεύονται μόνο όταν η πρόσβαση σε αυτή την πληροφορία μειώνει την προϋπάρχουσα αξία τους. Συμπαραστατικά, από την παραπάνω ανάλυση προκύπτει ότι η έννοια της ιδιωτικότητας είναι πράγματι σύνθετη και πολύμορφη. Όλοι όμως είτε υπέρμαχοι είτε κριτικοί αναγνωρίζουν τη σημαντικότητά της και την ιδιαιτερότητά της. Στη σημερινή εποχή ο όρος της ατομικής ιδιωτικότητας αντιμετωπίζεται από την πλειονότητα των θεωρητικών ως μία ανθρώπινη αξία υψίστης σημασίας. Επομένως αυτή η ανθρώπινη αξία θα πρέπει να προστατευθεί σε όλες τις εκφάνσεις της: και στους παραδοσιακούς τομείς αλλά και στους νέους αναπτυσσόμενους τομείς της εποχής της πληροφορίας.

Στην προσπάθειά μας να παρουσιάσουμε έναν ορισμό καταλήγουμε πως«με τον όρο ιδιωτικότητα εννοούμε την κατάσταση κατά την οποία η πρόσβαση στις ιδιωτικές πληροφορίες ενός συγκεκριμένου

ατόμου μπορεί να ελεγχθεί και να διαχειριστεί από το ίδιο το άτομο ακόμα και όταν κάποιο τρίτο μέρος έχει συλλέξει αυτήν την πληροφορία».

1.2. Η εξέλιξη της έννοιας ιδιωτικότητα

Η ιδιωτικότητα ως ιδέα, όπως και άλλες κοινωνικές έννοιες, δεν παραμένει στατική και συγκεκριμένη αλλά συνεχώς εξελίσσεται ακολουθώντας τα βήματα εξέλιξης της κοινωνίας. Στην εξέλιξη αυτή διακρίνουμε μερικά κύρια στάδια (Rhys and Shao 2007), τα οποία αναφέρουμε στη συνέχεια, σε κάθε ένα από τα οποία η ιδιωτικότητα αντιλαμβανόταν με διαφορετικό τρόπο και προστατευόταν αντιστοίχως διαφορετικά.

1.2.1. Η εμφάνιση της ιδιωτικότητας

Η ιδιωτικότητα είναι μία έννοια που οι ρίζες της πηγάζουν εδώ και2500 χρόνια όταν για πρώτη φορά ο Έλληνας φιλόσοφος Αριστοτέλης είχε εισάγει την έννοιά της στην αρχαία Αθήνα στο δοκίμιό του με τίτλο «Πολιτικά». Για πρώτη φορά γίνεται ένας ξεκάθαρος διαχωρισμός μεταξύ των δημοσίων θεμάτων του δήμου που απασχολούν όλους τους πολίτες της πόλης και των ιδιωτικών θεμάτων του οίκου που απασχολούν μόνο τα άτομα ενός σπιτιού. Στη συνέχεια οι Ρωμαίοι ανέπτυξαν ακόμα περισσότερο την ιδέα της ιδιωτικής ζωής σε σχέση με τη δημόσια ζωή κάθε ατόμου. Στη θηραϊκή κοινωνία η έννοια της δημόσιας ζωής είναι συνδεδεμένη με το καλό του κράτος και την πρόοδο της κοινωνίας ενώ η ιδιωτική ζωή αναφέρεται στα προσωπικά ενδιαφέροντα κάθε ατόμου στην αυτοκρατορία. Οι έννοιες αυτές είχαν τόσο μεγάλη απήχηση

και αποδοχή που συμπεριλήφθηκαν στο Ρωμαϊκό Δίκαιο το 533 μ.Χ. από τον αυτοκράτορα Ιουστινιανό (Weintraud 1997). Επομένως για πρώτη φορά οι όροι «ιδιωτικό» και «δημόσιο» καταγράφονται από τους Ρωμαίους.

Στη συνέχεια η έννοια της ιδιωτικότητας παρέμεινε στάσιμη και τίθεται στο περιθώριο μέχρι την εμφάνιση της Αναγέννησης όπου το ενδιαφέρον ανανεώνεται. Έτσι η έννοια της ιδιωτικότητας αρχίζει σταδιακά να αναγνωρίζεται ως μία βασική ανθρώπινη αξία. Πλέον γίνεται συστηματική προσπάθεια να κατοχυρωθεί νομικά και να προστατευθεί οπότε περνάμε σε μία νέα εποχή, αυτή της νομιμοποίησης της ιδιωτικότητας.

1.2.2. Η νομιμοποίηση της ιδιωτικότητας

Το αγγλικό δίκαιο ήταν ένα από τα πρώτα που αναγνωρίζει ορισμένες εκφάνσεις της ιδιωτικότητας και τις ενσωματώνει στις νομικές διατάξεις του. Ομοίως και το σύνταγμα των Η.Π.Α στα πρώτα άρθρα του αναφέρει σαφέστατα θέματα που σχετίζονται με την προστασία των προσωπικών δεδομένων. Σε κανένα από τα δύο όμως δεν αναφέρεται ρητά το δικαίωμα στην ιδιωτικότητα, όπως επίσης και το1789 στη Γαλλία στην «Διακήρυξη των δικαιωμάτων του ανθρώπου και του πολίτη» αναφέρονται μόνο κάποιες νομοθετικές διατάξεις για ορισμένα θέματα της ιδιωτικότητας.

Η πρώτη νεότερη αναφορά στην ανάγκη να επισημανθεί η αξία της ιδιωτικότητας προέρχεται από το άρθρο που δημοσίευσαν οι Warren and Brandeis το1890 στις Η.Π.Α. Για πρώτη φορά συνδέεται η ιδιωτικότητα με«το δικαίωμα να μείνει κανείς μόνος του» (“the right to be left alone”) και τονίζεται η αναγκαιότητα να κατοχυρωθεί συνταγματικά η έννοια της ιδιωτικότητας. Επίσης στο άρθρο αναφέρεται πως η

σημασία του θέματος της ιδιωτικότητας συνεχώς θα μεγαλώνει καθώς η αξία της είναι πολύ μεγαλύτερη από ότι στο παρελθόν. Μετά από μακροχρόνιες κοινωνικές συζητήσεις το1965 για πρώτη φορά θεσπίζεται το συνταγματικό δικαίωμα στην ιδιωτικότητα από το ανώτατο δικαστήριο των Η.Π.Α. και έτσι κατοχυρώνεται νομικά (Rhys and Shao 2007).

Πρέπει επίσης να αναφέρουμε πως το1948 το γενικό συμβούλιο των Ηνωμένων Εθνών στην «παγκόσμια δήλωση των ανθρωπίνων δικαιωμάτων» αναφέρεται γενικά στο θέμα της ιδιωτικότητας και προχωρώντας ένα βήμα πιο μπροστά το1950 η ευρωπαϊκή επιτροπή των ανθρωπίνων δικαιωμάτων θεσπίζει το δικαίωμα σεβασμού της ιδιωτικής ζωής των πολιτών. Επομένως παρατηρούμε πως η έννοια της ιδιωτικότητας κατοχυρώνεται νομικά σχετικά πρόσφατα και εκδηλώνεται η ανάγκη προστασίας της από το νόμο. Όμως λόγω της προόδου της κοινωνίας και της μετάβασης στην εποχή της τεχνολογίας επηρεάστηκαν τόσο η έννοια της ιδιωτικότητας όσο και οι μηχανισμοί προστασίας της.

1.2.3. Η ιδιωτικότητα στην τεχνολογική εποχή

Καθώς η τεχνολογία βρίσκεται σε διαρκή φάση ανάπτυξης νέες προκλήσεις έρχονται να προστεθούν στα μέχρι τώρα θέματα της ιδιωτικότητας (issues of privacy). Πρώτον το θέμα της παρακολούθησης της ιδιωτικής ζωής των πολιτών (Tuerkheimer 1993). Λόγω των νέων τεχνολογιών είναι πλέον δυνατός ο εντοπισμός της θέσης του αυτοκινήτου μέσω ασύρματων δικτύων, η καταγραφή των τηλεφωνημάτων, η παρακολούθηση της κίνησης του διαδικτύου, η εύρεση σύντομων ηλεκτρονικών μηνυμάτων (email) και αρκετές ακόμα εφαρμογές.

Δεύτερον το θέμα της προστασίας των ιδιωτικών δεδομένων των χρηστών διαδικτύου που σχεδόν ανεξέλεγκτα κυκλοφορούν, καταγράφονται ακόμα και παραποιούνται. Πλέον δημιουργούνται τεράστιες βάσεις δεδομένων που περιέχουν πληροφορίες σχετικά με τη ζωή, τα ενδιαφέροντα και τις προτιμήσεις των ατόμων.

Σε μία προσπάθεια να αντιμετωπιστούν οι νέες αυτές προκλήσεις, αρκετές χώρες όπως η Μεγάλη Βρετανία και η Σουηδία συντάσσουν νόμους, οδηγίες και νομοθετικά πλαίσια που κύριο σκοπό έχουν την προστασία των προσωπικών δεδομένων. Έτσι ο Οργανισμός Οικονομικής Ανάπτυξης (Organization of Economic Development) συντάσσει ένα κατάλογο οδηγιών (γνωστό και ως OECD privacy guidelines) που θέτει ελάχιστα αποδεκτά όρια για τη συλλογή, αποθήκευση, επεξεργασία και διασπορά των προσωπικών δεδομένων (Rhys and Shao 2007). Το1981 η Ευρωπαϊκή Ένωση συστήνει επιτροπή για την προστασία των ατομικών δεδομένων και έτσι το θέμα της ιδιωτικότητας τίθενται στο επίκεντρο. Όλες οι χώρες μέλη πρέπει να θεσπίσουν συγκεκριμένες νομικές διατάξεις για την προστασία των ιδιωτικών δεδομένων των πολιτών τους. Το 1998, ως επιστέγασμα των προσπαθειών να συντονιστούν όλα τα κράτη μέλη υπό ένα κοινό νομικό καθεστώς, κατατίθεται η ντιρεκτίβα της προστασίας των προσωπικών δεδομένων (γνωστή και ως officially Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data). Σύμφωνα με αυτή κάθε χώρα μέλος πρέπει να θεσπίσει συγκεκριμένες νομικές υποχρεωτικές διατάξεις και να δημιουργήσει αρμόδια υπηρεσία, τη γνωστή Αρχή Προστασίας των Προσωπικών Δεδομένων.

Στο πλαίσιο της παγκοσμιοποίησης της αγοράς που προσφέρει το διαδίκτυο θα πρέπει σε αυτό το σημείο να τονιστεί ένα αρκετά

ενδιαφέρον γεγονός: τη διαφορά νοοτροπίας ανάμεσα στις χώρες της Ευρωπαϊκής Ένωσης και στις Η.Π.Α. στο θέμα της προστασίας της ιδιωτικότητας. Οι ευρωπαϊκές χώρες έχουν υιοθετήσει ένα ξεκάθαρο νομικό πλαίσιο σε αντίθεση με τις Η.Π.Α που χρησιμοποιούν ένα σύνολο κανονισμών με σκοπό την αυτορύθμιση των επιχειρήσεων. Ως αποτέλεσμα ο έλεγχος τήρησης της ιδιωτικότητας να επαφίεται στα χέρια του καταναλωτή και όχι των αρμόδιων υπηρεσιών όπως στην Ευρώπη.

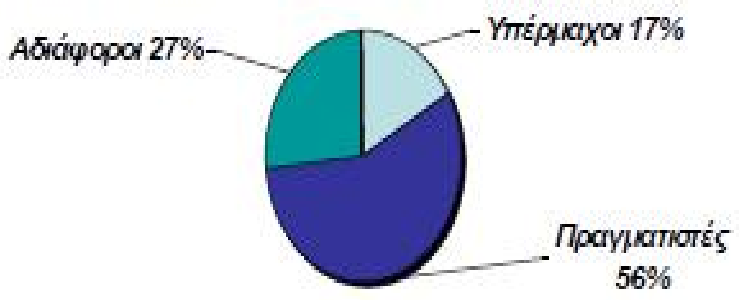
Αυτή η διαφορετική αντιμετώπιση της ιδιωτικότητας δημιούργησε αρκετά προβλήματα σε αμερικανικές επιχειρήσεις που θέλησαν να δραστηριοποιηθούν στην Ευρώπη, με αποτέλεσμα τη σύσταση το2000 ενός προαιρετικού καταλόγου αμερικανικών επιχειρήσεων (γνωστού και ως “Safe Harbor”) οι οποίες συμμετέχοντας σε αυτό τον κατάλογο έχουν εναρμονίσει τις λειτουργίες τους στα θέματα της ιδιωτικότητας με το ευρωπαϊκό περιβάλλον (Perkins and Markel 2004). Σε αυτή τη φάση της «ηλικιακής ωριμότητας» της έννοιας της ιδιωτικότητας, η τεχνολογία εξελίσσεται τόσο γρήγορα και βίαια που η προστασία της ιδιωτικότητας μόνο μέσω της νομικής οδού δεν επαρκεί αφού και χρονοβόρα είναι και συνήθως ακολουθεί αντί να προηγείται. Επομένως σε μία προσπάθεια να ανταποκριθεί στο πνεύμα των καιρών το νομοθετικό πλαίσιο αντί να δίνει γενικές οδηγίες και παρατηρήσεις, θα πρέπει να περιοριστεί σε πιο ειδικά και σύγχρονα (up-to-date) θέματα. Να επικεντρωθεί δηλαδή σε συγκεκριμένες παραβιάσεις της ιδιωτικότητας που απαιτούν πιο συγκεκριμένες και ουσιαστικές λύσεις.

1.2.4. Η ιδιωτικότητα στην εποχή της πληροφορίας

Στη σημερινή εποχή της πληροφορίας, ο όγκος των δεδομένων που καθημερινά

διακινείται μέσω του διαδικτύου είναι απλά ασύμμετρος. Σύμφωνα με τον Moor (1997) επειδή είναι σχεδόν αδύνατον να ελεγχθεί το σύνολο των πληροφοριών ενός ατόμου, στην σημερινή εποχή θα πρέπει να δημιουργηθούν ζώνες ιδιωτικότητας (zones of privacy), οι οποίες θα επιτρέπουν στα άτομα να ελέγχουν τα επίπεδα προσβασιμότητας στην ιδιωτική τους πληροφορία ανάλογα με τη συγκεκριμένη κατάσταση που βρίσκονται κάθε φορά. Επομένως η ιδιωτικότητα μπορεί να εκληφθεί ως μία σύνθεση από τη μία πλευρά της δυνατότητας ελέγχου της προσωπικής πληροφορίας και από την άλλη της περιορισμένης πρόσβασης σε αυτήν από άλλους.

Σύμφωνα με την έρευνα των Ackerman, Cranor and Reagle (1999) στις Η.Π.Α σε χρήστες του διαδικτύου οι καταναλωτές αν και γενικά δείχνουν υψηλό ενδιαφέρον και ανησυχούν για τα θέματα της ιδιωτικότητάς τους όταν έρχονται αντιμέτωποι με πραγματικές συνθήκες στο διαδίκτυο, η συμπεριφορά τους αλλάζει και γίνεται πιο πολύπλοκη. Οι καταναλωτές μπορούν να χωριστούν σε τρεις κατηγορίες:



i. οι υπέρμαχοι της ιδιωτικότητας (privacy fundamentalists): αποτελούν το17% των συμμετεχόντων στην έρευνα, ενδιαφέρονται πάρα πολύ για τα ιδιωτικά τους δεδομένα και είναι απρόθυμοι να ανταλλάξουν οποιαδήποτε ιδιωτική τους πληροφορία κάτω από οποιεσδήποτε συνθήκες.

ii. η πραγματιστική πλειοψηφία (pragmatic majority): αποτελούν την πλειοψηφία με 56%, έχουν ανησυχίες σχετικά με τα ιδιωτικά τους δεδομένα και είναι πρόθυμοι να δώσουν ορισμένες ιδιωτικές πληροφορίες για συγκεκριμένες καταστάσεις όταν βεβαιωθούν για την ύπαρξη μηχανισμών προστασίας των πληροφοριών που δίνουν. Οι χρήστες που αποτελούν την πραγματιστική πλειοψηφία μπορούν να χωριστούν σε δύο επιμέρους υποκατηγορίες:

α) τους χρήστες που είναι σκεπτικοί σχετικά με το να δώσουν ή όχι αυστηρά ιδιωτικά δεδομένα όπως όνομα, διεύθυνση, αριθμός πιστωτικής κάρτας και

β) τους χρήστες που προβληματίζονται περισσότερο για το αν θα δώσουν πληροφορίες σχετικά με τα χόμπι τους, τα ενδιαφέροντα τους, την υγεία τους.

iii. οι σχεδόν αδιάφοροι (marginally concerned): είναι το27% των συμμετεχόντων που δεν έχουν πρόβλημα να δώσουν ιδιωτικές τους πληροφορίες σχεδόν σε κάθε περίπτωση.

Το συμπέρασμα με τη μεγαλύτερη σημασία είναι ότι η ώριμη πλειοψηφία(73%) είναι ιδιαίτερα ανήσυχοι για θέματα που αφορούν τα ιδιωτικά τους δεδομένα στο διαδίκτυο. Επομένως σύμφωνα με τους Rhys and Shao (2007) ένα νέο μοντέλο προστασίας της ιδιωτικότητας είναι πλέον αναγκαίο στη σημερινή εποχή της πληροφορίας. Στο άρθρο αυτό υποστηρίζεται πως αντί να στηριζόμαστε αποκλειστικά στις νομικές διατάξεις να διαφυλάξουν την

ιδιωτικότητα των ατόμων ίσως η τεχνολογία μπορεί να δώσει τη λύση: οι κατάλληλες τεχνολογικές εφαρμογές που μπορούν να δώσουν στα άτομα τον πλήρη έλεγχο των ιδιωτικών τους πληροφοριών, και επομένως να τους επιτρέψουν να προστατεύουν τα ιδιωτικά τους στοιχεία στο βαθμό που εκείνοι επιθυμούν, δίνοντας τους τη δυνατότητα να απελευθερώσουν την συγκεκριμένη πληροφορία που θέλουν, όποτε εκείνοι θέλουν, για όποιο λόγο θέλουν ανά περίπτωση.

1.3.Τρόποι προστασίας της ιδιωτικότητας στο διαδίκτυο

Υπάρχουν τρεις κύριοι λογικοί τρόποι με τους οποίους σήμερα μπορεί να προστατευτεί η ιδιωτικότητα των χρηστών στο διαδίκτυο σύμφωνα με την Cranor (1999):

1. να μην ζητείται από τους ιστότοπους οι χρήστες να παρέχουν καμία ιδιωτική πληροφορία
2. η πηγή από την οποία προέρχονται τα ιδιωτικά δεδομένα να είναι κρυμμένη, επομένως να διατηρείται η ανωνυμία των χρηστών
3. οι πολιτικές ιδιωτικότητας των ιστοτόπων που υπόσχονται την υπεύθυνη και ορθή διαχείριση των ιδιωτικών δεδομένων.

1.3.1. Πολιτικές Ιδιωτικότητας (Privacy Policies)

Οι πολιτικές ιδιωτικότητας που αναγράφουν οι ιστότοποι στην αρχική τους σελίδα αποτελούν στην ουσία ένα είδος υπόσχεσης της διαδικτυακής εταιρείας να επεξεργαστεί τα ιδιωτικά δεδομένα των χρηστών της με έναν συγκεκριμένο τρόπο. Θεωρείται σαν ένα είδους συμβολαίου που επισυνάπτεται μεταξύ των επισκεπτών της ιστοσελίδας και της εταιρείας που πρέπει να τηρείται από τις δύο

πλευρές. Αποτελεί το πιο διαδεδομένο τρόπο προστασίας της ιδιωτικότητας των χρηστών και όλο και πιο συχνά στη δήλωση της πολιτικής ιδιωτικότητας των εταιρειών περιλαμβάνονται προτάσεις που αναφέρονται στο τρόπο συλλογής των ιδιωτικών δεδομένων, στη μη χρησιμοποίηση των δεδομένων αυτών για άλλους σκοπούς εκτός της παρούσας συναλλαγής και στη μη παροχή των δεδομένων αυτών προς τρίτα μέρη. Αν και οι προτάσεις αυτές κινούνται προς τη σωστή κατεύθυνση εντούτοις οι πολιτικές ιδιωτικότητας εμφανίζουν σημαντικά μειονεκτήματα (Pollach 2007):

- Ο χρήστης πρέπει να διαβάσει ολόκληρη την πολιτική ιδιωτικότητας του ιστότοπου πριν αποφασίσει να δώσει κάποιο μέρος των ιδιωτικών δεδομένων του, να σκεφτεί αν είναι ικανοποιημένος με όσα αναγράφονται και μετά να αποφασίσει αν συμφωνεί ή όχι. Μετά από αυτή τη συνήθως κοπιαστική διαδικασία σε περίπτωση διαφωνίας θα πρέπει να επικοινωνήσει και να διαπραγματευτεί με τη διαδικτυακή επιχείρηση, διαδικασία ιδιαιτέρως επίπονη αφού δεν υπάρχουν έτοιμες φόρμες οπότε ο χρήστης θα πρέπει να αναλάβει τη διαδικασία να την κάνει είτε από μόνος του είτε μέσω αποστολής σύντομου μηνύματος (email) είτε μέσω κάποιου τηλεφώνου είτε μέσω κάποιου άλλου μέσου.
- Η πολιτική ιδιωτικότητας μιας επιχείρησης μπορεί να αλλάξει ανά πάσα στιγμή. Κάθε νέα αλλαγή μπορεί να αναφέρεται σε ιδιωτικές πληροφορίες που έχουν ήδη συλλεχθεί από κάποια προηγούμενη έκδοση της πολιτικής ιδιωτικότητας που πιθανόν να πρόσφερε επιπλέον προστασία. Επίσης δεν υπάρχει κάποιος αυτόματος μηχανισμός ή πρωτόκολλο που να ενημερώνει διαρκώς το χρήστη για τις αλλαγές στις πολιτικές ιδιωτικότητας των διαδικτυακών επιχειρήσεων.
- Κανένας φυσικός ή τεχνικός(ηλεκτρονικός) μηχανισμός δεν μπορεί να επιβλέπει, να ελέγχει και το κυριότερο να προλαμβάνει

τη μη τήρηση των όσων αναφέρονται στην πολιτική ιδιωτικότητας της επιχείρησης. Σε περίπτωση που κάποια επιχείρηση ενεργήσει αντίθετα με τα όσα προβλέπει στην πολιτική ιδιωτικότητά της θα πρέπει ο χρήστης να το εντοπίσει από μόνος του και έπειτα να λάβει νομικά μέτρα ώστε να αποζημιωθεί από τη μη τήρηση εκ μέρους της επιχείρησης των δηλώσεων προστασίας των ιδιωτικών του δεδομένων. Όμως στην πράξη είναι σχεδόν αδύνατο ο απλός χρήστης να έχει τη δυνατότητα να εποπτεύει το τι πραγματικά συμβαίνει με τα ιδιωτικά του δεδομένα και πώς αυτά διαχειρίζονται από τις επιχειρήσεις. Επομένως η τήρηση ή μη της πολιτικής ιδιωτικότητας επαφίεται στην αυτορύθμιση των ίδιων των εταιρειών και στο βαθμό εμπιστοσύνης και αξιοπιστίας που καλλιεργούν στους χρήστες/πελάτες τους.

1.3.2.Τεχνολογικές εφαρμογές

Στην παρούσα ενότητα θα αναφέρουμε τις τεχνολογικές εφαρμογές που έχουν
χρησιμοποιηθεί κατά καιρούς για την προστασία των θεμάτων της ιδιωτικότητας στο διαδίκτυο (σύμφωνα με το άρθρο των Rhys and Shao, 2007). Κοινό χαρακτηριστικό όλων είναι ότι σχεδιάστηκαν με σκοπό την προστασία των δεδομένων και όχι με σκοπό την ολική εποπτεία και διαχείριση τους από τον πελάτη. Οι τεχνολογικές αυτές εφαρμογές μπορούν να διακριθούν σε δύο βασικές κατηγορίες:

α) στις τεχνολογίες ανωνυμίας ή ψευδωνυμίας και

β) στις ονομαστικές τεχνολογίες. Οι μεν πρώτες προσπαθούν να αποκρύψουν την πραγματική ταυτότητα του χρήστη και συνεπώς έχουν ως στόχο την όποια ιδιωτική πληροφορία διακινείται στο

διαδίκτυο να μην μπορούν οι ιστότοποι να την συνδέσουν με την πραγματική υπόσταση ενός ατόμου. Στον πίνακα 1.1 παραθέτουμε τις κυριότερες τεχνολογίες ανωνυμίας ή ψευδωνυμίας.

Technology	*Architecture*			*Usable*	*Application areas*		
	T3P	*3P*	*De*		*E-mail*	*Web*	*Other*
Anonymous techniques							
Anonymous e-mail	X			X	X		
"Anonymizer"	X			X		X	
"Crowds"			X	X		X	
Simple Chaum mix	X			X	X		
Network of Chaum mixes			X	X	X		
"Onion Routing"			X	X		X	X
Credential systems (CS)							
Chaum's CS	X			X		X	
Damgυård's CS		X				X	
Chen's CS	X			X		X	
Lysyanskaya et al.'s CS	X					X	
Camenisch et al.'s CS	X			X		X	
"Idemix"	X			X		X	
Database privacy							
Query restriction	X			X			
Data perturbation	X			X			
Output perturbation	X			X			

Key: T3P = Trusted third party
3P = Third party
De = Decentralized

Οι δε δεύτερες βοηθούν τους χρήστες να διατηρήσουν και να προστατεύσουν

κάποιες από τις ιδιωτικές τους πληροφορίες που δεν είναι αναγκαίες για τις συναλλαγές τους και επίσης παρέχουν εργαλεία αξιολόγησης για το ποιοι ιστότοποι μπορούν να εμπιστευτούν οι καταναλωτές σε μικρότερο ή μεγαλύτερο βαθμό. Συμπερασματικά αναφέρουμε ότι το πρωτόκολλο P3P (platform for privacy preferences) που επιτρέπει στο

χρήστη να εκφράσει την προτίμησή του για συγκεκριμένες πολιτικές ιδιωτικότητας εμφανίζει τη μεγαλύτερη διάδοση έχοντας ευρείας κλίμακας εφαρμογή ενώ και οι ασπίδες ιδιωτικότητας (privacy seals) που έχουν υιοθετήσει μερικοί ιστότοποι βοηθούν το χρήστη να γνωρίζει εποπτικά αν ένας ιστότοπος ενεργεί σοβαρά και υπεύθυνα ως προς την προστασία των ιδιωτικών δεδομένων των χρηστών του. Στον πίνακα 1.2 που ακολουθεί παραθέτουμε τις κυριότερες ονομαστικές τεχνολογίες.

Πίνακας 1.2. Ονομαστικές τεχνολογίες

Technology	*Privacy philosophy*		*T3P*	*Applicable to e-commerce*
	Helper	*Enforcement*		
TRUSTe	X		X	X
PS	X			X
P3P	X		X	X
E-P3P		X	X	X
ESM's		X		X
ROBM's		X	X	
SS's		X		X

Key: T3P = Trusted third party

1.4. Ιδιωτικότητα και ηλεκτρονικό εμπόριο

Στο πεδίο του ηλεκτρονικού εμπορίου οι καταναλωτές και οι επιχειρήσεις ανταλλάσουν μηνύματα επικοινωνίας, απόδοσης και ποιότητας των προϊόντων και των παρεχόμενων υπηρεσιών μέσω των ηλεκτρονικών μέσων. Οι συναλλαγές στο διαδίκτυο συνήθως απαιτούν την απελευθέρωση από την πλευρά του καταναλωτή μεγάλης ποσότητας ιδιωτικών πληροφοριών που είτε είναι απαραίτητη για την πραγματοποίηση της συναλλαγής (πιστωτική κάρτα, διεύθυνση,

ονοματεπώνυμο) είτε είναι επιθυμητή είτε πολλές αναγκαία από τις επιχειρήσεις με σκοπό την ανάλυση της συμπεριφοράς των πελατών, την καταγραφή νέων αναγκών και επιθυμιών που οδηγούν σε αύξηση της απόδοσης και των ικανοτήτων της επιχείρησης προς όφελος του τελικού καταναλωτή.

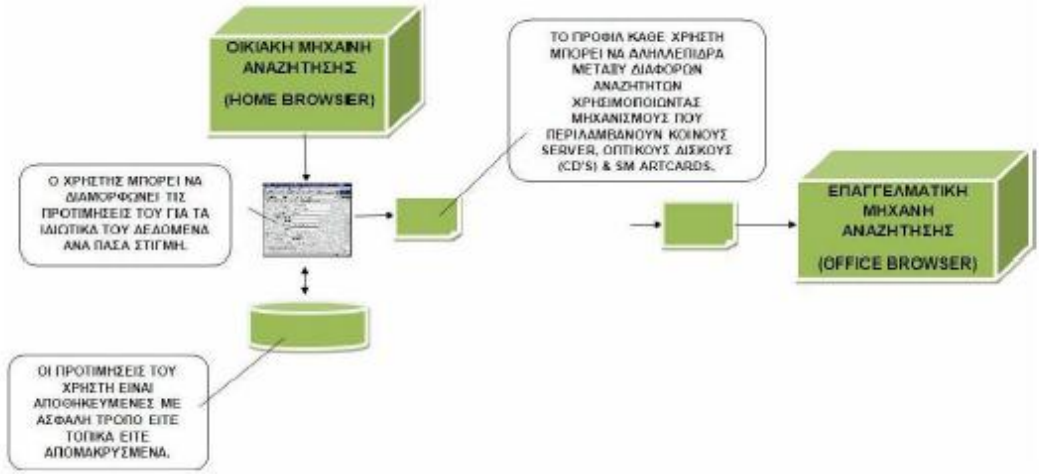
Τις περισσότερες φορές όμως είτε γιατί οι καταναλωτές δεν γνωρίζουν οι ίδιοι είτε γιατί δεν ενημερώνονται από τις ίδιες τις επιχειρήσεις που συναλλάσσονται δεν έχουν καμία πληροφορία για τη διαχείριση των ιδιωτικών τους δεδομένων από τη στιγμή που θα απελευθερωθούν στο διαδίκτυο. Μη γνωρίζοντας πού καταλήγουν και πώς χρησιμοποιούνται στη συνέχεια αυτά τα δεδομένα οι καταναλωτές αρχίζουν να αντιδρούν για ορισμένες συμπεριφορές και πρακτικές που έχουν παρατηρηθεί από την πλευρά των επιχειρήσεων. Φαινόμενα όπως η στρατηγική «διαφορισμού της τιμής» ανά τύπο και προφίλ καταναλωτή που χρησιμοποιείται από μερικούς ιστότοπους στο διαδίκτυο, η αποστολή ανεπιθύμητων σύντομων ηλεκτρονικών μηνυμάτων (e-mail) από τρίτα μέρη χωρίς να υπήρχε καμία προηγούμενη επαφή ή γνώση του καταναλωτή, η παρακολούθηση της διαδικτυακής (online) συμπεριφοράς των χρηστών διαδικτύου χωρίς οι ίδιοι να το γνωρίζουν έχουν ξεσηκώσει θύελλα αντιδράσεων από την πλειονότητα των καταναλωτών. Παρατηρούμε δηλαδή μία σύγκρουση μεταξύ της προστασίας των ιδιωτικών δεδομένων και γενικότερα της ιδιωτικότητας των καταναλωτών με την προσπάθεια απόκτησης των πληροφοριών αυτών από τις επιχειρήσεις, που λογικά επιθυμούν να τις κατέχουν για να βελτιώσουν τις λειτουργίες τους και να ανταποκριθούν στις απαιτήσεις των καταναλωτών. Η μέχρι τώρα πρακτική για να αντιμετωπιστεί η παραπάνω σύγκρουση ήταν ένας συμβιβασμός μεταξύ των αντικρουόμενων μερών, μία λεπτή ισορροπία που όμως

δεν επιλύει το πρόβλημα αλλά μάλλον το παρατείνει ή ακόμα και το μεγενθύνει. Η απάντηση
στην παραπάνω σύγκρουση μπορεί να προέρχεται από την υιοθέτηση μιας πελατοκεντρικής πολιτικής ιδιωτικότητας στο ηλεκτρονικό εμπόριο σύμφωνα με τους Rhys and Shao (2007). Αυτό σημαίνει ότι θα πρέπει να δοθεί η δυνατότητα σε κάθε άτομο να διατηρεί το μέγιστο δυνατό μέρος των ιδιωτικών του δεδομένων και να ελέγχει όσο είναι δυνατόν αυτή την πληροφορία ώστε να μπορεί να τη διαχειρίζεται ανά περίσταση. Μία πολιτική ιδιωτικότητας εστιασμένη στον πελάτη μπορεί να έχει θετικές συνέπειες τόσο για τον πελάτη όσο και για τις επιχειρήσεις σύμφωνα με τους παραπάνω συγγραφείς.

Από την πλευρά του πελάτη η μεγέθυνση του ελέγχου των θεμάτων της ιδιωτικότητάς του εκτός από τις θετικές επιπτώσεις στη ψυχολογία του, θα του προσφέρει και σημαντικά οικονομικά οφέλη:

1. Οι πελάτες θα θελήσουν να αποκτήσουν οφέλη από την κατοχή και τον έλεγχο των ιδιωτικών τους πληροφοριών που πλέον δεν θα κυκλοφορούν ελεύθερα στο διαδίκτυο και είναι πολύτιμες για τις επιχειρήσεις. Επομένως θα αυξηθεί η διαπραγματευτική ικανότητα των πελατών στις οικονομικές τους συναλλαγές με τις επιχειρήσεις επιτυγχάνοντας μεγαλύτερα απτά οικονομικά οφέλη (μειωμένες τιμές, προσφορές, εκπτώσεις και άλλα)
2. Εφόσον τα θέματα της ιδιωτικότητάς του θα ελέγχονται από τον ίδιο, ο πελάτης θα μπορεί πλέον να αισθάνεται πιο ασφαλής και σίγουρος για τις συναλλαγές του. Επομένως ολοένα και περισσότεροι καταναλωτές που μέχρι τώρα αντιμετώπιζαν κριτικά το διαδίκτυο θα νιώσουν πιο άνετα και θα θελήσουν να λάβουν μέρος στον κόσμο του ηλεκτρονικού εμπορίου. Οι ακόμα περισσότεροι πελάτες που μαζικά θα θελήσουν να κάνουν ηλεκτρονικές

συναλλαγές θα μεγαλώσουν σε τέτοιο ικανοποιητικό βαθμό την αγορά που θα οδηγήσει σε αύξηση του ανταγωνισμού από τις υπάρχουσες επιχειρήσεις αλλά και στην προσέλκυση πολλών νέων επιχειρήσεων να δραστηριοποιηθούν στο διαδίκτυο. Ο ολοένα και αυξανόμενος ανταγωνισμός θα επιφέρει μείωση των τιμών προς όφελος πάλι του καταναλωτή.



Στο σχήμα που παρατίθεται παραπάνω φαίνεται εποπτικά πως θα μπορούσε ο χρήστης να κατασκευάσει το δικό του διαδικτυακό προφίλ και πώς θα επιθυμούσε να χρησιμοποιούνται οι ιδιωτικές του πληροφορίες.

Από την πλευρά των επιχειρήσεων τα προσδοκώμενα οικονομικά οφέλη είναι επίσης σημαντικά. Παρόλο που πολλοί υποστηρίζουν ότι η έλλειψη του ελέγχου των ιδιωτικών στοιχείων των πελατών θα έχει αρνητικά αποτελέσματα για τις επιχειρήσεις με μία πιο προσεχτική ανάλυση της πελατοκεντρικής πολιτικής ιδιωτικότητας καταλήγουμε στα εξής οφέλη που φαίνεται να προκύπτουν για τις επιχειρήσεις:

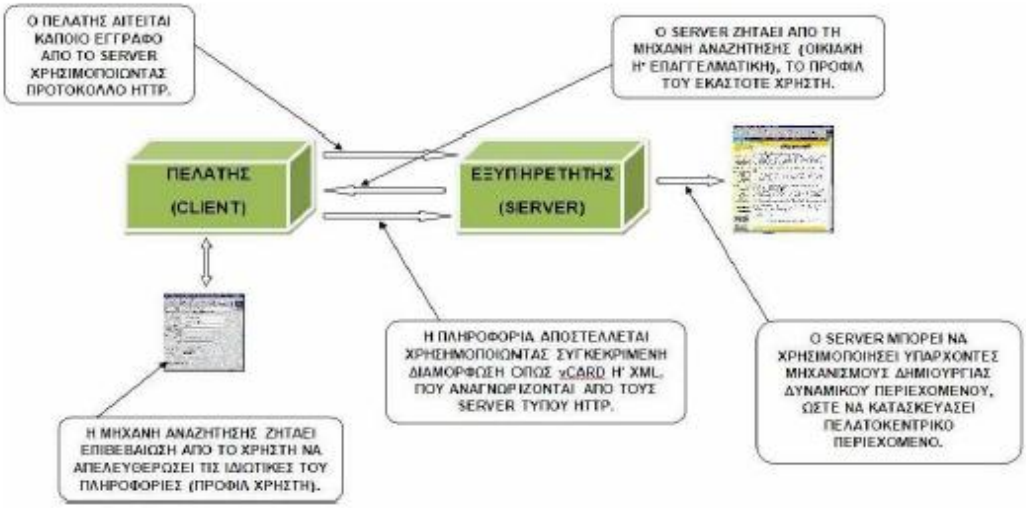
1. Η προσέλκυση πολλών νέων πελατών που μέχρι τώρα ήθελαν αλλά αμφισβητούσαν την αξιοπιστία των επιχειρήσεων να διαχειριστούν

σωστά τα ιδιωτικά τους δεδομένα θα έχει ως αποτέλεσμα την κατακόρυφη ανάπτυξη των πωλήσεων οπότε εκτός των μεγάλων κερδών και την αθρόα εισροή μετρητών (cold hard cash) στις επιχειρήσεις. Η εισροή λοιπόν μετρητών θα βοηθήσει οικονομικά τις επιχειρήσεις που κατά μέσο όρο μέχρι τώρα δεν καταγράφουν ιδιαίτερα υψηλό ποσοστό κερδών και πωλήσεων στο διαδίκτυο. Επίσης η ανάπτυξη της αγοράς θα μεγαλώσει και τον όγκο των κεφαλαίων που διακινούνται ή/και επενδύονται στο χώρο του ηλεκτρονικού εμπορίου προς όφελος των επιχειρήσεων.

2. Η δυνατότητα ελέγχου των θεμάτων της ιδιωτικότητας από κάθε πελάτη ατομικά, δηλαδή η εξατομικευμένη συναλλαγή κάνει πιο εύκολη την ανάπτυξη του σχεσιακού μάρκετινγκ από την πλευρά των επιχειρήσεων που μπορεί να φέρει πιστούς πελάτες και επαναλαμβανόμενες αγορές άρα επιπλέον κέρδη για τις επιχειρήσεις.

3. Η μετακύληση της διαχείρισης και του ελέγχου των προσωπικών δεδομένων από τις επιχειρήσεις στους πελάτες θα επιφέρει μείωση του κόστους των επιχειρήσεων οι οποίες δεν θα είναι αναγκασμένες να δαπανούν τεράστια ποσά για την υποστήριξη των λειτουργιών αυτών που αφορούν την ιδιωτικότητα.

Στο σχήμα1.3 που ακολουθεί παρατίθεται ο τρόπος που θα αλληλεπιδρά αυτό το προφίλ κάθε χρήστη με κάθε έναν από τους ιστότοπους που θα επισκέπτεται κάθε φορά. Τα σχήματα 2 και 3 έχουν συμπεριληφθεί κυρίως για εποπτικό– περιγραφικό ρόλο ώστε να αναλυθεί πλήρως η προσέγγιση που προτείνεται από τους Rhys and Shao (2007) και να παρουσιαστεί πώς θα μπορούσαν οι παραπάνω προτάσεις να εφαρμοστούν στην πράξη.



Όπως προκύπτει από την παραπάνω ανάλυση τα οικονομικά οφέλη μιας πελατοκεντρικής πολιτικής ιδιωτικότητας είναι εξίσου σημαντικά τόσο για τις επιχειρήσεις όσο και για τους πελάτες. Η πρόκληση λοιπόν είναι να καταφέρει η τεχνολογία να δημιουργήσει ειδικές εφαρμογές, απλές στη χρήση, φιλικές προς τον χρήστη-άνθρωπο και αποδεκτές από όλους που να δώσει τη δυνατότητα στους πολίτες να ρυθμίζουν οι ίδιοι τα θέματα ιδιωτικότητας τους. Βέβαια η παραπάνω προσέγγιση για το θέμα της ιδιωτικότητας στο διαδίκτυο αποτελεί μία περισσότερο θεωρητική προσέγγιση η οποία αν και ιδανική είναι αρκετά δύσκολο να εφαρμοστεί και να υλοποιηθεί, τουλάχιστον σήμερα. Αποτελεί όμως μία σημαντική καινοτομική θεωρητική προσέγγιση που βοηθά σημαντικά στο να καταλάβουν οι χρήστες περισσότερες πτυχές του θέματος της ιδιωτικότητας στο διαδίκτυο και να έχουν μια πιο ολοκληρωμένη άποψη για το τι συμβαίνει με τα ιδιωτικά τους δεδομένα. Επίσης η παραπάνω προσέγγιση εμφανίζει ορισμένα χαρακτηριστικά που έχουν μελετηθεί και στις έρευνες που θα αναφερθούν παρακάτω και επομένως προσφέρει μία εξαιρετική σύνδεση μεταξύ θεωρητικού πλαισίου και ερευνητικών προσεγγίσεων για την ιδιωτικότητα.

1.5. Ερευνητικές προσεγγίσεις για την ιδιωτικότητα

Αρκετές έρευνες έχουν πραγματοποιηθεί ώστε να διαπιστωθεί πως συμπεριφέρονται οι χρήστες του διαδικτύου ως προς τα ιδιωτικά τους δεδομένα όταν επισκέπτονται κάποιον ιστότοπο. Στον παρακάτω πίνακα παραθέτουμε τις σημαντικότερες έρευνες που έχουν διεξαχθεί και που αναφέρονται κυρίως στην ανησυχία των χρηστών για τα ιδιωτικά τους δεδομένα (προσαρμοσμένες από την έρευνα των Slyke , Shim, Johnson ,Jiang 2006).

Έρευνα	Θέμα	Ευρήματα
Hoffman et al. (1999)	Δυνατότητα ελέγχου Άλλη χρήση / χρήση από τρίτους των ιδιωτικών δεδομένων των χρηστών	Οι καταναλωτές δίνουν όλο και λιγότερες ιδιωτικές πληροφορίες σε ιστότοπους που δεν εμπιστεύονται
Phelps et al. (2000)	Άλλη χρήση / χρήση από τρίτους	Οι ανησυχίες των χρηστών για τη χρήση των ιδιωτικών τους δεδομένων για άλλους σκοπούς από αυτούς που τα έδωσαν μειώνει την πρόθεση των χρηστών να χρησιμοποιήσουν ιστότοπους για αγορές
Milne (2000)	Άλλη χρήση / χρήση από τρίτους	Οι ανησυχίες των χρηστών για τη χρήση των ιδιωτικών τους δεδομένων για άλλους σκοπούς από αυτούς που τα έδωσαν μειώνει την πρόθεση των χρηστών να χρησιμοποιήσουν ιστότοπους για αγορές
Kovar et al. (2000α)	Ιδιωτικά δεδομένα	Η δυνατότητα χρήσης ασπίδων ιδιωτικότητας από τους χρήστες δημιουργεί αυξημένες προσδοκίες για την ποιότητα των προϊόντων και υπηρεσιών που προσφέρει ένας ιστότοπος
Kovar et al. (2000β)	Ιδιωτικά δεδομένα	Η δυνατότητα χρήσης ασπίδων ιδιωτικότητας από τους χρήστες δημιουργεί προσδοκίες για θετική μελλοντική συμπεριφορά των ιστοτόπων στο θέμα της ιδιωτικότητας
Kimery & McCord (2002)	Ιδιωτικά δεδομένα	Οι ασπίδες ιδιωτικότητας (πχ TRUSTe, BBB,) δεν αυξάνουν την εμπιστοσύνη ή την πρόθεση των χρηστών να πραγματοποιήσουν αγορές από έναν ιστότοπο

Έρευνα	*Θέμα*	*Ευρήματα*
Miyazaki & Krishnamurthy (2002)	*Ιδιωτικά δεδομένα*	*Η χρήση των ασπίδων ιδιωτικότητας ενθαρρύνει το χρήστη να δώσει ιδιωτικά του δεδομένα και αυξάνει την πρόθεσή του να πραγματοποιήσει συναλλαγές σε έναν ιστότοπο όταν ο αντιλαμβανόμενος κίνδυνος είναι μεγάλος*
Malhotra et al (2004)	*Το ενδιαφέρον / ανησυχία των χρηστών διαδικτύου για τα ιδιωτικά τους δεδομένα*	*Η ανησυχία των χρηστών για τα ιδιωτικά τους δεδομένα είναι συσχετισμένη με λιγότερη εμπιστοσύνη και μεγαλύτερο κίνδυνο όταν οι χρήστες παρέχουν πληροφορίες για να κερδίσουν μία δωρεάν συνδρομή σε έναν ιστότοπο*
Earp, Antón, Aiman-Smith and Stuffledeam (2005)	*Οι πολιτικές ιδιωτικότητας σε σχέση με τα ενδιαφέροντα των χρηστών για τα ιδιωτικά τους δεδομένα*	*Οι υπάρχουσες πολιτικές ιδιωτικές δεν εκφράζουν τα πραγματικά ενδιαφέροντα των χρηστών για τα ιδιωτικά τους δεδομένα (αλλαγή περιεχομένου, γλώσσας γραφής και τρόπου παρουσίασης)*
Slyke , Shim, Johnson, Jiang (2006)	*Το ενδιαφέρον / ανησυχία των χρηστών διαδικτύου για τα ιδιωτικά τους δεδομένα και η πρόθεση αγοράς μέσω του διαδικτύου*	*Η ανησυχία των χρηστών διαδικτύου για τα ιδιωτικά τους δεδομένα επηρεάζει την πρόθεση τους να πραγματοποιήσουν συναλλαγές με έναν ιστότοπο κάτω από συγκεκριμένες προϋποθέσεις*
Tamara, Hart (2006)	*Το ενδιαφέρον / ανησυχία των χρηστών διαδικτύου για τα ιδιωτικά τους δεδομένα & η πρόθεσή τους να τα δώσουν για να πραγματοποιήσουν συναλλαγές*	*Το ενδιαφέρον των χρηστών για τα ιδιωτικά τους δεδομένα επηρεάζει αρνητικά την πρόθεσή τους να τα δώσουν για να κάνουν συναλλαγές στο διαδίκτυο ενώ η ανάπτυξη εμπιστοσύνης των χρηστών απέναντι σε έναν ιστότοπο επηρεάζει θετικά την πρόθεσή τους να δώσουν ιδιωτικά τους δεδομένα για να κάνουν συναλλαγές στο διαδίκτυο*
Van Dyke, Midhal and Nemati (2007)	*Η επίδραση της δυνατότητας ελέγχου της ιδιωτικότητας από τους ίδιους τους χρήστες στην εμπιστοσύνη και στο ενδιαφέρον των χρηστών για τα ιδιωτικά τους δεδομένα*	*Ο αντιλαμβανόμενος έλεγχος των χρηστών για τα ιδιωτικά τους δεδομένα επηρεάζει θετικά την ανάπτυξη εμπιστοσύνης για τον ιστότοπο και αρνητικά το ενδιαφέρον / ανησυχία των χρηστών για τα ιδιωτικά τους δεδομένα*

Η ανησυχία των χρηστών διαδικτύου για τα ιδιωτικά τους δεδομένα θεωρείται ως σημαντικό εμπόδιο στην υιοθέτηση του

ηλεκτρονικού εμπορίου (και ειδικότερα του B2C ηλεκτρονικού εμπορίου μεταξύ επιχειρήσεων και καταναλωτών) από μεγάλο αριθμό καταναλωτών(Hoffman et al., 1999, Sullivan, 2005). Όμως μερικά ευρήματα από έρευνες που έχουν διεξαχθεί στο θέμα της ανησυχίας των χρηστών για τα ιδιωτικά τους δεδομένα δεν είναι ξεκάθαρα. Άλλες έρευνες, όπως των Miyazaki and Krishnamurthy (2002), κατέληξαν πως οι μηχανισμοί που έχουν σχεδιαστεί για να παρέχουν προστασία στα ιδιωτικά δεδομένα του χρήστη όπως οι ασπίδες ιδιωτικότητας (privacy seals) ή οι πολιτικές ιδιωτικότητας (privacy policies) ενισχύουν θετικά την πρόθεση του χρήστη να πραγματοποιήσει συναλλαγές μέσω του διαδικτύου. Από την άλλη πλευρά, έρευνες όπως των Kimery and McCord (2002) υποστηρίζουν πως αυτοί οι μηχανισμοί δεν έχουν καμία σημαντική επίδραση στην πρόθεση των χρηστών να χρησιμοποιήσουν το διαδίκτυο για να πραγματοποιήσουν συναλλαγές.

Επίσης έρευνα των Hoffman et al.,(1999) καταλήγει πως η ανησυχία των χρηστών για τα ιδιωτικά τους δεδομένα μπορεί κάτω από προϋποθέσεις να επηρεάζει και τη πρόθεση χρήσης του διαδικτύου για συναλλαγές αλλά και την εμπιστοσύνη των χρηστών απέναντι στους ιστότοπους. Σχετικές έρευνες έχουν αποδείξει πως η εμπιστοσύνη των χρηστών απέναντι σε έναν ιστότοπο παίζει σημαντικό ρόλο στη πρόθεση χρήσης του διαδικτύου για συναλλαγές(Cheung and Lee 2001, Lee and Turban 2001).

Μία ακόμα ενδιαφέρουσα παράμετρος της έννοιας της ιδιωτικότητας στο διαδίκτυο είναι και ο αντιλαμβανόμενος έλεγχος των ίδιων των χρηστών πάνω στα ιδιωτικά τους δεδομένα. Σύμφωνα με έρευνα των Van Dyke, MidhaI and Nemati (2007), η δυνατότητα των χρηστών για εποπτεία, πρόσβαση και επιλογή στα ιδιωτικά τους δεδομένα επηρεάζει και την εμπιστοσύνη των χρηστών απέναντι στους

ιστότοπους αλλά και την πρόθεση χρήσης του διαδικτύου για πραγματοποίηση συναλλαγών.

Επομένως θα πρέπει να μελετήσουμε αν η ανησυχία των χρηστών για τα ιδιωτικά τους δεδομένα και ο αντιλαμβανόμενος έλεγχος των χρηστών σε αυτά έχουν άμεση και ξεκάθαρη επίδραση στην πρόθεση χρήσης του διαδικτύου για την πραγματοποίηση συναλλαγών. Ή, σε αντιδιαστολή, αν η ανησυχία των χρηστών και το αντιλαμβανόμενο εύρος ελέγχου επηρεάζουν έμμεσα τη πρόθεση χρήσης του διαδικτύου μέσω άλλων παραγόντων όπως της εμπιστοσύνης απέναντι στους ιστότοπους.

Κεφάλαιο 2.

2.1. Ιδιωτικότητα και ασφάλεια πληροφορίας.

Η πολυπλοκότητα της συλλογής, ταξινόμησης, συμπλήρωσης και πρόσβασης των πληροφοριών χειρονακτικά από αρκετές, διαφορετικές υπηρεσίες ήταν, σε πολλές περιπτώσεις, μια ενσωματωμένη προστασία από κακή χρήση ιδιωτικών πληροφοριών. Ήταν απλώς πολύ ακριβό, μπερδεμένο και περίπλοκο να σπάσει το απόρρητο.

Τα πράγματα έχουν αλλάξει. Η συγκέντρωση τεράστιων ποσοτήτων ηλεκτρονικής πληροφορίας για τους πολίτες από τις κυβερνήσεις, τους πιστωτικούς οργανισμούς και τις ιδιωτικές εταιρείες, συνδυασμένα με την ικανότητα των υπολογιστών να εξετάζουν, να επεξεργάζονται και να συνδυάζουν μεγάλες ποσότητες πληροφορίας για πολίτες έχουν δημιουργήσει μια σημαντική απειλή για την προσωπική ιδιωτικότητα. Η πιθανότητα όλη αυτή η πληροφορία και η τεχνολογία να συνδυαστούν έχει κάνει την εμφάνιση της σαν φάντασμα της σύγχρονης πληροφοριακής εποχής. Αυτό πολλές φορές αναφέρεται σαν φαινόμενο “Big Brother”.

Ωστόσο θα ήταν νομίζω σημαντική παράλειψη να μην αναφερθεί και η άλλη πλευρά του νομίσματος εδώ. Η εσωτερική ισχύς σε συστήματα που μπορούν να προσπελάσουν τεράστιες ποσότητες δεδομένων μπορεί να χρησιμοποιηθεί για το κοινωνικό καλό, και αυτό πράγματι γίνεται κάποιες φορές. Για παράδειγμα , ταιριάζοντας εγγραφές με την βοήθεια ενός υπολογιστή, είναι δυνατό να μειωθεί η απάτη, η κυβερνητική κακοδιαχείριση (πολλές φορές για να καλυφθεί άλλη κυβερνητική κακοδιαχείριση, αλλά τώρα ξεφεύγουμε από το θέμα μας), η αποφυγή καταβολής φόρων, η απάτες στην κοινωνική πρόνοια, οι κλέφτες οικογενειακών επιδομάτων, η παράνομη απασχόληση κ.λ.π. Η ερώτηση

είναι: Ποιο τίμημα πρέπει να πληρώσει κάποιος για την απώλεια του απορρήτου, έτσι ώστε το κράτος να μπορεί να βρίσκει καλύτερα τους παράνομους;

Μια έρευνα στην Αμερική έδειξε ότι το 5% των υπαλλήλων ενός παραρτήματος της εφορίας είχαν ψάξει τα εφοριακά στοιχεία φίλων, συγγενών και διασημοτήτων. Μερικοί από αυτούς τους υπαλλήλους χρησιμοποίησαν αυτές τις πληροφορίες για να δημιουργήσουν πλαστές επιστροφές φόρων, αλλά οι περισσότεροι το έκαναν απλά από περιέργεια. (Μια τέτοια έρευνα θα έπρεπε να γίνει και στον δικό μας τόπο. Είμαι σίγουρος ότι τα αποτελέσματα θα είναι άκρως ενδιαφέροντα).

Όπως και με τις μεγαλύτερες αρχές που διέπουν την ανθρωπότητα, οι άνθρωποι έχουν διαφορετικούς ορισμούς για την λέξη ιδιωτικότητα. Το λεξικό Merriam-Webster χρονολογεί την λέξη πίσω στον $15^{ο}$ αιώνα και την ορίζει σαν “την κατάσταση του να βρίσκεται κανείς ξέχωρα από συντροφιά ή παρατήρηση” και “ελευθερία από μη εξουσιοδοτημένη εισβολή”.

Το 1890, οι Samuel Warren και Louis Brandeis σε ένα άρθρο τους στο *Harvard Law Review*, αναφέρουν ότι θα πρέπει να υπάρχει δικαίωμα στην ιδιωτικότητα, και αυτό το δικαίωμα θα πρέπει “να προστατεύει αυτά τα άτομα των οποίων η κοινότητα δεν έχει κανένα νόμιμο ενδιαφέρον στις υποθέσεις τους, από το να διασυρθούν σε μια ανεπιθύμητη και δυσάρεστη δημοσιότητα” και “να προστατεύει όλα τα άτομα ανεξάρτητα από την θέση τους, από την δημοσιοποίηση υποθέσεων ενάντια στην θέληση τους, που θα προτιμούσαν να κρατήσουν ιδιωτικές.”

Πρέπει να τονιστεί ότι οι Warren και Brandeis έγραψαν πως “η αλήθεια της δημοσιοποιημένης πληροφορίας δεν αποτελεί υπεράσπιση για την πράξη ” Υποστήριξαν ότι η ιδιωτικότητα ενός ατόμου παραβιάζεται από

την απεικόνιση της ιδιωτικής του ζωής άσχετα αν αυτή η απεικόνιση είναι ακριβής ή όχι. Τέλος, έγραψαν ότι: "Η απουσία 'δόλου' από αυτόν που κάνει την δημοσιοποίηση, δεν αποτελεί υπεράσπιση για την πράξη του." Αν και η σχετική με την ιδιωτικότητα Αμερικάνικη νομοθεσία βασίζεται κύρια σε αυτό το άρθρο, οι Warren και Brandeis δεν δημιούργησαν μια βάση που να επεκτείνεται στην εποχή της πληροφορικής (πως θα μπορούσαν άλλωστε, αφού το άρθρο είναι πάνω από 100 χρόνων), όπου η προσωπική πληροφορία εκατομμυρίων τώρα συλλέγεται σε τακτική βάση, συνοψίζεται, πινακοποιείται, χρησιμοποιείται και πωλείται.

Ευτυχώς όμως , αρκετά χρόνια μετά το άρθρο των Warren και Brandeis και συγκεκριμένα το 1967, ο καθηγητής Alan Westin, του πανεπιστημίου Columbia, δημιούργησε έναν ορισμό της ιδιωτικότητας που είναι χρήσιμος σήμερα όσο ποτέ άλλοτε. Ο Westin όρισε σαν πληροφοριακή ιδιωτικότητα "την απαίτηση ατόμων , ομάδων, ή οργανισμών να ορίζουν οι ίδιοι πότε, πώς και σε ποιο βαθμό πληροφορίες γι' αυτούς θα μεταδίδονται σε άλλους."

Ο μεγαλύτερος αριθμός παραβιάσεων της προσωπικής ιδιωτικότητας στον Παγκόσμιο Ιστό εμπίπτουν στον χαρακτηρισμό του Westin για την πληροφοριακή ιδιωτικότητα. Δηλαδή πολλά άτομα έχουν χάσει την δυνατότητα να ελέγχουν πώς και σε ποιο βαθμό πληροφορία γι' αυτούς μεταδίδεται σε εταιρείες μάρκετινγκ, κυβερνητικά πρακτορεία και αδιάκριτους γείτονες στο παγκόσμιο ηλεκτρονικό χωριό.

Η πληροφορική περιλαμβάνει την εφαρμογή και την χρήση της πληροφορίας:

Η πληροφορία είναι πολύτιμη.

Τα πολύτιμα πράγματα αντιμετωπίζονται σαν ιδιοκτησία από τον νόμο.

Ο νόμος πρέπει να αντιμετωπίσει δύο καίρια ερωτήματα όσο αφορά τα προϊόντα της πληροφορίας:

Ποια από αυτά μπορούν να ανήκουν σε ένα άτομο;

Ποια δεν μπορούν να έχουν ιδιοκτήτη;

Το πρώτο πράγμα που είναι εμφανές όταν αρχίζει η ανάλυση του ορισμού του Westin είναι ότι υπάρχουν διάφορα είδη πληροφορίας στα οποία μπορεί να εφαρμοσθεί ο ορισμός. Ο όρος "πληροφορία" στον ορισμό του Westin μπορεί να εφαρμοσθεί στο ονοματεπώνυμο κάποιου και σίγουρα θα μπορούσε να εφαρμοσθεί σε ένα κομμάτι χαρτί που περιέχει το ονοματεπώνυμο κάποιου, το ΑΦΜ του, και μια λίστα με τις ιστοσελίδες που επισκέφθηκε τον τελευταίο μήνα. Όμως αν αυτό το χαρτί περιείχε μόνο την λίστα με τις ιστοσελίδες και τα τέσσερα πρώτα ψηφία του ΑΦΜ, θα μπορούσε αυτό το κομμάτι χαρτί να θεωρηθεί σαν προσωπική πληροφορία;

Για να αντιμετωπίσουν ερωτήσεις σαν αυτήν, οι ακαδημαϊκοί έχουν χωρίσει τον όρο "πληροφορία" σε αρκετές διαφορετικές κατηγορίες. Μερικές από αυτές (όπως αναφέρονται στο "Web Security, Privacy & Commerce" των Simson Garfinkel και Gene Spafford) είναι:

• Προσωπική πληροφορία **(Personal information)**.

Πληροφορία για κάποιο άτομο όπως το ονοματεπώνυμό του, η ημερομηνία γεννήσεως, τα ονόματα των γονέων του.

• Ιδιωτική πληροφορία **(Private information).**

Είναι προσωπική πληροφορία η οποία δεν είναι γενικά γνωστή. Μερικά είδη ιδιωτικής

πληροφορίας προστατεύονται από τον νόμο όπως π.χ. τα ιατρικά ιστορικά. Οι περισσότεροι άνθρωποι έχουν μια μεγάλη ποσότητα πληροφορίας που θεωρούν ιδιωτική αλλά δεν προστατεύεται νομικά. Για παράδειγμα, μπορεί κάποιος να θεωρεί το όνομα του ατόμου που φίλησε για πρώτη φορά σαν ιδιωτικό. Άλλες πληροφορίες θα έπρεπε να

διαχειρίζονται σαν ιδιωτικές, αν και είναι ευρέως διαθέσιμες. Για παράδειγμα, οι περισσότεροι από εμάς θεωρούν το ΑΦΜ τους σαν ιδιωτικό, αν και είναι καταχωρημένα (και διαθέσιμα σε πάρα πολλές κυβερνητικές αλλά και ιδιωτικές βάσεις δεδομένων. Αυτή η αμφιβολία προέρχεται εν μέρει από το γεγονός ότι το ιδιωτικό δεν είναι συνώνυμο με το μυστικό ή εμπιστευτικό. Το αν κάποιο κομμάτι πληροφορίας είναι ιδιωτικό συχνά εξαρτάται από τον περιβάλλοντα χώρο. Αν το ονοματεπώνυμο σας είναι καταχωρημένο στον τηλεφωνικό κατάλογο, αυτή η πληροφορία δεν είναι ιδιωτική. Αν όμως αυτός ο κατάλογος βρίσκεται αποθηκευμένος στον υπολογιστή κάποιου εμπλεκόμενου σε παράνομες ενέργειες, πιθανότατα να επιθυμείτε το γεγονός ότι το όνομά σας είναι στον τηλεφωνικό κατάλογο αυτού του ατόμου να παραμείνει εξαιρετικά ιδιωτικό.

• Προσωπικά αναγνωρίσιμη πληροφορία **(Personally identifiable information).**

Είναι η πληροφορία απο την οποία το όνομα ή η ταυτότητα κάποιου ατόμου μπορεί να αποκομιστεί όχι άμεσα αλλά μετά απο κάποια (ελάχιστη συνήθως) επεξεργασία ή διασταύρωση. Προσωπικά αναγνωρίσιμη πληροφορία είναι π.χ. κάποιος τραπεζικός λογαριασμός. Πολλοί ιστοχώροι που διεξάγουν ηλεκτρονικό εμπόριο αποθηκεύουν τέτοιου είδους πληροφορίες την πρώτη φορά που κάποιος χρήστης θα τα επισκεφθεί, έτσι ώστε να μην χρειάζεται να τα εισάγει κάθε φορά που επισκέπτεται τον συγκεκριμένο ιστόχωρο.

• Ανωνυμοποιημένη πληροφορία **(Anonymized information).**

Είναι η πληροφορία που έχει τις αντίστροφες ιδιότητες από την προσωπικά

αναγνωρίσιμη. Αποτελεί προσωπική ή ιδιωτική πληροφορία η οποία έχει τροποποιηθεί με κάποιο τρόπο έτσι ώστε οι ταυτότητες των ατόμων από τα οποία συλλέχθηκε αυτή η πληροφορία να μην μπορούν πια να εξαχθούν.

• Συναθροιστική πληροφορία **(Aggregate information).**
Είναι στατιστική πληροφορία προερχόμενη από πολλά διαφορετικά άτομα για να αποτελέσει μια ενιαία εγγραφή (record).

Αυτές οι κατηγορίες πληροφορίες είναι πολύ περισσότερο ρευστές απ' όσο φαίνονται αρχικά. Συχνά, συναθροιστική και η ανωνυμοποιημένη πληροφορία μπορούν να συνδυαστούν για να αναγνωρίσουν και να αποκαλύψουν ιδιαίτερα χαρακτηριστικά κάποιου ατόμου. Αυτή η μέθοδος ονομάζεται "τριγωνοποίηση" (triangulation). Για παράδειγμα αν κάποιος καθηγητής έχει μια τάξη από δέκα φοιτητές και φοιτήτριες, και ξέρει ότι εννέα από αυτά τα άτομα είναι αγόρια και ένα άτομο είναι έγκυο τότε γνωρίζει με βεβαιότητα ποιο άτομο βρίσκεται σε ενδιαφέρουσα.
Στο παρελθόν, για να συνδυαστούν πληροφορίες από διαφορετικές πηγές ένας πολίτης θα έπρεπε να ξοδέψει ολόκληρες εβδομάδες στην βιβλιοθήκη. Τώρα, με τους υπολογιστές και τα δίκτυα τους, μπορούν να συνδυαστούν κομμάτια πληροφορίας μέσα σε μερικά λεπτά. Αναλύοντας δημόσια δεδομένα με την βοήθεια υπολογιστών, κάποιος μπορεί να φανερώσει μυστικά χωρίς καν να έχει δει ποτέ του κάποια απόρρητη βάση δεδομένων. Αυτό συμφωνεί και με αυτό που έγραψε κάποτε ο Hugo Cornwall, συγγραφέας του (απαγορευμένου προς πώληση) βιβλίου "Hacker Handbook", ότι ένα μεγάλο μέρος πληροφορίας που δηλώνεται σαν "απόρρητη", είναι ανοικτά διαθέσιμη, αν ξέρεις που να ψάξεις και πως να εκτιμήσεις αυτό που βρίσκεις.

Πίσω στο 1985, ο αντιναύαρχος John Poindexter –που αρκετοί Αμερικανοί γνωρίζουν σαν τον βασικό ενδιάμεσο για την παροχή αμερικανικών όπλων στο Ιράν την δεκαετία του ΄80– άρχισε να ανησυχεί γι' αυτό ακριβώς το πρόβλημα. Προσπάθησε λοιπόν να δημιουργήσει μια καινούργια κατηγοριοποίηση της πληροφορίας "ευαίσθητη αλλά μη απόρρητη". Αυτή η πληροφορία ταίριαζε κάτω από τα γνωστά επίπεδα άκρως μυστικό (top secret), μυστικό (secret) και εμπιστευτικό (confidential). Η πρόσβαση σε αυτήν την πληροφορία ήταν απαγορευμένη για ορισμένους ξένους. Ο Poindexter προσπάθησε αδέξια να εφαρμόσει αυτόν τον διαχωρισμό στην ακαδημαϊκή κοινότητα· προφανώς τα πανεπιστήμια το απέρριψαν και η ιδέα του πέθανε εκεί. Οι ακαδημαϊκοί τελικά κατέληξαν στις κατηγορίες που αναφέρονται αναλυτικά παραπάνω.

Μια έρευνα του 1993 από το περιοδικό "MacWorld" ανέφερε δεδομένα από μια δημοσκόπηση που έγινε από την εταιρεία Louis Harris & Associates, στο οποίο μόνο το 33% των ερωτηθέντων ενδιαφέρονταν για την προσωπική ιδιωτικότητα κατά το έτος 1970. Το 1990, αυτό το ποσοστό είχε εκτιναχθεί στο 79%. Σήμερα αυτό το ποσοστό ίσως και να πλησιάζει το 100%.

Αν και το μέγεθος και το κοινωνικό κόστος από την απειλή της προσωπικής ιδιωτικότητας είναι δύσκολο να μετρηθεί, είναι εμφανές ότι η τεχνολογία της πληροφορίας γίνεται αρκετά ισχυρή έτσι ώστε να προκαλεί φόβο για κυβερνητικούς και εταιρικούς "Big Brothers".

2.2 Αρχεία καταγραφής (Log files)

Παρόλο που η πληροφορία που παρέχεται από τους ίδιους τους χρήστες είναι συνήθως η πιο λεπτομερής, η πιο διεισδυτική με διαφορά πληροφορία είναι αυτή που συλλέγεται από την λειτουργία του ίδιου του

δικτύου. Αυτά τα δεδομένα αποθηκεύονται σε αρχεία καταγραφής (*log files*) που δημιουργούνται από δικτυακά προγράμματα και συσκευές.

Τα αρχεία καταγραφής είναι πανταχού παρόντα. Οι προγραμματιστές προσθέτουν αρχεία καταγραφής στα προγράμματα τους για να τους βοηθήσουν στην συγγραφή και αποσφαλμάτωση. Οι διαχειριστές συστημάτων αφήνουν τα αρχεία καταγραφής ενεργοποιημένα για να μπορούν να επιβεβαιώνουν ότι το λογισμικό λειτουργεί σωστά, έτσι ώστε να μπορούν να διαγνώσουν την αιτία κάποιου προβλήματος όταν αυτό συμβεί. Οι κυβερνήσεις και οι διαφημιστικές εταιρείες χρησιμοποιούν τα αρχεία καταγραφής γιατί αποτελούν μια εξαιρετική πηγή δεδομένων.

Οι υπολογιστές είναι απίστευτα πολύπλοκες μηχανές· λίγοι διαχειριστές συστημάτων γνωρίζουν όλα τα αρχεία καταγραφής που διατηρούνται στα υπολογιστικά συστήματα που ελέγχουν. Υπάρχουν πολλές περιστάσεις όπου κάποιος διαχειριστής ισχυρίζεται πως ένα συγκεκριμένο κομμάτι πληροφορίας δεν κατακρατείται από το υπολογιστικό του σύστημα και μετά αποδεικνύεται πως στην πραγματικότητα η πληροφορία αυτή αποθηκεύεται κάπου μέσα σε κάποιο αρχείο καταγραφής.

Βασικά δεν υπάρχει κανένας τρόπος για να γνωρίζει με απόλυτη βεβαιότητα κάποιος χρήστης ενός συστήματος αν κάποιο αρχείο καταγράφει τις ενέργειες του. Πολλοί οργανισμοί που διαβεβαίωναν τους χρήστες τους ότι οι ενέργειες τους δεν καταγράφονται στην συνέχεια διαψεύστηκαν. Επίσης πολλοί οργανισμοί που υπέθεταν ότι οι ενέργειες των χρηστών καταγράφονται ανακάλυψαν στην συνέχεια προβλήματα με το σύστημα καταγραφής τους. Κάποια πληροφοριακά συστήματα αυτόματα καταστρέφουν τα παλιά αρχεία καταγραφής, μια διαδικασία που ονομάζεται περιτροπή (rotation). Σε άλλα συστήματα δεν υπάρχει επίσημη μέθοδος καταστροφής των παλιών αρχείων καταγραφής· αυτά τα συστήματα διατηρούν τα αρχεία καταγραφής μέχρι να γεμίζουν οι σκληροί δίσκοι και κάποιος να σβήσει τα αρχεία χειρωνακτικά.

Για τους ίδιους λόγους που είναι αδύνατον κάποιος χρήστης να γνωρίζει με απόλυτη σιγουριά αν οι ενέργειες του καταγράφονται, είναι επίσης αδύνατον να γνωρίζει για πόσο καιρό διατηρούνται αυτά τα αρχεία.

Τα αρχεία καταγραφής είναι επίσης ένας τεχνικός μηχανισμός που βοηθάει τους προϊστάμενους να διατηρήσουν την προσωπική υπευθυνότητα. Συμβουλεύοντας τους χρήστες ότι είναι προσωπικά υπεύθυνοι για τις ενέργειες του, οι οποίες καταγράφονται σε αρχεία, οι προϊστάμενοι μπορούν να προάγουν την πρέπουσα συμπεριφορά των χρηστών του υπολογιστικού συστήματος. Είναι λιγότερο πιθανό οι χρήστες να παρακάμψουν την πολιτική ασφάλειας αν γνωρίζουν ότι οι ενέργειες τους θα αποτυπωθούν σε αρχείο καταγραφής.

Τα αρχεία καταγραφής έχουν μια θεμελιώδη αδυναμία. Επειδή συχνά δημιουργούνται στο ίδιο το σύστημα, είναι υποκείμενα σε μετατροπές ή διαγραφές και γι' αυτόν τον λόγο είναι ιδιαιτέρως σημαντικό να εξασφαλιστεί η ακεραιότητα τους. Ένας τρόπος για να γίνει αυτό είναι μέσω ψηφιακών υπογραφών (*digital signatures*). Άλλος τρόπος αποτελεί η χρήση μέσων αποθήκευσης μίας εγγραφής όπως το CD. Η ακεραιότητα των αρχείων παρακολούθησης μπορεί να είναι ιδιαιτέρως σημαντική σε νομικές διαδικασίες όπως όταν αυτά τα αρχεία χρησιμοποιούνται σαν αποδεικτικά στοιχεία στο δικαστήριο. (Κάτι τέτοιο όμως μπορεί να απαιτεί καθημερινή εκτύπωση και υπογραφή των αρχείων παρακολούθησης).

Υπάρχουν πολλές τελικές προτάσεις που μπορούν να γίνουν για τα αρχεία καταγραφής. Η πρώτη έχει σχέση με τα αντίγραφα ασφαλείας. Είναι συνετό τα αρχεία καταγραφής να αποθηκεύονται σε αντίγραφα ασφαλείας σε τακτική βάση, προτιμότερα καθημερινώς.

Η δεύτερη πρόταση έχει να κάνει με το πόσο συχνά πρέπει να εξετάζονται αυτά τα αρχεία. Αυτό εξαρτάται κατά κύριο λόγο από το μέγεθος του πληροφοριακού συστήματος, αλλά γενικά τουλάχιστον μία

φορά την ημέρα ακούγεται καλό. Η τήρηση των αρχείων παρακολούθησης έχει μικρό όφελος αν δεν εξετάζονται σε τακτική βάση. Μπορούν να αποκαλύψουν προβλήματα του υλικού, με τις δικτυακές ρυθμίσεις, και (φυσικά) με την ασφάλεια. Συνεπώς, πρέπει να εξετάζονται τακτικά για να αποκαλύψουν πότε κάποιο πρόβλημα υπάρχει πραγματικά. Αν εξεταστούν καθυστερημένα, το πρόβλημα μπορεί να μεγαλώσει.

Η τρίτη πρόταση έχει να κάνει με την εμπιστοσύνη. Μην εμπιστεύεστε τα αρχεία καταγραφής απόλυτα! Αυτά τα αρχεία μπορούν να τροποποιηθούν από εισβολείς αλλά και από τοπικούς χρήστες με φυσική πρόσβαση ή αρκετές γνώσεις και κίνητρο. Και φυσικά, τα σφάλματα λογισμικού μπορούν να προκαλέσουν προβλήματα στην συλλογή και αποθήκευση τους. Έτσι πρέπει να δημιουργηθούν άφθονοι μηχανισμοί παρακολούθησης και καταγραφής· επειδή κάτι δεν έχει καταγραφεί δεν σημαίνει ότι δεν συνέβη. Φυσικά, απλά και μόνο επειδή κάτι καταγράφηκε δεν σημαίνει ότι συνέβη επίσης –κάποιος μπορεί να δημιουργήσει πλαστές εγγραφές σε ένα τέτοιο αρχείο για να αποσπάσει την προσοχή του διαχειριστή του συστήματος από κάποιο πραγματικό πρόβλημα ή για να ενοχοποιήσει κάποιον άλλο.

Ακόμη και ένα ελλιπές ή ημικατεστραμένο αρχείο καταγραφής μπορεί να αποβεί χρήσιμο για τον διαχειριστή του συστήματος. Υπάρχουν πάρα πολλές περιπτώσεις όπου εισβολείς καθώς τροποποιούσαν κάποιο αρχείο καταγραφής σβήνοντας τις εγγραφές που τους ενοχοποιούσαν, συνειδητοποίησαν ότι έσβησαν περισσότερα από όσα θα έπρεπε.

2.2.1 Αρχεία καταγραφής παγκόσμιου ιστού (Web logs).

Όπως αναφέρουν οι Simson Garfinkel και Gene Spafford, στο βιβλίο τους, “Web Security, Privacy & Commerce”, πρακτικά οποτεδήποτε

κάποιο πρόγραμμα εξερεύνησης του παγκόσμιου ιστού (π.χ. Internet Explorer, Netscape Navigator), μεταφέρει μια ιστοσελίδα στον υπολογιστή του χρήστη, μια εγγραφή που σημειώνει αυτήν την ενέργεια καταγράφεται συστηματικά σε ένα αρχείο παρακολούθησης στον εξυπηρετητή του παγκόσμιου ιστού. Σε αποτέλεσμα αυτού, η απλή εξερεύνηση του ιστού μπορεί να προκαλέσει μια πληθώρα από εγγραφές που δημιουργούνται σε υπολογιστές που ελέγχονται από μια πλειάδα οργανισμών.

Αυτά τα αρχεία παρακολούθησης βρίσκονται υπό τον έλεγχο του ατόμου ή οργανισμού που ελέγχει τον διακομιστή του παγκόσμιου ιστού και μπορούν να χρησιμοποιηθούν αν καταστεί αναγκαίο σε δικαστικές αποφάσεις ή αστυνομικές έρευνες. Μπορούν επίσης να χρησιμοποιηθούν από τους εργοδότες για να διαπιστώσουν τι κάνουν οι υπάλληλοι τους την ώρα της δουλειάς. Μπορούν να χρησιμοποιηθούν από κάποιο περίεργο διαχειριστή συστήματος για να κατασκοπεύσει άλλους. Αλλά στην συντριπτική πλειοψηφία των περιπτώσεων κανείς δεν τα κοιτάει, και επειδή τα περιεχόμενα των περισσοτέρων αρχείων παρακολούθησης δεν φανερώνονται ποτέ, οι περισσότεροι χρήστες του διαδικτύου δεν γνωρίζουν ότι οι ενέργειες τους καταγράφονται στην πλήρη έκταση τους.

Οι ακόλουθες πληροφορίες αποθηκεύονται είτε άμεσα στα περισσότερα αρχεία παρακολούθησης του παγκόσμιου ιστού ή μπορούν να εξαχθούν συμπερασματικά από άλλες πληροφορίες που περιέχονται σε αυτά τα αρχεία:

Το όνομα και η διεύθυνση IP του υπολογιστή που μετέφερε την ιστοσελίδα.

Η ώρα της μεταφοράς.

Η διεύθυνση του παγκόσμιου ιστού (*URL*) που ζητήθηκε.

Ο χρόνος που χρειάστηκε για να μεταφερθεί το αρχείο (αυτό είναι μια ένδειξη του είδους της σύνδεσης που διαθέτει ο χρήστης).

Αν χρησιμοποιήθηκε πιστοποίηση μέσω του παγκόσμιου ιστού (HTTP authentication), τότε το αρχείο καταγραφής περιέχει το username του χρήστη που μετέφερε το αρχείο.

Οποιαδήποτε σφάλματα μπορεί να συνέβησαν.

Την προηγούμενη σελίδα (refer link) που μεταφέρθηκε από το πρόγραμμα πλοήγησης. (Αναλυτικότερα βλέπε παρακάτω).

Το είδος του προγράμματος πλοήγησης που χρησιμοποιήθηκε.

Οι παραπάνω πληροφορίες μπορούν να συνδυαστούν με άλλα αρχεία καταγραφής όπως οι πληροφορίες σύνδεσης/αποσύνδεσης (*login/logout information*) από τους παροχείς υπηρεσιών διαδικτύου, ή από αρχεία προερχόμενα από διακομιστές ηλεκτρονικού ταχυδρομείου (*mail servers*), για να ανακαλυφθεί η πραγματική ταυτότητα του ατόμου που έκανε την μεταφορά. Υπό κανονικές συνθήκες αυτού του είδους η διασταύρωση πληροφοριών απαιτεί την συνδρομή κάποιου άλλου οργανισμού, αλλά αυτό δεν ισχύει πάντοτε.

Το πεδίο αναφέροντος (refer link) είναι άλλη μια πηγή παραβίασης ιδιωτικότητας. Λειτουργεί κάπως έτσι: Όποτε κάποιος χρήστης, ψάχνει για κάποια ιστοσελίδα, ένα από τα κομμάτια πληροφορίας που στέλνεται μαζί είναι και η διεύθυνση της σελίδας που κοιτάζει αυτήν την στιγμή ο χρήστης.

Μια από τις κύριες χρήσεις που έχουν βρει οι εταιρείες για το refer link είναι η μέτρηση της αποτελεσματικότητας των διαφημίσεων που αγοράζουν σε άλλους ιστοχώρους. Άλλη χρήση είναι η χαρτογράφηση της πορείας των χρηστών μέσα από έναν ιστοχώρο. Το refer link μπορεί επίσης να αποκαλύψει προσωπικές πληροφορίες· ειδικά, την διεύθυνση της ιστοσελίδας που κοιτούσε ο χρήστης πριν κάνει κλικ στην δική σας.

2.3 Παραβίαση απορρήτου.

Ορισμένες χώρες, σαν την Σουηδία και τον Καναδά, έχουν πολύ αυστηρούς νόμους για διασφάλιση του απορρήτου. Άλλες χώρες δεν έχουν κανένα νόμο. Για παράδειγμα, μέχρι το 1997, η Ιταλία, το Βέλγιο, η Ισπανία, η Πορτογαλία και η Ελλάδα είχαν ελάχιστη νομοθεσία που να προστατεύει τα δικαιώματα ενός ατόμου να ελέγχει προσωπικά δεδομένα σε κυβερνητικές ή εμπορικές βάσεις δεδομένων. Αυτό παρεμποδίζει την ροή των πληροφοριών ανάμεσα σε χώρες στην Ευρωπαϊκή Ένωση. Για να παρακαμφθεί αυτό το πρόβλημα, το 1998, η Ευρωπαϊκή Επιτροπή εξέδωσε οδηγίες προς όλα τα κράτη μέλη, οι οποίες αφορούν τα δικαιώματα των ατόμων για πρόσβαση πληροφοριών που τα αφορούν και για διόρθωση σφαλμάτων σε ότι τα αφορά (σημ.: ακόμη μια περίπτωση όπου η Ευρωπαϊκή Ένωση αναγκάζεται να μας ξυπνήσει από το εθνικό μας σπορ, τον λήθαργο, και να μας “σπρώξει” μπροστά).

Τα δεδομένα είναι περισσότερο από απλά το ζωτικό στοιχείο των πληροφοριακών κοινωνιών. Είναι η βάση ενός σύνθετου ιστού από εξαρτήσεις δεδομένων και συμβιωτικές σχέσεις. Σε τέτοιες κοινωνίες, η έξοδος πληροφοριών από διαδικασίες συλλογής δεδομένων και ανάλυσης αναδομείται για να γίνει είσοδος από ακόμα υψηλότερες διαδικασίες. Για παράδειγμα, αρχεία λιανικών αγορών μπορεί να γίνουν είσοδος για εταιρείες πωλήσεων μέσω αλληλογραφίας, ενώ τα δείγματα πωλήσεων τους μπορούν με τη σειρά τους να γίνουν είσοδος για διαφημιστές τοπικών περιοδικών και τηλεόρασης.

Πριν λίγα χρόνια, η American Express παραδέχτηκε στους 2,5 εκατομμύρια ιδιοκτήτες καρτών της ότι για χρόνια ταξινομούσε τα αρχεία συναλλαγών τους ως προς τα πρότυπα κατανάλωσης και μετά ενοικίαζε τις λίστες ονομάτων και διευθύνσεών τους σε οργανώσεις που κυμαίνονταν από καταστήματα μέχρι ασφαλιστικές εταιρείες.

Αυτές οι σύνθετες σχέσεις ανάμεσα σε συλλέκτες δεδομένων, καταναλωτές και επανεπεξεργαστές έχουν διαμορφώσει μια οικολογία πληροφοριών που προς τα πάνω διυλίζει την πληροφορία μέχρι οι μεγαλύτεροι οργανισμοί στην κορυφή της τροφικής αλυσίδας– μεγάλες επιχειρήσεις και κυβερνητικά σώματα– να μπορούν να την χρησιμοποιήσουν για να παίρνουν στρατηγικές αποφάσεις για άτομα, γειτονιές, κοινότητες, ακόμα και ολόκληρα τμήματα της κοινωνίας.

Αλλά για να λάβουν χώρα αυτοί οι ιστοί εισόδου και εξόδου, η βάση του τροφικού ιστού –τα ακατέργαστα δεδομένα– πρέπει να είναι διαθέσιμα, άμεσα και σε χρησιμοποιήσιμη μορφή. Και είτε είμαστε ενήμεροι είτε όχι, είτε μας αρέσει είτε όχι, οποιοσδήποτε που λειτουργεί σε μία σύγχρονη κοινωνία αναπόφευκτα δημιουργεί ένα ίχνος πληροφορίας που δρα ως το πλαγκτόν αυτής της σύνθετης πληροφοριακής οικολογίας. Για να πάρουν άδεια οδήγησης, δάνεια ή πιστωτική κάρτα, για να γίνουν δεκτοί σε ένα νοσοκομείο ή για να καταχωρίσουν την εγγύηση μιας νέας αγοράς, οι άνθρωποι στις Η.Π.Α. συμπληρώνουν μηχανικά φόρμες που παρέχουν μια αφθονία στοιχείων για τους εαυτούς τους. Λίγα από αυτά παραμένουν εμπιστευτικά. Ακόμα και οι κυβερνητικές υπηρεσίες των Η.Π.Α. εισχωρούν σε εμπορικές βάσεις δεδομένων για να πάρουν αποφάσεις για το δικαίωμα σε επιδόματα ιατρικής φροντίδας και κοινωνικής ασφάλειας. Προσωπικά οικονομικά, ιατρικά ιστορικά, αγοραστικές συνήθειες και άλλα σκαλίζονται από εταιρείες επεξεργασίας δεδομένων. Αυτές οι εταιρείες με τη σειρά τους συνδυάζουν τα αρχεία με πληροφορίες που αντλούνται από άλλες πηγές –για παράδειγμα από κυβερνήσεις πολιτειών που πωλούν λίστες αδειών οδήγησης– για να σχεδιάσουν μια καθαρότερη εικόνα, ή μωσαϊκό αν θέλετε, ενός ατόμου ή νοικοκυριού. Αυτά τα επανασυσκευασμένα μωσαϊκά, που περιλαμβάνουν λάθη και ανακρίβειες, πωλούνται στη συνέχεια σε κυβερνητικές υπηρεσίες, δανειστές, λιανέμπορους, μικρές επιχειρήσεις,

υπεύθυνους marketing και ασφαλιστές. Το αποτέλεσμα είναι μία βιομηχανία ενός δισεκατομμυρίου δολαρίων το χρόνο που προσθέτει λίγο στην απόδοση εξαγωγών, στην εθνική παραγωγικότητα ή στο ΑΕΠ.

Στη Γαλλία, μία χώρα που ποτέ δεν έγινε γνωστή για παραβίαση αρχείων ασφαλείας, 20.000 πολίτες εξεγέρθηκαν στις αρχές τις δεκαετίας του ΄90 για να διαμαρτυρηθούν όταν ανακαλύφθηκαν 900.000 κυβερνητικά αρχεία που δημιουργήθηκαν για την καταπάτηση του εγκλήματος. Ξεπερνώντας αυτές τις δυσκολίες η Ευρωπαϊκή Ένωση προώθησε προτάσεις για ανταλλαγή πληροφοριών μεταξύ υπηρεσιών συμπεριλαμβανομένου της διασταύρωσης στοιχείων μεταξύ των υπηρεσιών ασφαλείας. Η Γερμανία, Γαλλία και οι Benelux έχουν προτείνει ένα ενιαίο σύστημα δεδομένων (Schengen) που θα παρέχει στις υπηρεσίες ασφαλείας πληροφορίες και δεδομένα για 320 εκατομμύρια ανθρώπους. Διάφοροι συγγραφείς έχουν ισχυριστεί ότι ένα σύστημα ταυτοτήτων είναι απαραίτητο σε χώρες όπως η Μ. Βρετανία. Πράγματι σε χώρες όπως το Βέλγιο, Ελλάδα, Ιταλία, Γερμανία, Λουξεμβούργο, Πορτογαλία και Ισπανία λειτουργεί ήδη τέτοιο ολοκληρωμένο σύστημα. Οι υπέρμαχοι αντίστοιχα της ιδέας αυτής στη Μ. Βρετανία τονίζουν επίμονα τα πλεονεκτήματα που επιφέρει ένα τέτοιο διοικητικό σχήμα.

Στην χώρα μας, σε μερικούς μήνες απο τώρα ενεργοποιείται το νέο σύστημα παρακολούθησης των τηλεπικοινωνιών, το οποίο μεταξύ άλλων προβλέπει τήρηση αρχείου όλων των τηλεφωνικών κλήσεων, ακόμα και των αναπάντητων, και επιτρέπει την καταγραφή της κίνησης υπόπτων. Τα νέα μέτρα προβλέπουν:

Η τήρηση αρχείου με τις τηλεφωνικές συνδιαλέξεις επεκτείνεται από τους έξι μήνες στον ένα χρόνο. Τα αρχεία θα περιλαμβάνουν στο εξής και τις αναπάντητες κλήσεις - πολύ περισσότερες από τις συνδιαλέξεις- διογκώνοντας τον όγκο των πληροφοριών που πρέπει να αποθηκευτούν.

Επιβάλλεται η καταγραφή του «αναγνωριστικού κελιού, πλην του αρχικού κελιού». Αυτό σημαίνει ότι θα σημειώνονται για κάθε εξερχόμενη κλήση οι κυψέλλες (κεραίες) που χρησιμοποιήθηκαν. Με την καταγραφή της αρχικής και της τελικής κεραίας που χρησιμοποίησε ο ύποπτος, οι Αρχές θα μπορούν να συμπεραίνουν το δρομολόγιό του.

Οι εκπρόσωποι της αστυνομίας ζητούν την καταγραφή ακόμα περισσότερων στοιχείων από αυτά που απαιτεί η ΕΕ, όπως τον κωδικό IMEI, δηλαδή την ηλεκτρονική ταυτότητα της συσκευής. (σημ.: Που είναι αυτή η περίφημη Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα όταν την χρειάζεσαι;...)

Η τεχνολογία της πληροφορίας επιτρέπει σε ιδιώτες, κυβερνήσεις και εταιρείες να παραβιάζουν την ιδιωτικότητα των άλλων. Μια δημοκρατική κοινωνία πρέπει να βρει την χρυσή τομή ανάμεσα στον σεβασμό για την ιδιωτικότητα του κάθε πολίτη και την ελευθερία της πληροφορίας.

2.4. Ανώνυμοι αναμεταδότες ηλεκτρονικού ταχυδρομείου

Ο Richard Mansfield, στο βιβλίο του “Hacker Attack”, μας προσφέρει κάποιες γενικές πληροφορίες για τους ανώνυμους αναμεταδότες ηλεκτρονικού ταχυδρομείου. Έτσι λοιπόν, οι υπηρεσίες ανώνυμης αναμετάδοσης αποτελούν το ισοδύναμο των ανώνυμων τηλεφωνικών κλήσεων από τηλεφωνικούς θαλάμους δημόσιας χρήσης –εάν κάποιος ανιχνεύσει την κλήση, το μόνο που θα μπορέσει να βρει είναι ένας άδειος θάλαμος. Εσείς θα έχετε φύγει. Χρησιμοποιώντας μια υπηρεσία ανώνυμης αναμετάδοσης ηλεκτρονικού ταχυδρομείου (***anonymous remailer***), ο χρήστης μπορεί να κρύψει ολοκληρωτικά την πραγματική του ταυτότητα. Ορισμένες τέτοιες υπηρεσίες είναι δωρεάν, ενώ άλλες

χρεώνουν ένα αντίτιμο ή υποχρεώνουν τον χρήστη να συμπεριλάβει διαφημιστικά μηνύματα.

Οι υπηρεσίες αυτές χρησιμοποιούν ειδικά εργαλεία λογισμικού για να εξαλείψουν το όνομα και τη διεύθυνση από τα μηνύματα σας του χρήστη, υποκαθιστώντας τα με πλασματικά δεδομένα έτσι ώστε να μην μπορεί κανείς να τον εντοπίσει πραγματικά.

Η τεχνική αυτή η οποία είναι γνωστή με τον όρο μεταμφίεση (cloaking), χρησιμοποιείται ευρέως από τους spammers, αλλά μπορεί επίσης να χρησιμοποιηθεί από νομοταγείς ανθρώπους. Υπάρχουν καλοί λόγοι για τους οποίους θα ήθελε κανείς να στέλνει ανώνυμα μηνύματα ηλεκτρονικού ταχυδρομείου. Μπορεί να έχετε ισχυρές απόψεις για συγκεκριμένα πολιτικά θέματα, ή να θέλετε απλώς να εκφράσετε τις ιδέες σας σε διάφορες ομάδες συζήτησης χωρίς να αποκαλύψετε την ταυτότητα σας. Ακόμη μπορεί να θέλετε να επισημάνετε ή να καταγγείλετε κάτι σε μια κρατική υπηρεσία, σε ένα τοπικό σούπερ μάρκετ, στον εργοδότη σας, ή σε κάποιον άλλο. Εκμεταλλευόμενοι το cloaking μπορείτε να κρυφτείτε άνετα.

Εάν κάποιος απαντήσει στην πλασματική διεύθυνση σας, το μήνυμα του προωθείται στην πραγματική σας διεύθυνση η οποία αποθηκεύεται σε μια βάση δεδομένων στην υπηρεσία αναμετάδοσης. Αυτή η βάση δεδομένων συνδέει την πλασματική με την πραγματική σας ταυτότητα.

Επίσης, οι υπηρεσίες αναμετάδοσης καθυστερούν την αποστολή των μηνυμάτων για ένα τυχαίο χρονικό διάστημα. Αυτό βοηθά ακόμη περισσότερο στην απόκρυψη της πηγής ενός μηνύματος, επειδή εξαλείφει τη δυνατότητα χρονικού συσχετισμού των ενεργειών του χρήστη με τις ενέργειες της υπηρεσίας αναμετάδοσης.

Υπάρχουν δύο τύποι υπηρεσιών αναμετάδοσης ηλεκτρονικού ταχυδρομείου: οι πραγματικά ανώνυμες και οι ψευδο-ανώνυμες. Οι υπηρεσίες που διατηρούν την πλασματική και την πραγματική ταυτότητα

του χρήστη μαζί, στην ίδια βάση δεδομένων, θεωρούνται ψευδο-ανώνυμες επειδή τα άτομα που τις διαχειρίζονται γνωρίζουν την πραγματική του τα ταυτότητα και μπορεί να υποχρεωθούν να την αποκαλύψουν, π.χ. σε ένα δικαστήριο (αυτό έχει συμβεί πραγματικά). Οι πραγματικά ανώνυμες υπηρεσίες αναμετάδοσης δε γνωρίζουν την πραγματική ταυτότητα του χρήστη, αλλά είναι λιγότερο εύχρηστες.

Τέλος, η εταιρεία PrivateMailPlus υπόσχεται αντίστοιχη ασφάλεια χωρίς να πρέπει να αλλάξετε το αγαπημένο σας πρόγραμμα e-mail.

Μερικές διευθύνσεις όπου μπορείτε να βρείτε υπηρεσίες ανώνυμης αναμετάδοσης είναι οι εξής:

www.obscura.com

www.ziplip.com

www.privatemessenger.com

www.safemessage.com

www.hushmail.com

www.gilc.org/speech/anonymous/remailer.html

Για την προστασία της επαγγελματικής ηλεκτρονικής αλληλογραφίας υπάρχουν εργαλεία όπως το plug-in InterosaMail της Interosa, Inc. (www.interosa.com) το οποίο προσφέρει τη δυνατότητα για κρυπτογράφηση και για καθορισμό των περιοριστικών μέτρων (χρονικών, παραλήπτη) στα μηνύματα που αποστέλλονται.

-Εάν δεν πιστεύετε ότι αποκαλύπτετε πληροφορίες για τον εαυτό σας όταν βρίσκεστε στο διαδίκτυο , μεταβείτε στην διεύθυνση www.privacy.net και κάνετε κλικ στο κουμπί ***Full Analysis (πλήρης ανάλυση).*** Θα χρειαστούν ίσως ένα-δύο λεπτά για να εμφανιστεί η αναφορά στην οθόνη σας, αλλά όπως θα δείτε και μόνοι σας είναι ιδιαίτερα αποκαλυπτική.

2.5. Διατήρηση ανωνυμίας.

Η διατήρηση της ανωνυμίας είναι σχετικά εύκολη υπόθεση, αρκεί να προσεχθούν μερικά απλά σημεία:

• Αγοράστε ένα πακέτο πρόσβασης στο Internet από ένα κατάστημα που δεν σας γνωρίζουν (είναι σημαντικό), πληρώνοντας μετρητοίς (και όχι με πιστωτική κάρτα) και αποφύγετε να δώσετε τα στοιχεία σας κατά την εγγραφή. Με αυτόν τον τρόπο κανείς δεν θα γνωρίζει ότι ο συγκεκριμένος κωδικός πρόσβασης ανήκει σε εσάς. Σε περίπτωση που επιλέγετε εσείς τον κωδικό πρόσβασης στον ISP σας, αυτονόητο είναι ότι ο κωδικός πρόσβασης που θα επιλέξετε, δεν πρέπει να έχει καμία σχέση με τα πραγματικά στοιχεία σας.

• Επιλέξτε για ISP σας την εταιρεία εκείνη που σας δίνει τα περισσότερα εχέγγυα για την προστασία των δεδομένων σας. Διαβάστε τα "ψιλά γράμματα" της σύμβασης που υπογράφετε με τον παροχέα, και μην διστάσετε να διατυπώσετε οποιαδήποτε απορία ή ερώτηση έχετε.

• Όταν εγκαθιστάτε τα Windows ή διάφορα άλλα προγράμματα, μην εισάγετε τα πραγματικά σας στοιχεία όπου σας ζητείται, αφού αρκετές φορές υπήρξαν περιπτώσεις που αυτά υποκλάπηκαν από τρίτους.

• Εάν είναι δυνατόν, χρησιμοποιήστε περισσότερους του ενός κωδικούς πρόσβασης σε διαφορετικούς ISP και εναλλάσσετέ τους τακτικά.

• Ποτέ μην χρησιμοποιείτε τη διεύθυνση e-mail που σας παρέχει ο ISP σας, αλλά χρησιμοποιήστε σαν κύρια διεύθυνση αλληλογραφίας σας, ένα από τα δωρεάν e-mails που παρέχονται από τρίτες εταιρείες (π.χ. http://www.yahoo.gr)

• Μια εναλλακτική επιλογή είναι τα Internet καφέ που μπορείτε να χρησιμοποιείτε, όταν θέλετε να έχετε εξασφαλισμένη την ανωνυμία σας.

• Εγκαταστήστε ένα λειτουργικό σύστημα που προσφέρει ασφαλές σύστημα διαχείρισης αρχείων (file system) και ενημερώνετέ το συνεχώς με updates και patches.
• Αποφύγετε με κάθε τρόπο να δώσετε τα προσωπικά σας στοιχεία εάν δεν είναι απολύτως απαραίτητο.
• Σε περίπτωση που χρειάζεται να στείλετε ένα πολύ σημαντικό μήνυμα μέσω ηλεκτρονικού ταχυδρομείου, "σπάστε" το σε δύο ή περισσότερα μέρη και στείλτε τα από διαφορετικούς κωδικούς.

2.6 Cookies

Ένα αδύνατο σημείο στο θέμα της ασφάλειας είναι τα cookies, μια λειτουργία η οποία έχει σαν στόχο να κάνει τη ζωή των χρηστών του Διαδικτύου ευκολότερη. Στον Παγκόσμιο Ιστό, χρειάζεται να υπάρχει κάποιος τρόπος αποθήκευσης των προτιμήσεων των χρηστών. Τα cookies είναι ο λόγος που όταν κάποιος χρήστης επιστρέφει ξανά σε κάποια ιστοσελίδα, η σελίδα τον “αναγνωρίζει” και του εμφανίζει κάποιο μήνυμα του στυλ “Καλώς ήρθες Val!”.
Τα cookies είναι μικρά αρχεία δεδομένων, που αποθηκεύονται στους υπολογιστές των χρηστών. Ο σκοπός αυτών των αρχείων είναι να παρέχουν πληροφορίες για τους χρήστες, στους web servers που αυτοί συχνάζουν. Τα cookies μπορούν να απειλήσουν την ιδιωτικότητα και την ανωνυμία των χρηστών αφού προσωπικά δεδομένα μπορούν να επεξεργαστούν από διάφορους ιστοχώρους και να δημιουργηθεί το προφίλ (web profile) του χρήστη με ευκολία.
Ένα cookie είναι ένα κομμάτι κειμένου το οποίο στέλνεται απο έναν web server στον υπολογιστή του χρήστη μέσω του προγράμματος πλοήγησης που αυτός χρησιμοποιεί. Μόλις ληφθεί, το πρόγραμμα πλοήγησης (ή

φυλλομετρητής) στέλνει αυτό το cookie κάθε φορά που ο χρήστης ζητάει κάποιο καινούργιο έγγραφο απο τον web server.

Τα cookies μπορούν να χρησιμοποιηθούν για να αφαιρέσουν την ανωνυμία από τους χρήστες ή να την ενισχύσουν. Δυστυχώς, η επιλογή δεν είναι στα χέρια του χρήστη· βρίσκεται κάτω από τον έλεγχο του web server. Επιπρόσθετα, μπορεί να είναι πολύ δύσκολο για τους χρήστες να καταλάβουν για ποιό λόγο χρησιμοποιείται κάθε cookie. Τυπικές εφαρμογές των cookies αποτελούν:

Ένας ιστοχώρος με εμπορικά προϊόντα μπορεί να χρησιμοποιεί κάποιο cookie για να υλοποιήσει ένα ηλεκτρονικό “καλάθι προϊόντων”.

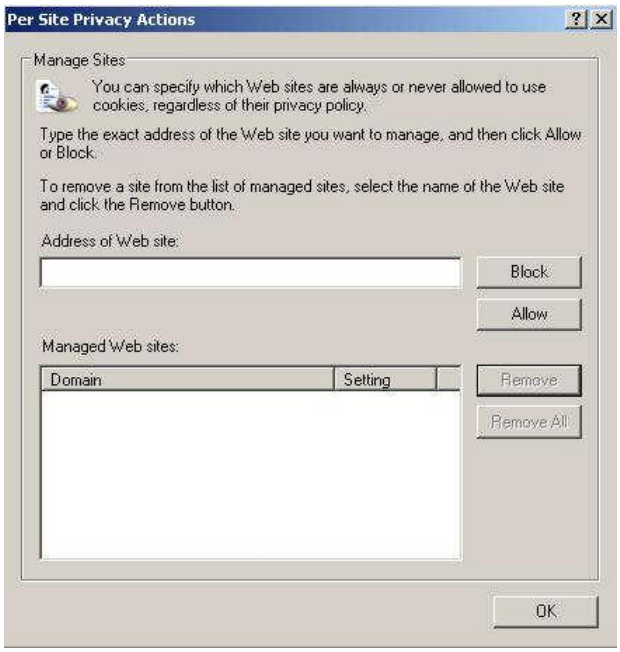
Ένας ιστοχώρος με νέα μπορεί να χρησιμοποιεί cookies για να παρέχει στους συνδρομητές της τοπικά νέα και πρόγνωση καιρού.

Ένας ιστοχώρος που παρέχει υπηρεσίες μόνο σε συνδρομητές, μπορεί να χρησιμοποιεί cookies για να αποθηκεύει πληροφορίες σχετικές με κάθε συνδρομητή έτσι ώστε κάθε φορά που κάποιος συνδρομητής μπαίνει στον ιστοχώρο να μην χρειάζεται να πληκτρολογεί το συνθηματικό του.

Μερικές ιστοχώροι είναι με τέτοιο τρόπο ρυθμισμένες έτσι ώστε αν κάποιος χρήστης έχει ήδη κάποιο cookie, να του παρέχεται πλήρης πρόσβαση στις πληροφορίες του λογαριασμού του. Άλλοι ιστοχώροι όμως απαιτούν απο τον χρήστη να εισάγει κάποιον κωδικό ακόμη και αν ο υπολογιστής του έχει το κατάλληλο cookie. Γενικά, αυτές οι ιστοχώροι είναι πιο ασφαλείς. Αυτό οφείλεται στο γεγονός ότι κάποιο cookie ενός χρήστη μπορεί εύκολα να καταλήξει στον υπολογιστή κάποιου άλλου για παράδειγμα αν κάποιος χρήστης μπει στον ιδιωτικό λογαριασμό του χρησιμοποιώντας κάποιον κοινόχρηστο υπολογιστή (π.χ. από κάποια σχολή) ή τον υπολογιστή κάποιου φίλου του. Όσο αφορά αυτούς που αναπτύσσουν εφαρμογές για τον Παγκόσμιο Ιστό, δεν θα πρέπει ποτέ να κάνουν το λάθος να νομίσουν ότι τα cookies είναι ασφαλή.

Ο φυλλομετρητής της Microsoft, Internet Explorer αλλά και αυτός της Netscape, ο Navigator παρέχουν επιλογές που επιτρέπουν στον χρήστη να ειδοποιείται κάθε φορά που στέλνεται κάποιο cookie στον υπολογιστή του και να επιλέγει αν θα το δεχθεί ή όχι. Οι τρέχουσες εκδόσεις των παραπάνω προγραμμάτων περιλαμβάνουν επιλογές όπως αποδοχή όλων των cookies, απόρριψη όλων των cookies, ή επιλογή αποδοχής/απόρριψης για κάθε cookie. Οι νεότερες εκδόσεις των εφαρμογών αυτών επιτρέπουν τον έλεγχο των cookies με βάση την συγκεκριμένη ιστοσελίδα από την οποία προέρχονται.

Δυστυχώς κανένας από τους δύο φυλλομετρητές δεν επιτρέπει την απενεργοποίηση αποστολής cookies που έχουν ήδη γίνει αποδεκτά στο παρελθόν. Για να γίνει αυτό πρέπει ο χρήστης να διαγράψει τα cookies από τον υπολογιστή του.



Εικόνα. Αποδοχή ή απόρριψη των cookies για συγκεκριμένα sites, στον Internet Explorer.

Υπάρχουν επιπρόσθετες τεχνικές για την αποτροπή των cookies. Αυτές οι τεχνικές λειτουργούν με όλους τους φυλλομετρητές, άσχετα αν διαθέτουν έλεγχο για cookies ή όχι και αναφέρονται στο “Practical Unix & Internet Security” των Simson Garfinkel και Gene Spafford:

Σε Unix συστήματα, οι χρήστες μπορούν να σβήσουν το αρχείο των cookies και να το αντικαταστήσουν με έναν σύνδεσμο στο /dev/null. Σε Windows συστήματα, το αρχείο μπορεί να αντικατασταθεί με ένα αρχείο μηδενικού μεγέθους με απενεργοποιημένα τα δικαιώματα διαβάσματος και γραψίματος. Σε έναν υπολογιστή Macintosh το αρχείο μπορεί να αντικατασταθεί με ένα κλειδωμένο, μηδενικού μεγέθους αρχείο ή φάκελο.

Εναλλακτικά, ο χρήστης μπορεί απλά να αποδεχθεί τα cookies που επιθυμεί και μετά να μετατρέψει το αρχείο των cookies σε αρχείο μόνο για διάβασμα. Αυτό θα αποτρέψει την αποθήκευση περισσότερων cookies μέσα.

Τα cookies μπορούν να απενεργοποιηθούν ολοκληρωτικά με μια αλλαγή μέσα στο εκτελέσιμο αρχείο του Internet Explorer ή του Netscape Navigator. Ο χρήστης πρέπει να ψάξει για την φράση Set-Cookie και να την αλλάξει σε κάτι άλλο π.χ. Set- Fookie. Δεν είναι πιθανό κάποιος να θέλει να στείλει Fookies στον υπολογιστή σας, οπότε αυτή η αλλαγή θα πρέπει να είναι αρκετή.

Διάφορα προγράμματα φιλτραρίσματος και διαδικτυακής ασφάλειας του εμπορίου, μπορούν επίσης να δώσουν στους χρήστες έλεγχο πάνω στα cookies. Εξετάστε τα AdSubtract, InterMute (www.intermute.com), Luckman Interactive (www.cookiecentral.com), Guard Dog (www.mcafee.com), Norton Internet Security, Privacy Companion (www.idcide.com). Υπάρχουν και αρκετά ενδιαφέροντα δωρεάν εργαλεία γι’ αυτόν τον σκοπό, όπως το Pretty Good Privacy’s Cookie Cutter, το οποίο χρησιμοποιεί φίλτρα για να μπλοκάρει ή να επιτρέπει

cookies ανάλογα με τις επιθυμίες του χρήστη. Το Luckman’s Anonymous Cookie επιτρέπει σε χρήστες να ψάχνουν στο Παγκόσμιο Ιστό ανώνυμα. Το Cookie Crusher δέχεται ή απορρίπτει αυτόματα cookies από δικτυακούς τόπους που επιλέγει ο χρήστης.

Οποιοσδήποτε φυλλομετρητής υλοποιεί ***cookies*** θα πρέπει να παρέχει στους χρήστες τουλάχιστον τις ακόλουθες δυνατότητες*:*

• Την δυνατότητα να απενεργοποιήσουν πλήρως την αποστολή και αποθήκευση των ***cookies.***

• Μια ένδειξη (κατά προτίμηση οπτική) για το αν χρησιμοποιούνται ***cookies*** ή όχι την προκείμενη στιγμή..

• Ένα τρόπο ορισμού ενός συνόλου περιοχών ***(domains)*** για τις οποίες τα ***cookies*** θα πρέπει ή δεν θα πρέπει να αποθηκεύονται.

2.6.1 Cookies και ιδιωτικότητα.

Όπως αναφέρεται στο “Web Security, Privacy & Commerce” των Simson Garfinkel και Gene Spafford, τα cookies δημιουργήθηκαν αρχικά για να αποτελέσουν ένα μέρος αποθήκευσης στον υπολογιστή/πελάτη του χρήστη όπου οι εξυπηρετητές του Παγκόσμιου Ιστού θα μπορούσαν να αποθηκεύσουν τις προτιμήσεις του χρήστη και τις προσωπικές του πληροφορίες. Με αυτόν τον τρόπο καμία προσωπική πληροφορία δεν θα χρειαζόταν να αποθηκευτεί στον εξυπηρετητή. Σύντομα αφότου η εταιρεία Netscape παρουσίασε για πρώτη φορά τα cookies, οι ιδιοκτήτες των ιστοχώρων ανακάλυψαν μια ισχυρή και απρομελέτητη εφαρμογή της συγκεκριμένης τεχνολογίας: τον εντοπισμό των κινήσεων των χρηστών καθώς αυτοί εξερευνούν έναν ιστοχώρο ή καθώς μεταφέρονται από έναν ιστόχωρο σε έναν άλλο.

Σήμερα μια από τις δημοφιλέστερες εφαρμογές των cookies είναι να δίνουν έναν μοναδικό αριθμό αναγνώρισης σε κάθε χρήστη έτσι ώστε το

πλήθος των “μοναδικών επισκεπτών” ενός ιστοχώρου να μπορεί να μετρηθεί σωστά. Αυτοί οι αριθμοί μπορούν να είναι πολύ σημαντικοί όταν μια εταιρεία προσπαθεί να πουλήσει χώρο διαφήμισης στον ιστόχωρο της.

Πολλοί διαφημιστές χρησιμοποιούν τα cookies για να χτίσουν αναλυτικά προφίλ των χρηστών του Παγκόσμιου Ιστού. Αυτά τα cookies συνοδεύονται από διαφημίσεις. Κάθε φορά που ο χρήστης βλέπει μια διαφήμιση, ο κεντρικός υπολογιστής (όπου κρατούνται οι βάσεις δεδομένων) της διαφημιστικής εταιρείας σημειώνει τα περιεχόμενα της ιστοσελίδας που βλέπει ο χρήστης εκείνην την στιγμή. Αυτή η πληροφορία συνδυάζεται για να δημιουργηθεί ένα προφίλ (web profile). Ένα τέτοιο τυπικό προφίλ μπορεί να λέει πόσο ενδιαφέρεται κάποιος χρήστης για τα αθλητικά ή για τις οικιακές ηλεκτρονικές συσκευές ή πόσο ακολουθεί τα κοινωνικά και πολιτικά τεκταινόμενα. Οι διαφημιστές του Παγκόσμιου Ιστού μας πληροφορούν πως αυτά τα προφίλ είναι “ανώνυμα” γιατί δεν περιέχουν ονόματα, διευθύνσεις ή άλλα είδη προσωπικά αναγνωρίσιμων πληροφοριών. Ωστόσο είναι δυνατόν να ξεσκεπαστούν αυτά τα ανώνυμα δεδομένα αν συνδυαστούν με άλλες πληροφορίες, όπως οι διευθύνσεις IP (κάθε συνδεδεμένος στο Διαδίκτυο υπολογιστής αντιστοιχίζεται σε ένα μοναδικό δωδεκαψήφιο αριθμό που λέγεται διεύθυνση IP) ή πληροφορίες εγγραφής που παρέχονται στις ιστοσελίδες.

Τα cookies επιτρέπουν στους διαφημιστές να έχουν μεγάλο έλεγχο πάνω στις διαφημίσεις που βλέπει κάθε χρήστης, άσχετα από την συγκεκριμένη ιστοσελίδα που επισκέπτεται. Για παράδειγμα, χρησιμοποιώντας cookies κάποιος διαφημιστής μπορεί να εξασφαλίσει ότι κάθε χρήστης θα δει μια συγκεκριμένη διαφήμιση μόνο μία φορά (εκτός και αν έχει πληρώσει για επαναλαμβανόμενη έκθεση φυσικά). Τα cookies μπορούν να χρησιμοποιηθούν για να εμφανιστεί μια ακολουθία

απο διαφημίσεις σε ένα χρήστη, ακόμη και αν αυτός μετακινείται μεταξύ διαφορετικών ιστοσελίδων. Τα cookies επιτρέπουν την κατηγοριοποίηση των χρηστών με βάση τα ενδιαφέροντα τους.

Όλα τα cookies είναι ανοικτά προς εξέταση. Δυστυχώς, μπορεί να είναι πολύ δύσκολο να εξακριβωθεί για ποιόν ακριβώς λόγο χρησιμοποιείται κάποιο cookie με την απλή εξέταση του.

Τα cookies μπορούν να χρησιμοποιηθούν για να βελτιώσουν την ιδιωτικότητα αλλά και για να την αποδυναμώσουν. Δυστυχώς, είναι πολύ δύσκολο να εξακριβωθεί πότε κάποιο cookie χρησιμοποιείται για τον ένα σκοπό και πότε για τον άλλο.

Τα cookies μπορούν να αποδυναμώσουν σημαντικά την προσωπική ιδιωτικότητα όταν χρησιμοποιούνται για να συνθέσουν ένα σύνολο από φαινομενικά ασύνδετα γεγονότα και κομμάτια πληροφορίας απο διαφορετικούς ιστοχώρους για να δημιουργήσουν ένα ηλεκτρονικό δακτυλικό αποτύπωμα από τις ενέργειες ενός χρήστη στο διαδίκτυο. Τα cookies που χρησιμοποιούνται γι’ αυτόν τον σκοπό συνήθως περιέχουν ένα μμοναδικό αναγνωριστικό στοιχείο. Αυτό το στοιχείο αποτελεί κλειδί για μια βάση δεδομένων. Παράδειγμα ενός τέτοιου cookie αποτελεί το παρακάτω:

ad.doubleclick.net FALSE / FALSE 942191940 IAF 22348bb

Τα περισσότερα cookies είναι αυτού του είδους. Το μοναδικό κλειδί δείχνει προς μια βάση δεδομένων που την διαχειρίζεται ο ιστοχώρος, και έτσι αναγνωρίζεται ο χρήστης. Αυτή η βάση δεδομένων μπορεί να χρησιμοποιηθεί για να εντοπίζει συγκεκριμένους χρήστες για εκτεταμένες χρονικές περιόδους.

Ωστόσο όπως θα διαβάσετε στην αμέσως επόμενη υποενότητα, δεν λειτουργούν όλα τα cookies με αυτόν τον τρόπο.

2.6.1.1 Cookies που μπορούν να προστατεύσουν την ιδιωτικότητα.

Η τήρηση πληροφοριών για κάποιο χρήστη μέσα σε ένα cookie, αντί για μια βάση δεδομένων σε κάποιο web server, σημαίνει ότι δεν είναι απαραίτητη η παρακολούθηση των ενεργειών του χρήστη. Το ποιο σημαντικό ίσως είναι ότι δεν υπάρχει κάποια βάση δεδομένων με προσωπικές πληροφορίες που να πρέπει να προστατευθεί από εισβολές ή περίεργα μάτια.

Αυτό είναι ιδιαίτερα σημαντικό για τους διαχειριστές ιστοχώρων που ψάχνουν να βρουν τρόπους προσφοράς παραμετροποιήσιμων διεπαφών (interfaces) και εξατομικευμένης παράδοσης πληροφοριών. Με την χρήση των cookies, αυτές οι υπηρεσίες μπορούν να υλοποιηθούν χωρίς την αποθήκευση προσωπικής πληροφορίας για κάθε συνδρομητή.

Για την εξάλειψη της κεντρικής βάσης δεδομένων, είναι απαραίτητο να αποθηκευθούν οι προτιμήσεις των χρηστών μέσα στο ίδιο το cookie. Για παράδειγμα, μια ιστοσελίδα μπορεί να στείλει ένα cookie στο φυλλομετρητή ενός χρήστη που καταγράφει αν το συγκεκριμένο άτομο προτιμά να βλέπει τις ιστοσελίδες με κόκκινο ή μπλε φόντο.

Το cookie από τον ιστόχωρο της DigiCrime είναι ένα τέτοιου είδους cookie που προστατεύει την ιδιωτικότητα:

www.digicrime.com FALSE FALSE 942189160
DigiCrime virus=1

Αυτό το cookie καταγράφει πόσες φορές ο χρήστης επισκέφθηκε τον ιστόχωρο της Digicrime χωρίς να απαιτεί την δημιουργία μιας τεράστιας βάσης δεδομένων στην ίδια την ιστοσελίδα. Την πέμπτη φορά που ο

χρήστης θα επισκεφθεί τον συγκεκριμένο ιστόχωρο, το cookie θα αλλάξει στην εξής μορφή:

www.digicrime.com FALSE FALSE 942189160
DigiCrime virus=5

Διατηρώντας την πληροφορία για τον χρήστη σε ένα cookie, παρά σε μια βάση δεδομένων στον web server, σημαίνει ότι δεν είναι απαραίτητο να παρακολουθούνται οι κινήσεις του χρήστη· ο εξυπηρετητής μπορεί να είναι ουσιαστικά στατικός (stateless). Και δεν υπάρχει λόγος ανησυχίας για το αν θα σβηστούν αυτόματα παλιές εγγραφές από την βάση δεδομένων για τους χρήστες που μπήκαν στον ιστοχώρο έξι μήνες πριν και δεν ακούστηκαν ξανά από τότε.

Δυστυχώς, χρησιμοποιώντας cookies κατ' αυτόν τον τρόπο απαιτεί πολλή δουλειά και επίπονο προγραμματισμό . Είναι πολύ πιο απλό να εκσφενδονισθεί ένα cookie με ένα
μοναδικό αναγνωριστικό (συνήθως κάποιος κωδικός) στον φυλλομετρητή του χρήστη και μετά να συσχετισθεί αυτός ο κωδικός σε μια βάση δεδομένων στον εξυπηρετητή. Για παράδειγμα, είναι ευκολότερη η ανανέωση της πληροφορίας στην βάση γιατί δεν υπάρχει απαίτηση να μπορούν να διαβαστούν και να αποκρυπτογραφηθούν cookies με παλιά μορφή (format).

Οι ιστοχώροι που θα αποφασίσουν να αποθηκεύουν λεπτομερείς προσωπικές πληροφορίες μέσα στο ίδιο το αρχείο cookie –για να προστατεύσουν την ιδιωτικότητα των χρηστών– θα καταλήξουν να απαιτούν τεχνικές συμπίεσης δεδομένων για να αποτρέψουν την υπερβολική μεγέθυνση των cookies. Θα είναι σχεδόν αδύνατο να διαχωριστούν αυτά τα cookies από αυτά που παραβιάζουν την

ιδιωτικότητα συνδέοντας τον χρήστη σε μια μεγάλη βάση δεδομένων. Αυτό δεν είναι ένα αξεπέραστο πρόβλημα, αλλά δεν είναι και μικρό.

Κεφάλαιο 3

3.1. Υπηρεσίες Διαδικτύου

3.1.1. Ορισμός υπηρεσιών διαδικτύου

Μια υπηρεσία Web είναι μια μέθοδος επικοινωνίας μεταξύ δύο ηλεκτρονικών συσκευών μέσω του διαδικτύου. Μια υπηρεσία Web είναι μια λειτουργία λογισμικού που παρέχεται σε μια διεύθυνση δικτύου πάνω από το διαδίκτυο ή το νέφος (cloud), είναι μια υπηρεσία που είναι "always on" όπως στην έννοια της υπολογιστικής χρησιμότητας.

Το W3C (World Wide Web Concortium) ορίζει μια "υπηρεσία Web" ως "ένα σύστημα λογισμικού που έχει σχεδιαστεί για τη στήριξη διαλειτουργικών αλληλεπιδράσεων μηχανής-προς-μηχανή μέσω δικτύου". Έχει μια διεπαφή που περιγράφεται με ένα format επεξεργάσιμο από μηχανή (πιο συγκεκριμένα την Web Services Description Language, που είναι γνωστή με το ακρωνύμιο WSDL). Άλλα συστήματα αλληλεπιδρούν με την υπηρεσία Web με έναν τρόπο που προβλέπεται από την περιγραφή του, χρησιμοποιώντας μηνύματα SOAP (Simple Object Access Protocol), τα οποία συνήθως μεταφέρονται μέσω του πρωτοκόλλου HTTP.

Οι "Μεγάλες υπηρεσίες Web" χρησιμοποιούν Extensible Markup Language (XML) μηνύματα που ακολουθούν το πρότυπο SOAP και ήταν δημοφιλής με τις παραδοσιακές επιχειρήσεις. Σε τέτοια συστήματα, υπάρχει συχνά μια περιγραφή εργασιών, ή οποία είναι εύκολα αναγνώσιμη από μηχανές, γραμμένη στη γλώσσα Web Services Description Language (WSDL).

3.1.2. Πρωτόκολλα για υπηρεσίες διαδικτύου

Αυτοματοποιημένα εργαλεία μπορούν να βοηθήσουν στη δημιουργία μιας υπηρεσίας Web. Για υπηρεσίες που χρησιμοποιούν WSDL είναι δυνατό να δημιουργήθούν αυτόματα είτε WSDL για τις υπάρχουσες κατηγορίες (από κάτω προς τα επάνω στρατηγική) είτε να δημιουργηθεί ένας σκελετός, δεδομένου του υπάρχοντος WSDL (από πάνω προς τα κάτω στρατηγική).

Ένας προγραμματιστής χρησιμοποιώντας μια μέθοδο από κάτω προς τα πάνω γράφει την εφαρμογή (σε κάποια γλώσσα προγραμματισμού), και στη συνέχεια χρησιμοποιεί ένα εργαλείο δημιουργίας WSDL για να εκθέσει τις μεθόδους από αυτές τις κατηγορίες ως μια υπηρεσία Web.

Αυτό είναι συχνά η πιο απλή προσέγγιση. Ένας προγραμματιστής χρησιμοποιώντας μια μέθοδο πάνω προς τα κάτω γράφει το έγγραφο WSDL και στη συνέχεια χρησιμοποιεί ένα εργαλείο παραγωγής κώδικα για την παραγωγή του σκελετού, που θα ολοκληρωθεί. Με αυτό τον τρόπο είναι γενικά θεωρείται πιο δύσκολη, αλλά μπορεί να παράγει καθαρότερα σχέδια.

SOAP, που αρχικά ορίζεται ως απλό πρωτόκολλο πρόσβασης αντικειμένου, είναι μια προδιαγραφή πρωτόκολλου για την ανταλλαγή δομημένης πληροφορίας για την εφαρμογή των Υπηρεσιών του Παγκοσμίου Ιστού σε δίκτυα υπολογιστών. Στηρίζεται στην Extensible Markup Language (XML) για τη μορφή του μηνύματος, και συνήθως βασίζεται σε άλλα πρωτόκολλα επιπέδου εφαρμογής, κυρίως Hypertext Transfer Protocol (HTTP) ή Simple Mail Transfer Protocol (SMTP), για τη διαπραγμάτευση και τη μετάδοση μηνυμάτων.

Η Web Services Description Language είναι βασισμένη σε XML γλώσσα περιγραφής διεπαφής που χρησιμοποιείται για την περιγραφή της λειτουργικότητας που προσφέρει μια υπηρεσία web. Μια περιγραφή WSDL της υπηρεσίας web (που αναφέρεται επίσης ως ένα αρχείο WSDL) παρέχει μια αναγνώσιμη από μηχάνημα περιγραφή για το πώς η υπηρεσία μπορεί να κληθεί, τι αναμένει από τις παραμέτρους, και τι δομές δεδομένων επιστρέφει. Εξυπηρετεί έτσι ένα κατά προσέγγιση παρόμοιο σκοπό, ως μια μέθοδος υπογραφής σε μια γλώσσα προγραμματισμού.

3.1.3. Υπηρεσίες διαδικτύου στην καθημερινότητά μας

Στην καθημερινή μας διαδικτυακή ζωή μπορούμε να εντοπίσουμε πολλές υπηρεσίες διαδικτύου που χρησιμοποιούμε κατά κόρον. Αρχικά το e-mail μας είναι η νούμερο ένα υπηρεσία καθώς η επικοινωνίας μας

διαδικτυακά εξαρτάται από αυτό. Οι υπηρεσίες κοινωνικής δικτύωσης όπως το facebook και το twitter αποτελούν κύρια ασχολία των νέων στον ελεύθερο τους ή μη χρόνο. Ακόμα όμως και υπηρεσίες όπως η online παραγγελία φαγητού έχουν κάνει αισθητή την παρουσία τους στον ελληνικό ιστοχώρο. Όμως πως διασφαλίζεται η ιδιωτικότητα του κάθε χρήστη σε καθεμία από τις υπηρεσίες αυτές;

Όλες οι εταιρίες παροχής υπηρεσιών διαδικτύου είναι υποχρεωμένες βάσει νόμου για την κατοχύρωση της πολιτικής ιδιωτικότητάς του. Πρέπει δηλαδή να παρέχεται σαφής πληροφορία για το ποιες είναι οι ενέργειες και οι μηχανισμοί που χρησιμοποιούν για να προστατεύσουν την ασφάλεια και την ιδιωτικότητα των χρηστών που χρησιμοποιούν τις υπηρεσίες αυτές.

Παρακάτω εναποθέτουμε ένα παράδειγμα πολιτικής απορρήτου (ιδιωτικότητας), όπως αυτή αναφέρεται ξεκάθαρα στην εταιρία clickdelivery.gr, η οποία παρέχει υπηρεσίες διαδικτυακής παραγγελίας φαγητού.

Πολιτική Απορρήτου (www.clickdelivery.gr)

3.2. Υπηρεσίες διαδικτύου του κλάδου

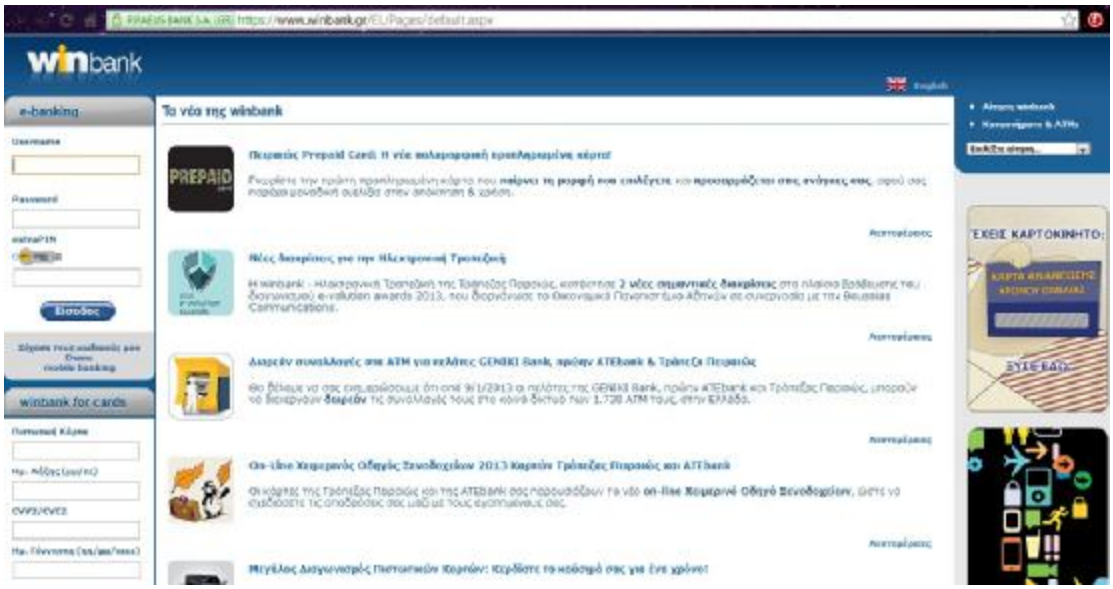
Στον κλάδο της λογιστικής, καθημερινά χρησιμοποιούμε κρατικές υπηρεσίες διαδικτύου για την εύκολη εξυπηρέτηση μας και των πελατών μας, καθώς και διαδικτυακές υπηρεσίες που παρέχονται από τις τράπεζες με τις οποίες συναλλασσόμαστε.

3.2.1. Γενική γραμματεία πληροφοριακών συστημάτων (www.gsis.gr)

Στην ιστοσελίδα της Γενικής γραμματείας πληροφοριακών συστημάτων ο χρήστης μπορεί να βρει πληροφορίες σχετικά με τη φορολογική του δήλωση (κατάθεση, έκδοση εκκαθαριστικού σημειώματος, κλπ) ή για τα τέλη κυκλοφορίας του οχήματός του (έκδοση), κλπ. Τα στοιχεία του χρήστη που υπάρχουν αποθηκευμένα στη Βάση Δεδομένων του αντίστοιχου Υπουργείου αποτελούν ευαίσθητα προσωπικά δεδομένα και πρέπει να διασφαλίζεται η ασφάλεια τους και επομένως η ιδιωτικότητα του κάθε χρήστη.

3.2.2. Ασφάλεια συναλλαγών Τράπεζας Πειραιώς

Η Τράπεζα Πειραιώς στο ενημερωτικό της φυλλάδιο αναφέρει εκτενώς την πολιτική απορρήτου που χρησιμοποιεί και ενημερώνει τους πελάτες της για την σωστή χρήση των υπηρεσιών διαδικτύου που παρέχει ώστε να διασφαλίζεται η ιδιωτικότητα του κάθε χρήστη. Παρακάτω εναποθέτουμε ένα απόσπασμα της πολιτικής της τράπεζας ως προς την ασφάλεια των συναλλαγών στο διαδίκτυο.



“Η winbank αναγνωρίζει τη σημασία της κατοχύρωσης της ασφάλειας των συναλλαγών και της διασφάλισης του απορρήτου των προσωπικών σας στοιχείων και των τραπεζικών σας πληροφοριών. Γι’ αυτό χρησιμοποιεί τις πιο σύγχρονες και αυστηρές μεθόδους ασφάλειας τόσο από άποψη τεχνολογιών, όσο και διαδικασιών και οργάνωσης. Ειδικότερα:

Αναγνώριση και πιστοποίηση πελάτη

Σε όλες τις υπηρεσίες έχετε προσωπικούς κωδικούς για την αναγνώρισή σας πριν τη χρήση της κάθε υπηρεσίας. Πρόκειται για τον Κωδικό Εισόδου (User ID) και τον Κωδικό Ασφαλείας (PIN) που θα σας δοθούν στο κατάστημα ή θα σας αποσταλούν με courier κατά την εγγραφή σας.

- Η αλλαγή τους είναι υποχρεωτική την πρώτη φορά που θα συνδεθείτε.
- Τους κωδικούς αυτούς μπορείτε να τους αλλάζετε όσο συχνά θέλετε.

- Η αλλαγή PIN είναι υποχρεωτική κάθε δύο μήνες (Το PIN είναι αλφαριθμητικό και ευαίσθητο προσωπικό δεδομένο).
- Μετά από τρεις λανθασμένες προσπάθειες εισαγωγής τους δεν επιτρέπεται η πρόσβαση στις υπηρεσίες.

Στην υπηρεσία SMS banking γίνεται πιστοποίηση του αριθμού του κινητού σας τηλεφώνου και οι συναλλαγές εκτελούνται μόνο στον αριθμό αυτό.

Εξασφάλιση του Απορρήτου της Μεταφοράς των Δεδομένων

Στην υπηρεσία Winbank χρησιμοποιείται ασφαλής σύνδεση και κρυπτογράφηση με βάση το πρωτόκολλο κρυπτογράφησης SSL-128bits, την τελευταία λέξη της τεχνολογίας στον τομέα της κρυπτογράφησης.
Επιπλέον, για την εκτέλεση των συγκεκριμένων συναλλαγών, η χρήση του κωδικού extraPIN ανήκει στην κατηγορία “one time password” και επιτρέπει την εφαρμογή της μεθόδου ταυτοποίησης “two factor authentication”. Τον κωδικό extraPIN τον λαμβάνετε ως γραπτό μήνυμα sms στον αριθμό του κινητού τηλεφώνου που θα μας δηλώσετε ή από την ειδική συσκευή παραγωγής κωδικών μία χρήσης extraPIN generator. Κωδικό extraPIN θα χρειαστείτε και για τις συναλλαγές σας μέσω της υπηρεσίας Πειραιώς phone banking.

Αυτόματη Αποσύνδεση

Εάν δεν υπάρξει καμία δραστηριότητα για εφτά λεπτά γίνεται αυτόματη αποσύνδεση από την υπηρεσία Winbank. Για τη δική σας εξυπηρέτηση δημιουργήσαμε τη δυνατότητα ελέγχου και ανανέωσης του χρόνου παραμονής σας στην υπηρεσία ώστε να μην αποσυνδεθείτε από την

υπηρεσία εφόσον δεν το επιθυμείτε και να ολοκληρώσετε τις συναλλαγές σας.

TIP: Μην κοινοποιείτε σε τρίτους τους Κωδικούς Εισόδου και Ασφαλείας. Είναι αυστηρά προσωπικοί και απόρρητοι. Δεν θα σας ζητηθεί ΠΟΤΕ, ούτε από την Τράπεζα Πειραιώς, να αποκαλύψετε τον Κωδικό Ασφαλείας (PIN).
Μην ενεργοποιήσετε τη δυνατότητα να "θυμάται" τους κωδικούς πρόσβασης στο φυλλομετρητή του υπολογιστή σας.
Αλλάζετε τον Κωδικό Ασφαλείας (PIN) ανά τακτά χρονικά διαστήματα και αποφεύγετε κωδικούς που εύκολα μπορεί να μαντέψει κάποιος, π.χ. ημερομηνία γέννησης, αριθμούς τηλεφώνων κλπ.
Μη σημειώνετε τους Κωδικούς Ασφαλείας σε χαρτί, αρχεία υπολογιστών ή σε μηνύματα στο κινητό σας τηλέφωνο.
Εξασφαλίστε ότι η πρόσβαση στον υπολογιστή σας ή στο κινητό σας τηλέφωνο από τρίτους δεν πρόκειται να επηρεάσει τη χρήση των υπηρεσιών της winbank ή να μετριάσει το βαθμό ασφάλειάς τους. Όταν χρησιμοποιείτε τις υπηρεσίες από το γραφείο σας ή από ηλεκτρονικούς υπολογιστές κοινής χρήσης ή από το εξωτερικό φροντίστε ώστε οι κωδικοί σας να παραμείνουν μακριά από βλέμματα τρίτων και να αποσυνδέεστε από τις υπηρεσίες όταν απομακρύνεστε από τον Η/Υ σας."

3.2.3. Υπηρεσία ηλεκτρονικού ταχυδρομείου (e-mail)

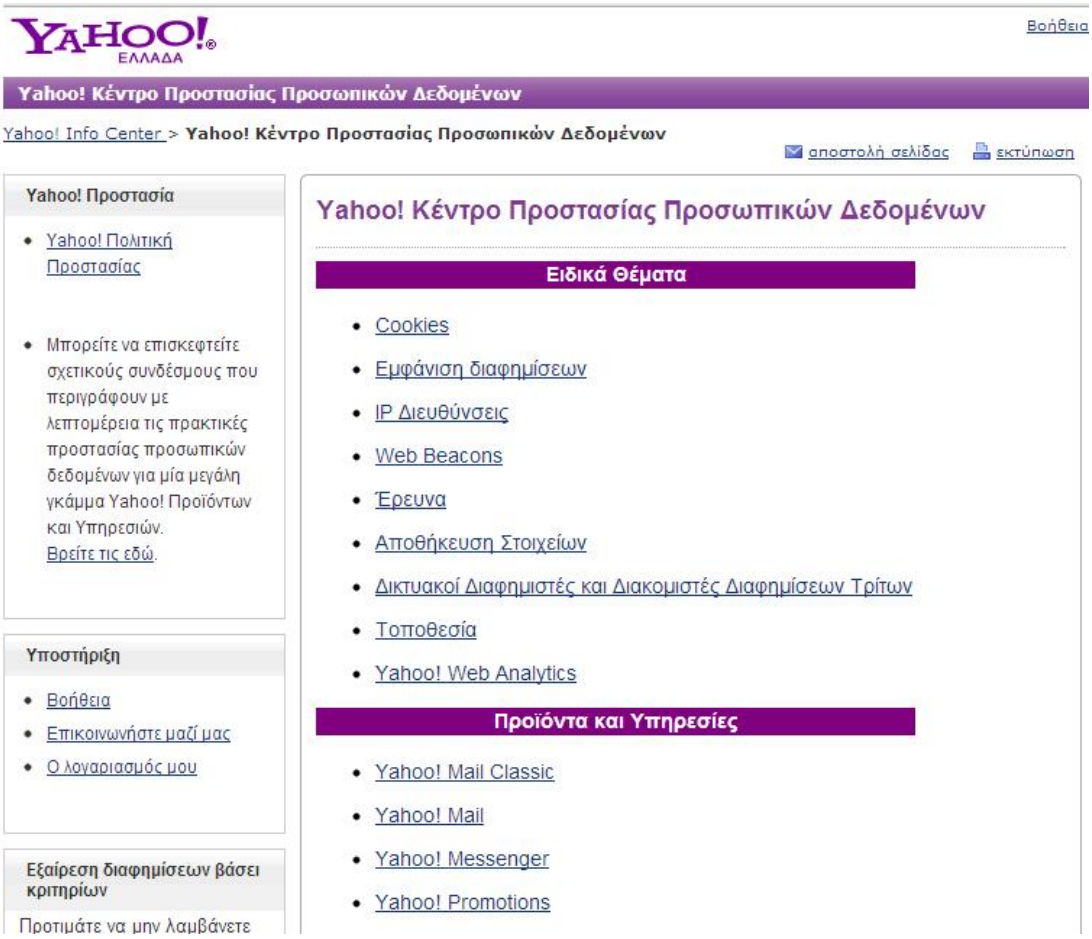
Για όλες τις παραπάνω υπηρεσίες κύρια προϋπόθεση αποτελεί η ύπαρξη και χρήση ηλεκτρονικού ταχυδρομείου του κάθε χρήστη. Οι περισσότερες υπηρεσίες διαδικτύου απαιτούν από τον εκάστοτε χρήστη το λογαριασμό του ηλεκτρονικού του ταχυδρομείου, ώστε να

επιβεβαιώσουν τη φυσική ύπαρξη του προσώπου, αλλά και για την αποστολή ενημερωτικών δελτίων για νέες υπηρεσίες, κλπ.

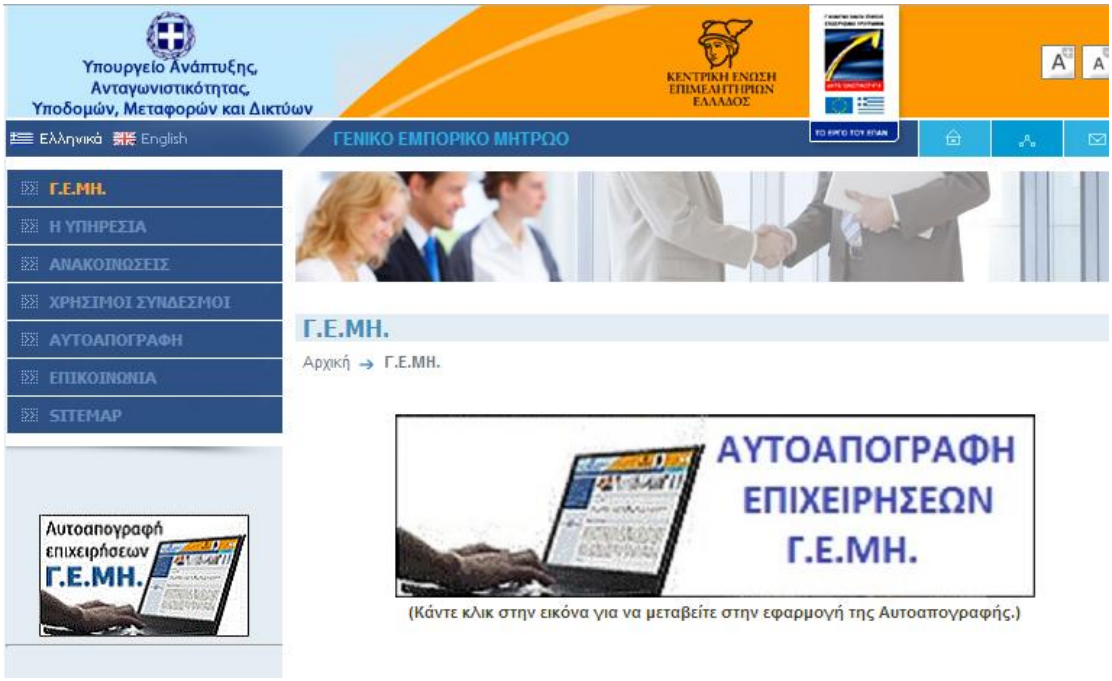
Επομένως, και το ηλεκτρονικό ταχυδρομείο αποτελεί βασική υπηρεσία διαδικτύου και ιδιαίτερα στον κλάδο της λογιστικής, όπου η επικοινωνία και η αποστολή αρχείων με ευαίσθητα προσωπικά δεδομένα είναι καθημερινή.

Πάροχοι υπηρεσιών ηλεκτρονικού ταχυδρομείου, όπως ή Google ή η Yahoo στον διαδικτυακό τους ιστοχώρο έχουν μεγάλες αναφορές σχετικά με την προστασία των προσωπικών δεδομένων των χρηστών τους.

Παρακάτω εναποθέτουμε την κεντρική σελίδα της Yahoo για την προστασία των προσωπικών δεδομένων.



3.2.4. Γενικό Εμπορικό Μητρώο



Σκοπός του παρόντος έργου είναι η υλοποίηση του Γ.Ε.ΜΗ. με βασικό στόχο την ηλεκτρονικοποίηση και αυτοματοποίηση των διαδικασιών εγγραφής και παρακολούθησης των εμπορικών επιχειρήσεων.

Η ανάγκη συγκρότησης ενός ενιαίου πλαισίου οργάνωσης, ενημέρωσης και χρήσης των μητρώων της δημόσιας διοίκησης αποτελούσε ανέκαθεν πάγια απαίτηση των συναλλασσόμενων με τους φορείς του δημόσιου και ευρύτερου δημόσιου τομέα. Ιδιαίτερα για την επιχειρηματική κοινότητα, οι επικαλύψεις στοιχείων, τα προβλήματα στην ονοματολογία, οι διαφορετικές κωδικοποιήσεις, η αποσπασματική συγκέντρωση στοιχείων από φορείς, η έλλειψη στοιχείων ιστορικότητας επιχειρήσεων κ.λ.π., αποτελούσαν μερικά μόνο από τα προβλήματα τα οποία αντιμετώπιζε, με αποτέλεσμα να παρατηρούνται προβλήματα στις διαδικασίες του γενικότερου επιχειρείν.

Για όλους αυτούς τους λόγους, ήταν πάγιο αίτημα του εμπορικού κόσμου της χώρας εδώ και πολλά χρόνια η δημιουργία ενός ενιαίου εμπορικού μητρώου. Είναι ευρέως αποδεκτό ότι η δημιουργία ενός Γενικού Εμπορικού Μητρώου (Γ.Ε.ΜΗ.) όλων των νομικών μορφών επιχειρήσεων στην Ελλάδα θα βοηθήσει στην παρακολούθηση των εμπορικών επιχειρήσεων από την πολιτεία και την καλύτερη εξυπηρέτηση των ίδιων των επιχειρήσεων από την κεντρική διοίκηση και τους αρμόδιους φορείς της.

3.2.5. ΙΚΑ (Ενιαίο Ταμείο Ασφάλισης Μισθωτών)

Ηλεκτρονικές Υπηρεσίες προς Εργοδότες

Ηλεκτρονική Υποβολή Α.Π.Δ.

Μαζική Ταυτοποίηση Ασφαλισμένων

Βεβαίωση Ασφαλιστικής Ενημερότητας
Ηλεκτρονική Έκδοση Ατομικού Λογαριασμού Ασφάλισης
Βοήθεια Εργοδοτών

Ηλεκτρονικές Υπηρεσίες προς Ασφαλισμένους / Συνταξιούχους :

Πιστοποίηση Ασφαλισμένου
Ατομικός Λογαριασμός Ασφάλισης
(Απόσπασμα Ατομικού Λογαριασμού Ασφάλισης)
Ηλεκτρονική Υποβολή Αίτησης Συνταξιοδότησης
Ηλεκτρονική Παρακολούθηση της Πορείας της Αίτησης Συνταξιοδότησης
Οδηγός Θεμελίωσης Συνταξιοδοτικού Δικαιώματος
Εργαλείο Υπολογισμός Βασικού Ποσού Σύνταξης

Ηλεκτρονικές Υπηρεσίες προς Πιστοποιημένους Φορείς:

Πιστοποίηση Φορέων για Ασφαλιστική Ενημερότητα
Λήψη Ασφαλιστικής Ενημερότητας
Επιβεβαίωση Εγκυρότητας Ασφαλιστικής Ενημερότητας
Βεβαιώσεις που εκδόθηκαν έως 9/1/2012
Βεβαιώσεις που εκδόθηκαν από 10/1/2012 και μετά
Εγχειρίδια Χρήσης για τη Λήψη Βεβαιώσεων Ασφαλιστικής Ενημερότητας
για τη Διαχείριση Χρηστών Πιστοποιημένου Φορέα

Ηλεκτρονικές Υπηρεσίες προς Παρόχους Προγράμματος Κατ' Οίκον Φροντίδας Συνταξιούχων :

Αίτηση συμμετοχής υποψηφίου παρόχου στο Πρόγραμμα - Δήλωση Στοιχείων

Πιστοποίηση Παρόχων για το Πρόγραμμα Κατ΄Οίκον Φροντίδας Συνταξιούχων

Παροχή Υπηρεσιών κατ' Οίκον Φροντίδας Συνταξιούχων

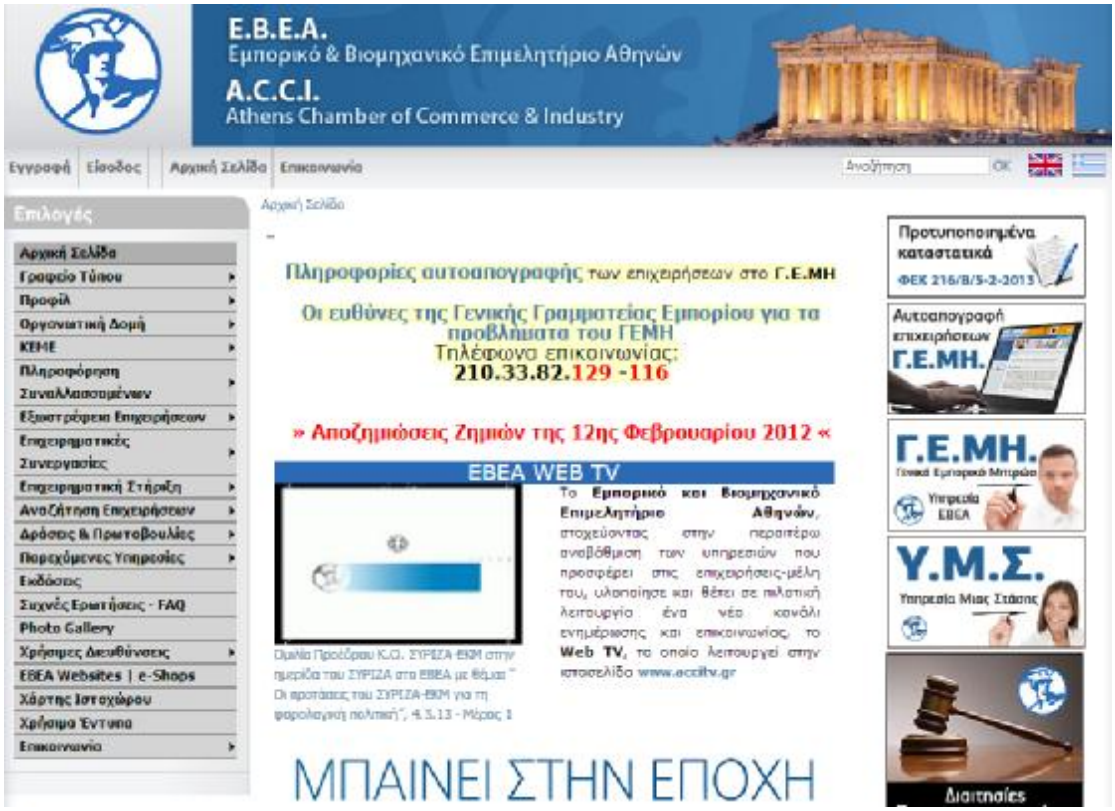
ενημερωση σχετικα με τα προγραμματα επιδοτησης του οαεδ για νεους , ανεργους , επιχειρησεις

3.2.6. Οργανισμός Απασχόλησης Εργατικού Δυναμικού (Ο.Α.Ε.Δ.)

Παραπομπή από τον ιστοχώρο του ΟΑΕΔ στον ιστοχώρο του υπουργείου εργασίας:

Όπου γνωστοποιούμε τις προσλήψεις, τις απολύσεις, την όποια τροποποίηση σε σύμβαση (αλλαγή ωραρίου, ορισμένου – αορίστου χρόνου, κλπ.), καταστάσεις προσωπικού επιχείρησης, κ.ά.

3.2.7. Εμπορικό & Βιομηχανικό Επιμελητήριο Αθηνών



Όπως αναφέρεται και στον ιστοχώρο του, το Εμπορικό και Βιομηχανικό Επιμελητήριο Αθηνών οι επιχειρήσεις, οι οποίες εγγράφονται σε αυτό βρίσκονται στις παρακάτω κατηγορίες:

Αεροπορικές Εταιρίες

Παλαιοπώλεις – Ενεχυροδανειστές

Βιομηχανία

Γραφεία τουρισμού και εκμίσθωσης επιβατικών αυτοκινήτων

Εμπορικός αντιπρόσωπος επιχειρήσεων εξωτερικού

Εμπόριο όπλων – πυρομαχικών και εκρηκτικών

Εμπόριο οπτικών

Εξαγωγικό εμπόριο

Επιχείρηση παροχής υπηρεσιών ασφάλειας

Ιδιωτικό γραφείο συμβούλου εργασίας

Ιδιωτικό εκπαιδευτήριο – Κέντρο ξένων γλωσσών

Ιδιωτικό ΙΕΚ

Κατάστημα υγειονομικού ενδιαφέροντος

Κολλέγιο – Εργαστήριο ελευθέρων σπουδών

Οδική βοήθεια οχημάτων

Παραγωγή ηλεκτρικής ενέργειας και ανανεώσιμων πηγών ενέργειας

Παροχή υπηρεσιών υγείας

Ταχυμεταφορές

Τηλεοπτικές παραγωγές

Τραπεζικές συναλλαγές – χρηματιστηριακές

Φαρμακαποθήκη και εμπόριο φαρμάκων – ιδιοσκευασμάτων

3.3. Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα είναι το εκτελεστικό όργανο του κράτους για την πάταξη και τη συμμόρφωση όλων των παρόχων υπηρεσιών διαδικτύου στην Ελλάδα με το νομοθετικό πλαίσιο που υπάρχει, σχετικά με την προστασία της ιδιωτικότητας των χρηστών.

“Η προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής αποτελεί θεμελιώδες ανθρώπινο δικαίωμα. Ο νόμος παρέχει ορισμένα δικαιώματα στα φυσικά πρόσωπα (τα υποκείμενα των δεδομένων) και θέτει συγκεκριμένες υποχρεώσεις σε όσους τηρούν και επεξεργάζονται προσωπικά δεδομένα (τους υπευθύνους επεξεργασίας).

Στη σελίδα μας μπορείτε να βρείτε πληροφορίες για το θεσμικό πλαίσιο της προστασίας των προσωπικών δεδομένων στην Ελλάδα και στην Ευρώπη, καθώς επίσης και σχετικές αποφάσεις και γνωμοδοτήσεις, ετήσιες εκθέσεις πεπραγμένων και δελτία Τύπου της Αρχής.

Μπορείτε να εγγραφείτε στο site μας και να κάνετε χρήση των ηλεκτρονικών υπηρεσιών της Αρχής για πολίτες και για υπεύθυνους επεξεργασίας (ηλεκτρονική υποβολή ερωτημάτων, καταγγελιών και

γνωστοποιήσεων, εγγραφή στη λίστα του άρθρου 13, λήψη της λίστας άρθρου 13)", αναφέρει το μήνυμα που καλωσορίζει το χρήστη στην ιστοσελίδα.

Στην σελίδα, ο χρήστης μπορεί να βρει τις ετήσιες εκθέσεις της Αρχής σχετικά με τη δράση της. Επίσης, ο χρήστης μπορεί να ενημερωθεί για τα δικαιώματά του ως πολίτη, αλλά και τι ορίζει η νομοθεσία του κράτους για τη διασφάλιση της ιδιωτικότητάς του.

Κάθε πολίτης μπορεί να απευθυνθεί στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα για να προσφύγει εναντίον κάποιου που είναι αντίθετος με τους νόμους και του κανόνες που ορίζει το κράτος σε ζητήματα ιδιωτικότητας και διασφάλισης της προστασίας των προσωπικών δεδομένων (ευαίσθητων ή μη).

3.4. Δίωξη Ηλεκτρονικού Εγκλήματος

Η αποστολή της Υποδιεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος συμπεριλαμβάνει την πρόληψη, την έρευνα και την καταστολή εγκλημάτων ή αντικοινωνικών συμπεριφορών, που διαπράττονται μέσω του διαδικτύου ή άλλων μέσων ηλεκτρονικής επικοινωνίας.

Η Δίωξη Ηλεκτρονικού Εγκλήματος, στην εσωτερική της δομή, αποτελείται από τέσσερα τμήματα που συμπληρώνουν όλο το φάσμα προστασίας του χρήστη και ασφάλειας του Κυβερνοχώρου. Έτσι, στη νέα αναβαθμισμένη δομή της αποτελείται από:

Το Τμήμα Γενικών Υποθέσεων και Προστασίας Προσωπικών Δεδομένων που ασχολείται με τις εγκληματικές πράξεις που διαπράττονται στα μέσα ηλεκτρονικής επικοινωνίας και ψηφιακής αποθήκευσης ή μέσω αυτών σε ολόκληρη τη χώρα.

Το Τμήμα Προστασίας Ανηλίκων που ασχολείται με τα εγκλήματα που διαπράττονται κατά των ανηλίκων με τη χρήση του διαδικτύου και των άλλων μέσων ηλεκτρονικής ή ψηφιακής επικοινωνίας και αποθήκευσης.

Το Τμήμα Προστασίας Λογισμικού και Πνευματικών Δικαιωμάτων που ασχολείται με τις υποθέσεις παράνομης διείσδυσης σε υπολογιστικά συστήματα και κλοπής, καταστροφής ή παράνομης διακίνησης λογισμικού υλικού, ψηφιακών δεδομένων και οπτικοακουστικών έργων, που τελούνται σε ολόκληρη τη χώρα.

Το Τμήμα Ασφάλειας Ηλεκτρονικών Επικοινωνιών, που ασχολείται με την πρόληψη και καταστολή εγκλημάτων παραβίασης του απορρήτου των ηλεκτρονικών επικοινωνιών.

Η Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος υπάγεται στην Υπηρεσία Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος και συνιστά μία από τις νεοσύστατες υπηρεσίες της Ελληνικής Αστυνομίας.

Παρακάτω παραθέτουμε κάποια δελτία τύπου της Υποδιεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος από την Δράση της το τελευταίο τρίμηνο και τις επιτυχείς συλλήψεις δραστών για εγκληματικές πράξεις μέσω διαδικτύου.

“Αθήνα, 13 Δεκεμβρίου 2012

ΔΕΛΤΙΟ ΤΥΠΟΥ

Με επιτυχία πραγματοποιήθηκε από τη Δίωξη Ηλεκτρονικού Εγκλήματος ημερίδα, μέσω τηλεδιάσκεψης σε σχολεία της χώρας

Με ιδιαίτερη επιτυχία πραγματοποιήθηκε σήμερα (13-12-2012), από την Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, ημερίδα μέσω τηλεδιάσκεψης σε δέκα (10) σχολεία της χώρας.

Η ημερίδα πραγματοποιήθηκε μετά από πρωτοβουλία του Υπουργείου Δημοσίας Τάξης και Προστασίας του Πολίτη και της Υπηρεσίας Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος, στο πλαίσιο ενημέρωσης και ευαισθητοποίησης των παιδιών, σχετικά με την ασφάλεια στο διαδίκτυο.

Κύριος στόχος των τηλεδιασκέψεων, είναι να ευαισθητοποιηθούν τα παιδιά, ηλικίας από 5 έως 18 ετών, για τους κινδύνους που κρύβει το διαδίκτυο, να μάθουν περισσότερα για τους τρόπους αντιμετώπισης των προκλήσεων του ψηφιακού κόσμου και να προσαρμοστούν στα νέα δεδομένα.

Μέσα από τη διαδραστική συμμετοχή τους τα παιδιά, ενημερώθηκαν από τον Προϊστάμενο της Δίωξης Ηλεκτρονικού Εγκλήματος, Αστυνομικό Διευθυντή Εμμανουήλ Σφακιανάκη, αλλά και εξειδικευμένους Αξιωματικούς, τόσο για την ασφάλεια στο Διαδίκτυο, όσο και για τους κινδύνους που ελλοχεύουν κατά τη πλοήγησή τους σε αυτό.

Κατά τη διάρκεια της τηλεδιάσκεψης, την οποία παρακολούθησαν και στην οποία συμμετείχαν περίπου -600- μαθητές, έγινε σύνδεση με τα ακόλουθα σχολεία:

Γενικό Λύκειο Ζωσιμαίας Σχολής Ιωαννίνων

1ο Γυμνάσιο Ν. Ηρακλείου Αττικής

3ο Γυμνάσιο Ν. Σμύρνης

5ο Γυμνάσιο Ν. Σμύρνης

1ο Γενικό Λύκειο Πτολεμαΐδας

4ο Γενικό Λύκειο Λαμίας

1ο Γυμνάσιο Κοζάνης

Ιδιωτικό Γυμνάσιο "Σύγχρονα Εκπαιδευτήρια Μάνεση"

Γενικό Λύκειο Ελευθερίου Βενιζέλου Χανίων

3ο Γυμνάσιο Τρίπολης

Ο Προϊστάμενος της Δίωξης Ηλεκτρονικού Εγκλήματος, μαζί με τους συνεργάτες του, συνομίλησαν διαδραστικά με τους μαθητές και τους καθηγητές και αναφέρθηκαν κυρίως:

στο σκοπό διοργάνωσης των τηλεδιασκέψεων για την ασφαλή πλοήγηση στο διαδίκτυο,

στην αποστολή της Υποδιεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος,

στα αδικήματα και στον τρόπο που αυτά διαπράττονται μέσω διαδικτύου, καθώς και σε πρακτικές πρόληψης,

σε στατιστικά στοιχεία, που αφορούν τη διείσδυση των Ελλήνων στο διαδίκτυο και τις υποθέσεις που καλείται να αντιμετωπίσει η Δίωξη Ηλεκτρονικού Εγκλήματος με συγκεκριμένα παραδείγματα και περιστατικά.

Σημειώνεται ότι η συγκεκριμένη πρωτοβουλία υποστηρίζεται από την εταιρεία Vodafone και περιλαμβάνει τη νέα υπηρεσία Microsoft 365.

Αθήνα, 29 Δεκεμβρίου 2012

ΔΕΛΤΙΟ ΤΥΠΟΥ

Συνελήφθη από τη Δίωξη Ηλεκτρονικού Εγκλήματος 47χρονος ημεδαπός ο οποίος κατείχε παράνομα και διέθετε προς πώληση πάνω από

2.000.000 εγγραφές δεδομένων προσωπικού χαρακτήρα, σε ψηφιακά αρχεία

Συνελήφθη χθες (28-12-2012) το μεσημέρι σε προάστιο της Αττικής, από αστυνομικούς της Υπηρεσίας Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος, 47χρονος αλλοδαπός, υπήκοος Ουκρανίας, γιατί κατείχε και διέθετε προς πώληση πάνω από 2.000.000 εγγραφές δεδομένων προσωπικού χαρακτήρα (διευθύνσεις ηλεκτρονικού ταχυδρομείου - emails) σε ψηφιακά αρχεία .

Όπως προέκυψε, ο δράστης κατείχε και διέθετε τα αρχεία αυτά χωρίς να έχει υποβάλλει την προβλεπόμενη γνωστοποίηση στην αρμόδια Αρχή, ως όφειλε.

Προηγήθηκε καταγγελία ιδιώτη σχετικά με αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου στην θυρίδα του, τα οποία προέτρεπαν στην αγορά υπηρεσίας μαζικής αποστολής διαφημιστικών μηνυμάτων ηλεκτρονικού ταχυδρομείου, έναντι αμοιβής.

Στο πλαίσιο προκαταρκτικής εξέτασης, που πραγματοποιήθηκε μετά από σχετική εισαγγελική παραγγελία, διενεργήθηκε μεθοδική ψηφιακή έρευνα από τη Δίωξη Ηλεκτρονικού Εγκλήματος και ταυτοποιήθηκε ο 47χρονος ως ο αποστολέας των επίμαχων μηνυμάτων.

Σε έρευνα που πραγματοποίησαν αστυνομικοί της Δίωξης Ηλεκτρονικού Εγκλήματος, με τη συμμετοχή ειδικών επιστημόνων της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, σε κατάστημα που διατηρεί ο δράστης στο κέντρο της Αθήνας, βρέθηκαν και κατασχέθηκαν πέντε (5) εσωτερικοί σκληροί δίσκοι χωρητικότητας 250, 300, 1000, 15000 και 1500 GB αντίστοιχα.

Ο συλληφθείς με την εις βάρος του σχηματισθείσα δικογραφία οδηγήθηκε στον κ. Εισαγγελέα Πρωτοδικών Αθηνών.

Αθήνα, 8 Ιανουαρίου 2013

ΔΕΛΤΙΟ ΤΥΠΟΥ

Αστυνομική επιχείρηση και έρευνα της Υπηρεσίας Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος σε εταιρεία, που κατείχε παράνομα μεγάλο όγκο προσωπικών δεδομένων φυσικών και νομικών προσώπων

Σε τρεις διακομιστές (servers) της εταιρείας, εντοπίστηκε ψηφιακή βάση δεδομένων με πάνω από 67 εκατομμύρια εγγραφές και καταχωρήσεις δεδομένων προσωπικού χαρακτήρα, όπως ονοματεπώνυμα, διευθύνσεις κατοικίας, στοιχεία οχημάτων και ιδιοκτητών, αριθμοί τηλεφώνων, φορολογικά στοιχεία κ.ά.

Συνελήφθη με την αυτόφωρη διαδικασία, ο Γενικός Διευθυντής της εταιρείας, ενώ αναζητούνται ο Πρόεδρος - Διευθύνων Σύμβουλος και ο υπεύθυνος Πληροφορικής

Κατασχέθηκαν, μεταξύ άλλων, 2 κεντρικοί διακομιστές (servers) με 6 σκληρούς δίσκους ο καθένας, 1 κεντρικός διακομιστής με 3 σκληρούς δίσκους, 1 εξωτερικός σκληρός δίσκος ηλεκτρονικού υπολογιστή και 9 κασέτες δημιουργίας αντιγράφων ασφαλείας (backup tapes)

Αστυνομική επιχείρηση και έρευνα της Υπηρεσίας Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος, πραγματοποιήθηκε χθες (07.01.2013) σε εταιρεία που βρίσκεται στη Δάφνη Αττικής, η οποία κατείχε παράνομα μεγάλο όγκο προσωπικών δεδομένων φυσικών και νομικών προσώπων.

Συγκεκριμένα, σε τρεις (3) διακομιστές της (servers), εντοπίστηκε ψηφιακή βάση δεδομένων (σε ξεχωριστούς πίνακες) με πάνω από 67 εκατομμύρια εγγραφές φυσικών και νομικών προσώπων και καταχωρήσεις δεδομένων προσωπικού χαρακτήρα, όπως ονοματεπώνυμα, διευθύνσεις κατοικίας, στοιχεία οχημάτων και ιδιοκτητών, αριθμοί τηλεφώνων, φορολογικά στοιχεία (π.χ. Α.Φ.Μ.) κ.ά.

Συνελήφθη για την υπόθεση αυτή, ο Γενικός Διευθυντής της εταιρείας (59χρονος ημεδαπός), ενώ αναζητούνται άλλοι δύο ημεδαποί, ο 31χρονος Πρόεδρος - Διευθύνων Σύμβουλος και ο 35χρονος υπεύθυνος Πληροφορικής. Σε βάρος τους σχηματίστηκε ποινική δικογραφία για παραβίαση των νομικών διατάξεων περί προστασίας των προσωπικών δεδομένων.

Κατασχέθηκαν, μεταξύ άλλων, 2 κεντρικοί διακομιστές (servers με 6 σκληρούς δίσκους ο καθένας με συνολική χωρητικότητα 870 GB, 1 κεντρικός διακομιστής (server) με 3 σκληρούς δίσκους συνολικής χωρητικότητας 218,4 GB, 1 εξωτερικός σκληρός δίσκος ηλεκτρονικού υπολογιστή και 9 κασέτες δημιουργίας αντιγράφων ασφαλείας (backup tapes).

Αναλυτικότερα, η διερεύνηση της υπόθεσης ξεκίνησε ύστερα από έρευνα της Υπηρεσίας Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος, σχετικά με την ύπαρξη εταιρείας, η οποία συγκεντρώνει, επεξεργάζεται και στη συνέχεια διαθέτει έναντι αμοιβής, φορολογικά στοιχεία και δεδομένα φυσικών και νομικών προσώπων.

Στο πλαίσιο αυτό, εκδόθηκε σχετική παραγγελία του Εισαγγελέα Πρωτοδικών Αθηνών, για τη διενέργεια προκαταρτικής εξέτασης. Κλιμάκιο αστυνομικών εντόπισε την συγκεκριμένη εταιρεία στην περιοχή της Δάφνης Αττικής και πραγματοποίησε έρευνα στα γραφεία της, με την συνδρομή κλιμακίου της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

Από την επιτόπια αυτοψία, αλλά και από την ειδική τεχνική έρευνα που πραγματοποίησαν εξειδικευμένα στελέχη της Υπηρεσίας Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος και της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα διαπιστώθηκε, ότι σε τρεις (3) διακομιστές της εταιρείας, υπήρχε ψηφιακή βάση δεδομένων (σε κωδικοποιημένους πίνακες) με πάνω από (67) εκατομμύρια εγγραφές

φυσικών και νομικών προσώπων, πλην όμως ο ακριβής αριθμός δεν κατέστη δυνατό να μετρηθεί στην επιτόπια έρευνα λόγω δυσχέρειας συσχέτισης μεταξύ των πινάκων και της βάσης δεδομένων.

Κατά την έρευνα βρέθηκαν συνολικά και κατασχέθηκαν:

δύο (2) κεντρικοί διακομιστές (servers) με έξι (6) σκληρούς δίσκους ο καθένας, συνολικής χωρητικότητας 870 GB

ένας (1) κεντρικός διακομιστής (server) με τρεις (3) σκληρούς δίσκους συνολικής χωρητικότητας 218,4 GB

ένας (1) εξωτερικός σκληρός δίσκος ηλεκτρονικού υπολογιστή

εννέα (9) κασέτες δημιουργίας αντιγράφων ασφαλείας (backup tapes) και

πλήθος από χειρόγραφες σημειώσεις.

Όλα τα ψηφιακά πειστήρια που κατασχέθηκαν θα αποσταλούν στα Εγκληματολογικά Εργαστήρια της Ελληνικής Αστυνομίας για τις απαραίτητες εργαστηριακές εξετάσεις.

Ο 59χρονος συλληφθείς Γενικός Διευθυντής της εταιρείας, σε βάρος του οποίου εκκρεμούν επιπλέον καταδικαστικές αποφάσεις για φορολογικές παραβάσεις, θα οδηγηθεί σήμερα στον κ. Εισαγγελέα Πλημμελειοδικών Αθηνών, ενώ παράλληλα ερευνάται η προέλευση αλλά και η περαιτέρω διαχείριση των δεδομένων αυτών.

Αθήνα, 16 Ιανουαρίου 2013

ΔΕΛΤΙΟ ΤΥΠΟΥ

Έρευνα της Δίωξης Ηλεκτρονικού Εγκλήματος σε εταιρεία που κατείχε παράνομα μεγάλο όγκο δεδομένων προσωπικού χαρακτήρα.

Σε υπολογιστές της εταιρείας εντοπίστηκαν ψηφιακές βάσεις με εκατοντάδες χιλιάδες δεδομένα προσωπικού χαρακτήρα, όπως

ονοματεπώνυμα, στοιχεία οχημάτων και ιδιοκτητών, ποσά εισοδημάτων, αριθμοί απόρρητων τηλεφώνων, φορολογικά στοιχεία κ.ά.

Συνελήφθη με την αυτόφωρη διαδικασία, ο ιδιοκτήτης και νόμιμος εκπρόσωπος της εταιρείας

Κατασχέθηκαν, τρεις εσωτερικοί σκληροί δίσκοι συνολικής χωρητικότητας παραπάνω από 13.000 GB

Αστυνομική έρευνα πραγματοποιήθηκε χθες (15.01.2013) από την Υπηρεσία Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος, σε εταιρεία, η οποία δραστηριοποιείται στο χώρο της επικοινωνίας και όπως διαπιστώθηκε κατείχε και διακινούσε παράνομα μεγάλο όγκο δεδομένων προσωπικού χαρακτήρα.

Συνελήφθη για την υπόθεση αυτή, ο ιδιοκτήτης και νόμιμος εκπρόσωπος της εταιρείας (45χρονος ημεδαπός), σε βάρος του οποίου σχηματίστηκε ποινική δικογραφία για παραβίαση των νομικών διατάξεων περί προστασίας των προσωπικών δεδομένων.

Προηγήθηκε κατάλληλη αξιοποίηση πληροφοριών από την Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, σχετικά με ύπαρξη εταιρείας η οποία εμπορεύεται παράνομα δεδομένα προσωπικού χαρακτήρα. Με βάση τα στοιχεία που προέκυψαν από την έρευνα κλιμάκιο αστυνομικών εντόπισε την έδρα της εταιρείας, σε περιοχή του κέντρου της Αθήνας και πραγματοποίησε έρευνα στα γραφεία της.

Από την επιτόπια έρευνα στα γραφεία της εταιρείας, εντοπίστηκαν, σε τρεις (3) ηλεκτρονικούς υπολογιστές ψηφιακές βάσεις με εκατοντάδες χιλιάδες καταχωρήσεις δεδομένων προσωπικού χαρακτήρα, όπως ονοματεπώνυμα, στοιχεία οχημάτων, αριθμοί απόρρητων τηλεφωνικών συνδέσεων, ποσά εισοδημάτων, φορολογικά στοιχεία (π.χ. Α.Φ.Μ.), για τα οποία η εταιρεία δεν κατείχε την προβλεπόμενη άδεια από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

Κατασχέθηκαν, τρείς (3) εσωτερικοί σκληροί δίσκοι συνολικής χωρητικότητας 13.200 GB, οι οποίοι θα αποσταλούν στα Εγκληματολογικά Εργαστήρια της Ελληνικής Αστυνομίας για τις απαραίτητες εργαστηριακές εξετάσεις.

Σημειώνεται ότι στη διερεύνηση της υπόθεσης και στις σχετικές έρευνες συμμετείχε ανώτατο στέλεχος της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

Ο 45χρονος συλληφθείς θα οδηγηθεί σήμερα στον κ. Εισαγγελέα Πλημμελειοδικών Αθηνών.

Η έρευνα συνεχίζεται προκειμένου να προσδιοριστεί επακριβώς ο αριθμός των προσωπικών δεδομένων, καθώς επίσης η προέλευση αλλά και η περαιτέρω διαχείριση – διάθεση τους.

Αθήνα, 24 Ιανουαρίου 2013

ΑΝΑΚΟΙΝΩΣΗ

Από την Υπηρεσία Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος, μετά από διαδικτυακές έρευνες και ψηφιακή διερεύνηση καταγγελιών, ανακοινώνεται ότι έχει εντοπιστεί προσπάθεια αλίευσης και υποκλοπής κωδικών (Phishing Attack) από τραπεζικούς πελάτες, οι οποίοι είναι χρήστες υπηρεσιών e-banking, με σκοπό την διενέργεια συναλλαγών και τη μεταφορά χρημάτων τους σε τραπεζικούς λογαριασμούς τρίτων προσώπων στο εξωτερικό.

Ειδικότερα, οι δράστες χρησιμοποιούν κακόβουλο λογισμικό, που εγκαθίσταται στους υπολογιστές των χρηστών διαδικτυακών υπηρεσιών internet banking και παγιδεύει τον ηλεκτρονικό υπολογιστή τους, με αποτέλεσμα να υφαρπάζει τους κωδικούς ασφαλείας και η συναλλαγή (π.χ. για μεταφορά χρημάτων ή πληρωμή πιστωτικής κάρτας) να

ολοκληρώνεται από τρίτα πρόσωπα, τα οποία μεταφέρουν σε δικούς τους λογαριασμούς χρηματικά ποσά, χωρίς την έγκριση του δικαιούχου.

Διευκρινίζεται ότι οι παραβιάσεις ή επιθέσεις έχουν εντοπιστεί σε χρήστες υπηρεσιών internet banking και όχι σε υπολογιστικά συστήματα Ελληνικών Τραπεζών.

Στο πλαίσιο αυτό η Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος συμβουλεύει τους πολίτες:

Να μην συνεχίζουν τη διαδικασία εισαγωγής στην Υπηρεσία internet banking, εφόσον παρατηρήσουν διαφορετική λειτουργικότητα από τη συνηθισμένη και να επικοινωνούν καταρχήν με την Τράπεζα ή/και με την Υπηρεσία Δίωξης Ηλεκτρονικού Εγκλήματος στο τηλέφωνο 11012 ή στο 210-6476464.

Να έχουν ενημερωμένο λογισμικό για προστασία από ιούς και malware.

Σε περίπτωση που διαπιστώσουν ότι ο υπολογιστής τους έχει μολυνθεί από το κακόβουλο λογισμικό να εκτελέσουν ένα ενημερωμένο πρόγραμμα προστασίας, προκειμένου να απομακρύνουν το κακόβουλο λογισμικό από τον υπολογιστή τους.

Να αλλάξουν τον κωδικό πρόσβασης μετά τον καθαρισμό του υπολογιστή από το κακόβουλο λογισμικό.

Η Υπηρεσία Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος διενεργεί έρευνα για τον εντοπισμό των δραστών σε διεθνές επίπεδο.”

Κεφάλαιο 4

4.1. Νομική κατοχύρωση

Εάν για έναν «πληροφορικό» η *ιδιωτικότητα* και η προστασία της αποτελεί έγνοια ή και πρόκληση προς αντιμετώπιση, για τον νομικό εγείρεται επιπρόσθετα - ή έστω, εντονότερα - το πρόβλημα, αν όχι το καθήκον, του (προσδι)ορισμού της έννοιας και της αναζήτησης του περιεχομένου της. Η αναζήτηση αυτή δεν συνιστά απλά ένδειξη ή εκπλήρωση μιας μεθοδολογικής, επιστημονικής υποχρέωσης. Συνδέεται με προϋποθέσεις και αποτελέσματα, τόσο ως προς το εύρος της προστασίας της ιδιωτικότητας όσο και ως προς τις πολιτικές και το κανονιστικό πλαίσιο που τη διασφαλίζουν.

Το ζήτημα της ιδιωτικότητας δεν είναι ζήτημα που απασχόλησε για πρώτη φορά την «Κοινωνία της Πληροφορίας». Νοούμενη, εν γένει, ως προστασία έναντι της έξωθεν επιτήρησης και της ετερόνομης ρύθμισης της ανθρώπινης ύπαρξης και ζωής, η ιδιωτικότητα ανάγεται στις απαρχές της καταγεγραμμένης ανθρώπινης ιστορίας και διατρέχει την εξέλιξή της. Μάλιστα ορισμένοι συγγραφείς, όπως ο ***John Curtis Raines*** εντοπίζουν την πρώτη «εκδήλωση ιδιωτικότητας» ήδη στη «Γένεση», όταν ο Θεός αντιστάθηκε στη δύναμη να προσηλώσει το βλέμμα του στους γυμνούς πρωτόπλαστους, ενώ στην κλασική ελληνική σκέψη η διάκριση μεταξύ ιδιωτικού και δημόσιου χώρου και βίου συνιστούσε μία αυταπόδεικτη και αξιωματική παραδοχή .

Η έννοια της ιδιωτικότητας δεν είχε πάντα την ίδια βαρύτητα και το ίδιο περιεχόμενο. Αν και η ίδια η διάκριση μεταξύ ιδιωτικού «οίκου» και «δημόσιου» εξωτερικού χώρου ανάγεται ήδη στην αρχαιότητα, δεν ισχύει το ίδιο με την έννοια του «οίκου», καθώς σήμερα ως «ιδιωτικός χώρος» μπορεί να νοείται και ένας δημόσια προσιτός χώρος, στον οποίο

ωστόσο κανείς αναζητά την απόσυρση, ή και ο τερματικός τηλεπικοινωνιακός εξοπλισμός. Αντίστοιχα, τα όρια δημόσιου και ιδιωτικού βίου, δημόσιου και ιδιωτικού χώρου, συχνά δυσδιάκριτα και διαρκώς μεταβαλλόμενα, υποδηλώνουν, κάθε φορά, την υφή και την ποιότητα των σχέσεων του ατόμου με την κοινωνία και το Κράτος καθώς και τη θέση και αξία του μέσα σε αυτά. Οι έννοιες της κοινωνίας και της ιδιωτικότητας είναι πάντως έννοιες απόλυτα *αλληλένδετες*, καθώς χωρίς κοινωνία δεν θα υπήρχε καν η ανάγκη και το αίτημα της ιδιωτικότητας.

Η ιδιωτικότητα δεν αποτελεί μία ανθρωπολογική σταθερά. Προσδιορίζεται σε σχέση με τον κοινωνικό περίγυρο του ατόμου. Η εμβέλεια της ιδιωτικότητας ορίζεται από τις αντιλήψεις και τα ήθη μιας (δεδομένης κάθε φορά) εποχής και κοινωνικής οργάνωσης, τα οποία υπόκεινται σε διαρκή αλλαγή. Οι αλλαγές στο μέγεθος, στη δομή και τη φύση της οικογένειας, η ανάδειξη νέων κοινωνικών χώρων και πεδίων δραστηριότητας, οι μεταλλαγές του αστικού χώρου και του οικιστικού περιβάλλοντος, η διάκριση χώρου εργασίας και χώρου κατοικίας, οι νέες τεχνολογίες επικοινωνίας μεταλλάσσουν την πραγματικότητα αλλά και τις αντιλήψεις σχετικά με το τι είναι «ιδιωτικό» και τι «δημόσιο». Εξάλλου, σε θεσμικό επίπεδο, η αξίωση της ιδιωτικότητας δεν εμφανίζεται ως η εκπλήρωση μιας "φυσικής ανάγκης" όλων των ατόμων αλλά ως η κατάκτηση ενός προνομίου από μία κοινωνική ομάδα. Η κατοχύρωση των ατομικών δικαιωμάτων, αποτέλεσμα των επαναστάσεων του 18^{ου} και 19^{ου} αιώνα, δημιούργησε μία πολιτική και κοινωνική δομή, στο πλαίσιο της οποίας μπόρεσε, σταδιακά, να διατυπωθεί ένα ατομικό δικαίωμα στην ιδιωτικότητα. Η ιδιωτικότητα διατυπώνεται ως δικαίωμα, συχνά συνδεδεμένο με το δικαίωμα της προσωπικότητας. Εντασσόμενη στο συνταγματικό-νομικό πολιτισμό του 20^{ου} αιώνα, η ιδιωτικότητα αναπτύσσει καταρχήν και πρωτίστως έναν

αμυντικό χαρακτήρα, καθώς θωρακίζει το άτομο έναντι των προσβολών από τη δημόσια-κρατική εξουσία.

4.2. Πληροφοριακή ιδιωτικότητα

Με την πάροδο του χρόνου - και αναμφίβολα και υπό την επίδραση της εξέλιξης των νέων τεχνολογιών – γινόταν όλο και περισσότερο κατανοητό ότι η ιδιωτικότητα ως αξίωση σεβασμού της απόσυρσης ή του απόρρητου παρέχει αναγκαία μεν, ανεπαρκή ωστόσο προστασία στο άτομο . Η διεύρυνση του προστατευτέου αγαθού αλλά και η αναγκαιότητα της κανονιστικής αντιμετώπισης των προσβολών της ιδιωτικότητας πρόβαλε επιτακτικότερη, όταν κατέστη αντιληπτή η ποιοτική διαφορά στις δυνατότητες συλλογής, επεξεργασίας, διάχυσης, συσχετισμού των πληροφοριών που δημιούργησαν τα πληροφοριακά και επικοινωνιακά συστήματα και κυρίως η δυνατότητα χρήσης, ανταλλαγής και συσχετισμού των δεδομένων που έχουν συλλεχθεί για πολλαπλούς και διαφορετικούς από τους αρχικούς σκοπούς. Η τεχνολογική δυνατότητα διείσδυσης στη ζωή και στην επικοινωνία, στην προσωπικότητα και στις συνήθειες του χρήστη ανέδειξε και την ποιοτική διάσταση των κινδύνων που συνδέονται με την αναδυόμενη Κοινωνία της Πληροφορίας, καθώς ήδη η ποσοτική αύξηση συνεπέφερε την αύξηση της έντασης, του βαθμού προσβολής των δικαιωμάτων. Ήδη, στις αρχές του’ 70 τα φιλοσοφικά, πολιτικά και νομικά ζητήματα που υπογράμμιζαν το δικαίωμα στην - πληροφοριακή πλέον- ιδιωτικότητα βρέθηκαν στο επίκεντρο μιας συζήτησης που διέβλεπε στην τεχνολογία της πληροφορικής τους κινδύνους ενός νέου «Πανοπτικού», το οποίο, σε αντίθεση με το Panopticon του Bentham , δεν περιοριζόταν σε κλειστές επιτηρούμενες κοινότητες αλλά αφορούσε προοπτικά το σύνολο των ατόμων και των δραστηριοτήτων τους.

Η «διαφανής κοινωνία» ή ο «διαφανής πολίτης», συνήθεις εκφράσεις-μεταφορές κυρίως στα κείμενα των δεκαετιών του ’70 ή και του ’ 80, δεν είναι ακριβώς μόνο το αποτέλεσμα μιας συγκεντρωτικής κρατικής εξουσίας που εντείνει τη συλλογή πληροφορίας, η εκπλήρωση της κασσάνδρειας προφητείας του Orwell (1948), αλλά, πολύ περισσότερο, συνέπεια της διάχυσης της επεξεργασίας της πληροφορίας στο κράτος, την οικονομία και την κοινωνία. Κατέστη επίσης προφανές ότι η γεωμετρική αύξηση των δυνατοτήτων επεξεργασίας της προσωπικής πληροφορίας τελούσε σε σχέση αντιστρόφως ανάλογη προς την ικανότητα του προσώπου να έχει εποπτεία της χρήσης των πληροφοριών που το αφορούν. Το διακυβευόμενο αγαθό δεν εντοπίζεται πλέον στην προστασία της αξίωσης για ανενόχλητη ιδιωτική σφαίρα αλλά αφορά την απώλεια ή – θετικά διατυπωμένο - την άσκηση ελέγχου επί των ιδίων, προσωπικών πληροφοριών . Σύμφωνα μάλιστα με τον «κλασικό» ορισμό του Westin , η ίδια η έννοια της ιδιωτικότητας προσδιορίζεται ακριβώς ως η αξίωση των ατόμων, ομάδων ή θεσμών να προσδιορίζουν οι ίδιοι πότε, πως και σε ποια έκταση οι πληροφορίες που τους αφορούν θα γίνονται γνωστές στους τρίτους.

Η θεωρία του ελέγχου, όπως διατυπώθηκε στις ΗΠΑ, εξελίχθηκε με την έμφαση στη σχέση ιδιωτικότητας και ελευθερίας: Η ιδιωτικότητα αναφέρεται στην ικανότητα των προσώπων να διαμορφώνουν άποψη για τη ζωή τους και να ζουν σύμφωνα με αυτή . Στο σημείο αυτό η σχετική αμερικανική θεωρία συναντάται, χωρίς να ταυτίζεται, με την κυρίαρχη ευρωπαϊκή προσέγγιση, όπως αυτή εκφράζεται τόσο από τη θεωρία όσο και από τη νομολογία. Η προστασία της ιδιωτικότητας αναφέρεται στην αυτονομία του ανθρώπου, στη συμμετοχή του στην κοινωνική ζωή και την επικοινωνία του με τους άλλους . Όπως χαρακτηριστικά επισημαίνει το Ευρωπαϊκό Δικαστήριο των Δικαιωμάτων του Ανθρώπου, το άρθρο 8 της Ευρωπαϊκής Σύμβασης Δικαιωμάτων του Ανθρώπου που

κατοχυρώνει την προστασία του ιδιωτικού βίου αποσκοπεί κυρίως στην εξασφάλιση της ανάπτυξης, χωρίς εξωτερική παρέμβαση, της προσωπικότητας κάθε ατόμου στη σχέση του με άλλους ανθρώπους . Η προσέγγιση αυτή φαίνεται να είναι κρατούσα στη νομική θεωρία και τη νομολογία τω δικαστηρίων, υπερεθνικών και εθνικών. Το γερμανικό Ομοσπονδιακό Συνταγματικό Δικαστήριο, διατυπώνοντας το δικαίωμα του πληροφοριακού αυτοπροσδιορισμού, εξαρτούσε την ανάπτυξη της προσωπικότητας στην κοινωνική συναναστροφή, τη διαμόρφωση ίδιας γνώμης, την ελευθερία απόφασης και τη συμμετοχή στον κοινωνικό και πολιτικό διάλογο από την ελευθερία του πολίτη να (συμ)προσδιορίζει ποιες πληροφορίες που τον αφορούν θα καταστούν γνωστές στο περιβάλλον του και αφετέρου τη δυνατότητα να εποπτεύει τον πληροφοριακό και αξιολογικό ορίζοντα αυτών με τους οποίους έρχεται σε επικοινωνία. Η προστασία των επιλογών ζωής έναντι του δημόσιου ελέγχου σχετίζεται περαιτέρω με την ισότητα καθώς προστατεύει τα άτομα έναντι της κοινωνικής δυσμένειας ή των διακρίσεων που μπορεί να συνεπάγεται η – συχνά μη σύννομη ή/και μη εξουσιοδοτημένη - γνώση μίας πληροφορίας .

Στην ικανότητα των ατόμων για ελεύθερες αποφάσεις και επιλογές, χωρίς παρεμβάσεις, καταγραφή και έλεγχο, βασίζει τη λειτουργία της μια κοινωνία ελευθερίας . Η ελευθερία της απόφασης δεν είναι σημαντική μόνο σε συνάρτηση με το άτομο, δεν συνιστά απλώς μέσο για την πραγμάτωση των αντιλήψεων και των στόχων του σύμφωνα με τις αντιλήψεις του. Η πληροφοριακή ιδιωτικότητα αποσκοπεί στο να καταστήσει δυνατή στο άτομο μία συγκεκριμένη συμμετοχή στις διαδικασίες της κοινωνίας. Καθιστά ταυτόχρονα δυνατή την άσκηση άλλων ελευθεριών και την απόλαυση άλλων ατομικών δικαιωμάτων, όπως η ελευθερία της έκφρασης, η συμμετοχή σε πολιτικές ή συνδικαλιστικές ενώσεις, η θρησκευτική ελευθερία . Με κάθε τέτοια

απόφαση διασφαλίζεται το δημόσιο συμφέρον για μία σταθερή και εξελίξιμη κοινωνία που βασίζεται στη συμμετοχή των ατόμων στις κοινωνικές και πολιτικές διεργασίες, στον ελεύθερο δημόσιο διάλογο και την πολλαπλότητα .

Το περιεχόμενο της ιδιωτικότητας σε σχέση με τον κοινωνικό περίγυρο συνιστά μία αξιοσημείωτη διαφορά μεταξύ της κυρίαρχης αμερικανικής και της αντίστοιχης ευρωπαϊκής προσέγγισης. Το Ευρωπαϊκό Δικαστήριο Δικαιωμάτων του Ανθρώπου έχει συμβάλει σημαντικά στην εξέλιξη της έννοιας της ιδιωτικότητας που δηλώνει μια «κοινωνική ιδιότητα» και συνδέεται με την ικανότητα και την εγγύηση των συνθηκών συναναστροφής με τον περιβάλλοντα κόσμο εν γένει. Το Δικαστήριο επεκτείνει την ιδιωτικότητα πέρα από το «κατώφλι» και τους τοίχους του σπιτιού και αυτό που αντιλαμβανόμαστε ως «στενά προσωπική σφαίρα». Απορρίπτει τη σχηματική διάκριση μεταξύ ιδιωτικής και επαγγελματικής ζωής και δέχεται επίσης ότι «…υπάρχει μια ζώνη αλληλεπίδρασης των ατόμων ακόμη και σε δημόσιο πλαίσιο, η οποία εμπίπτει στο πεδίο του ιδιωτικού βίου». Το Δικαστήριο αναγνωρίζει, έστω και περιορισμένη, αξίωση ιδιωτικότητας ακόμη και στον δημόσιο χώρο . Η αντίληψη αυτή αναπτύσσει κρίσιμες συνέπειες για την αντιμετώπιση των ζητημάτων προσβολής της πληροφοριακής/επικοινωνιακής ιδιωτικότητας στο πλαίσιο των εργασιακών σχέσεων ή σε σχέση με τη χρήση κλειστών κυκλωμάτων τηλεόρασης στο δημόσιο χώρο. Σε αντίθεση με την Ευρώπη, στις ΗΠΑ π.χ. δεν γίνεται, κατά κανόνα, αποδεκτή η ύπαρξη «εύλογης προσδοκίας ιδιωτικότητας» στον χώρο εργασίας ή στον δημόσιο χώρο .

Σύμφωνα με την αντίληψη του Ευρωπαϊκού Δικαστηρίου Δικαιωμάτων του Ανθρώπου το δικαίωμα του ιδιωτικού βίου περιλαμβάνει τόσο την αρνητική, όσο και τη θετική διάσταση: εάν η πρώτη αναφέρεται στο δικαίωμα κάποιου να μην υφίσταται παρεμβάσεις, η δεύτερη οδηγεί στην

αξίωση για υποστήριξη της ολοκλήρωσης και απόλαυσης της ιδιωτικής ζωής . Συγκεκριμένα το Δικαστήριο αναγνωρίζει αφενός την υποχρέωση του κράτους να λαμβάνει μέτρα για την προστασία των δικαιωμάτων των προσώπων στην ιδιωτικότητα και αφετέρου την πιθανή ευθύνη του κράτους για παραβιάσεις της ιδιωτικότητας εκ μέρους ιδιωτών, εφόσον δεν έχει λάβει μέτρα για την αποτροπή ή την κύρωσή τους . Στο σημείο αυτό εντοπίζεται μία βασική διαφορά της ευρωπαϊκής συνταγματικής προσέγγισης σε σχέση με την αντίστοιχη των ΗΠΑ. Στις ΗΠΑ ένα άτομο μπορεί να επικαλεστεί την ιδιωτικότητα ως δικαίωμα μόνο έναντι του Κράτους, το οποίο δεν υποχρεούται σε παρέμβαση έναντι των ιδιωτών .

4.3. Αξία του ανθρώπου ή αξία της πληροφορίας;

Η ελευθερία και η ιδιωτικότητα συνιστούν αλληλεξαρτώμενες έννοιες: η κάθε μία βασίζεται στην άλλη προκειμένου να αναπτύξει τη λειτουργία της κατά τον πλέον αποτελεσματικό τρόπο. Αμφότερες οι έννοιες εκφράζουν τον «σεβασμό», με τον οποίο μία φιλελεύθερη, δημοκρατική κοινωνία αντιμετωπίζει τα άτομα. Στην ευρωπαϊκή προσέγγιση, η ιδιωτικότητα συνδέεται, κυρίως και ιδιαίτερα στενά, με την αξία του ανθρώπου (dignity) και εκφράζεται ως αξίωση να μην καθίσταται το άτομο ένα πληροφοριακό αντικείμενο, ένα σύνολο δεδομένων προς επεξεργασία ή προς συναλλαγή. Η αντίληψη αυτή ανάγεται στην ηθική αυτονομία, των ανθρώπων και συνακόλουθα στην αξίωση να μην αντιμετωπίζονται ως απλά «μέσα» για την επίτευξη ενός σκοπού .

4.3.1. Ιδιωτικότητα ως ιδιοκτησία;

Συνεπάγεται μία τέτοια προσέγγιση την απόκρουση των αντιλήψεων που ερμηνεύουν το δικαίωμα της πληροφοριακής ιδιωτικότητας ως δικαίωμα (αυτό)διάθεσης των πληροφοριών, εξισωμένο κατ' αποτέλεσμα με ένα δικαίωμα κυριότητας, άρα και ευχέρειας παραίτησης από την ιδιωτικότητα και απαλλοτρίωσης των ιδίων δεδομένων; Στην αντίληψη αυτή ο έλεγχος επί των ιδίων πληροφοριών εξελίσσεται – ή, εκπίπτει - σε ένα «ιδιοκτησιακό δικαίωμα» που επιτρέπει στον φορέα του να διαπραγματεύεται την ιδιωτικότητά του αλλά και την τιμή της. Βέβαια, το δικαίωμα παραίτησης από την ιδιωτικότητα προβάλλεται ως συνέπεια της άσκησης ελέγχου επί των ιδίων πληροφοριών ή ισοδύναμο του δικαιώματος πληροφοριακού αυτοκαθορισμού που εκφράζεται, μεταξύ των άλλων, με την παροχή συγκατάθεσης ενός προσώπου για την επεξεργασία των προσωπικών πληροφοριών του.

Μία γνήσια προσέγγιση της «αγοράς της ιδιωτικότητας» βασίζεται στη διάδραση ανάμεσα στο άτομο και σε αυτόν που επεξεργάζεται πληροφορία, ώστε να δημιουργούνται και να διατηρούνται οι όροι της συναλλαγής - επεξεργασίας, έναν ρόλο που στην κανονιστική, κυρίως ευρωπαϊκή, προσέγγιση επιτελεί ρυθμιστικά ο νομοθέτης. Εγγενές χαρακτηριστικό της απαλλοτρίωσης ενός αγαθού είναι ότι αυτός που το αποκτά, έχει το δικαίωμα της περαιτέρω μεταβίβασης. Κατά συνέπεια αυτός που «μεταβιβάζει» την πληροφορία του δεν μπορεί να ελέγξει τις περαιτέρω χρήσεις και μεταβιβάσεις της πληροφορίας. Βέβαια, όπως και το κράτος, έτσι και η αγορά είναι δημιούργημα ανθρώπινων επιλογών και δεν λειτουργεί απαραίτητα εύρυθμα και ισότιμα για τους συμμετέχοντες στις πληροφοριακές συναλλαγές. Δύο λόγοι συνιστούν βασικά εμπόδια στην αποδοχή της «ιδιοκτησιακής προσέγγισης» : ο πρώτος αφορά το πληροφοριακό χάσμα και ο δεύτερος την «παγίδα» ή

– έστω -την ψευδαίσθηση της συγκατάθεσης. Ένα πρώτο αποτέλεσμα της πληροφοριακής ασυμμετρίας ή, για να ακριβολογούμε, της άγνοιας είναι ότι τα άτομα εμποδίζονται να διαπραγματευτούν αποτελεσματικά τα συμφέροντα που σχετίζονται με την ιδιωτικότητά τους. Η αδυναμία των προσώπων να προσδιορίσουν τις πιθανές μελλοντικές χρήσεις άρα και την οικονομική αξία κτήσης και χρήσης των πληροφοριών τους, η άγνοια των όρων της προστασίας προσωπικών πληροφοριών οδηγεί σε ανισότητα των διαπραγματευόμενων μερών .

Λόγω της πληροφοριακής ανισότητας είναι αμφίβολο εάν μιλάμε για πληροφορημένη συγκατάθεση και κατά συνέπεια και για ενσυνείδητη συγκατάθεση . Ιδίως στο Διαδίκτυο, η χρήση προσωπικών δεδομένων στο διαδίκτυο δομείται γύρω από μία συνήθως κενή περιεχομένου διαδικασία συγκατάθεσης που λαμβάνει είτε τυπικές είτε άτυπες μορφές. Πρόκειται για το φαινόμενο “just click submit”: οι χρήστες σπάνια θα διαβάσουν με προσοχή ένα «privacy statement» πριν πιέσουν το επόμενο πλήκτρο για να πλοηγηθούν βαθύτερα σε μία ιστοσελίδα, να αποκτήσουν ή να αναρτήσουν πληροφορία.

4.3.2. Αξία του ανθρώπου και ισότητα

Περαιτέρω, η σύνδεση πληροφοριακής ιδιωτικότητας και αξίας του ανθρώπου δεν επιτρέπει την αντιμετώπιση της προσωπικής πληροφορίας ως αγαθού υποκείμενου σε δικαιώματα κυριότητας και συνεπώς ελευθερίας διαθέσεως έναντι ανταλλάγματος. Στην ελληνική έννομη τάξη το ζήτημα αυτό τέθηκε με ιδιαίτερη έμφαση και ένταση στην υπόθεση «Big Brother», της οποίας επιλήφθηκε η Αρχή Προστασίας Προσωπικών Δεδομένων. Στη σχετική απόφαση επισημαίνεται ότι η ιδιωτικότητα συνδέεται στενά με την αξία του ανθρώπου, μία θεμελιώδη αρχή της συνταγματικής-πολιτειακής τάξης (άρθρο 2 § 1 Συντ.). «Η αξία

του ανθρώπου και η προστασία της υλικής και ηθικής του υπόστασης είναι υπέρτατη δημόσιας τάξης αρχή από την οποία δεν είναι δυνατή η παραίτηση». Αυτό που επιχείρησε να προστατεύσει η Αρχή με την προαναφερόμενη απόφαση δεν ήταν τα συγκεκριμένα πρόσωπα, αλλά μια αφηρημένη ιδέα περί της αξίας του ανθρώπου, σύμφωνα με την οποία η τηλεοπτική επίδειξη της προσωπικής ζωής με σκοπό το κέρδος ή τη δημοσιότητα προσβάλλει την αξιοπρέπεια της ανθρώπινης ύπαρξης αυτήν καθεαυτή, δηλαδή την αξιοπρέπεια ως ουσία της ανθρώπινης κοινωνίας, ανεξάρτητα από το γεγονός ότι η προσβολή αυτή δεν γίνεται αντιληπτή ως τέτοια από τα συγκεκριμένα πρόσωπα που εκτίθενται στο βλέμμα του κοινού .

Η πληροφοριακή ασυμμετρία, στην οποία αναφερθήκαμε παραπάνω, αντιστοιχεί συχνά σε – συχνά εγγενή- ανισότητα που σε κάθε περίπτωση δεν επιτρέπει να θεωρήσουμε το επίπεδο και την προστασία της ιδιωτικότητας ζήτημα προς διαπραγμάτευση. Η συσχέτιση της αξίας του ανθρώπου και προστασίας της ιδιωτικότητας καθώς και τα αδιέξοδα της αντίληψης που αντιμετωπίζει την ιδιωτικότητα ως αντικείμενο διαπραγμάτευσης είναι καταφανή, εάν αναλογιστούμε τα ζητήματα που αφορούν την επεξεργασία και προστασία προσωπικών δεδομένων στο χώρο εργασίας: Η αξίωση ιδιωτικότητας είναι μεν περιορισμένη στον χώρο εργασίας λόγω της φύσης του και της ανάγκης να γίνονται επίσης σεβαστά τα δικαιώματα και έννομα συμφέροντα των άλλων, και κυρίως του εργοδότη . Ωστόσο η αντίληψη ότι ο «εργαζόμενος μπορεί να διαπραγματευτεί την ιδιωτικότητά του, ανταλλάσσοντας την με κάτι αντίστοιχης αξίας, όπως μία θέση εργασίας» μπορεί ίσως να εκφράζει την πραγματικότητα σε πολλούς χώρους εργασίας αλλά σε κάθε περίπτωση δεν βρίσκει έρεισμα, αν μη τι άλλο, στον ευρωπαϊκό συνταγματικό πολιτισμό. Το κατασκοπευτικό λογισμικό (spyware) που παρήγαγε η Microsoft και συνίσταται στη διασύνδεση των εργαζομένων

με τους υπολογιστές τους μέσω ασύρματων αισθητήρων, επιτρέποντας στους εργοδότες να παρακολουθούν διαρκώς την πίεση, τη θερμοκρασία του σώματος, τον ρυθμό της καρδιάς και την έκφραση του προσώπου των εργαζομένων μπορεί – ενδεχομένως! - να αποσκοπεί στην πρόληψη εμφραγμάτων ή εγκεφαλικών λόγω του φόρτου εργασίας αλλά ταυτόχρονα συνιστά το πιο παραστατικό παράδειγμα της ολοκληρωτικής επιτήρησης, η οποία - μέσω τεχνολογικών μεθόδων – στοχεύει εν τέλει στη χειραγώγηση συμπεριφορών, επιλογών και σκέψεων. Πρόκειται εν τέλει για τη «δημιουργία» του «πρότυπου εργαζόμενου», η οποία εξυπηρετείται από τις λεγόμενες κανονιστικές τεχνολογίες, δηλ. τεχνολογικές εφαρμογές που προσδιορίζουν και περιορίζουν συμπεριφορές με προφανή συνέπεια τον περιορισμό της αυτονομίας του προσώπου και, σε τελευταία ανάλυση, την προσβολή της αξίας του .

Το παράδειγμα των περιορισμών ή/και προσβολών της ιδιωτικότητας στον εργασιακό τομέα καταδεικνύει ότι η αποδοχή της ιδιωτικότητας ως «συναλλάγματος» θα έθετε εν γένει μείζονα ζητήματα ισότητας καθώς εν τέλει θα εξαρτούσε τον βαθμό απόλαυσης ενός θεμελιώδους δικαιώματος από την οικονομική και κοινωνική κατάσταση του φορέα του και από την ικανότητα ή ανάγκη του να διαπραγματευτεί την ιδιωτικότητά του . Εάν η διατήρηση και προάσπιση της ιδιωτικότητας κοστίζει σε χρήμα ή άλλα αγαθά ή ο περιορισμός της αποδίδει στον φορέα της π.χ. την ανεμπόδιστη πρόσβαση σε ιστοσελίδες και υπηρεσίες, τότε το δικαίωμα αυτό που συνδέεται τόσο άμεσα με την αξία του ανθρώπου ενδέχεται να καταλήξει «δικαίωμα πολυτελείας» . Η αντίληψη της ιδιωτικότητας ως αγαθού, το οποίο μπορεί χωρίς περιορισμό να διατεθεί από τον φορέα του, παραγνωρίζει και τη σημασία της προστασίας του δικαιώματος αυτού για την θέση του ατόμου στην κοινωνία, την ικανότητά του να συμμετέχει αυτόνομα στις διεργασίες της και εν τέλει για την υφή και ποιότητα μιας – δημοκρατικής – κοινωνικής

οργάνωσης. Ορισμένοι μάλιστα συγγραφείς συνδέουν τόσο στενά τον αναπαλλοτρίωτο χαρακτήρα της ιδιωτικότητας με τη δημοκρατική δομή της κοινωνίας, ώστε να θεωρούν ότι η προσέγγιση της ιδιωτικότητας ως περιουσιακού δικαιώματος ισοδυναμεί με την εμπορευματοποίηση των εκλογικών δικαιωμάτων .

4.4. Προστασία προσωπικών δεδομένων

Όπως ήδη επισημάνθηκε, η αναγκαιότητά της προστασίας της ιδιωτικότητας προβάλλει, εντονότερα όταν γίνεται αντιληπτή η ποσοτική και ποιοτική διαφορά στις δυνατότητες συλλογής και επεξεργασίας πληροφοριών που επέτρεπαν τα πληροφοριακά συστήματα, η οποία καθιστά δυνατή την πολυλειτουργική χρήση και την «αποξένωση» της πληροφορίας από τον φορέα της, το αρχικό περιβάλλον και τους αρχικούς σκοπούς της συλλογής και επεξεργασίας της. Η σύγκλιση των τεχνολογιών πληροφορικής και επικοινωνιών, η αποκέντρωση της επεξεργασίας, η διείσδυση της επεξεργασίας και της δικτύωσης στο σύνολο σχεδόν της ανθρώπινης δραστηριότητας αλλάζουν ριζικά το περιβάλλον χρήσης της προσωπικής πληροφορίας, αλλά και τα ζητήματα που εγείρονται σε σχέση με την προστασία της.

Σε αυτό το πλαίσιο διαμορφώνεται το αίτημα για προστασία προσωπικών δεδομένων. Σε αντίθεση με την ιδιωτικότητα υπό στενή έννοια, η προστασία προσωπικών δεδομένων εγείρεται ως αίτημα αναπόσπαστα συνδεδεμένο με την τεχνολογική εξέλιξη, καθώς αξιολογείται πως οι υφιστάμενες ρυθμίσεις δεν προσφέρουν επαρκή προστατευτική ασπίδα έναντι των διαφαινόμενων κινδύνων.

Λαμβάνοντας υπόψη τις ιδιαίτερες δυνατότητες και επιπτώσεις της ηλεκτρονικής επεξεργασίας προσωπικής πληροφορίας, η προστασία προσωπικών δεδομένων δεν περιορίζεται στη ρύθμιση και προστασία της

πληροφορίας που το άτομο θεωρεί ιδιωτική και ευαίσθητη και για τον λόγο αυτό επιθυμεί να απαγορεύσει ή να περιορίσει τη συλλογή, χρήση και διάδοσή της. Αφορά κάθε πληροφορία που αναφέρεται σε ένα φυσικό πρόσωπο , καθώς η πληροφοριακή αξία ακόμη και μίας καταρχήν «αβλαβούς» πληροφορίας καθορίζεται εν τέλει από την επεξεργασία της, τον συνδυασμό της με άλλες πληροφορίες, από το περιβάλλον εντός του οποίου χρησιμοποιείται και αξιολογείται.

Η προστασία των προσωπικών δεδομένων υπερβαίνει τη διάκριση μεταξύ ιδιωτικής και δημόσιας σφαίρας, καθώς καταρχήν δεν διακρίνει ανάμεσα σε «απλές» και «ιδιωτικές/απόρρητες» πληροφορίες. Υπό την έννοια αυτή, η έννοια της προστασίας των προσωπικών δεδομένων είναι ευρύτερη της ιδιωτικότητας υπό την κλασική της θεώρηση. Είναι ωστόσο παράλληλα και στενότερη καθώς η τελευταία περιλαμβάνει, όπως προαναφέρθηκε, και άλλα στοιχεία πέραν των προσωπικών δεδομένων, όπως το δικαίωμα στη μοναξιά και την απόσυρση

Στο πλαίσιο της προστασίας προσωπικών δεδομένων ο πληροφοριακός αυτοκαθορισμός δεν εξαντλείται στην αξίωση για παρεμπόδιση της μη εξουσιοδοτημένης χρήσης ή της αποκάλυψης σε άλλους. Αποτελείται και συνίσταται σε ένα πλέγμα αρχών, δικαιωμάτων και εγγυήσεων. Ως δίκαιο προστασίας προσωπικών δεδομένων αντιλαμβανόμαστε συνεπώς το σύνολο των κανόνων, προϋποθέσεων, όρων, εξουσιών και απαγορεύσεων σε σχέση με τη συλλογή και επεξεργασία προσωπικών δεδομένων, καθώς και τις ρυθμίσεις που αφορούν διαδικασίες, θεσμικούς ελέγχους, εγγυήσεις και αντίβαρα των περιορισμών των δικαιωμάτων προστασίας των προσωπικών δεδομένων των προσώπων.

4.5. Ιδιωτικότητα, απόρρητο και ασφάλεια

Μία από τις πιο συνήθεις προσλήψεις της έννοιας της ιδιωτικότητας είναι ότι αυτή συνίσταται στον απόρρητο χαρακτήρα ορισμένων ζητημάτων και υπό αυτήν την έννοια η ιδιωτικότητα προσβάλλεται με την αποκάλυψη απόρρητης πληροφορίας . Ιδίως η «κλασική» προσέγγιση της ιδιωτικότητας ως refugium (καταφυγίου) παρουσιάζει στοιχεία ταύτισης ή και σύγχυσης με την έννοια του απορρήτου (secrecy) και της εμπιστευτικότητας (confidentiality).

Οι όροι αυτοί, αν και συχνά γίνονται αντιληπτοί και χρησιμοποιούνται ως ισοδύναμοι, εκφράζοντας σε τελευταία ανάλυση παρεμφερείς αξιώσεις προστασίας, εντούτοις δεν ταυτίζονται: Η έννοια του απόρρητου (secrecy) αναφέρεται είτε στη μη προσπελασιμότητα ορισμένων πληροφοριών που εμπίπτουν στη σφαίρα επιρροής ενός ατόμου είτε στο καθήκον ή την υποχρέωση προσώπων ή οργανισμών να διαφυλάσσουν πληροφορίες που είτε ένα άτομο έχει εμπιστευτεί σε αυτά, στο πλαίσιο μιας γενικότερης σχέσης εμπιστοσύνης (όπως το ιατρικό απόρρητο ή το τραπεζικό απόρρητο) είτε τις κατέχουν επί τη βάσει της θέσης και της αρμοδιότητάς τους (όπως το υπηρεσιακό απόρρητο). Εάν μάλιστα πρόκειται για πληροφορία που εμπίπτει στη δημόσια σφαίρα δεν είναι νοητή η προστασία από το απόρρητο. Για να είναι απόρρητη/εμπιστευτική η πληροφορία θα πρέπει να είναι σε μία κατάσταση περιορισμένης προσβασιμότητας από πρόσωπα, ομάδες κ.λπ.

Το “απόρρητο” αποκλείει τους (περαιτέρω) τρίτους από τη γνώση, τη χρήση και αξιοποίηση των πληροφοριών, εφόσον δεν συντρέχει κάποιος νόμιμος λόγος και η αντίστοιχη διαδικασία που επιτρέπουν την άρση του απορρήτου. Αξίζει πάντως να σημειωθεί ότι σε ορισμένες έννομες τάξεις, όπως αυτή των ΗΠΑ, ήδη το γεγονός ότι ένα πρόσωπο εμπιστεύεται μία πληροφορία που το αφορά σε ένα άλλο πρόσωπο ή οργανισμό οδηγεί

στη στέρηση της προστασίας που επιφυλάσσεται στην ιδιωτικότητα. Η άποψη αυτή συνδέεται με κρίσιμες για τα πρόσωπα συνέπειες, όπως π.χ. το εύρος και οι προϋποθέσεις για περαιτέρω κοινοποίηση των πληροφοριών αυτών. Το Supreme Court (Ανώτατο Δικαστήριο των ΗΠΑ) έκρινε ότι ένα πρόσωπο δεν έχει εύλογη προσδοκία ιδιωτικότητας (reasonable expectation of privacy), όσον αφορά πληροφορίες που αποκάλυψε εθελοντικά σε ένα τρίτο πρόσωπο ή οργανισμό και στη συνέχεια διαβιβάστηκαν από αυτό σε μία δημόσια αρχή, ακόμη και εάν η πληροφορία δόθηκε αρχικά με την υπόθεση ότι θα χρησιμοποιηθεί για έναν περιορισμένο σκοπό (υποθέσεις US v. Miller, Smith v. Maryland) . Στο σημείο αυτό εντοπίζεται μία βασική ατέλεια της επίκλησης της ιδιωτικότητας ως πληροφοριακής απομόνωσης: η χρησιμότητά της (και συνακόλουθα η προστασία του υπό συζήτηση αγαθού) εν τέλει παύει να υφίσταται κατά τη στιγμή που η πληροφορία “παραδίδεται” σε κάποιον άλλον, “διαφεύγει” από το πρόσωπο που αφορά και παύει να είναι “μυστική” .

Ως προς την ευρωπαϊκή προσέγγιση, ο απόρρητος χαρακτήρας των προσωπικών πληροφοριών δεν συνάγεται μόνο από τη φύση τους αλλά προβλέπεται και ρητά στο σχετικό κανονιστικό πλαίσιο. Το άρθρο 16 της Οδηγίας 95/46/ΕΚ για την προστασία προσωπικών δεδομένων περιέχει μία -ιδιότυπης αρνητικής διατύπωσης – ρύθμιση για το απόρρητο, καθώς ορίζει ότι όποιος επεξεργάζεται δεδομένα για λογαριασμό του υπεύθυνου επεξεργασίας ή του εκτελούντος επεξεργασία το πράττει μόνο κατ’ εντολή του υπεύθυνου επεξεργασίας . Ο ελληνικός νόμος για την προστασία προσωπικών δεδομένων (ν. 2472/97) στο άρθρο 10 § 1 περιέχει μεν μία ανάλογη διατύπωση αλλά ταυτόχρονα προσδιορίζει συνολικά την επεξεργασία δεδομένων προσωπικού χαρακτήρα ως απόρρητη.

Το απόρρητο υπό την έννοια της εμπιστευτικότητας σχετίζεται επίσης με την ασφάλεια των πληροφοριών (information security) αλλά δεν ταυτίζεται με αυτή. Η ασφάλεια της πληροφορίας δεν εξυπηρετείται μόνο από την εγγύηση της εμπιστευτικότητας. Η εμπιστευτικότητα αποτελεί μόνο μία από τις παραμέτρους που συγκροτούν την ασφάλεια των πληροφοριών, στην οποία περιλαμβάνεται η εγκυρότητα, η αυθεντικότητα, η ακεραιότητα και η διαθεσιμότητα . Η ασφάλεια προϋποθέτει ένα οργανωμένο πλαίσιο από έννοιες, αντιλήψεις, αρχές, πολιτικές, διαδικασίες, τεχνικές και μέτρα που απαιτούνται για να προστατευτούν τα στοιχεία ενός πληροφοριακού συστήματος και προφανώς δεν διασφαλίζεται μόνο, ίσως ούτε καν κυρίως, από νομικές επιταγές .

Σε κάθε περίπτωση, τόσο η κοινοτική όσο και η ελληνική νομοθεσία για την προστασία προσωπικών δεδομένων απαιτούν τη λήψη «κατάλληλων» μέτρων ασφάλειας, ώστε να προστατεύονται τα δεδομένα από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας . Ο νομοθέτης επάγει μάλιστα στον υπεύθυνο επεξεργασίας την υποχρέωση να εξασφαλίζει επίπεδο ασφάλειας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων. Αξίζει να επισημανθεί ότι ο Έλληνας νομοθέτης συνδέει την υποχρέωση της εμπιστευτικότητας με τις υπόλοιπες διαστάσεις της ασφάλειας, επιλέγοντας μάλιστα να περιλάβει τις υποχρεώσεις απορρήτου και ασφαλείας σε ένα άρθρο(άρθρο 10 ν. 2472/97).

Κεφάλαιο 5.

5.1. Κανονιστικές προσεγγίσεις της ιδωτικότητας

5.1.1. Βασικές κανονιστικές προσεγγίσεις

Η τεχνολογική εξέλιξη και η συνακόλουθη συνειδητοποίηση των κινδύνων και απαιτήσεων προστασίας του ατόμου δεν αντιμετωπίζεται ωστόσο με τον ίδιο τρόπο από τις διάφορες έννομες τάξεις. Η κανονιστική αντιμετώπιση, όπως και η επιλογή της μη αντιμετώπισης ή της αντιμετώπισης με προυφιστάμενα δικαιικά εργαλεία αντικατοπτρίζουν τις διαφορετικές προσεγγίσεις της πληροφοριακής ιδιωτικότητας που εκτέθηκαν συνοπτικά και τη θέση αυτής στην εκάστοτε κλίμακα συνταγματικών αξιών και δημόσιων αγαθών.

Αν και ο αριθμός των νομοθετημάτων αυξάνεται η προστασία των προσωπικών δεδομένων παραμένει μάλλον εξαίρεση στο διεθνές περιβάλλον , καθώς ουσιαστικά εκτός Ευρώπης, λίγες μόνο χώρες έχουν εισαγάγει δεσμευτικούς κανόνες προστασίας προσωπικών δεδομένων. Όσον αφορά τις χώρες που διαθέτουν πλαίσιο προστασίας των προσωπικών δεδομένων, τα κανονιστικά μοντέλα θα μπορούσαν σχηματικά να διαχωριστούν σε δύο μείζονες κατηγορίες: α) σε εκείνες που προάγουν μία ολιστική ρύθμιση όλων των τομέων κρατικής και ιδιωτικής δραστηριότητας και β) σε εκείνες που επιλέγουν ή/και αρκούνται σε ρύθμιση ορισμένων τομέων και πεδίων κρατικής και ιδιωτικής δραστηριότητας επενδύοντας, κυρίως ή ταυτόχρονα, στη λύση της αυτορρύθμισης, δηλ. της διατύπωσης και εφαρμογής κανόνων δεοντολογίας και συμπεριφοράς χωρίς την κρατική παρέμβαση – συμμετοχή. Η ίδια η εξέλιξη της ηλεκτρονικής επεξεργασίας και του Διαδικτύου συνοδεύεται από τη συζήτηση για την αυτορρύθμιση ως μία

εναλλακτική λύση, πιο ευέλικτη και πιο προσαρμοσμένη στις ανάγκες των «δικτυακών» επικοινωνιών και συναλλαγών .

5.2. Η ευρωπαϊκή προσέγγιση

Η ανάγκη προστασίας της ιδιωτικότητας διατυπώνεται ήδη στη Σύμβαση της Ρώμης της 4ης Νοεμβρίου 1950 για την προστασία των ανθρώπινων δικαιωμάτων και των θεμελιωδών ελευθεριών: στο άρθρο 8 ρυθμίζεται το δικαίωμα κάθε προσώπου να γίνεται σεβαστή η ιδιωτική και οικογενειακή του ζωή, η κατοικία και η αλληλογραφία του. Δικαίωμα που μπορεί, κατά τη Σύμβαση, να περιορισθεί, εφόσον ο περιορισμός αυτός προβλέπεται από το νόμο και αποτελεί μέτρο, το οποίο σε μια δημοκρατική κοινωνία είναι αναγκαίο για το συμφέρον της εθνικής και της δημόσιας ασφάλειας, της οικονομικής ευημερίας της χώρας, για την προάσπιση της τάξης και της πρόληψης των ποινικών παραβάσεων, για την προστασία της υγείας ή των ηθών, ή για την προστασία των δικαιωμάτων και των ελευθεριών τρίτων προσώπων.
Ο κατάλογος των δυνητικών περιορισμών είναι, όντως, ευρύς. Απηχεί ωστόσο την πεποίθηση ότι η διαμόρφωση των κανόνων για τη χρήση της προσωπικής πληροφορίας ανταποκρίνεται στο αίτημα της διασφάλισης ατομικών δικαιωμάτων, λαμβάνοντας υπόψη ταυτόχρονα τα δικαιώματα των άλλων (όπως το δικαίωμα της πληροφόρησης, της έρευνας κλπ.) αλλά και τις ανάγκες μιας κοινωνίας, η λειτουργία της οποίας εξαρτάται όλο και περισσότερο από τη διαθεσιμότητα, ροή και επεξεργασία πληροφορίας. Η προστασία της ιδιωτικότητας, άλλως ο πληροφοριακός αυτοκαθορισμός, δεν ταυτίζεται με πλήρη αποκλεισμό της πληροφόρησης των άλλων ή δικαιώματα κυριότητας επί των ιδίων πληροφοριών. Ως κοινωνική ιδιότητα του προσώπου , η (πληροφοριακή) ιδιωτικότητα υπόκειται σε περιορισμούς. Οι περιορισμοί αυτοί, ανεκτοί

μόνο υπό την αίρεση της νομιμότητας και της αναλογικότητας, αφορούν (συνήθως) είτε ένα υπέρτερο δημόσιο συμφέρον είτε τα «δικαιώματα των άλλων». Η διαδικασία, τα κριτήρια και το αποτέλεσμα των αναγκαίων σταθμίσεων είτε κατά την εκπόνηση των κανονιστικών μέτρων είτε κατά την εφαρμογή τους συνιστά και το μέτρο δημοκρατίας του εκάστοτε κοινωνικού/κρατικού σχηματισμού. Το Δικαστήριο των Δικαιωμάτων του Ανθρώπου εξύφανε με τη νομολογία του ένα –πυκνό - πλέγμα προστασίας της ιδιωτικότητας, την οποία αντιλαμβάνεται, όπως προεκτέθηκε, με ευρύ πνεύμα .

Στην Ευρώπη, τόσο σε εθνικό όσο και σε υπερεθνικό επίπεδο, καταγράφονται οι πρώτες δεσμευτικές κανονιστικές ρυθμίσεις για την προστασία προσωπικών δεδομένων. Τα νομοθετικά κείμενα της πρώτης γενιάς, δηλ. της δεκαετίας του ’70, που απαντώνται στα σκανδιναβικά κράτη καθώς και στη Γερμανία και τη Γαλλία, απηχούν, παρά τις διαφορές τους , την συνειδητοποίηση αφενός της σημασίας της επεξεργασίας προσωπικής πληροφορίας για την άσκηση δημόσιας πολιτικής και αφετέρου των κινδύνων που αυτή συνεπιφέρει. Αξιοσημείωτη είναι η επιρροή της Σύμβασης 108/28.1.1981 «για την προστασία των ατόμων από την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα» του Συμβουλίου της Ευρώπης που συνιστά την πρώτη ουσιαστική (έστω και μη πλήρη) «κωδικοποίηση» των αρχών που αποτελούσαν τον «σκληρό πυρήνα» της προστασίας δεδομένων προσωπικού χαρακτήρα κι αποτέλεσε την αφετηρία μιας δεύτερης «γενιάς» νομοθεσίας στην Ευρώπη . Πέραν των ρυθμίσεων που αφορούσαν την ποιότητα της επεξεργασίας (αρχή της αναλογικότητας, της ακρίβειας, αρχή του σκοπού) η Σύμβαση περιείχε ειδικούς κανόνες για τα ευαίσθητα δεδομένα καθώς και τα δικαιώματα των προσώπων, τα δεδομένα των οποίων υφίσταντο επεξεργασία. Ταυτόχρονα, έθεσε κανόνες για την προστασία των ατόμων στην περίπτωση της

διασυνοριακής ροής πληροφοριών. Η αρχική Σύμβαση δεν έκανε καμία αναφορά στην αναγκαιότητα πρόβλεψης μηχανισμών ανεξάρτητου ελέγχου, στοιχείο που προστέθηκε με το Πρόσθετο Πρωτόκολλο του 2001 .

Σταθμός όμως για την προστασία δεδομένων προσωπικού χαρακτήρα θεωρείται η κοινοτική Οδηγία 95/46/ΕΚ «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών», με την οποία επιδιώχθηκε η εναρμόνιση των ευρωπαϊκών νομοθεσιών σε ένα υψηλό επίπεδο προστασίας . Η Οδηγία θέσπισε βασικές αρχές επεξεργασίας, των προσωπικών δεδομένων , την οποία θεωρεί σύννομη μόνο εφόσον θεμελιώνεται σε μία από τις περιοριστικά απαριθμούμενες βάσεις επεξεργασίας . Ο κοινοτικός νομοθέτης κατοχύρωσε τα δικαιώματα των προσώπων (ενημέρωση, πρόσβαση, αντίταξη) ενώ αναγνώρισε τον πρωταρχικό ρόλο των ανεξάρτητων ελεγκτικών αρχών για την αποτελεσματική προστασία των προσωπικών δεδομένων. Αξίζει να υπενθυμίσουμε ότι η Οδηγία εισάγει ειδικές υποχρεώσεις όσον αφορά την ασφάλεια των προσωπικών δεδομένων.

Η εισαγωγή προηγμένων ψηφιακών τεχνολογιών στα δίκτυα ηλεκτρονικών επικοινωνιών δημιούργησε ειδικές απαιτήσεις όσον αφορά την προστασία δεδομένων προσωπικού χαρακτήρα και την ιδιωτική ζωή των συνδρομητών και χρηστών. Προκειμένου να αντιμετωπιστούν τα ειδικά προβλήματα που ανακύπτουν αλλά και χάριν της ασφάλειας δικαίου και κατά συνέπεια της αποτελεσματικότερης προστασίας των χρηστών, το κοινοτικό κανονιστικό πλαίσιο για την προστασία των προσωπικών δεδομένων συμπληρώθηκε από την Οδηγία 97/66/ΕΚ για την προστασία του ατόμου έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα. Η Οδηγία αυτή αντικαταστάθηκε από την Οδηγία 2002/58/ΕΚ για την

προστασία δεδομένων προσωπικού χαρακτήρα στον τομέα των ηλεκτρονικών επικοινωνιών που τελεί και αυτή υπό τροποποίηση, στο πλαίσιο της οποίας έχουν εγερθεί ιδιαίτερα έντονες συζητήσεις για ζητήματα όπως π.χ. η φύση των διαδικτυακών διευθύνσεων (IP addresses) και η συνεπακόλουθη νομική αντιμετώπισή τους .

Οι Οδηγίες αυτές προέκυψαν, πάνω σε μία γενική και οριζόντια βάση, ως αναγκαία εργαλεία για την ολοκλήρωση της εσωτερικής αγοράς, στην οποία αγαθά, υπηρεσίες, κεφάλαια και άνθρωποι θα έπρεπε να κυκλοφορούν ελεύθερα και για τον λόγο αυτό το πεδίο εφαρμογής τους περιορίζεται στη ρύθμιση σχέσεων μεταξύ ιδιωτών . Ωστόσο, η βαρύτητα που απέδιδε η ΕΕ στο ζήτημα της προστασίας προσωπικών δεδομένων αποτυπώθηκε και αγκυρώθηκε περαιτέρω ήδη στη Συνθήκη του Άμστερνταμ (1997) με το άρθρο 286, το οποίο εισήγαγε την εφαρμογή των σχετικών κανόνων στο εσωτερικό των κοινοτικών οργάνων και οργανισμών, προβλέποντας επίσης την ίδρυση ενός "ανεξάρτητου εποπτικού οργάνου" με αντικείμενο τον έλεγχο της τήρησης των ουσιαστικών ρυθμίσεων. Το δικαίωμα προστασίας του πολίτη από την επεξεργασία των προσωπικών του στοιχείων κατοχυρώνεται σε ορισμένα ευρωπαϊκά συντάγματα ως ένα από τα θεμελιώδη ανθρώπινα δικαιώματα. Απέκτησε έναν ικανό αριθμό ιδιαίτερων χαρακτηριστικών, ώστε να δικαιολογεί την ιδιαίτερη θέση και την αναγνώρισή του ως ενός ξεχωριστού θεμελιώδους δικαιώματος. Η διαπίστωση αυτή εξάλλου υπήρξε η βάση για την ένταξή του στον Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (2000-2001) , στο κείμενο του οποίου διαχωρίζεται ο σεβασμός της ιδιωτικής και οικογενειακής ζωής (άρθρο 7) από την προστασία των δεδομένων προσωπικού χαρακτήρα (άρθρο 8) . Η αναγνώριση πλέον (2007) του Χάρτη ως κειμένου ίσης νομικής αξίας με τις Συνθήκες της Ευρωπαϊκής

Ένωσης έχει ιδιαίτερη σημασία για την ισχύ και προστασία του δικαιώματος προστασίας προσωπικών δεδομένων.

Η ιδιαίτερη αυτή αξία αναδεικνύεται ακριβώς στις δραστηριότητες της Ένωσης και των κρατών –μελών στον τομέα της αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις. Στο πλαίσιο της Ευρωπαϊκής Ένωσης έχουν υιοθετηθεί κανονιστικές ρυθμίσεις που αφορούν τα πεδία αυτά , ρυθμίσεις που χαρακτηρίζονται από σημαντικές διαφορές ως προς το επίπεδο προστασίας των προσωπικών δεδομένων . Η πολιτική της ΕΕ στον τομέα αυτό χαρακτηρίζεται από έλλειψη συνοχής και ολιστικής αντίληψης. Η ανάγκη για την εναρμόνιση των σχετικών ρυθμίσεων κατέστη επιτακτική μετά την υιοθέτηση του λεγόμενου «Προγράμματος της Χάγης για την ενδυνάμωση της ελευθερίας, ασφάλειας και δικαιοσύνης στην ΕΕ» (2004). Σε αυτό εντάσσεται η Απόφαση-Πλαίσιο του Συμβουλίου σχετικά με την ενοποιημένη προστασία προσωπικών δεδομένων στο πεδίο της αστυνομικής και δικαστικής συνεργασίας . Η απόφαση αποσκοπεί στην υιοθέτηση συνεκτικών κανόνων προστασίας δεδομένων, εντασσόμενη όμως στον στόχο της πρόληψης και καταπολέμησης της εγκληματικότητας και την υλοποίηση της αρχής της διαθεσιμότητας (availability) των πληροφοριών , ούτως «ώστε η ανταλλαγή σχετικών πληροφοριών ανάμεσα στα κράτη-μέλη - για την πρόληψη και καταπολέμηση της εγκληματικότητας -να μην παρεμποδίζεται από διαφορετικά επίπεδα προστασίας» . Παρά την αναγνώριση του δικαιώματος προστασίας προσωπικών δεδομένων στη Συνθήκη της Λισσαβόνας (άρθρο 16 της Συνθήκης για τη λειτουργία της ΕΕ) και την εμπλοκή του Ευρωπαϊκού Κοινοβουλίου στην εκπόνηση των σχετικών κανόνων το αποτέλεσμα των μακρόχρονων διαβουλεύσεων δεν κρίνεται ικανοποιητικό, καθώς ομογενοποιεί μεν την επεξεργασία

προσωπικών δεδομένων σε αυτούς τους τομείς χωρίς ωστόσο να ενισχύει το επίπεδο προστασίας τους .

5.3. Το ελληνικό κανονιστικό πλαίσιο

Η Ελλάδα υπήρξε από τις πρώτες χώρες που μετέφεραν την κοινοτική Οδηγία στο εσωτερικό δίκαιο . Το ελληνικό νομοθετικό πλαίσιο για την προστασία προσωπικών δεδομένων συγκροτείται από το συνταγματικό δικαίωμα προστασίας προσωπικών δεδομένων όπως κατοχυρώνεται στο άρθρο 9 Α του Συντάγματος, τον νόμο 2472/97 (ΦΕΚ Α' 50/10.04.1997) για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, όπως ισχύει μετά τις τροποποιήσεις που κατά καιρούς εισήχθησαν καθώς και τον νόμο 3471/06 (ΦΕΚ Α' 133/28.06.2006) που – εκτός των τροποποιήσεων που επέφερε στον Ν. 2472/97 – αφορά την προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών .

5.3.1. Η συνταγματική κατοχύρωση της προστασίας προσωπικών δεδομένων

Κατά την αναθεώρηση του Συντάγματος το 2001 κρίθηκε επιβεβλημένη η κατοχύρωση ενός νέου, ειδικού δικαιώματος προστασίας των προσωπικών δεδομένων. Το νέο άρθρο 9Α του Συντάγματος που περιλήφθηκε στο Σύνταγμα με την τελευταία αναθεώρηση του 2001 ορίζει ότι «καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει. Η διασφάλιση της προστασίας των προσωπικών δεδομένων ανατίθεται από τον αναθεωρητικό νομοθέτη σε ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, όπως νόμος ορίζει».

Το δικαίωμα προστασίας προσωπικών δεδομένων εντάσσεται στα νέα δικαιώματα που προέκυψαν από αυτή τη συνταγματική αναθεώρηση, κοινό χαρακτηριστικό των οποίων είναι η μέριμνα για τη διαφύλαξη της προσωπικής αυτονομίας και τη θωράκιση του ήδη γνωστού χώρου αυτοκαθορισμού σε συνθήκες οικονομικής ανάπτυξης και αξιοποίησης της τεχνολογίας . Η προστασία προσωπικών δεδομένων ανήκει στην κατηγορία των νέων δικαιωμάτων που κατοχυρώνει το αναθεωρημένο Σύνταγμα, κοινό στοιχείο των οποίων είναι η εξασφάλιση όχι μόνο έναντι της κρατικής εξουσίας αλλά και έναντι των ιδιωτών . Η συνταγματική διάταξη, εξ ορισμού λιτή, δεν αναφέρεται σε συγκεκριμένα στοιχεία του δικαιώματος, όπως δεν αναφέρεται επίσης σε συγκεκριμένες αρμοδιότητές της ανεξάρτητης αρχής. Γνώμονας και όριο της διακριτικής ευχέρειας του κοινού νομοθέτη αποτελεί η «διασφάλιση της προστασίας προσωπικών δεδομένων». Εκτός από την θετική επιταγή προς τον νομοθέτη για ίδρυση ή/και διατήρηση (και υποστήριξη;) μιας τέτοιας αρχής η διάταξη αυτή δηλώνει ότι τυχόν περιορισμός των αρμοδιοτήτων, εξουσιών και ευχερειών της ελεγκτικής αρχής σε βαθμό που δεν μπορεί πλέον να διασφαλιστεί η αποτελεσματική προστασία του δικαιώματος προφανώς θέτει ζητήματα συνταγματικότητας.

5.3.2. Το νομοθετικό πλαίσιο για την προστασία του ατόμου από την επεξεργασία προσωπικών δεδομένων

Ο Ν. 2472/97 μετέφερε τις ρυθμίσεις της κοινοτικής Οδηγίας για την προστασία δεδομένων (95/46/ΕΚ) στην εσωτερική έννομη τάξη. Αντικείμενο του νόμου είναι η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και σκοπός του η προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής. Ο νομοθέτης με το ν.

2472/97 οριοθετεί με ουσιαστικούς, οργανωτικούς, διαδικαστικούς και κυρωτικούς κανόνες τη συνταγματικά ανεκτή επεξεργασία προσωπικών δεδομένων και με τον τρόπο αυτό ρυθμίζει τη ροή των προσωπικών δεδομένων στο πλαίσιο του κράτους, της οικονομίας και της κοινωνίας και οργανώνει τις πληροφοριακές σχέσεις μεταξύ των προσώπων.

Οι διατάξεις και επιταγές του νόμου καταλαμβάνουν, χωρίς διαφοροποιήσεις, αφενός τον δημόσιο και ιδιωτικό τομέα και αφετέρου την αυτοματοποιημένη αλλά και την «κλασική», με συμβατικές μεθόδους διεξαγόμενη, επεξεργασία. Ο ν. 2472/97 συνιστά ένα (προστατευτικό) πλαίσιο κανόνων που εδράζεται σε τέσσερις πυλώνες: α) σε ένα σύστημα ουσιαστικών ρυθμίσεων που θέτει αφενός τις προϋποθέσεις νομιμότητας της επεξεργασίας προσδιορίζοντας δεσμευτικά το σημείο ισορροπίας μεταξύ των αντιτιθεμένων δικαιωμάτων και συμφερόντων και αφετέρου τις βασικές αρχές του νόμου με έμφαση στην αρχή του σκοπού και της αναλογικότητας (άρθρα 4-10), β) στην απονομή δικαιωμάτων στα πρόσωπα ώστε να προστατεύσουν τα δικαιώματα και συμφέροντά τους (άρθρα 11-14), γ) στην εισαγωγή και οργάνωση ανεξάρτητου θεσμικού ελέγχου της προστασίας προσωπικών δεδομένων ώστε να εξασφαλίζεται η εφαρμογή της νομοθεσίας (άρθρα 15-20) και δ) στους κανόνες που προβλέπουν διοικητικές, ποινικές και αστικές κυρώσεις σε περιπτώσεις παράβασης του νόμου (άρθρα 21-23).

Θα μπορούσε να υποστηριχθεί ότι η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα συνιστά το θεμέλιο του ελληνικού συστήματος προστασίας δεδομένων επί του οποίου δομείται το σύστημα ελέγχου και ο μηχανισμός της εφαρμογής, της τήρησης αλλά και της εξέλιξης των νομικών ρυθμίσεων . Τόσο ο νόμος όσο και η ελεγκτική αρμοδιότητα της Αρχής καταλάμβανε το σύνολο της επεξεργασίας. Ρήγμα στην σύστημα προστασίας επέφερε το άρθρο 8 του ν. 3625/07 που εισήγαγε την

εξαίρεση ενός ευρύτατου φάσματος επεξεργασίας προσωπικών δεδομένων, συγκεκριμένα αυτής που πραγματοποιείται από τις δικαστικές – εισαγγελικές αρχές και τις διωκτικές αρχές για την εξυπηρέτηση των αναγκών της λειτουργίας τους με σκοπό τη βεβαίωση εγκλημάτων, από το πεδίο εφαρμογής του νόμου και κατ' επέκταση από την εποπτεία της Αρχής. Η εξαίρεση αυτή που αφορά έναν τομέα εντασσόμενο στον σκληρό πυρήνα της κρατικής δράσης θέτει μείζονα ζητήματα συνταγματικότητας .

Ο «γενικός» νόμος συμπληρώνεται από τον ν. 3471/06 για την προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών που αντικατέστησε τον προισχύσαντα ν. 2774/1999 για την προστασία των προσωπικών δεδομένων στον τηλεπικοινωνιακό τομέα. Ο νόμος αυτός, ενσωματώνοντας την Οδηγία 2002/58/ΕΚ, αποσκοπεί στην εισαγωγή ειδικών ρυθμίσεων που αφορούν τόσο το απόρρητο της επικοινωνίας και την προστασία της ιδιωτικότητας των χρηστών από πρακτικές όπως π.χ. η εγκατάσταση κατασκοπευτικού λογισμικού (spyware) όσο και την οργάνωση της προστασίας των δεδομένων των συνδρομητών και χρηστών έναντι των παρόχων .

5.4. Το διεθνές κανονιστικό περιβάλλον

Ως προς την αντίδραση της διεθνούς κοινότητας στους κινδύνους των νέων ΤΠΕ για τα ανθρώπινα δικαιώματα, η απόφαση 2450/19.12.1968 της Γ.Σ. των Ηνωμένων Εθνών κατατάσσεται στα πρώτα σχετικά κείμενα. Ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ) υπήρξε ο δεύτερος διεθνής οργανισμός που ασχολήθηκε με την προστασία προσωπικών δεδομένων, εκδίδοντας τις λεγόμενες «Κατευθυντήριες Αρχές που διέπουν την προστασία της ιδιωτικότητας

και τις διασυνοριακές ροές προσωπικών δεδομένων» (1980) . Αυτό το αρχικό και ταυτόχρονα minimum πλαίσιο γενικών αρχών στερείται δεσμευτικού χαρακτήρα και παρά – ή ακριβώς για - τον λόγο αυτόν συγκέντρωσε για μεγάλο διάστημα τη συναίνεση πολλών χωρών και κυρίως εκείνων που στερούνταν (ή εξακολουθούν να στερούνται) συνολικής νομοθεσίας για την προστασία προσωπικών δεδομένων, όπως οι ΗΠΑ .

Η διαρκώς και ραγδαία αυξανόμενη διασυνοριακή ροή προσωπικών δεδομένων δημιουργεί ωστόσο συνθήκες πίεσης αναφορικά με την υιοθέτηση κανόνων και διαδικασιών που θα καθιστούν ευχερή και νόμιμη τη ροή αυτή. Μία πηγή πίεσης συνιστά η ανάγκη να εξασφαλιστεί η εμπιστοσύνη χρηστών και καταναλωτών ως προς την τύχη των δεδομένων τους. Η πίεση αυτή επιτείνεται από τη θεσμική πραγματικότητα που έχει διαμορφώσει η Ευρώπη: η Οδηγία 95/46/ΕΚ (άρθρο 25) απαιτεί την ύπαρξη «ικανοποιητικού επιπέδου προστασίας» των προσωπικών δεδομένων για να είναι σύννομη η διαβίβαση δεδομένων σε μία Τρίτη χώρα. Διαπιστώνεται μία αύξηση των εθνικών νόμων αλλά και η ανάπτυξη περιφερειακών πρωτοβουλιών, όπως αυτή των χωρών του APEC (Asia-Pacific Economic Cooperation) με σκοπό τη διαμόρφωση κανόνων, προδιαγραφών και διαδικασιών για τη χρήση και τη διασυνοριακή ροή προσωπικών πληροφοριών ή την Ιβηρο-νοτιοαμερικανική πρωτοβουλία εκπόνησης κατευθυντήριων αρχών προστασίας προσωπικών δεδομένων (2007).

5.5. Τα όρια και οι προκλήσεις της (προστασίας της) ιδιωτικότητας

Η προστασία των προσωπικών πληροφοριών (δεν μπορεί παρά να) αποτελεί εγγενές στοιχείο της νέας πληροφοριακής συνταγματικής τάξης. Αποκτά περίγραμμα και περιεχόμενο σταδιακά και σύστοιχα

προς την εξελισσόμενη Εποχή της Πληροφορίας. Όπως διαφαίνεται ωστόσο από την συνοπτική ανάλυση που προηγήθηκε, η προστασία της πληροφοριακής ιδιωτικότητας δεν συνιστά αναντίρρητη παραδοχή. Η αμφισβήτησή της ή η αμφισβήτηση της εμβέλειας και των μέσων της οφείλονται σε ποικίλες αιτίες: τον νομικό πολιτισμό μιας χώρας, τις κυρίαρχες αντιλήψεις για τη σχέση ιδιωτικής-δημόσιας σφαίρας, την έμφαση σε άλλες πολιτικο-οικονομικές επιδιώξεις, στις οποίες η προστασία της ιδιωτικότητας προβάλλει προσκόμματα, την επίκληση της εκπλήρωσης άλλων δικαιωμάτων και συμφερόντων.

Τα όρια της ιδιωτικότητας και της προστασίας της καθορίζονται από τεχνολογικούς παράγοντες, την παγκοσμιοποίηση της επεξεργασίας και της επικοινωνίας, τις αλλαγές των αντιλήψεων τόσο των ατόμων όσο και των κρατικών και κοινωνικών οργανώσεων ως προς το περιεχόμενο της ιδιωτικότητας όσο και ως προς τη σχέση της με άλλα δημόσια και ιδιωτικά αγαθά και επιδιώξεις. Η πληροφοριακή ιδιωτικότητα διάγει περίοδο κρίσεως που οφείλεται τόσο στην περιρρέουσα πολιτικο-οικονομική πραγματικότητα όσο και σε βασικά δομικά χαρακτηριστικά των ΤΠΕ, όπως αυτές εξελίσσονται και λειτουργούν.

Η ανάλυσή μας έχει σημείο αφετηρίας ακριβώς τον τεχνολογικό παράγοντα ή την τεχνολογική «δοκιμασία της ιδιωτικότητας». Η τεχνολογία τελεί σε μία «διαλεκτική» σχέση προς τις άλλες εξελίξεις: ο νέος ρόλος του κράτους και οι αλλαγές στη διάρθρωση της οικονομίας ενέτειναν τις ανάγκες για επεξεργασία δεδομένων. Οι νέες τεχνολογίες είναι προϊόν της κοινωνίας, η προέλευση και η εξέλιξή τους προσδιορίζονται από αυτή. Από την άλλη πλευρά οι τεχνολογίες επηρεάζουν, ενίοτε δε καθορίζουν την εξέλιξη της κοινωνίας και των θεσμών της. Η ανάπτυξη των τεχνολογιών της πληροφορίας και επικοινωνίας με την αλματώδη πρόοδό τους αλλάζουν το τοπίο: στη νέα κοινωνία της πληροφορίας οι υπηρεσίες που προσφέρονται από τις νέες

τεχνολογίες συνιστούν κρίσιμο παράγοντα καθορισμού των κοινωνικών και οικονομικών δομών και σχέσεων.

5.6. Η τεχνολογία

Αν οι τεχνολογικές εξελίξεις οδήγησαν στην αναγνώριση και κατοχύρωση ενός πλέγματος προστατευτικών κανόνων, οι ίδιες αυτές εξελίξεις θέτουν, διαρκώς και αυξανόμενα, σε δοκιμασία τη ρυθμιστική ικανότητά των νομικών κανόνων . Κατά την ψήφιση των πρώτων σχετικών κανονιστικών κειμένων για την προστασία της πληροφοριακής ιδιωτικότητας, όπως π.χ. η κοινοτική Οδηγία για την προστασία προσωπικών δεδομένων (95/46/ΕΚ) το τεχνολογικό περιβάλλον κυριαρχούνταν από «αρχεία» και μεγάλα υπολογιστικά συστήματα. Στη συνέχεια και διαρκώς το τεχνολογικό υπόβαθρο της επεξεργασίας προσωπικών πληροφοριών γνωρίζει ριζικές αλλαγές που με τη σειρά τους έχουν επιπτώσεις στη λογική αλλά και στην έκταση και ένταση της επεξεργασίας πληροφοριών. Εάν κατά την έναρξη των συζητήσεων για την κοινοτική Οδηγία (1990) το Διαδίκτυο εντασσόταν στις γνωστικές προνομίες ορισμένων πανεπιστημιακών εργαστηρίων, σχεδόν 20 χρόνια μετά η διείσδυση του αφορά 56% των νοικοκυριών στις χώρες της Ευρώπης και 95% των επιχειρήσεων στις χώρες του ΟΟΣΑ .

Αν και αποτελεί κοινό τόπο, αξίζει να επισημανθεί ότι η διάδοση των προσωπικών υπολογιστών συνεπέφερε την απώλεια ή έστω την αποδυνάμωση του υπολογιστικού «μονοπωλίου» του κράτους και των μεγάλων επιχειρήσεων. Η επεξεργασία αποκεντρώνεται, η ευχέρεια συλλογής, διαβίβασης, μετάδοσης δεδομένων διαχέεται σε μεμονωμένα υπολογιστικά συστήματα άρα και σε μεμονωμένους υπαλλήλους, εργαζόμενους εμπόρους, μικρές επιχειρήσεις, εργοδότες κ.ά., μεγιστοποιώντας κατά τον τρόπο αυτό την κινητικότητα των χρηστών

τους με συνέπεια την “ευελιξία” και την αποκέντρωση των διαδικασιών που αντιστοιχεί περαιτέρω στη δυνατότητα α ριζικής αποκέντρωσης των αρχείων. Περαιτέρω, η εισαγωγή και διαρκής εξέλιξη ποικίλων και ανά τομέα διαφορετικών chipcards και η αλματώδης ανάπτυξη των δικτύων, γνωστότερο των οποίων είναι το World Wide Web, διαμορφώνουν ένα ριζικά διαφορετικό πλαίσιο παραγωγής και επεξεργασίας πληροφοριών. Η σύγκλιση των τεχνολογιών, συνοδευόμενη από τη σύγκλιση οικονομικών δραστηριοτήτων, οδήγησε στην εξάλειψη τεχνολογικών εμποδίων και στη λειτουργική ολοκλήρωση πληροφοριακών και επικοινωνιακών συστημάτων. Ο κόσμος εξελίσσεται σε μία «δικτυωμένη κοινωνία, όπου τα προσωπικά δεδομένα συλλέγονται, εμπλουτίζονται, τροποποιούνται, ανταλλάσσονται και επαναχρησιμοποιούνται διαρκώς» . Οι εξελίξεις στην πληροφορική τεχνολογία έχουν ως συνέπεια ότι, θεωρητικά τουλάχιστον, δεν υπάρχει πλέον όριο στην πληροφορία που μπορεί να καταχωριστεί, στην ανάλυση που μπορεί να γίνει, στο χρονικό διάστημα για το οποίο μπορεί να τηρηθεί . Αντίστοιχα απεριόριστες μοιάζουν να είναι οι δυνατότητες εκμετάλλευσης: Διατυπώσεις όπως η «εξόρυξη δεδομένων» (data mining) δεν αποδίδουν μόνο περιγραφικά τεχνικές αλλά υποδηλώνουν έναν νέο «πυρετό του (πληροφοριακού) χρυσού» . Σε αυτό συντελεί το αδιαμφισβήτητο γεγονός ότι όλο και περισσότερες δραστηριότητες, της πιο ποικίλης φύσης, οργανώνονται και διεκπεραιώνονται online. Ήδη ως προς την ποσοτική διάσταση πρέπει να παρατηρηθεί ότι η ηλεκτρονική επικοινωνία, αμφίδρομη ή μη, παράγει πολύ περισσότερα δεδομένα, δεδομένα που απεικονίζουν την κίνηση (πλοήγηση, επικοινωνία) του χρήστη μέσα στα δίκτυα. Τα όρια μεταξύ των εξωτερικών στοιχείων και του περιεχομένου μιας επικοινωνίας είναι πλέον δυσδιάκριτα ενώ σταδιακά γίνεται όλο και πιο σαφές ότι η επεξεργασία προσωπικών πληροφοριών και η επικοινωνία είναι διαδικασίες που αναπόφευκτα συμπλέκονται. Περαιτέρω, στα

δίκτυα χάνει εν τέλει τη σημασία της η διάκριση σε συλλογή, καταχώριση και διαβίβαση των δεδομένων .

Η συλλογή πληροφορίας για πρόσωπα δεν είναι καινοφανές στοιχείο στην κρατική, κοινωνική, οικονομική οργάνωση. Εκτός όμως της ποσοτικής και ποιοτικής αύξησης της επεξεργασίας πρέπει να επισημανθεί μία ακόμη παράμετρος: η διαθεσιμότητα και διάδοση των νέων τεχνολογιών όχι μόνο αποκεντρώνει τις δυνατότητες επεξεργασίας αλλά καθιστά τον καθένα χρήστη τους και ταυτόχρονα πηγή παραγωγής και διάθεσης πληροφορίας. Στο περιβάλλον του Web 2.0 συζητείται και προωθείται η παροχή διαδραστικών υπηρεσιών, όπου όλο και περισσότερο εξαφανίζονται τα όρια μεταξύ παρόχων και χρηστών. Η παραγωγή και διάδοση της πληροφορίας δεν είναι πλέον θέμα και αντικείμενο μιας κατηγορίας ειδικών: το Web 2.0 (θα) επικυριαρχείται από το περιεχόμενο που παράγουν οι χρήστες (user generated content), από πληροφορίες που αυτοί διαμοιράζονται, αναζητούν και λαμβάνουν.

Ωστόσο είναι αμφίβολο, εάν το άτομο αποκτά εποπτεία του πληροφοριακού ορίζοντα των άλλων, κράτους και ιδιωτών, και, εάν έχει ουσιαστικά την πρωτοβουλία της επικοινωνίας, εάν –απλούστερα- γνωρίζει και συμπροσδιορίζει ουσιαστικά τι γνωρίζουν οι άλλοι για αυτό. Το πρόβλημα επιτείνεται καθώς οι ΤΠΕ χαρακτηρίζονται επίσης από πολυπλοκότητα και αδιαφάνεια έναντι του (μέσου) χρήστη τους: τα ηλεκτρονικά κείμενα/αρχεία περιέχουν πληροφορίες, τις οποίες δεν γνωρίζει καν ο αποστολέας. Η «αδιαφάνεια», συνέπεια συνδεδεμένη με τον γεωμετρικό πολλαπλασιασμό της επεξεργασίας και των πληροφοριακών ροών, βρίσκει ίσως την πιο απτή απεικόνισή της στις «νανοτεχνολογίες» : η ικανότητα των nanorobots να συλλέγουν πληροφορία και να ρυθμίζουν περιβάλλοντα που προηγουμένως δεν ήταν προσιτά, όπως π.χ. το ανθρώπινο σώμα, δημιουργεί όχι μόνο νέες

τεχνολογικές δυνατότητες αλλά και νέες κατηγορίες πληροφοριών που μπορεί να συλλεχθούν.

Ποτέ στην ιστορία δεν μπορούσε να αποτυπωθεί με τεχνικό τρόπο και σε τεχνικά μέσα όλη η ζωή ενός προσώπου , όπως αυτό συμβαίνει σήμερα. Η καταγραφή των δεδομένων κίνησης, η αξιοποίηση των δεδομένων που παράγονται και ανταλλάσσονται στα δίκτυα κοινωνικής δικτύωσης όπως το Facebook, ο πολλαπλασιασμός των κλειστών κυκλωμάτων τηλεόρασης, η αυξημένη χρήση βιομετρίας και τεχνολογιών RFID ως μέσου αποθήκευσης πληροφορίας και παρακολούθησης πραγμάτων και ανθρώπων επιτρέπουν τη διεισδυτική όσο και ολιστική διάγνωση και αποτύπωση ιδιαίτερων πτυχών της προσωπικότητας και καθημερινότητας ενός προσώπου αλλά και την ανασύνθεση αυτών μέσω των ψηφίδων πληροφορίας που συμπληρώνουν το puzzle της ζωής του.

Ιδιαίτερα ζητήματα θέτει η χρήση βιομετρικών μεθόδων. Η βιομετρία αναφέρεται σε μετρήσεις βιολογικών/φυσιολογικών χαρακτηριστικών και χαρακτηριστικών συμπεριφοράς ενός ανθρώπου με σκοπό την αναγνώριση ή επαλήθευσης της ταυτότητας κάποιου . Τέτοια είναι τα συστήματα που βασίζονται στα δακτυλικά αποτυπώματα, τη γεωμετρία της παλάμης, την αναγνώριση του προσώπου(face recognition) , της ίριδας του ματιού και της φωνής . Βιομετρικά χαρακτηριστικά και μέθοδοι χρησιμοποιούνται πλέον όλο και περισσότερο για τον έλεγχο της πρόσβασης ή την ταυτοποίηση προσώπων. Η χρήση τους αφορά έναν ιδιαίτερα ευρύ κύκλο προσώπων καθώς σχεδιάζεται πλέον η ένταξή δακτυλικών αποτυπωμάτων και βιομετρικών προσώπου στα λεγόμενα ηλεκτρονικά διαβατήρια ή άλλα αναγνωριστικά έγγραφα, χωρίς ωστόσο να έχει επιβεβαιωθεί η αξιοπιστία τους .

Η συλλογή πληροφορίας δεν περιορίζεται στην ορατή πλευρά της ύπαρξης. Στα βιομετρικά συμπεριλαμβάνεται και το γενετικό υλικό, η συλλογή και ανάλυση του οποίου συνδέεται με ιδιαίτερα προβλήματα,

καθώς αποκαλύπτει πληροφορία όχι μόνο για την ταυτότητα αλλά και για τη βιολογική κατάσταση και την υγεία –τόσο του ιδίου του προσώπου όσο και των συγγενών του. Η συλλογή και χρήση των γενετικών δεδομένων θέτει ιδιαίτερα προβλήματα είτε πρόκειται για χρήση ταυτοποίησης στο πλαίσιο διερεύνησης εγκλημάτων είτε πρόκειται για χρήση για ερευνητικούς, θεραπευτικούς ή ασφαλιστικούς σκοπούς . Τα ζητήματα αυτά επιτείνονται από τον συνδυασμό των βιολογικών επιστημών και της πληροφορικής. Η βιοπληροφορική αντιμετωπίζει τα βιολογικά δεδομένα, όπως αυτά που προκύπτουν από την ανάλυση το DNA ή το RNA, ως ψηφιακή πληροφορία και αναπτύσσει πληροφορικά (computational) εργαλεία και προσεγγίσεις για να διευρύνει τη χρήση βιολογικών και ιατρικών δεδομένων καθώς και δεδομένων που αφορούν τη συμπεριφορά και την υγεία . Μέσω της εφαρμογής μεθόδων τεχνητής νοημοσύνης ή/και τεχνολογιών GRID αλλά και του συνδυασμού με βιοτράπεζες, βάσεις δεδομένων ασθενών, βιολογικών συστημάτων επιχειρείται εδώ και λίγα χρόνια στην Ευρώπη η πολυεπίπεδη μοντελοποίηση και προσομοίωση της ανθρώπινης ανατομίας και φυσιολογίας (γνωστή και ως Virtual Physiological Human) .

Ταυτόχρονα, οι RFID εφαρμογές, τα κινητά τηλέφωνα πολλαπλών λειτουργιών και οι μικροεπεξεργαστές (micro-chips) σε κάρτες και έγγραφα πιστοποίησης ταυτότητας είναι οι προπομποί της εποχής του απανταχού υπολογίζειν (ubiquitous computing) και της ανοιχτής νοημοσύνης (ambient intelligence) . Σε συνδυασμό με τεχνολογίες προσδιορισμού θέσης τα αντικείμενα με ενσωματωμένους αισθητήρες (sensors) αποκτούν πρωτόγνωρες ιδιότητες και ποιότητες, καθώς θα μπορούν να γνωρίζουν που βρίσκονται τα ίδια ή ποια άλλα αντικείμενα και πρόσωπα βρίσκονται στο περιβάλλον . Στο ubiquitous computing η ηλεκτρονική επεξεργασία πληροφορίας δεν διαχωρίζεται από τις άλλες

καθημερινές δραστηριότητες, δεν γίνεται καν αντιληπτή ως τέτοια και προσαρμόζεται στο εκάστοτε περιβάλλον . Όπως σημειώνει ο Marx, με την τάση προς το ubiquitous computing, η επιτήρηση και οι αισθητήρες εξαφανίζονται σε συνήθεις δραστηριότητες και αντικείμενα, όπως αυτοκίνητα, κινητά τηλέφωνα, κτίρια ή ρούχα . Συνακόλουθα, εξυφαίνεται μεσοπρόθεσμα το«Διαδίκτυο των πραγμάτων» (Internet of things), όπου τα επικοινωνιακά δίκτυα και άλλες εφαρμογές προσδίδουν σε φυσικά αντικείμενα μία διαδικτυακή διεύθυνση, επιτρέποντας τη διασύνδεση μιας ευρείας κλίμακας συσκευών. Πρόκειται για εξέλιξη που σε συνδυασμό με άλλες τεχνολογίες, όπως τα RFID, θα συνεπιφέρουν ευρύτατες – και ακόμη δυσδιάγνωστες - επιπτώσεις τόσο για τις ποικίλες εκφάνσεις της ζωής όσο και για το δίκαιο που είναι δομημένο με τρόπο ώστε να ρυθμίζει τις σχέσεις μεταξύ προσώπων.

5.7. Η εμπορευματοποίηση της προσωπικής πληροφορίας

Η τεχνολογική υποδομή των δικτύων σε συνδυασμό με τις τεχνολογίες πληροφορικής κατέστησε τη συλλογή και τη χρήση πληροφοριών ευχερή και οικονομικά προσιτή. Οι καταναλωτές έχουν στην online αγορά πολύ λιγότερες επιλογές να διαφυλάξουν τα προσωπικά δεδομένα τους. Συχνά είναι οι ίδιοι οι χρήστες που παρέχουν τα δεδομένα τους, είτε γιατί αυτά προαπαιτούνται για τη δημιουργία ενός λογαριασμού είτε ως «αντάλλαγμα» για την πρόσβαση σε μία υπηρεσία ή πληροφορία . Τα συστήματα είναι συνήθως έτσι σχεδιασμένα ώστε να παρακολουθούν τα άτομα ήδη από την έναρξη της πλοήγησής τους στο δίκτυο, χρησιμοποιώντας τις διευθύνσεις IP καθώς και cookies. Ιστοσελίδες, δικτυακές επιχειρήσεις, πάροχοι συλλέγουν μεγάλο όγκο προσωπικών πληροφοριών, χωρίς απαραίτητα τα άτομα να έχουν συναινέσει ή και να έχουν γνώση της συλλογής, καθώς αυτή μπορεί μάλιστα να λαμβάνει

χώρα με αδιαφανή τρόπο. Αν δε ο τεχνολογικά ενήμερος χρήστης μπορεί να περιορίσει τα cookies χρησιμοποιώντας τις σχετικές ρυθμίσεις, θα αντιμετωπίσει τον αποκλεισμό της πρόσβασης σε σελίδες υψηλής ζήτησης, συμπεριλαμβανομένης αυτής της Google.

Προηγμένες τεχνολογίες εξόρυξης δεδομένων (data mining) επιτρέπουν την παραγωγή νέας πληροφορίας που αποδεικνύεται πολύ χρήσιμη για τις έρευνες αγοράς και τη διαφήμιση. Αρκετές εταιρίες συνδυάζουν δεδομένα και προσαρμόζουν τη διαφημιστική τακτική αλλά και τη στοχευμένη διαφήμιση στα ενδιαφέροντα του χρήστη, όπως αυτά εκφράζονται και αποκαλύπτονται μέσα από την πλοήγηση ή/και άλλη διαδικτυακή δραστηριότητά του. Διαφημιστικές πρακτικές, όπως το λεγόμενο behavioural targeting ή άλλες εξατομικευμένες υπηρεσίες υπογραμμίζουν την εξέλιξη των προσωπικών πληροφοριών σε οικονομικό μέγεθος για τις επιχειρήσεις, ιδίως αυτές που δραστηριοποιούνται στο πλαίσιο της ψηφιακής οικονομίας. Οι εταιρίες αντιμετωπίζουν τις πληροφορίες αυτές ως εταιρική περιουσία , επενδύοντας στην ανάπτυξη λογισμικού που διευκολύνει τη συλλογή δεδομένων από τους χρήστες. Τα προσωπικά δεδομένα έχουν ως «το ζωοποιό στοιχείο ή το βασικό συνάλλαγμα» της «οικονομίας της πληροφορίας» (information economy). Αντίστοιχη είναι και η πίεση για την οικονομική αξιοποίησή τους. Συχνά υποστηρίζεται ότι σκοπός της επεξεργασίας προσωπικών δεδομένων είναι η βελτίωση της αποτελεσματικότητας και της ευρυθμίας των αγορών αλλά και η συνακόλουθη καλύτερη ανταπόκριση στις ανάγκες των καταναλωτών. Η επίτευξη της στόχευσης αυτής θα προϋπέθετε ωστόσο την παροχή καλύτερης πληροφόρησης και ουσιαστικών επιλογών στον καταναλωτή.

Ορισμένες παράμετροι που επιτείνουν τον προβληματισμό για την προστασία των προσωπικών δεδομένων αφορούν τις επιχειρηματικές αλλαγές που συντελούνται στο πεδίο της ψηφιακής οικονομίας.. Στο

πλαίσιο αυτό, εξαιρετικό ενδιαφέρον αλλά και κινδύνους παρουσιάζει π.χ. η πρόσφατη εξαγορά της Double Click, ,της μεγαλύτερης διαφημιστικής εταιρίας στον κόσμο από την Google, τη μεγαλύτερη και πλέον δημοφιλή μηχανή αναζήτησης. Κρίσιμα στοιχεία είναι ταυτόχρονα η αύξουσα πολυπλοκότητα στην οργάνωση των φορέων που επεξεργάζονται δεδομένα, με μορφές όπως το outsourcing ή το off-shoring καθώς οδηγούν σε πιο πολύπλοκες σχέσεις μεταξύ αυτών που συλλέγουν, επεξεργάζονται ή χρησιμοποιούν τις προσωπικές πληροφορίες. Το πρόβλημα επιτείνεται καθώς, ιδίως, αλλά όχι μόνο, στην περίπτωση πολυεθνικών εταιριών η επεξεργασία λαμβάνει χώρα σε πολλές και διαφορετικές ως προς το επίπεδο προστασίας χώρες.

5.8. Η έλλειψη ορίων και η δικτυακή παγκοσμιοποίηση

Οι ΤΠΕ δημιούργησαν περαιτέρω τις προϋποθέσεις για την αποσύνδεση της επεξεργασίας από συγκεκριμένο τόπο. Η παγκοσμιοποίηση δεν έχει απλώς μία προφανή τεχνολογική διάσταση αλλά, πολύ περισσότερο, συντελείται ακριβώς πάνω σε τεχνολογική βάση. Η παγκοσμιοποίηση των οικονομικών και κοινωνικών δικτύων αλλά και της επίτευξης συνεργασιών και της επίλυσης προβλημάτων σε οργανωσιακό και κρατικό επίπεδο αντιστοιχεί στην παγκοσμιοποίηση των πληροφοριακών ανταλλαγών, την υπηρετεί και υπηρετείται από αυτή. Η κυκλοφορία της πληροφορίας και η προσπελασιμότητά της δεν υπερβαίνει απλώς τα εδαφικά σύνορα. Αίρει, μέσω των δικτύων, αυτή καθεαυτή την έννοια των πεπερασμένων εδαφικών ορίων. Η παγκοσμιοποίηση, η ανάπτυξη των επιχειρηματικών μοντέλων “follow the sun”, η ανάπτυξη του Διαδικτύου σε συνδυασμό με τη μείωση του τηλεπικοινωνιακού κόστους έχει ως αποτέλεσμα τη δραματική αύξηση της διασυνοριακής ροής δεδομένων . Η «μετανάστευση» (de-

localisation) της επεξεργασίας έχει ως αποτέλεσμα την αδυναμία ελέγχου (της νομιμότητας) των ροών πληροφορίας πάνω στα δίκτυα.

Το ρυθμιστικό βάρος και οι επιταγές της προστασίας της πληροφοριακής ιδιωτικότητας παραμένουν (αναπόφευκτα;) σημαντικά προσανατολισμένοι σε εδαφικούς όρους. Ένα πρώτο ζήτημα που τίθεται αφορά τη δυσχέρεια προσδιορισμού και εφαρμογής του δικαίου ή/και των δικαστικών αποφάσεων, καθώς το δίκαιο και οι υποχρεώσεις που επιβάλλει συνδέονται άρρηκτα με την έννοια της εδαφικά προσδιορισμένης επικράτειας. Ποιο ρυθμιστικό πλαίσιο εφαρμόζεται στην περίπτωση της γερμανικής πολυεθνικής εταιρίας, η οποία διεκπεραιώνει τα λογιστικά της στην Ινδία, διατηρεί τη βάση δεδομένων όλων των εργαζομένων στη Σιγκαπούρη, ενώ ο εξυπηρετητής του ηλεκτρονικού ταχυδρομείου (e-mail server) διατηρείται στο San Francisco;

Μία δεύτερη επίπτωση του ρυθμιστικού προσανατολισμού στα γεωγραφικά όρια είναι ακριβώς ότι αγνοούνται οι νέες μορφές δεδομένων και οι νέες μορφές επεξεργασίας τους. Η Ευρωπαϊκή Ένωση επέβαλε με την Οδηγία 95/46/ΕΚ αυστηρούς κανόνες ως προς τη διασυνοριακή ροή δεδομένων σε τρίτες χώρες καθώς η νομιμότητά της εξαρτάται από το εάν η χώρα υποδοχής των προσωπικών δεδομένων (κρίνεται ότι) παρέχει «ικανοποιητικό επίπεδο» προστασίας των δεδομένων αυτών. Η εφαρμογή τους όμως εξαρτάται σε μεγάλο βαθμό από το αίσθημα υποχρέωσης συμμόρφωσης που έχουν οι αποδέκτες των ρυθμίσεων καθώς οι μηχανισμοί επιβολής του δικαίου δοκιμάζονται από την τεχνική ευκολία με την οποία, με ένα mouse-click, μία βάση δεδομένων μπορεί να διαβιβαστεί σε μία τρίτη χώρα.

Περαιτέρω η ροή των πληροφοριών στα δίκτυα εγείρει σοβαρά ζητήματα ως προς την έννοια όρων που είναι κομβικοί για την προστασία των προσωπικών πληροφοριών, την κατανόηση και εφαρμογή των σχετικών

κανόνων, όπως η έννοια της διασυνοριακής διαβίβασης δεδομένων: Η κρίση του Δικαστηρίου των Ευρωπαϊκών Κοινοτήτων ότι η ανάρτηση δεδομένων σε ιστοσελίδα, στην οποία υπάρχει δυνατότητα πρόσβασης από οπουδήποτε δεν συνιστά καθεαυτή διασυνοριακή διαβίβαση, δεν είναι βέβαιο ότι συνιστούσε μία στέρεη νομική θέση ή μία πραγματιστική λύση καθώς στην αντίθετη περίπτωση θα σήμαινε υποχρέωση εφαρμογής των κανόνων για τη διασυνοριακή ροή σε κάθε δημοσιοποίηση δεδομένων στο Δίκτυο . Κάτι τέτοιο θα σήμαινε εν τοις πράγμασι απαγόρευση ανάρτησης προσωπικών δεδομένων καθώς είναι προφανές ότι δεν διαθέτουν όλες οι χώρες το «ικανοποιητικό επίπεδο προστασίας» των πληροφοριών που απαιτεί η κοινοτική Οδηγία για τη διασυνοριακή ροή προσωπικών δεδομένων. Αντίστοιχα ζητήματα είχαν τεθεί στην πολύκροτη υπόθεση των λεγόμενων PNR-data, όπου το Ευρωπαϊκό Κοινοβούλιο υποστήριξε ότι η πρόσβαση δημόσιων αρχών των ΗΠΑ στα δεδομένα PNR (σύστημα pull), σε αντίθεση με την εναλλακτική λύση της προώθησης δεδομένων (σύστημα push), συνιστά μια μη ρυθμιζόμενη από την Οδηγία και γι' αυτό μη επιτρεπτή σύμφωνα με το ευρωπαϊκό δίκαιο επεξεργασία δεδομένων .

Κεφάλαιο 6

Συμπεράσματα

Η αυτορρύθμιση προτάσσεται συχνά ως λύση για την αντιμετώπιση του παγκοσμιοποιημένου χαρακτήρα των πληροφοριακών ροών. Η παγκοσμιοποίηση των πληροφοριακών ανταλλαγών, η μη υποκείμενη σε φυσικά σύνορα δια-δικτυακή επικοινωνία και πραγματικότητα και σε τελευταία ανάλυση, η παγκοσμιοποίηση των πληροφοριακών αναγκών και απαιτήσεων εγείρει περαιτέρω το μείζον ζήτημα της φύσης των ρυθμιστικών κανόνων. Όπως ήδη επισημάνθηκε, αφενός οι ρυθμιστικές προσεγγίσεις , εφόσον και όπου υφίστανται, παρουσιάζουν σημαντικές αποκλίσεις. Αξίζει πάντως να επισημανθεί ότι η βασική διακήρυξη της τελευταίας (2008) Παγκόσμιας Διάσκεψης των Επιτρόπων και Αρχών Προστασίας Προσωπικών Δεδομένων αναφέρεται ακριβώς στην ανάγκη «να εκπονηθεί μία κοινή πρόταση για τη θέσπιση διεθνών προδιαγραφών για την προστασία της ιδιωτικότητας και των προσωπικών δεδομένων» .
Η λύση ενός παγκόσμιας εμβέλειας ρυθμιστικού εργαλείου είναι τόσο προφανής όσο και εξαιρετικά δυσχερής ως προς την επίτευξή της. Η δυσχέρεια αυτή αφορά τόσο την αδυναμία επίτευξης συναίνεσης ως προς τις κανονιστικές επιλογές όσο και το επίπεδο στο οποίο θα επιτευχθεί μία παγκόσμια συναίνεση, το οποίο – σχεδόν αναπόφευκτα – θα είναι η συνισταμένη ή ο ελάχιστος κοινός παρονομαστής των διαφόρων προσεγγίσεων για την προστασία της ιδιωτικότητας. Οι νομοθετικές επιλογές δεν είναι ζήτημα τεχνολογικής νομοτέλειας. Οι ροές δεδομένων, πληροφοριών, κεφαλαίου είναι εκφράσεις των διαδικασιών που κυριαρχούν στην οικονομία, την κοινωνία, την κρατική και διακρατική οργάνωση .

Δεν είναι λίγοι αυτοί που αναφέρονται σε «κρίση» της προστασίας της ιδιωτικότητας. Πρόκειται για κρίση δομική, καθώς κυρίως λόγω της τεχνολογικής εξέλιξης και της διάχυσης της επεξεργασίας των προσωπικών πληροφοριών τίθενται σε δοκιμασία τα βασικά εργαλεία αλλά και οι ίδιες οι προϋποθέσεις της προστασίας της ιδιωτικότητας. Ορισμένοι συγγραφείς υποστηρίζουν ότι η μεταφορά του Μεγάλου Αδελφού (1984) για τον συμβολισμό της επιτήρησης και των επιπτώσεών της δεν ανταποκρίνεται πλέον στη φύση της επιτήρησης και των σχέσεων, τις οποίες παράγει ή και επηρεάζει. Ήδη στο δημόσιο, θεωρητικό και κοινωνικοπολιτικό διάλογο, γίνεται αναφορά στους πολλούς «Μικρούς αδελφούς», στους οποίους δεν συμπεριλαμβάνονται μόνο οργανισμοί του ιδιωτικού τομέα που αποτελούν πηγή διακινδύνευσης για τα δικαιώματα αλλά και μεμονωμένα πρόσωπα .

Η διαθεσιμότητα και διάδοση της τεχνολογίας καθιστά τον καθένα δυνάμει πηγή επεξεργασίας πληροφορίας και συνακόλουθα πηγή παραβίασης δικαιωμάτων. Εν προκειμένω το παράδειγμα της διάδοσης της βιντεοεπιτήρησης στο επίπεδο της οικιακής και οικογενειακής χρήσης είναι χαρακτηριστικό. Το παγκόσμιο χωριό Facebook των εκατομμυρίων μελών, όπου οι χρήστες αυτό- και αλληλοεκτίθενται ή το Google Street View καταδεικνύουν δύο άλλες διαστάσεις της επιτήρησης, την αλληλοεπιτήρηση και την αυτό-έκθεση. Τα ψηφιακά κοινωνικά δίκτυα δεν λειτουργούν μόνο ως πλατφόρμες αυτοέκθεσης και κοινωνικών επαφών. Κάθε επικοινωνιακή συναλλαγή, όπως η ανάρτηση φωτογραφίας ή και αυτή καθεαυτή η πρόσκληση να ενταχθεί κάποιος στον «κύκλο» των «φίλων» ενέχει ή συνεπάγεται την επεξεργασία πληροφορίας για τρίτα πρόσωπα αλλά και την πιθανότητα της προσβολής των δικαιωμάτων τους.

Ακριβώς λόγω των μεταλλαγών ως προς τις επικοινωνιακές σχέσεις και τη διάχυση της επεξεργασίας προσωπικών πληροφοριών, προβάλλεται το

τελευταίο διάστημα, εκ νέου και με έμφαση, το μοντέλο του «αυτοπροστατευόμενου ατόμου-χρήστη». Ακριβέστερα, η προσέγγιση αυτή συντίθεται αφενός από την παροχή της δυνατότητας στο άτομο να προσδιορίσει με τον μηχανισμό της συγκατάθεσης το εύρος των πληροφοριών που οι άλλοι θα επεξεργάζονται για αυτό και αφετέρου από τη χρήση τεχνικών εργαλείων για να θωρακίσει την ιδιωτικότητά του. Υποστηρίζεται ότι είναι προτιμότερη η παροχή προϋποθέσεων εξατομικευμένης αυτοπροστασίας από την γενικευμένη επιταγή που «εξαναγκάζει» σε προστασία.

Το δίπολο αυτονομία – ετερονομία δοκιμάζεται ποικιλοτρόπως ακριβώς σε αυτό το πεδίο, όπου η αυτονομία του ατόμου είναι το βασικό διακύβευμα. Η προστασία δεδομένων αποσκοπεί στη διατήρηση της αυτονομίας μέσω της προστασίας δεδομένων αλλά ταυτόχρονα σε ορισμένες περιπτώσεις «υποκαθιστά» την αυτονομία μέσω κανονιστικών μηχανισμών προστασίας. Η συγκατάθεση του ατόμου ή η αυτοδιαχείριση της δικτυακής εικόνας και παρουσίας είναι όντως μία πρωταρχική έκφραση του δικαιώματος πληροφοριακού αυτοκαθορισμού. Ζητούμενο είναι να μπορεί το άτομο να καθιστά δυνατή την επιθυμητή επεξεργασία και να παρεμποδίζει την ανεπίτρεπτη. Ωστόσο, όπως ήδη επισημάνθηκε, η συγκατάθεση είναι ατελές παράδειγμα θεμελίωσης της επεξεργασίας καθώς η τεχνολογία επιτρέπει την πλήρη αυτονόμηση και αποξένωση της αρχικής επεξεργασίας της πληροφορίας, στην οποία αναφέρεται η συγκατάθεση-πηγή της νομιμότητας. Όσο και εάν η προσέγγιση της αυτοπροστασίας θα μπορούσε να είναι η απάντηση στη δυναμική τεχνική εξέλιξη και στην παγκοσμιοποίηση των πληροφοριακών ροών, είναι αμφίβολο, εάν υφίστανται οι - αντικειμενικές και υποκειμενικές - συνθήκες που εγγυώνται την ενσυνείδητη και ελεύθερη, άρα και υπεύθυνη, επιλογή των ατόμων.

Βιβλιογραφία

- “Προστασία της ιδιωτικότητας και τεχνολογίες πληροφορικής και επικοινωνιών (Νομικά και τεχνικά θέματα)”, Εκδόσεις Παπασωτηρίου, Ιούνιος 2010.
- “Ασφάλεια πληροφοριακών συστημάτων”, Εκδόσεις Νέων Τεχνολογιών, 2004.
- “Privacy in e-commerce: examining user scenarios and privacy preferences”. Ackerman, M.S., Cranor, L.F. and Reangle, J. (1999).
- “Preserving Privacy in Web Services”, Abdelmounaam Rezgui, Mourad Ouzzani, Athman Bouguettaya, Brahim Medjahed.
- “Network Security Essentials”, William Stallings, 2003.

Σύνδεσμοι

http://www.gsis.gr/gsis_site/

http://www.ika.gr/

https://www.winbank.gr/EL/Pages/default.aspx

http://gr.yahoo.com/

http://www.businessportal.gr/

http://www.oaed.gr/

http://www.acci.gr/acci/Home/tabid/28/language/el-GR/Default.aspx

http://www.dpa.gr/portal/page?_pageid=33,15048&_dad=portal&_schema=PORTAL

http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1763&Itemid=378

http://www.w3.org/TR

http://en.wikipedia.org/wiki/Web_Services_Description_Language