

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΜΕΡΟΣ 1 ^ο - ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ.....	3
ΚΕΦΑΛΑΙΟ 1	3
Εισαγωγή	3
1.1 Η σημασία της πληροφορίας σήμερα	3
1.2 Διαχείριση γνώσης.....	5
1.3 Κοινωνία της Πληροφορίας	8
ΚΕΦΑΛΑΙΟ 2	12
Επεξεργασία προσωπικών δεδομένων για άμεση διαφήμιση.....	12
2.1 Άμεσο Μκτ.....	12
2.2 Λόγοι ανάπτυξης του άμεσου Μκτ.....	13
2.3 Data base Μκτ & η σχέση του με το άμεσο Μκτ.....	14
2.4 Μοντέλο RADAR στο Data base Μκτ	23
2.5 Εργαλεία συλλογής και επεξεργασίας προσωπικών δεδομένων.....	24
2.6 Γεωγραφικά Πληροφοριακά Συστήματα	26
2.7 Παράδειγμα επεξεργασίας προσωπικών δεδομένων για σκοπούς άμεσης διαφήμισης.....	28
ΚΕΦΑΛΑΙΟ 3	30
Κίνδυνοι απ' την επεξεργασία προσωπικών δεδομένων.....	30
ΚΕΦΑΛΑΙΟ 4	34
Προστασία προσωπικών δεδομένων	34
4.1 Εισαγωγή.....	34
4.2 Τα πρώτα διεθνή κείμενα προστασίας προσωπικών δεδομένων	34
4.3 Κείμενα διεθνών οργανισμών για την προστασία προσωπικών δεδομένων	35
4.4 Η προστασία των δεδομένων προσωπικού χαρακτήρα στην Ελλάδα.....	50
ΚΕΦΑΛΑΙΟ 5	69
Ευαίσθητα προσωπικά δεδομένα	69
5.1 Εισαγωγή.....	69
5.2 Νομοθετική προστασία ευαίσθητων προσωπικών δεδομένων	70
ΚΕΦΑΛΑΙΟ 6	74
Αρχή προστασίας προσωπικών δεδομένων.....	74
6.1 Βασικές δραστηριότητες της Αρχής.....	74
6.2 Ηλεκτρονικό Κέντρο Εξυπηρέτησης του Πολίτη για την προστασία προσωπικών δεδομένων.....	77
6.3 Οδηγία για τους όρους της νόμιμης επεξεργασίας δεδομένων προσωπικού χαρακτήρα νέων μητέρων για τους σκοπούς της άμεσης εμπορίας ή διαφήμισης στο χώρο των Μαιευτηρίων	78
6.4 Όροι για την νόμιμη επεξεργασία δεδομένων προσωπικού χαρακτήρα για τους σκοπούς της άμεσης εμπορίας ή διαφήμισης και της διαπίστωσης πιστοληπτικής ικανότητας.....	79

ΚΕΦΑΛΑΙΟ 7.....	83
Διαβίβαση δεδομένων σε τρίτες χώρες.....	83
ΜΕΡΟΣ 2° ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ..	87
ΚΕΦΑΛΑΙΟ 1	87
Εισαγωγή	87
1.1 Ηλεκτρονικό εμπόριο και οι συνέπειές του στην οικονομία	87
1.3 Οφέλη του διαδικτύου για τις επιχειρήσεις.....	93
1.4 Παραβίαση ιδιωτικότητας στο διαδίκτυο	96
ΚΕΦΑΛΑΙΟ 2.....	99
Διαφήμιση στο διαδίκτυο	99
2.1 Εισαγωγή.....	99
2.2 Μέθοδοι διαφήμισης στο διαδίκτυο	99
2.3 Γνώση του προφίλ των πελατών για αποτελεσματικό spamming.....	105
2.4 Επεξεργασία δεδομένων με μεθόδους εξόρυξης δεδομένων	109
2.5 Δυσμενείς συνέπειες του spamming - τεχνικά μέτρα αντιμετώπισης.....	110
2.6 Τρόποι ρύθμισης του spam: opt in - opt out	115
2.7 Νομοθεσία για το spamming.....	120
2.8 Νομολογία για spamming	132
ΚΕΦΑΛΑΙΟ 3	137
Άλλα νομοθετήματα για την προστασία δεδομένων στο διαδίκτυο	137
3.1 Νομοθεσία για την προστασία του απορρήτου στο διαδίκτυο	137
3.2 Αυτορρύθμιση στο διαδίκτυο.....	140
3.3 Συγκριτική μελέτη για την πολιτική προστασίας της ιδιωτικότητας στα sites των ΗΠΑ-Αγγλία-Γαλλία.....	142
ΚΕΦΑΛΑΙΟ 4	146
Τεχνικά μέτρα προστασίας των δεδομένων στο διαδίκτυο	146
4.1 Εισαγωγή.....	146
4.2 Συστήματα PET (Privacy Enhancing Technologies).....	146
4.3 Πρότυπο καταγραφής στοιχείων OPS (Open Profiling Standard)	147
4.4 Πρότυπο P3P.....	147
4.5 Λογισμικό για τη διαχείριση προγραμμάτων cookies	149
4.5 Αναταχυδρόμοι (re-mailers).....	149
4.6 Ενδιάμεσοι εξυπηρετητές (Proxy Servers).....	150
4.7 The Mail Abuse Prevention System (MAPS)	151
4.7 Κρυπτογραφία	151
ΚΕΦΑΛΑΙΟ 5	156
Νομοθεσία άλλων χωρών για την προστασία δεδομένων.....	156
5.1 Γαλλία	156
5.2 Γερμανία	157
5.3 Ηνωμένο Βασίλειο.....	157
5.4 Ηνωμένες Πολιτείες Αμερικής.....	158
ΣΥΜΠΕΡΑΣΜΑΤΑ	160
ΒΙΒΛΙΟΓΡΑΦΙΑ.....	162

ΜΕΡΟΣ 1^ο - ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

ΚΕΦΑΛΑΙΟ 1

Εισαγωγή

1.1 Η σημασία της πληροφορίας σήμερα

Ζούμε σε μια εποχή όπου οι παραδοσιακοί πυλώνες της οικονομικής δύναμης- δηλαδή το χρήμα, η γη, οι πρώτες ύλες και η τεχνολογία- έχουν πάψει να αποτελούν τους μοναδικούς καθοριστικούς παράγοντες επιτυχίας για μια επιχείρηση. Σήμερα το μέλλον και η βιωσιμότητα μιας επιχείρησης καθορίζονται πλέον απ' την ικανότητά της να αξιοποιεί τον πολυτιμότερο ίσως πόρο της: την πληροφορία.¹ Η πληροφορία είναι το αποτέλεσμα που προκύπτει από κάποια κατάλληλη επεξεργασία δεδομένων, η οποία γίνεται με τη βοήθεια της σύγχρονης τεχνολογίας. Όπως ακριβώς τα ακατέργαστα υλικά, με κάποια επεξεργασία μετατρέπονται σε έτοιμα προϊόντα, έτσι και τα δεδομένα που συνίστανται σε ακωδικοποίητα μηνύματα, μετασχηματίζονται σε πληροφορίες μέσα απ' την διαδικασία της επεξεργασίας. Οι πληροφορίες που παίρνουμε απ' την επεξεργασία δεδομένων μπορεί να χρησιμοποιηθούν ως νέα δεδομένα για περαιτέρω επεξεργασία και να δώσουν ως αποτελέσματα νέες πληροφορίες.²

Η πληροφορία είναι απαραίτητη σε όλους τους τομείς της ανθρώπινης σκέψης και δράσης. Οι πληροφορίες είναι απαραίτητες σε μεμονωμένα άτομα για να οργανώσουν τη ζωή τους, τις σπουδές τους ακόμη και τη διασκέδασή τους, π.χ. για να οργανώσουν τις διακοπές τους, ή να επιλέξουν τη σχολή που θα σπουδάσουν κτλ. Επίσης οι πληροφορίες είναι απαραίτητες σ' αυτούς που παίρνουν αποφάσεις σε μεγάλους οργανισμούς. Τα διοικητικά στελέχη σε μια επιχείρηση εκτελούν τις λειτουργίες του σχεδιασμού (planning), της οργάνωσης (organizing), της στελέχωσης (staffing), και του ελέγχου (controlling), απ' την επιτυχή διεκπεραίωση των οποίων εξαρτάται και η κερδοφορία της εταιρίας. Για

¹ Με τον όρο "πληροφορία" εννοείται κάθε στοιχείο γνώσης και κρίσης που μεταδίδεται με τη βοήθεια του λόγου, του ήχου ή της εικόνας, καθώς και με το σύνολο των συμβόλων που είναι κατανοητό στους ανθρώπους, με σκοπό να τους ενημερώσει για κάποιο γεγονός ή θέμα. Εμμ.Κριαράς "Νέο ελληνικό λεξικό της σύγχρονης δημοτικής γλώσσας, γραπτής και προφορικής"

² Γ.Δ. Μπώκος, "Τεχνολογία και πληροφόρηση", σελ.5-6

να εκτελεστούν όμως επιτυχώς οι παραπάνω λειτουργίες απ' τη διοίκηση, απαιτείται η λήψη πληροφοριών προκειμένου να ληφθούν οι σωστές αποφάσεις. Ωστόσο η πληροφορία είναι ένα αγαθό, το οποίο όπως όλα τα αγαθά δεν παρέχεται δωρεάν. Είναι αναγκαίο το κόστος που απαιτείται για την απόκτηση της πληροφορίας να είναι συγκρίσιμο με την αξία της.³

Επιθυμητές ιδιότητες μιας πληροφορίας είναι η ακρίβεια, η επικαιρότητα, η πληρότητα και η σχετικότητα.

1. Η **ακρίβεια** μπορεί να οριστεί ως ο λόγος της σωστής πληροφορίας προς την παραγόμενη μέσα σε μια χρονική περίοδο. Για παράδειγμα, αν παράγονται 1000 πληροφορίες και 980 είναι σωστές, τότε ο λόγος ακρίβειας είναι 0,98.

2. Η **επικαιρότητα** είναι ένα άλλο σπουδαίο χαρακτηριστικό της πληροφορίας. Ακριβής πληροφορία που φθάνει αργά και δεν μπορεί να χρησιμοποιηθεί δεν έχει καμιά αξία. Η ακρίβεια και μόνο δεν είναι αρκετή. Παλαιότερα υπήρχε κάποια ασυμφωνία μεταξύ ακρίβειας και επικαιρότητας. Μεγαλύτερη ακρίβεια με περισσότερους ελέγχους στα δεδομένα εισόδου είχε ως αποτέλεσμα την ελάττωση της ταχύτητας επεξεργασίας και επομένως και της επικαιρότητας της πληροφορίας. Η χρήση των υπολογιστών ελάττωσε τη σημασία αυτής της αντίθεσης μεταξύ ακρίβειας και ταχύτητας επεξεργασίας.

3. Η **πληρότητα** είναι ένα σημαντικό χαρακτηριστικό της πληροφορίας. Μια έκθεση είναι πλήρης όταν δίνει στη διοίκηση όλες τις πληροφορίες που είναι αναγκαίες για να πάρει απόφαση.

4. Η **σχετικότητα** τέλος, θεωρείται ένα επίσης χαρακτηριστικό της πληροφορίας. Πολλά συστήματα έχουν σχεδιασθεί με την προϋπόθεση ότι η έλλειψη πληρότητας είναι το σημαντικότερο μειονέκτημα της πληροφόρησης. Η διοίκηση συχνά κατακλύζεται με πληροφορίες, πολύ περισσότερες απ' όσες μπορεί να χρησιμοποιήσει. Σημαντικές πληροφορίες κρύβονται μέσα στους σωρούς της λεπτομέρειας. Η συνοπτική και σχετική πληροφορία δίνει περιληπτικά τα δεδομένα που παρουσιάζουν ενδιαφέρον.⁴

³ Βασίλειος Σκούρης, Κρατερός Ιωάννου, "Ελευθερία της διαφήμισης", σελ. 125

⁴ Kenneth C. Laudon, Jane P. Laudon, "Management Information Systems", σελ. 436

Η πληροφορία, εκτός του ότι αποτελεί σημαντικό εργαλείο λήψης αποφάσεων απ' τις επιχειρήσεις, συμβάλει επίσης στην αποτελεσματικότερη άσκηση της κρατικής πολιτικής. Το κράτος δεν μπορεί πλέον να λειτουργήσει αποτελεσματικά χωρίς την πρόσβαση σε όλες εκείνες τις πληροφορίες, η γνώση και επεξεργασία των οποίων θεωρείται απαραίτητη για την παρακολούθηση των οικονομικών και κοινωνικών εξελίξεων. Η επεξεργασία των πληροφοριών αυτών όπως π.χ. εκκαθάριση φορολογικών δηλώσεων, υπολογισμός τελών κυκλοφορίας κτλ. που συνεχώς αυξάνονται σε όγκο, γίνεται με τη βοήθεια σύγχρονων τεχνολογιών πληροφορικής. Τέλος πρέπει να τονιστεί η αποφασιστική συμβολή της πληροφορίας στην ανάπτυξη της προσωπικότητας του ατόμου, αφού αποτελεί θεμελιώδη ανάγκη του η δυνατότητα να αντλεί πληροφορίες από κάθε πηγή με σκοπό τη διεύρυνση των γνώσεών του. Επίσης σημαντική είναι η συμβολή της πληροφορίας και στην εύρυθμη λειτουργία του δημοκρατικού πολιτεύματος, αφού μόνο ο πληροφορημένος πολίτης είναι σε θέση να ενεργεί υπεύθυνα.⁵

1.2 Διαχείριση γνώσης

Ιδιαίτερη σημασία για τα θέματα της πληροφορίας έχει η έννοια της "Γνώσης", η οποία παράγεται από το συνδυασμό πληροφοριών.⁶ Μέχρι πρόσφατα, πολλές επιχειρήσεις λειτουργούσαν βασισμένες στην ατομική γνώση ορισμένων βασικών στελεχών τους. Ωστόσο οι ανάγκες που παρουσιάζονταν απέδειξαν ότι ναι μεν η εξατομικευμένη γνώση είναι τεράστιας αξίας και συχνά αναντικατάστατη, το σύγχρονο όμως επιχειρηματικό περιβάλλον απαιτεί την πλήρη αξιοποίηση της επιχειρηματικής γνώσης του συνόλου μιας εταιρίας.

Η επιχειρηματική γνώση βρίσκεται ενσωματωμένη τόσο στις δεξιότητες των στελεχών όσο και στα συστήματα και τα δίκτυα που χρησιμοποιούνται απ' τα στελέχη για τη διεκπεραίωση των επιχειρηματικών λειτουργιών. Οι ικανότητες και οι εμπειρίες των στελεχών μιας επιχείρησης, οι δυνατότητες καινοτομίας και

⁵ Γέροντας Απόστολος, "Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία προσωπικών δεδομένων", σελ.91-93

⁶ "Γνώση" νοείται το αποτέλεσμα κάθε πνευματικής διαδικασίας για την κατανόηση της πραγματικότητας, είτε άμεσα με τις αισθήσεις είτε έμμεσα με την παρέμβαση του λογικού. Λεξικό της Κοινής Νεοελληνικής, ΑΠΘ Ινστιτούτο Νεοελληνικών Σπουδών

δημιουργικότητας, οι βέλτιστες επιχειρηματικές πρακτικές, οι πατέντες, το know-how που η επιχείρηση έχει συσσωρεύσει για την αγορά και τους πελάτες της, καθώς και η γνώση για τους ανταγωνιστές της, είναι ζωτικής σημασίας.⁷

Πρόκειται για το πλέον σημαντικό περιουσιακό στοιχείο μιας εταιρίας και το μόνο διατηρήσιμο συγκριτικό πλεονέκτημά της. Στην πράξη, η εταιρία είναι υποχρεωμένη όχι μόνο να συγκεντρώνει κάθε πληροφορία που κυκλοφορεί στο περιβάλλον της, αλλά και να μετουσιώσει τις πληροφορίες αυτές σε γνώση, προκειμένου να αυξήσει την ταχύτητα αντίδρασης στις εξελίξεις και να πετύχει τη βέλτιστη δυνατή εξυπηρέτηση του πελάτη μέσω της κατανόησης των αναγκών του.

Με τον όρο “διαχείριση γνώσης”, εννοούμε την πρακτική της «δημιουργίας, σύλληψης, μεταβίβασης και πρόσβασης στη σωστή γνώση, η οποία απαιτείται τόσο για τη λήψη αποτελεσματικών αποφάσεων απ’ τα διευθυντικά στελέχη, όσο και για την ανάληψη των πλέον κατάλληλων ενεργειών (υλοποίησης στρατηγικής) που θα υποστηρίξουν την ακολουθούμενη επιχειρηματική στρατηγική»⁸. Η διαχείριση γνώσης αποτελεί μια νέα διοικητική πρακτική που αφορά τη συστηματική και συλλογική δημιουργία, τη διάχυση, χρήση και αξιοποίηση της επιχειρηματικής γνώσης με σκοπό τη ριζική βελτίωση της επιχειρηματικής ανταγωνιστικότητας και την ανάπτυξη της καινοτομίας.

Τα οφέλη που έχει για την επιχείρηση η διαχείριση της γνώσης είναι τα εξής:⁹

- Ωφέλεια χρόνου

Οι εργαζόμενοι δεν χρειάζεται πλέον να σπαταλούν χρόνο στην κατηγοριοποίηση ή την αναγνώριση της προέλευσης αρχείων που δεν είναι κωδικοποιημένα. Αυτό σημαίνει ότι στους κόλπους μιας επιχείρησης οι εργαζόμενοι μπορούν να ανταλλάξουν τις απόψεις τους για κάποια θέματα είτε απέχουν δύο γραφεία ο ένας απ’ τον άλλο είτε βρίσκονται σε δύο διαφορετικές χώρες. Έτσι μπορούν ακόμα να χρησιμοποιούν το χρόνο τους στην ανάλυση

⁷ Περιοδικό ‘‘ΧΡΗΜΑ’’, τεύχος 2^ο, Οκτώβριος 2001, σελ.2

⁸ J. Birkinshaw, ‘‘Why is knowledge Management so difficult?’’, Business Strategy Review 2001, σελ. 11-18,

⁹ Kenneth C. Laudon, Jane P. Laudon, ό.π., σελ. 434-435

πληροφοριών και όχι στην ανεύρεσή τους. Επίσης επιτυγχάνεται σοβαρή μείωση του χρόνου ανταπόκρισης σε αλληλογραφία και σε οποιαδήποτε μορφή εγγράφου απαιτεί μια έγκαιρη απάντηση, γεγονός που ισοδυναμεί με πιο ολοκληρωμένη, ταχύτατη και τεκμηριωμένη εξυπηρέτηση.

- Ωφέλεια κόστους

Γίνεται οικονομία στις ανθρωποώρες που καταναλώνονται για να παραχθεί ή να εντοπιστεί ένα έγγραφο, γεγονός που σημαίνει ότι επιτυγχάνεται άμεση μείωση του λειτουργικού κόστους της επιχείρησης (όπως αποθηκευτικοί χώροι, χρόνοι αναζήτησης και αναπαραγωγής εγγράφων). Ακόμα, όταν μια εταιρία έχει άμεση πρόσβαση σε ένα μεγάλο όγκο δεδομένων και γνώσεων μπορεί να απολαμβάνει σημαντικά οφέλη, όπως η γρήγορη ανάπτυξη προϊόντων, πιο εξειδικευμένο προσωπικό και μια εμπειριστατωμένη και πλούσια γκάμα υπηρεσιών που ανταποκρίνονται στις ανάγκες της πελατειακής βάσης, δηλαδή στοιχεία που είτε μειώνουν το κόστος είτε αυξάνουν τα έσοδα.

- Ωφέλεια Στρατηγικής

Η πρόσβαση στην πληροφορία προσφέρει καλύτερη ενημέρωση, αλλά και διαδικασίες λήψης αποφάσεων που λαμβάνουν υπόψη τους όλα τα στοιχεία και όχι μόνο εκείνα που φθάνουν στην διοίκηση φιλτραρισμένα. Έτσι, οι όποιες αποφάσεις στατιστικά αποφεύγουν τα πιο συνηθισμένα λάθη, τα οποία προέρχονται από άγνοια κρίσιμων δεδομένων ή δεδομένων της τελευταίας στιγμής.

- Ωφέλεια ελέγχου

Η εταιρία γνωρίζει τί γνωρίζουν οι υπάλληλοί της! Και μάλιστα άμεσα (online) ακόμα και για τον νεοδιοριζόμενο. Έτσι, υπάρχει ρεαλιστικός έλεγχος του τί κάνει ο καθένας, με τί ασχολείται, πού πραγματικά αξιοποιεί τα ταλέντα του και πού φρενάρει η παραγωγικότητά του. Ένα σύστημα διαχείρισης γνώσης μπορεί να είναι το ιδανικό συμπλήρωμα σε ένα σύστημα διαχείρισης έργου, καθώς ενημερώνει πραγματικά για την πρόοδο των εργασιών.

1.3 Κοινωνία της Πληροφορίας

Η σημασία της πληροφορίας και της διαχείρισης της γνώσης, διαπιστώνεται με τις δυνατότητες της σύγχρονης τεχνολογίας, η οποία καθιστά δυνατή την αύξηση της συλλογής και αποθήκευσης πληροφοριών και τη μείωση του χρόνου πρόσβασης στα αρχεία. Οι νέες τεχνολογίες πληροφορίας αποτελούν μια κομμάτι της καθημερινότητας όλων των πολιτών. Οι νέες αυτές τεχνολογίες εφαρμόζονται κάθε φορά που χρησιμοποιούμε την πιστωτική μας κάρτα, όταν αγοράζουμε προϊόντα απ' το internet, όταν σαρώνονται οι κωδικοί των προϊόντων στο ταμείο του super market κτλ. Στο κατώφλι του 21^{ου} αιώνα, η ραγδαία εξέλιξη αυτών των τεχνολογιών και η διαδοσή τους σε όλες τις εκφάνσεις της καθημερινής μας ζωής, χτίζουν μια παγκόσμια Κοινωνία της Πληροφορίας με νέα δεδομένα και νέες ευκαιρίες για την ανάπτυξη, την απασχόληση, την ευημερία και την ποιότητα ζωής των πολιτών. Σήμερα η Κοινωνία της Πληροφορίας τείνει να ταυτιστεί με το διαδίκτυο, το οποίο συνιστά ένα μέσο και πεδίο επικοινωνίας και συναλλαγής. Μέσω του internet εκατομμύρια άνθρωποι μπορούν να επικοινωνούν μεταξύ τους και να έχουν πρόσβαση σε τεράστιο όγκο πληροφοριών σε ολόκληρο τον κόσμο.^{10,11} Η χρήση του internet τα τελευταία χρόνια έχει αυξηθεί δραματικά, καθώς οι χρήστες το χρησιμοποιούν για διάφορους λόγους, όπως π.χ. για αναζήτηση πληροφοριών ή ακόμα και για αγορές προϊόντων ή υπηρεσιών.

Μερικές απ' τις νέες δυνατότητες και ευκαιρίες που προσφέρει η εποχή της Πληροφορικής Επανάστασης παρουσιάζονται συνοπτικά παρακάτω:

➤ Ηλεκτρονική Επικοινωνία: Όλο και περισσότεροι άνθρωποι επικοινωνούν καθημερινά μέσω των υπολογιστών παρά μέσω τηλεφώνου, ταχυδρομείου ή άλλων παραδοσιακών μέσων. Το Ηλεκτρονικό Ταχυδρομείο προσφέρει τη δυνατότητα αποστολής και λήψης οποιουδήποτε γραπτού μηνύματος σε όλο τον κόσμο μέσα σε μερικά δευτερόλεπτα.

➤ Τηλε-διάσκεψη: Η τηλε-διάσκεψη επιτρέπει την άμεση επικοινωνία με χρήση εικόνας και ήχου μέσω υπολογιστή. Το υψηλό κόστος των υποδομών

¹⁰ Λίλιαν Μήτρου, "Το δίκαιο στην Κοινωνία της Πληροφορίας", σελ. 16-17

¹¹ Thornburg D. David, "Welcome to the communication age", www.emeraldinsight.com

καθιστούν την τεχνολογία αυτή περισσότερο προσιτή στις μεγάλες επιχειρήσεις και στους δημόσιους οργανισμούς που επιθυμούν να παρέχουν υπηρεσίες σε απομακρυσμένες τοποθεσίες. Η χρησιμοποίηση των τηλεδιασκέψεων αναμένεται ότι θα επεκταθεί όταν θα κυκλοφορήσουν στο εμπόριο φθηνές επιτραπέζιες βιντεοκάμερες που θα μπορούν να συνδεθούν με προσωπικό υπολογιστή.

➤ Υπηρεσίες: Οι ηλεκτρονικές υπηρεσίες αποτελούν ταχέως αναπτυσσόμενο τομέα του Ηλεκτρονικού Εμπορίου. Λογιστικές επιχειρήσεις προσφέρουν ήδη συμβουλευτικές υπηρεσίες με ηλεκτρονικά μέσα. Οι συνδρομητές έχουν πρόσβαση στη διεύθυνση της επιχείρησης στο web, όπου μπορούν να αναζητήσουν κάποια βάση δεδομένων για πληροφόρηση ή να παρακολουθήσουν σχετικές ειδήσεις.

➤ Χρηματοπιστωτικές υπηρεσίες: Σχεδόν όλα τα χρηματοπιστωτικά ιδρύματα επιτρέπουν στους πελάτες την αγορά και πώληση χρεογράφων με ηλεκτρονικά μέσα.

➤ Αναζήτηση πληροφοριών: Η αναζήτηση και ανάκτηση πληροφοριών είναι πλέον υπόθεση ρουτίνας για πολλούς ανθρώπους που μπορούν να προσπελάσουν απομακρυσμένες πηγές πληροφοριών. Το διαδίκτυο επιτρέπει σε ερευνητές αλλά και απλούς ανθρώπους να έχουν πρόσβαση σε μια πληθώρα γνώσεων για όποιο θέμα τους ενδιαφέρει¹²

➤ Ηλεκτρονικές Αγορές: Η δυνατότητα διεξαγωγής πραγματικών αγορών απ'το σπίτι ξεκίνησε με τη χρήση της τηλεόρασης και του τηλεφώνου, αλλά σήμερα έχει επεκταθεί και γίνεται κυρίως μέσω των Η/Υ και του διαδικτύου. Σήμερα ο πελάτης μπορεί να αναζητήσει με απλό και φιλικό τρόπο τα προϊόντα που επιθυμεί, να τα παραγγείλει και να τα εξοφλήσει μέσα απ'το διαδίκτυο. Επιπλέον οι επιχειρήσεις έχουν τη δυνατότητα να εξατομικεύσουν και να αναλύσουν τη συμπεριφορά των πελατών τους, όπως θα αναφέρουμε αναλυτικά στη συνέχεια, να ελέγξουν και να αναπληρώσουν τα αποθέματά τους με πιο αποδοτικό τρόπο και να προωθήσουν αποτελεσματικότερα τα προϊόντα τους. Τέλος στο διαδίκτυο έχουν αναπτυχθεί συστήματα κρατήσεων (πχ για τουριστικά

¹² Δουκίδης Ι. Γεώργιος, “Ηλεκτρονικό Εμπόριο”, σελ. 58

γραφεία, για κρατήσεις εισιτηρίων κτλ) που επιτρέπουν στους χρήστες να κάνουν ηλεκτρονικά την κράτησή τους, εξοικονομώντας πολύτιμο χρόνο.¹³

Αξίζει να αναφερθεί ότι οι εξελίξεις στον τομέα της πληροφορικής, συνέβαλαν στην ταχύτερη και αποτελεσματικότερη ροή πληροφοριών. Η αύξηση της χωρητικότητας και της ταχύτητας των υπολογιστών και των δικτύων έχει οδηγήσει σε μια υπερπροσφορά πληροφοριών και γνώσεων που ταξιδεύουν καθημερινά σε "υπερλεωφόρους πληροφοριών". Ένα CD-ROM ζυγίζει 15 γραμμάρια και χωράει περισσότερες πληροφορίες από 330,000 σελίδες χαρτί. Η χρήση προηγμένων υπολογιστικών συστημάτων δίνει τη δυνατότητα στις επιχειρήσεις να διαχειρίζονται μεγάλο όγκο πληροφοριών σε μικρό χρονικό διάστημα και να αντιμετωπίζουν περίπλοκα προβλήματα. Επίσης οι νέες γενιάς Η/Υ μπορούν να εντοπίσουν ζητούμενες πληροφορίες μέσα από μεγάλους όγκους στοιχείων σε χρόνο μικρότερο του ενός δευτερολέπτου καθώς και να τις διατηρήσουν αμετάβλητες και αναλλοίωτες. Ωστόσο ο Η/Υ δε συλλέγει μόνο πληροφορίες, αλλά τις επεξεργάζεται κιόλας. Είναι σε θέση να συνδυάζει αρχεία πληροφοριών και να συσχετίζει τα δεδομένα προκειμένου να παραχθεί γνώση, καθώς και να μεταδίδει τις πληροφορίες αυτές.¹⁴

Στα πλαίσια της τεχνολογικής εξέλιξης σε συνδυασμό με την ελευθερία στην πληροφόρηση, αποτελεί πάγια τακτική των επιχειρήσεων η συλλογή, αποθήκευση, επεξεργασία και μεταβίβαση πληροφοριών που αφορούν προσωπικά δεδομένα των καταναλωτών με τη βοήθεια Η/Υ. Σύμφωνα με το άρθρο 2 του νόμου 2472/1997, "προσωπικά δεδομένα" είναι «κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων. Δεν λογίζονται ως δεδομένα προσωπικού χαρακτήρα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, απ' τα οποία δεν μπορούν πλέον να προσδιορισθούν τα υποκείμενα των δεδομένων». Προσωπικό δεδομένο θεωρείται λοιπόν, το όνομα, η ηλικία, η επαγγελματική κατάσταση του ατόμου, ο τόπος διαμονής του, η θρησκευτική του συνείδηση, οι πολιτικές του πεποιθήσεις, η υγεία του, η ερωτική του ζωή κτλ. Ένας απ' τους

¹³ Waiman Cheung, "The use of the World Wide Web for commercial purposes", www.emeraldinsight.com

¹⁴ Έκθεση Αρχής Προστασίας Προσωπικών Δεδομένων, 2002

λόγους που οδήγησε τις επιχειρήσεις στη συλλογή και επεξεργασία προσωπικών δεδομένων των καταναλωτών είναι οι σύγχρονες πολιτικές προώθησης των προϊόντων που εφαρμόζουν στα πλαίσια του άμεσου Μκτ, οι οποίες θα εξετασθούν παρακάτω.¹⁵

¹⁵ Μπαλωμένου Χριστίνα, ‘‘Προσωπικά Δεδομένα’’, 2004, www.lawnet.gr

ΚΕΦΑΛΑΙΟ 2

Επεξεργασία προσωπικών δεδομένων για άμεση διαφήμιση

2.1 Άμεσο Μκτ

Πριν 50 χρόνια οι επιχειρήσεις χρησιμοποιούσαν ως αποκλειστική μέθοδο προώθησης των προϊόντων τους το λεγόμενο “παραδοσιακό Μκτ” (Mass Mkt) για να προσεγγίσουν τους δυνητικούς τους πελάτες και προσπαθούσαν να πείσουν τους καταναλωτές να αγοράσουν το προϊόν τους μέσω διαφόρων καναλιών επικοινωνίας όπως π.χ. τηλεόραση, ραδιόφωνο, εφημερίδες, περιοδικά κτλ, τα οποία επιστρατεύονταν για την προβολή του προϊόντος σε μια μεγάλη μάζα καταναλωτών. Οι επιχειρήσεις δεν ελάμβαναν υπ’ όψη τους τις διαφορετικές ανάγκες των καταναλωτών και στόχευαν σε όλους με το ίδιο μίγμα Μκτ.

Ωστόσο τη δεκαετία του ’80, τα πράγματα άρχισαν να αλλάζουν και οι επιχειρήσεις στράφηκαν στο άμεσο Μκτ. Άρχισαν να τμηματοποιούν την αγορά ανάλογα με τις ανάγκες των καταναλωτών, να δημιουργούν ομογενείς αγορές-στόχους και να στοχεύουν σ’αυτές με διαφορετικά μίγματα Μκτ. Η λογική του άμεσου Μκτ στηρίζεται στην πεποίθηση ότι κάθε πελάτης είναι μοναδικός, ότι έχει πολλές και εξατομικευμένες ανάγκες, και γι’ αυτό αν η επιχείρηση επιθυμεί να δημιουργήσει μια δυνατή σχέση μαζί του, θα πρέπει να τον προσεγγίσει ξεχωριστά, δείχνοντας ότι σκύβει πάνω απ’ αυτόν και τις ανάγκες του. Απευθύνεται λοιπόν σ’ αυτόν με προσωποποιημένα μηνύματα, κατάλληλα προσαρμοσμένα στις ανάγκες του.^{16 17} Στα πλαίσια του άμεσου Μκτ, βασικό ρόλο διαδραματίζει η άμεση διαφήμιση. Άμεση διαφήμιση είναι η μετάδοση διαφημιστικού μηνύματος απευθείας στον καταναλωτή μέσω τηλεφώνου,

¹⁶ Γαλάνης Π. Βασίλειος, “Direct Marketing: η λογική του άμεσου μάρκετινγκ”, σελ.28

¹⁷ Richards A. Feinberg and Mary Ann Eastlick, “Direct Marketing in the USA”, www.emeraldinsight.com

τηλεομοιοτυπίας (φαξ), ηλεκτρονικού ταχυδρομείου, αυτόματης κλήσης ή άλλου ηλεκτρονικού μέσου επικοινωνίας¹⁸

2.2 Λόγοι ανάπτυξης του άμεσου Μκτ

Ιδίως τα τελευταία χρόνια η ανάπτυξη τεχνικών άμεσου Μκτ για την προσέλκυση πελατών και τη διατήρηση μακροχρόνιων σχέσεων μαζί τους, είναι ραγδαία. Αξίζει να αναφερθεί ότι σύμφωνα με έρευνα του Direct Marketing Association που διεξήχθη το 2002, οι πωλήσεις από άμεσο Μκτ στην Αμερική σημείωσαν αύξηση το 2001 κατά 9% σε σχέση με τον προηγούμενο χρόνο, αγγίζοντας τα \$1,86 τρις συγκριτικά με τα \$1,71 τρις το 2000. Το 2002 το ποσό αυτό έφθασε τα \$2 τρις. Σύμφωνα με προβλέψεις της ίδιας έρευνας, τα έσοδα θα αυξάνονται με ετήσιο ρυθμό 8,3% μέχρι το 2006, την ίδια στιγμή που οι συνολικές πωλήσεις στην Αμερική αυξάνονται με ρυθμό 4,8% ετησίως. Οι τομείς οι οποίοι σημείωσαν μεγαλύτερες πωλήσεις οφειλόμενες σε μεθόδους άμεσου Μκτ είναι: Υπηρεσίες (\$176,9 δις), κτηματομεσιτικές εταιρίες (\$63 δις) και ασφάλειες (\$61,4 δις). Τέλος, τα έξοδα που έκαναν οι επιχειρήσεις το 2001 για την εφαρμογή στρατηγικών άμεσου Μκτ καταλάμβαναν το 55,2% των συνολικών διαφημιστικών εξόδων, ποσοστό που θεωρείται υψηλό.¹⁹ Οι λόγοι που οδήγησαν στην ανάπτυξη αυτή είναι πολλοί και διάφοροι. Κατ'αρχήν οι αυξημένες απαιτήσεις των σημερινών καταναλωτών για καλύτερη ικανοποίηση των αναγκών τους, αποτελεί έναν απ'τους σημαντικότερους λόγους. Σήμερα οι ανάγκες των καταναλωτών έχουν διαφοροποιηθεί σε σημαντικό βαθμό και προκειμένου να ικανοποιηθούν αποτελεσματικότερα, οι επιχειρήσεις πρέπει να αντιμετωπίζουν τον κάθε πελάτη ως μεμονωμένη περίπτωση και να απευθύνονται σ' αυτόν με προσωποποιημένα μηνύματα που να καλύπτουν πλήρως τις δικές του ανάγκες. Επίσης οι τεχνικές της άμεσης διαφήμισης, όπως π.χ. e-mail, telemarketing, ταχυδρομείο κτλ, έχουν χαμηλότερο κόστος ανά αποδέκτη σε σχέση με την τηλεοπτική ή άλλες μορφές μαζικής διαφήμισης και προσφέρουν τη δυνατότητα ελέγχου της αποτελεσματικότητας των μηνυμάτων

¹⁸ Έννο Μαγιάση, "Διαφήμιση και internet", www.lawnet.gr

¹⁹ Dawn Anfuso, "Sales Revenue from DM and eMarketing On Rise", 2002, www.imediconnection.com

μέσω της ανταπόκρισης των αποδεκτών. Η ανταπόκριση του καταναλωτή στα μηνύματα που δέχεται μπορεί να συνίσταται σε αγορά του προϊόντος, σε αναζήτηση περισσότερων πληροφοριών μέσω τηλεφώνου ή διαδικτύου, ή ακόμα μια επίσκεψη στο κατάστημα που πουλάει το προϊόν. Μ'αυτόν τον τρόπο λοιπόν, μια επιχείρηση μπορεί να διαπιστώσει την αποτελεσματικότητα των μεθόδων του άμεσου Μκτ που εφαρμόζει. Στην περίπτωση του internet η ανταπόκριση των χρηστών σ' ένα διαφημιστικό μήνυμα φαίνεται απ' τα "click through rates". Τα "click through rates" μετρούν το ποσοστό των χρηστών που έκαναν "κλικ" πάνω σ' ένα διαφημιστικό μήνυμα προκειμένου να μπουν στο εν λόγω site που αφορά ένα συγκεκριμένο προϊόν και αποτελούν ένα μέτρο μέτρησης της **άμεσης** ανταπόκρισης των χρηστών σε μια διαφήμιση.²⁰ Τέλος, η ανάπτυξη νέων τρόπων πληρωμής μέσω πιστωτικών καρτών, έχει συμβάλει στην ανάπτυξη του άμεσου Μκτ, καθώς οι αγορές μπορούν να γίνουν πλέον μέσω διαδικτύου, ή fax ή ακόμα μέσω τηλεφώνου. Η άμεση διαφήμιση, σε αντίθεση με τη μαζική, δίνει κίνητρο στους καταναλωτές να προχωρήσουν σε αγορές απ' το σπίτι τους με τη χρήση της πιστωτικής τους κάρτας. Παραδείγματος χάριν, ένας χρήστης του διαδικτύου που λαμβάνει ένα διαφημιστικό μήνυμα μέσω e-mail, μπορεί να κάνει "κλικ" πάνω στο μήνυμα αυτό, και να προχωρήσει απ' ευθείας σε αγορά του προϊόντος χωρίς να χρειάζεται να επισκεφθεί το κατάστημα πώλησης. Αντίθετα, η διαφήμιση μέσω τηλεόρασης δημιουργεί μόνο μια εικόνα για το προϊόν και πληροφορεί τον καταναλωτή σχετικά μ'αυτό, χωρίς όμως να του δίνει τη δυνατότητα να το αγοράσει απ' το σπίτι του.^{21, 22}

2.3 Data base Mkt & η σχέση του με το άμεσο Μκτ

Απ' την προηγούμενη ανάλυση εξάγεται το συμπέρασμα ότι το άμεσο Μκτ αποτελεί ένα προσωπικό τρόπο προσέγγισης υφιστάμενων και δυνητικών πελατών, εστιάζοντας αποτελεσματικά και με σχετικά χαμηλό κόστος σε προκαθορισμένες ομάδες πελατών. Αποτελεί, δηλαδή, μια μορφή άμεσης επικοινωνίας μεταξύ πελατών και επιχείρησης, που της παρέχει τη δυνατότητα

²⁰ "Click Through Rates (CTR)", Web hosting glossary

²¹ Martin Evans, Lisa O'Malley and Maurice, "Direct Marketing: rise and rise or rise and fall?", www.emeraldinsight.com

²² William D. Perreault, Jr. E. Jerome McCarthy, "Basic Marketing",σελ. 450

μέτρησης και αξιολόγησης των αποτελεσμάτων της με την καταγραφή της ανταπόκρισης των πελατών.

Για να γίνουν όμως πιο αποτελεσματικές οι μέθοδοι άμεσου Μκτ που εφαρμόζει μια επιχείρηση, ικανοποιώντας στο μέγιστο βαθμό τις ανάγκες της αγοράς-στόχου, πρέπει η επιχείρηση να συγκεντρώσει πρώτα πληροφορίες σχετικά με τους πελάτες που απαρτίζουν αυτή την αγορά. Κι εδώ πρέπει να γίνει αναφορά στο Μκτ βάσει δεδομένων (Data base Mkt).²³ Το Μκτ βάσει δεδομένων αποτελεί μια εντελώς νέα προσέγγιση στο χώρο του Μκτ, καθώς στηρίζεται στην τεχνολογία της συλλογής, επεξεργασίας, και χρήσης μεγάλων όγκων πληροφοριών που αφορούν προσωπικά δεδομένα πελατών με στόχο την αποτελεσματικότερη προώθηση προϊόντων. Η επιχείρηση διαθέτει μεγάλες βάσεις δεδομένων καταναλωτών που περιλαμβάνουν λεπτομερή στοιχεία συμπεριφοράς τους και δημογραφικές πληροφορίες. Τέτοιες πληροφορίες περιλαμβάνουν:

- ✓ Το όνομα και τη διεύθυνση του πελάτη
- ✓ Την ηλικία του, την οικονομική και οικογενειακή του κατάσταση, τις αγοραστικές του συνήθειες κτλ, όπως και παρόμοιες πληροφορίες για όλα τα υπόλοιπα μέλη της οικογένειάς του
- ✓ Στοιχεία κατά τη συναλλαγή του με την επιχείρηση, όπως π.χ. τι αγοράζει απ' τη συγκεκριμένη εταιρία, κάθε πότε, γιατί την προτιμάει σε σχέση με τους ανταγωνιστές της, ποια είναι η αξία των αγορών του, πόσο διάστημα είναι πελάτης της, πόσες αγορές πραγματοποιεί ετησίως κτλ

Μάλιστα η επιχείρηση πρέπει να διαχωρίζει τους πιστούς απ' τους περιστασιακούς της πελάτες και οι πληροφορίες που αφορούν τους βασικούς πελάτες, οι οποίοι συνήθως αποφέρουν το 70-75% των εσόδων της, πρέπει να είναι εύκολα προσιτές στη διοίκηση, καθώς έχουν μεγάλη βαρύτητα για τη λήψη επιχειρηματικών αποφάσεων.²⁴

²³ ‘‘Vertical Market Trends in Direct Mail and the Impact on Production Service Providers’’, FreshAddress Inc., www.the-dma.org

²⁴ Jeff Wuorio, ‘‘7 Tips for keeping customers for life’’, www.microsoft.com

Οι παραπάνω πληροφορίες που αφορούν προσωπικά δεδομένα πελατών, συγκεντρώνονται με διάφορους τρόπους: στο σημείο αγοράς, απ' τα τηλεφωνήματα των πελατών για εξυπηρέτηση, από έρευνες σχετικά με την ικανοποίηση των πελατών, από έκδοση καρτών προϊόντων (product registration cards), κατά την εγγραφή ενός υποψήφιου πελάτη στην ιστοσελίδα της επιχείρησης, από εκστρατείες προώθησης των προϊόντων και τέλος από προσπάθειες τηλεφωνικών πωλήσεων.²⁵ Οι πηγές απ' τις οποίες η επιχείρηση αντλεί τις πληροφορίες αυτές είναι τρεις: είτε απ' τον ίδιο τον πελάτη, είτε από κάποιο τρίτο (με την έγκριση του πελάτη ή χωρίς αυτή) είτε από κάποιο δημόσιο μητρώο ή άλλη δημόσια πηγή, προσιτή στο ευρύ κοινό όπως εφημερίδες, κατάλογος διευθύνσεων κτλ. Η άντληση πληροφοριών απ' τον ίδιο τον πελάτη-ενδιαφερόμενο, γίνεται συνήθως με την παροχή κάποιων κινήτρων, όπως πχ συμπλήρωση ερωτηματολογίου μέσω της διανομής εκπαιδευτικών κουπονιών και άλλων προσφορών.²⁶

Μετά το στάδιο της συλλογής πληροφοριών που αφορούν προσωπικά δεδομένα πελατών, έπεται το στάδιο της επεξεργασίας τους και η διαφοροποίηση των πελατών. Η επιχείρηση διαφοροποιεί τους πελάτες και τους κατατάσσει σε κατηγορίες με βάση διάφορα κριτήρια, όπως πιστότητα, όγκο αγορών, συχνότητα αγορών, κτλ²⁷. Όλοι οι πελάτες δεν είναι ίδιοι για την επιχείρηση, πρέπει λοιπόν να χρησιμοποιηθούν κάποια μοντέλα αξιολόγησής τους, όπως η διαβάθμισή τους με βάση το βαθμό πιστότητας και διασύνδεσης με την επιχείρηση με μια σκάλα αξιολόγησης, η χρήση μοντέλων βαθμολογικής αξιολόγησης (scoring-models), και η ανάπτυξη χαρτοφυλακίου πελατών. Παρακάτω θα γίνει μια συνοπτική αναφορά στα μοντέλα αυτά.

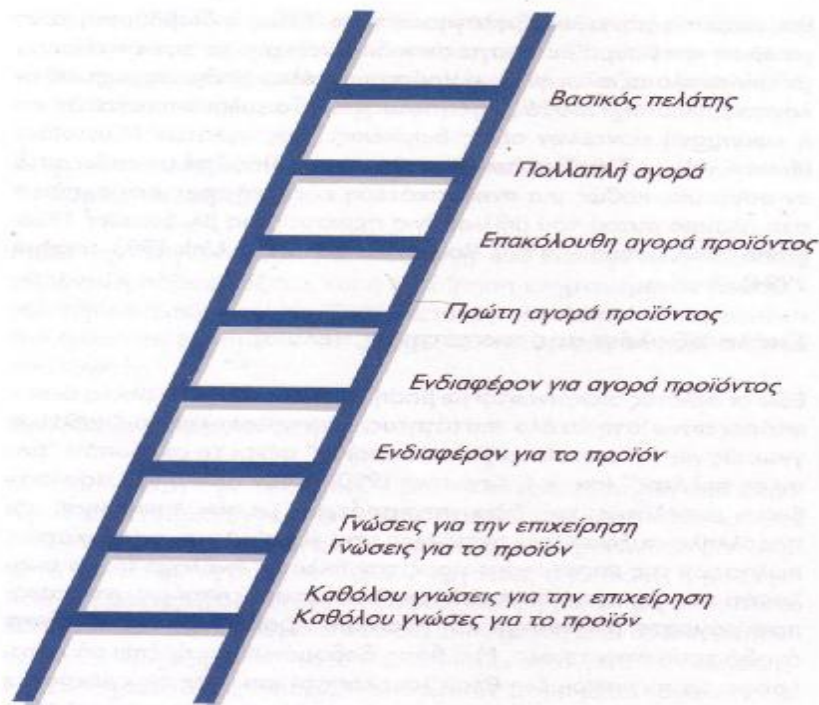
²⁵ Sharp Brenda, "Direct Marketing-the database", www.emeraldinsight.com

²⁶ "CRM architecture for enterprise relationship Mkt in the new millenium", White Paper, www7hp.com

²⁷ Denise D. Schoenbachler, Geoffrey L.Cordon, "Understanding consumer database marketing", www.emeraldinsight.com

Ι. Σκάλα αξιολόγησης πιστότητας πελάτη

Εδώ οι πελάτες διακρίνονται με βάση το σκαλοπάτι στο οποίο έχουν φτάσει πάνω στη σκάλα πιστότητας απ' το σκαλοπάτι "καθόλου γνώσεις για την επιχείρηση και το προϊόν" μέχρι το σκαλοπάτι "βασικός πελάτης". Κάθε σκαλοπάτι που ανεβαίνει ο πελάτης, τον δένει περισσότερο με την επιχείρηση και παράλληλα αυξάνεται η πιστότητά του και η πιθανότητα πωλήσεων της επιχείρησης προς τον πελάτη. Ανάλογα με το σκαλοπάτι που βρίσκονται οι πελάτες, αντιμετωπίζονται με αντίστοιχα προγράμματα, με στόχο την άνοδό τους στη σκάλα. Μια βάση δεδομένων θα πρέπει να καταγράφει τη συγκεκριμένη θέση (σκαλοπάτι) και όλες τις τρέχουσες μετακινήσεις για να αποφεύγεται για παράδειγμα, να αντιμετωπίζεται ένας βασικός πελάτης ως νέος πελάτης.²⁸



Πηγή: Kreutzer 1990

Σχήμα 4.4: Σκάλα αξιολόγησης πιστότητας του πελάτη (Loyalty)

²⁸ Simon Cooke, "Database Marketing: Strategy or tactical tool?", www.emeraldinsight.com

II. Μοντέλα βαθμολόγησης-scoring models

Μια άλλη δυνατότητα αξιολόγησης των πελατών είναι τα διαφόρων ειδών βαθμολογικά μοντέλα. Ένα απ' τα γνωστότερα μοντέλα είναι το RFMR μοντέλο (Recency –χρονική στιγμή τελευταίας αγοράς, frequency- συχνότητα αγοράς, Monetary Ratio- αξία αγοράς). Η βασική ιδέα του μοντέλου αυτού είναι ότι οι πελάτες δεν παρουσιάζουν την ίδια πιθανότητα για την αγορά ενός προϊόντος και ως εκ τούτου η διαβάθμισή τους θα επιτρέψει τη διαφοροποιημένη προσέγγισή τους ιδιαίτερα μέσω καταλόγων, διαφημιστικών εντύπων κτλ. Ξεκινώντας μια αρχική αξιολόγηση/βαθμολόγηση, προστίθενται ή αφαιρούνται πόντοι για κάθε πελάτη ανάλογα με τη συχνότητα και την αξία των πραγματοποιούμενων αγορών. Αφαιρούνται πόντοι, όταν για παράδειγμα η επιχείρηση επενδύει στον πελάτη στέλνοντας καταλόγους, δίχως αυτός να πραγματοποιεί για μακρύ χρονικό διάστημα αγορές. Όταν λοιπόν ένας πελάτης έχει πολλούς πόντους, η επιχείρηση ξέρει ότι αξίζει περισσότερο να ασχοληθεί με τον πελάτη αυτόν, υπάρχει δηλαδή μεγαλύτερη πιθανότητα να ανταποκριθεί σε μια προσφορά, και οργανώνει την άμεση διαφήμιση με βάση τις παραπάνω πληροφορίες.²⁹

²⁹ Βλαχοπούλου Μάρω, 'E-Marketing: πληροφοριακά συστήματα-νέες τεχνολογίες στο μάρκετινγκ'', σελ.157

ΜΕΘΟΔΟΣ R.F.M.R**Διαβάθμιση:**

50

35

15

Recency (χρόνος της τελευταίας αγοράς)

Frequency (συχνότητα αγοράς)

Monetary Ratio (αξία της αγοράς)

**ΠΑΡΑΓΟΝΤΕΣ
ΑΡΧΙΚΗ ΑΞΙΑ**

25 βαθμοί

Τελευταία ημερομηνία αγοράς (βαθμοί)	έως 6 μήνες + 40	έως 9 μήνες + 25	έως 12 μήνες + 15	έως 18 μήνες + 5	έως 24 μήνες - 5	πιο πριν - 15
ΣΥΧΝΟΤΗΤΑ ΑΓΟΡΑΣ ΚΑΤΑ ΤΟΥΣ ΤΕΛΕΥΤΑΙΟΥΣ 18 ΜΗΝΕΣ	Αριθμός των αγρών πολλαπλασιάζεται με τον παράγοντα 6					
Μέσος τζίρος στις 3 τελευταίες αγορές (βαθμοί)	έως 50 χιλ. + 5	έως 100 χιλ. + 15	έως 200 χιλ. + 25	έως 300 χιλ. + 35	έως 400 χιλ. + 40	άνω 400 χιλ. + 45
Αριθμός επιστροφών (βαθμοί)	0 - 1 0	2 - 3 - 5	4 - 6 - 10	7 - 10 - 20	11 - 15 - 30	άνω των 15 - 40

Αριθμός των
διαφημιστικών
εντύπων που
στάληκαν
μετα την
τελευταία
αγορά**Κύριος
κατάλογος**
κάθε ένας
-12**Ειδικός
κατάλογος**
κάθε ένας
-6**Ταχυδρομικός
κατάλογος**
κάθε ένας
-2**Πίνακας 4.1:** Παράδειγμα μοντέλου βαθμολογήσεως

III. Μοντέλα χαρτοφυλακίου πελατών

Ένα απ' τα σημαντικότερα μοντέλα χαρτοφυλακίου πελατών, είναι το χαρτοφυλάκιο αξίας-πιστότητας πελάτη. Σύμφωνα με αυτό, αναπτύσσονται διαφοροποιημένες στρατηγικές προσέγγισης του πελάτη ανάλογα με την αξία του και την πιστότητά του απέναντι στην επιχείρηση και το προϊόν . Συγκεκριμένα, μπορεί να αναπτυχθεί μια διαβαθμισμένη πολιτική προβολής για τα 4 πεδία που σχηματίζονται ως εξής³⁰:

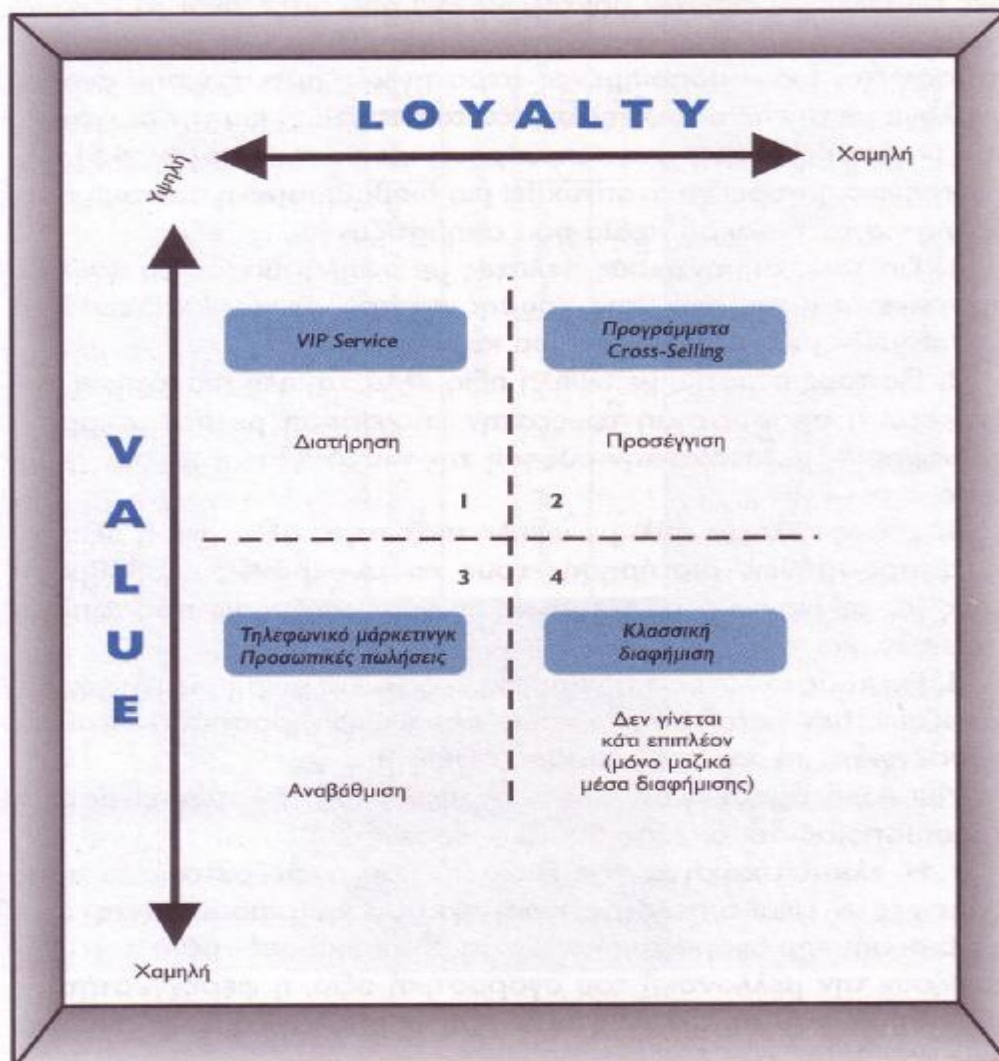
1. Για τους σημαντικούς πελάτες με υψηλή πιστότητα και αξία, προτείνεται η παροχή "της χρυσής κάρτας", που σημαίνει ιδιαίτερα προνόμια και παροχές.

2. Για τους πελάτες με υψηλή αξία αλλά χαμηλή πιστότητα, επιδιώκεται η προσάρτησή τους στην επιχείρηση με προγράμματα προσφορών με στόχο την αύξηση της πιστότητας ή με cross-selling.

3. Στους πελάτες με υψηλή πιστότητα αλλά μικρή αξία, γίνεται προσπάθεια διατήρησής τους και συγχρόνως αναβάθμισής τους με τηλεφωνικό Μκτ και ενίσχυση μέσω προσωπικών πωλητών.

4. Για τους πελάτες που και μικρή αξία και μικρή πιστότητα εμφανίζουν, δεν καταβάλλεται καμιά περαιτέρω προσπάθεια άμεσης προσέγγισης πέραν της κλασσικής διαφήμισης.

³⁰ Βλαχοπούλου Μάρω , 'E-Marketing: πληροφοριακά συστήματα-νέες τεχνολογίες στο μάρκετινγκ'', σελ.162



Σχήμα 4.5: Μοντέλο του καρτοφυλακίου αξίας πιστότητας πελάτη (Value Loyalty)

IV. Κατηγοριοποίηση με βάση την αξία του πελάτη για την επιχείρηση

Με βάση την αξία που έχει ο κάθε πελάτης για την επιχείρηση, γίνεται διαχωρισμός των πελατών σε **Πλατινένιους, Χρυσούς, Ασημένιους, Χάλκινους** και **Σιδερένιους**. Είναι μάλιστα φυσικό ότι θα διαθέσει περισσότερους

πόρους στους πιο επικερδείς πελάτες της, ενώ τους μη επικερδείς ίσως δεν τη συμφέρει να τους εξυπηρετεί και τους απομακρύνει.³¹

Πλατινένιοι

Είναι οι πελάτες που έχουν τη μεγαλύτερη αξία για την επιχείρηση γιατί συνεισφέρουν περισσότερο απ' τους άλλους στα κέρδη της. Η εταιρία δημιουργεί στρατηγικές συμμαχίες μαζί τους, γεγονός που δημιουργεί οφέλη και στις δύο πλευρές αλλά και αυξάνει το κόστος που υφίσταται ο πελάτης όταν αλλάζει προμηθευτή. Αποτελούν το 10% του συνόλου των πελατών και συμμετέχουν κατά 25% στο κέρδος.

Χρυσοί

Αποφέρουν σχεδόν την ίδια κερδοφορία στην εταιρία όσο και οι προηγούμενοι, αλλά δεν έχουν τα πλεονεκτήματα των στρατηγικών συμμαχιών. Αυτοί αποτελούν το 15% του συνόλου, και συνεισφέρουν επίσης το 25% του συνολικού κέρδους.

Ασημένιοι

Είναι λιγότερο κερδοφόροι απ' τους προηγούμενους, ωστόσο η επιχείρηση επιθυμεί να τους κρατήσει και τους δίνει κίνητρα. Αποτελούν το 35% του συνόλου και συνεισφέρουν το 45% του κέρδους.

Χάλκινοι

Οι πελάτες αρχίζουν να γίνονται ζημιογόνοι για την επιχείρηση, αφού συμβάλλουν μόνο στο 5% του κέρδους, ενώ αποτελούν το 20% του συνόλου.

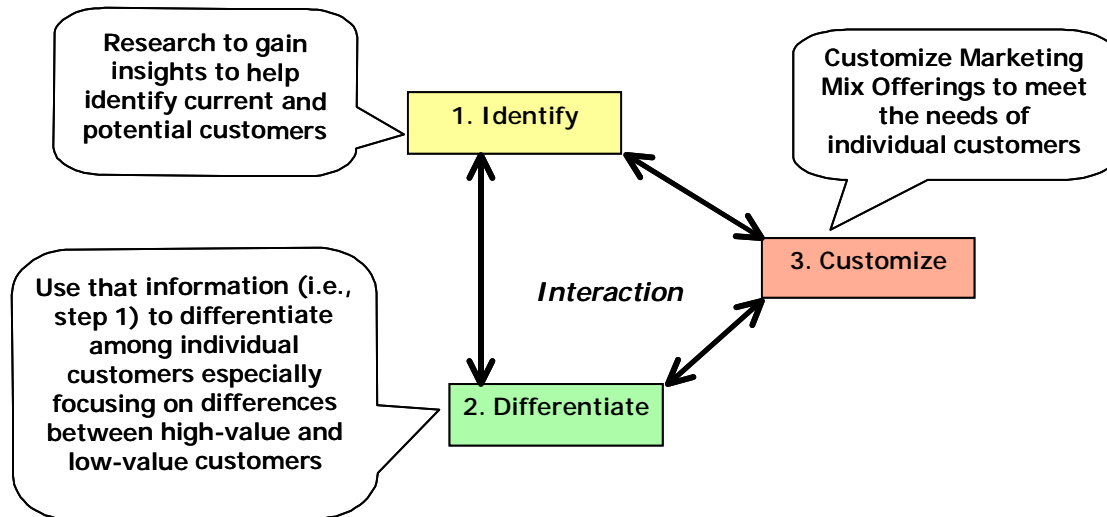
Σιδερένιοι

Οι Σιδερένιοι πελάτες αποφέρουν ζημιές στην εταιρία της τάξης του 15% και γι' αυτό πρέπει να ανακαλύψει τρόπους να τους κάνει επικερδείς αλλιώς θα τους διώξει.

Το τελευταίο στάδιο, μετά την επεξεργασία των προσωπικών πληροφοριών των πελατών με στόχο τη διαφοροποίησή τους και την κατηγοριοποίησή τους σε ομάδες, είναι το στάδιο της προσαρμογής στις απαιτήσεις τους. Η επιχείρηση

³¹ D. Peppers and M. Rpgers, "Enterprise One to One: Tools for Competing in the Interactive Age", σελ.28

δηλαδή, προσαρμόζει το μίγμα Μκτ ανάλογα με τις ανάγκες του καθενός, έτσι ώστε να πετύχει μεγαλύτερο επίπεδο ικανοποίησης.³²



2.4 Μοντέλο RADAR στο Data base Mkt

Στην προηγούμενη ανάλυση, έγινε εκτενής αναφορά στην έννοια του data base Mkt, κύριο αντικείμενο του οποίου είναι η συλλογή και επεξεργασία προσωπικών δεδομένων των πελατών, όπως π.χ. δημογραφικά στοιχεία και αγοραστικές συνήθειες, η διαφοροποίηση των πελατών με βάση διάφορα κριτήρια, η ομαδοποίησή τους με βάση κοινά χαρακτηριστικά και η επιλογή των κατάλληλων μεθόδων άμεσου Μκτ με στόχο την αποτελεσματικότερη ικανοποίηση των αναγκών τους και την αύξηση των πωλήσεων.

Μια έννοια που συνδέεται στενά με το data base Mkt είναι το μοντέλο RADAR, το οποίο αποτελείται απ' τα αρχικά των λέξεων Research, Analysis, Detection, Action & Reaction. Η προσπάθεια συγκέντρωσης και συστηματικής καταχώρισης όλων των αναγκαίων για το Μκτ πληροφοριών απ' την πλευρά της επιχείρησης, ονομάζεται "αρχή του RADAR". Το Research αναφέρεται στον εντοπισμό και την απόκτηση εκείνων των πληροφοριών που αφορούν κάθε πελάτη και είναι απαραίτητες για την επιχείρηση. Με τις κατάλληλες πληροφορίες

³² Richard Cross, Janet Smith, 'Customer Bonding, 5 steps to lasting customer loyalty', σελ.52

η επιχείρηση θα μπορεί να κάνει τις ανάλογες προσφορές που αρμόζουν σε κάθε πελάτη.

Η οργανωμένη αποθήκευση των συγκεντρωθέντων πληροφοριών για κάθε πελάτη, αποτελεί τη βάση για την εφαρμογή διαφόρων μεθόδων ανάλυσης των δεδομένων αυτών για τη συναγωγή συγκεκριμένων πληροφοριών για τον κάθε πελάτη. Αυτό είναι το στάδιο της “Analysis”.

Τα αποτελέσματα της ανάλυσης πελατών οδηγούν στον εντοπισμό (Detection) ευκαιριών και κινδύνων που μπορεί να αφορά τόσο τον κάθε πελάτη ξεχωριστά, όσο και ένα τμήμα της αγοράς ή ακόμα και το σύνολο της αγοράς. Πάνω σ’ αυτή τη βάση πραγματοποιείται λοιπόν ο σχεδιασμός και η πραγματοποίηση συγκεκριμένων δραστηριοτήτων Μκτ (Action) απευθυνόμενων προς τον πελάτη.

Οι δραστηριότητες αυτές της επιχείρησης προς τον πελάτη έχουν ως αποτέλεσμα κάποιες αντιδράσεις/ανταποκρίσεις του πελάτη (Reaction), όπως αποδοχή ή απόρριψη μιας προσφοράς. Αυτή λοιπόν η αντίδραση καταγράφεται μαζί με τη δραστηριότητα της επιχείρησης στη βάση δεδομένων, για τη χρήση των δεδομένων αυτών για μελλοντικές αναλύσεις.³³

2.5 Εργαλεία συλλογής και επεξεργασίας προσωπικών δεδομένων

Για τη συλλογή και επεξεργασία προσωπικών δεδομένων πελατών, απαιτούνται σύγχρονα τεχνολογικά συστήματα, τα οποία συμβάλλουν στη συγκέντρωση πληροφοριών για τα χαρακτηριστικά των πελατών και το προφίλ τους, στην αποθήκευσή τους, καθώς και στην ανάλυση και μετατροπή τους σε γνώση για τους πελάτες. Έτσι είναι ευκολότερο για τις επιχειρήσεις να εντοπίσουν τις επιθυμίες και ανάγκες των πελατών και να δημιουργήσουν μίγματα Μκτ που θα ικανοποιούν αποτελεσματικότερα τις συγκεκριμένες ανάγκες. Τα συστήματα αυτά τεχνολογίας είναι τα εξής:

³³ Βλαχοπούλου Μάρω, ‘E-Marketing: πληροφοριακά συστήματα-νέες τεχνολογίες στο μάρκετινγκ’, σελ.165

I. Συστήματα EPOS (Electronic Point of Sale)

Με τα συστήματα αυτά είναι δυνατή η παρακολούθηση των αγορών που πραγματοποιεί ο καταναλωτής, συγκεκριμένα η ημερομηνία και ο χρόνος των αγορών, τα εμπορεύματα που αγοράστηκαν καθώς και οι τιμές που πληρώθηκαν. Τα προσωπικά δεδομένα των αγοραστών που συγκεντρώνονται από ένα σύστημα ηλεκτρονικού σημείου πώλησης (EPOS), μπορούν να αποθηκευτούν και να αναλυθούν από ένα υπολογιστή, παρέχοντας στην επιχείρηση έναν αξιόλογο όγκο πληροφοριών για τη λήψη αποφάσεων Μκτ και ειδικότερα για τον προγραμματισμό των ενεργειών Μκτ όπως π.χ. προγράμματα προώθησης πωλήσεων, κουπόνια, δώρα κτλ.³⁴ Βασικό εργαλείο του ηλεκτρονικού σημείου πώλησης είναι ένας ηλεκτρονικός καταχωρητής εξαργύρωσης- Electronic Cash Register (ECR)- που μπορεί να χειριστεί κωδικούς και έχει τη δυνατότητα εκτύπωσης, χωρητικότητας μνήμης και ανάγνωσης τιμών. Με τη βοήθεια ακτίνων λέιζερ γίνεται το διάβασμα τιμών και κωδικών και έτσι μπορούν να υπολογιστούν αυτόματα όχι μόνο οι λογαριασμοί του πελάτη, αλλά και οι πωλήσεις για κάθε προϊόν χωριστά. Συνοπτικά, η λειτουργία του συστήματος EPOS έχει ως εξής: Βασική προϋπόθεση είναι κάθε προϊόν να έχει έναν κωδικό. Το σύστημα με τη σειρά του πρέπει να διαθέτει τους κωδικούς αυτούς στη μνήμη του, καθώς και τη σχετιζόμενη περιγραφή και τιμή του προϊόντος. Όταν το προϊόν έρθει σε επαφή με το Electronic Cash Register, διαβάζονται οι πληροφορίες του προϊόντος και το τερματικό αναγράφει και εκτυπώνει την τιμή του προϊόντος. Μ'αυτόν τον τρόπο η επιχείρηση μπορεί να γνωρίζει τι προϊόντα αγοράζει ο πελάτης, την αξία των αγορών του και έτσι να εφαρμόσει τα κατάλληλα προγράμματα άμεσου Μκτ.³⁵

II. Customer Data-base: Είναι μια βάση που περιέχει πληροφορίες που αφορούν τον πελάτη (τηλέφωνο, όνομα κτλ)

III. Data Warehouse: Είναι ένας κεντρικός αποθηκευτικός χώρος για όλα ή τα σχετικά μέρη της πληροφορίας που συλλέχθηκε με ένα εταιρικό σύστημα. Τα data warehouses μπορούν να χρησιμοποιηθούν σαν αποθήκες ιστορικών

³⁴ Yurong Xu, David C.Yen, Binshan Cin, "Adopting customer relationship management technology", www.emeraldinsight.com

³⁵ John Connell, "Electronic Point of Sale", www.techrepublic.com

στοιχείων και είναι εύκολα προσβάσιμα και επεξεργάσιμα για υποστήριξη στις διαδικασίες λήψης αποφάσεων³⁶

IV. Data Mining: Είναι μια διεργασία που χρησιμοποιεί μια ποικιλία από τεχνικές ανάλυσης δεδομένων και μοντελοποίησης προκειμένου να ανακαλύψει στα δεδομένα πρότυπα και σχέσεις που χρησιμοποιούνται για να κατανοηθούν και να προβλεφθούν οι επιθυμίες των πελατών. Βοηθά ώστε να επιλεγούν οι κατάλληλοι υποψήφιοι πελάτες στους οποίους η επιχείρηση θα πρέπει να επικεντρωθεί, να προσφέρει τα κατάλληλα επιπρόσθετα προϊόντα στους ήδη υπάρχοντες πελάτες και να αναγνωρίσει τους καλούς πελάτες που ενδέχεται να αποχωρήσουν.³⁷

V. Querying-tools: Είναι προγράμματα που βοηθούν στην αναζήτηση δεδομένων που είναι αποθηκευμένα σε ένα σύστημα διαχείρισης βάσης δεδομένων. Ο βασικός ρόλος των εργαλείων αυτών είναι, πέρα απ' την αναζήτηση δεδομένων, η διαμόρφωση ερωτημάτων, που συχνά απαιτούν την ένωση πινάκων σ' ένα query, αλλά και την ομαδοποίηση δεδομένων για παρουσίαση (π.χ. πόσοι πελάτες πραγματοποίησαν συνολικές αγορές μέσα στο εξάμηνο πάνω από 300 ευρώ;).³⁸

2.6 Γεωγραφικά Πληροφοριακά Συστήματα

Οι νέες τεχνολογίες πληροφορικής, η οργάνωση των δεδομένων σε βάσεις δεδομένων και τα πληροφοριακά συστήματα αποτελούν, όπως ήδη αναφέρθηκε, πολύτιμα εργαλεία για την υποστήριξη της πολιτικής Μκτ της επιχείρησης. Ωστόσο, λόγω της ραγδαίας εξέλιξης της τεχνολογίας έχουν ανακαλυφθεί νέοι τρόποι προβολής και συσχέτισης των δεδομένων και πληροφοριών που χρησιμοποιούνται για τη λήψη αποφάσεων Μκτ. Μέσα στα πλαίσια αυτά εντάσσεται και η σχετικά νέα τεχνολογία των Γεωγραφικών Πληροφοριακών Συστημάτων (GIS), που δίνει στους Μκτ μάνατζερς τη δυνατότητα πρόσβασης και διαχείρισης χαρτογραφικών/γεωγραφικών

³⁶ In Jazz J.Chen, Karen Popovich, "Understanding customer relationship management (CRM): people, process and technology", www.emeraldinsight.com

³⁷ Ben Light, "CRM packaged software: a study of organizational experiences", www.emeraldinsight.com

³⁸ "Your Resource for success in Customer Relationship Management", DCI e-university, www.crmcommunity.com

πληροφοριών. Σύμφωνα με τον DeMers «Γεωγραφικά Συστήματα Πληροφοριών είναι ένα σύστημα διαδικασιών για τη συστηματική συλλογή, κωδικοποίηση και εισαγωγή, αποθήκευση και διαχείριση, επεξεργασία και ανάλυση, χαρτογράφηση και ανάκληση γεωγραφικών δεδομένων και άλλων δεδομένων με γεωγραφική διάσταση, που αφορούν την αγορά και την επιχείρηση, με στόχο την υποστήριξη της λήψης επιχειρησιακών αποφάσεων και ειδικότερα αποφάσεων Μκτ».³⁹ Τα συστήματα αυτά λοιπόν, έχουν ευρεία εφαρμογή στα πλαίσια του Μκτ, καθώς η πλειοψηφία των δεδομένων που συλλέγονται και χρησιμοποιούνται καθημερινά για τη λήψη αποφάσεων Μκτ έχουν γεωγραφικές αναφορές. Χρησιμοποιώντας τα Γεωγραφικά Συστήματα Πληροφοριών οι επιχειρήσεις μπορούν να παρουσιάσουν και να αναλύσουν τα δεδομένα που έχουν συγκεντρώσει και να συνδυάσουν γεωγραφικά δεδομένα με δεδομένα που αφορούν το Μκτ. Κατ' αυτόν τον τρόπο οι ψηφιακοί χάρτες αποκαλύπτουν συσχετισμούς μεταξύ συγκεκριμένων γεωγραφικών περιοχών και των πωλήσεων των προϊόντων μιας επιχείρησης, καθώς και των δημογραφικών χαρακτηριστικών και της αγοραστικής συμπεριφοράς των πελατών της που αποτελούν προσωπικά δεδομένα. Πρέπει επίσης να αναφερθεί, ότι τα Γεωγραφικά Πληροφοριακά Συστήματα υποστηρίζουν προγράμματα άμεσης διαφήμισης, συμβάλλοντας στη αύξηση της αποτελεσματικότητας των προγραμμάτων αυτών.⁴⁰ Για παράδειγμα, μια επιχείρηση που επιθυμεί την αποστολή ταχυδρομικού διαφημιστικού υλικού σε πιθανούς πελάτες, θα πρέπει να συγκεντρώσει δεδομένα της αγοράς-στόχου που περιορίζεται σε μια γεωγραφική περιοχή και περιλαμβάνει τους κατοίκους της περιοχής με τα δημογραφικά χαρακτηριστικά και γενικότερα το προφίλ που έχει καθοριστεί απ' τον Μκτ μάνατζερ για το συγκεκριμένο διαφημιζόμενο προϊόν. Απ' την παραπάνω ανάλυση λοιπόν, εξάγεται το συμπέρασμα ότι ένα Σύστημα Γεωγραφικών Πληροφοριών επεξεργάζεται πληροφορίες προσωπικού χαρακτήρα των κατοίκων μιας περιοχής όπως πχ διευθύνσεις, αγοραστική συμπεριφορά των κατοίκων, αξία αγορών κτλ, για τη λήψη αποφάσεων Μκτ.^{41,42}

³⁹ P.Thirlby, ‘‘Geographic Information Systems in commercial property’’, www.emeraldinsight.com

⁴⁰ John Tombarge, ‘‘Using management software for geographic information systems (GIS)’’, www.emeraldinsight.com

⁴¹ Βλαχοπούλου Μάρω, ‘‘E-Marketing: πληροφοριακά συστήματα-νέες τεχνολογίες στο μάρκετινγκ’’,σελ.177

⁴²James D. Gordon, ‘‘ Geographic Information Systems’’, www.gim.com

2.7 Παράδειγμα επεξεργασίας προσωπικών δεδομένων για σκοπούς άμεσης διαφήμισης

Στην μέχρι τώρα ανάλυση έγινε αναφορά στην ανάπτυξη του άμεσου Μκτ ως εργαλείου για την αύξηση των πωλήσεων της επιχείρησης, καθώς και στην τακτική συλλογής και επεξεργασίας προσωπικών δεδομένων πελατών προκειμένου να γίνουν πιο αποτελεσματικά τα προγράμματα άμεσου Μκτ που εφαρμόζει η επιχείρηση. Για να γίνει πιο κατανοητό αυτό, παραθέτουμε το πιο κάτω παράδειγμα.⁴³

Ας υποθέσουμε ότι κάποιος έχει αγοράσει κάποιο θαλάσσιο σκάφος και επιθυμεί να επιλέξει μια μαρίνα προκειμένου να το τοποθετήσει. Μετά από πλοήγηση στο διαδίκτυο, εντοπίζει τη μαρίνα “Marina”. Μπαίνει λοιπόν στην ηλεκτρονική σελίδα της εταιρίας για να αναζητήσει πληροφορίες. Εκεί του ζητήθηκε να δημιουργήσει ένα όνομα χρήστη (username) και κωδικό (password) προκειμένου να λάβει τις πληροφορίες που χρειαζόταν και του παραχωρήθηκε η δική του (διαμορφωμένη σύμφωνα με τα δικά του πρότυπα) σελίδα. Αυτό συνέβη κατά τη διαδικασία εγγραφής του στην ιστοσελίδα, όταν του έγιναν ερωτήσεις σχετικά με τις προτιμήσεις του και συνεπώς φτιάχτηκε μια προσωπική σελίδα η οποία αντανάκλούσε τα ενδιαφέροντά του. Π.χ. του ζητήθηκε να αναφέρει τις αγαπημένες του τοποθεσίες για κρουαζιέρα και αυτόματα του έδειξε τα θαλάσσια ρεύματα και τις προβλέψεις για κάθε τοποθεσία. Επίσης του ανακοινώθηκε ότι αν γινόταν πελάτης της μαρίνας θα μπορούσε να έχει την προσωπική του ιστοσελίδα προκειμένου:

- Να ελέγχει τη θέση του στη μαρίνα για όσο διάστημα θα έλειπε ταξίδια γιατί ενδεχομένως η θέση του να έχει διατεθεί σε άλλο σκάφος
- Να εγγράψει τα παιδιά του σε πρόγραμμα ιστιοπλοΐας
- Να στέλνει ερωτήσεις μέσω διαδικτύου στο τμήμα εξυπηρέτησης της μαρίνας, με εγγυημένο χρόνο απάντησης τη 1 ώρα

⁴³ Murphy T. Daniel, Salinas Andres, ‘Customer Relationship Management Technology and the Marina of the Near Future’, σελ. 56

Με βάση τις πληροφορίες που συγκέντρωσε για το προφίλ του, η εταιρία τον τοποθέτησε σε μια απ' τις κατηγορίες πελατών που σχημάτισε και σκοπεύει το επόμενο χρονικό διάστημα να του στέλνει διαφημίσεις για προϊόντα και υπηρεσίες που ταιριάζουν στις ανάγκες του. Μια εβδομάδα αργότερα ο συγκεκριμένος υποψήφιος πελάτης έλαβε ένα μήνυμα με βάση το οποίο του παρέχεται 10% έκπτωση αν γίνει πελάτης της μαρίνας μέχρι μια συγκεκριμένη ημερομηνία. Μέχρι εδώ λοιπόν, παρατηρούμε ότι η επιχείρηση δημιούργησε μια βάση δεδομένων (database) με στοιχεία που αφορούν το προφίλ του υποψήφιου πελάτη. Στη συνέχεια με βάση τα στοιχεία αυτά τον κατέταξε σε μια απ' τις κατηγορίες στις οποίες είχε διαχωρίσει τους πελάτες της προκειμένου να του απευθύνει ένα μίγμα Μκτ που θα ανταποκρίνεται πλήρως στις ανάγκες και τα ενδιαφέροντά του.

Κατόπιν ο υποψήφιος πελάτης ανταποκρίθηκε στο "κάλεσμα" της μαρίνας και δέχθηκε να γίνει πελάτης. Εισηγάγε τον αριθμό της πιστωτικής του κάρτας και ζήτησε μηνιαίες πληρωμές. Όταν μετά από 2 ημέρες μπήκε στην ιστοσελίδα του, είδε ότι ο λογαριασμός του είχε χρεωθεί με το ενοίκιο του 1^{ου} μήνα. Μετά από λίγο καιρό, η εταιρία του έστειλε διαφήμιση μέσω e-mail για να εγγράψει τα παιδιά του σ' ένα πρόγραμμα παιδικής ιστιοπλοΐας. Ο πελάτης αγόρασε την υπηρεσία αυτή και μ' αυτόν τον τρόπο η μαρίνα πραγματοποίησε cross-selling.⁴⁴ Συνοπτικά λοιπόν, πρέπει να αναφερθεί ότι η συγκεκριμένη μαρίνα, αφού συγκέντρωσε πληροφορίες σχετικά με τα ενδιαφέροντα του υποψήφιου πελάτη και διαμόρφωσε το προφίλ του, του απηύθυνε ηλεκτρονικά μηνύματα κατάλληλα προσαρμοσμένα στις απαιτήσεις του προκειμένου να πετύχει την καλύτερη εξυπηρέτησή του και την αύξηση των πωλήσεών της.

⁴⁴ Με τον όρο "cross-selling", εννοούμε την πώληση περισσότερων προϊόντων και υπηρεσιών σε υφιστάμενους πελάτες

ΚΕΦΑΛΑΙΟ 3

Κίνδυνοι απ' την επεξεργασία προσωπικών δεδομένων

Μέχρι τώρα είδαμε πόσο σημαντική είναι η συλλογή και επεξεργασία προσωπικών δεδομένων πελατών για σκοπούς άμεσης διαφήμισης καθώς και τις τεχνολογίες που χρησιμοποιούν οι επιχειρήσεις για την επεξεργασία των πληροφοριών αυτών. Ωστόσο όμως, η διαδικασία αυτή εγκυμονεί παράλληλα σοβαρούς κινδύνους για την προσωπικότητα και την ιδιωτική ζωή του ατόμου. Σήμερα μάλιστα που η εξέλιξη της πληροφορικής έχει οδηγήσει στην αυτοματοποιημένη επεξεργασία δεδομένων, οι κίνδυνοι αυτοί είναι κατά πολύ μεγαλύτεροι.

Ένας απ' τους κινδύνους που συνεπάγεται ιδίως η αλόγιστη συλλογή και επεξεργασία μεγάλου όγκου πληροφοριών που αφορούν προσωπικά δεδομένα των καταναλωτών, είναι η παραβίαση της ιδιωτικής ζωής του ατόμου,⁴⁵ η οποία προστατεύεται συνταγματικά όπως θα εξετάσουμε στη συνέχεια, με αποτέλεσμα να θίγεται η ησυχία του και το δικαίωμά του στη μόνωση. Π.χ. η αποστολή μη ζητηθείσης ηλεκτρονικής αλληλογραφίας (spamming) μπορεί να παρενοχλεί τον αποδέκτη της.⁴⁶

Επίσης η χρήση προσωπικών δεδομένων των καταναλωτών απ' τις επιχειρήσεις, είναι δυνατόν να τους καταστήσει ένα απλό "πληροφοριακό αντικείμενο". Με την εξέλιξη των πληροφοριακών συστημάτων, οι προσωπικές πληροφορίες μπορούν όπως είδαμε να συσχετισθούν και να συμπληρωθούν από άλλες, σχηματίζοντας ένα πλήρες "πορτραίτο" της προσωπικότητας του πολίτη. Με τη σύνθεση ενός πλήρους "βιοπορτραίτου", παρακολουθείται και ελέγχεται η συμπεριφορά του ατόμου, με αποτέλεσμα να μετατρέπεται σε πληροφοριακό αντικείμενο και να είναι εύκολα χειραγωγήσιμο.⁴⁷

⁴⁵ Απόστολος Γέροντας, 'Πληροφορική και δίκαιο', σελ.44

⁴⁶ Ιγγλεζάκης Ι. , 'Ευαίσθητα Προσωπικά Δεδομένα', σελ.9

⁴⁷ Απόστολος Γέροντας, ό.π., σελ.71

Επιπρόσθετα, η χωρίς προϋποθέσεις χρήση προσωπικών στοιχείων που αναφέρονται στην ταυτότητα του ατόμου, την περιουσιακή του κατάσταση, το επάγγελμά του, τις πολιτικές του πεποιθήσεις κτλ., περιορίζουν σε σημαντικό βαθμό το δικαίωμα του πληροφοριακού αυτοκαθορισμού. Το δικαίωμα αυτό συνίσταται στη δυνατότητα του ατόμου να αποφασίζει μόνος του πότε, ποιες και κάτω από ποιες προϋποθέσεις είναι δυνατή η επεξεργασία και η κοινοποίηση προσωπικών του στοιχείων. Όταν το εν λόγω άτομο, δε γνωρίζει ποιες πληροφορίες που τον αφορούν είναι γνωστές στον κοινωνικό του περίγυρο, περιορίζεται σημαντικά στην ελευθερία του να προγραμματίζει και να ενεργεί αυτόνομα. Και σε μια πολιτεία που οι πολίτες δεν έχουν αυτονομία, δε λειτουργεί σωστά το δημοκρατικό πολίτευμα, αφού η αυτονομία είναι απαραίτητη προϋπόθεση λειτουργίας του. Ένα ακόμα φαινόμενο που θίγει το δικαίωμα πληροφοριακού αυτοκαθορισμού του ατόμου και προσβάλλει την ιδιωτικότητα του πολίτη, είναι οι λεγόμενες “τράπεζες πληροφοριών”, οι οποίες έχουν αποκτήσει στην εποχή μας τεράστια οικονομική και πολιτική δύναμη και οι οποίες συνιστούν τη σημαντικότερη εφαρμογή της πληροφορικής και των Η/Υ. Οι τράπεζες πληροφοριών αποτελούν τεράστια ηλεκτρονικά αρχεία, στα οποία καταγράφονται πληροφορίες που αφορούν την ιδιωτική ζωή των ατόμων όπως π.χ. οικονομική και περιουσιακή κατάσταση, πληροφορίες για την υγεία, κτλ, οι οποίες συγκεντρώνονται με διάφορους τρόπους, όχι πάντοτε θεμιτούς, και οι οποίες στη συνέχεια μπορεί να αποτελέσουν αντικείμενο εμπορικών συναλλαγών χωρίς πολλές φορές να το γνωρίζουν οι κάτοχοί τους. Οι πληροφορίες αυτές καταχωρούνται και ταξινομούνται αυτόματα και η πρόσβαση του χρήστη στο πληροφοριακό αυτό υλικό, μπορεί να γίνει αυτόματα μέσω του διαδικτύου. Χαρακτηριστικό και ευρέως γνωστό παράδειγμα τέτοιας τράπεζας είναι ο “Τειρεσίας”, για τον οποίο θα γίνει λόγος παρακάτω. Για την προστασία λοιπόν του πολίτη απ’ την κατάχρηση των προσωπικών του δεδομένων, απαιτείται η μέριμνα του κράτους για τη διαφύλαξη του δικαιώματος του πληροφοριακού αυτοκαθορισμού, η οποία επιτυγχάνεται αποτελεσματικά με τη θέσπιση νόμων. Το δικαίωμα του πληροφοριακού αυτοκαθορισμού πρέπει να περιορίζεται μόνο για λόγους υπέρτερου γενικού συμφέροντος, εφόσον υπάρχει νομοθετική πρόβλεψη. Ωστόσο αυτό δε σημαίνει ότι πρέπει να απαγορευτεί πλήρως η

συλλογή και επεξεργασία προσωπικών δεδομένων απ' τις επιχειρήσεις, αλλά να επιτρέπεται υπό προϋποθέσεις, καθώς και να προστατευθεί η ελεύθερη ροή της πληροφορίας.⁴⁸

Εκτός απ' την παραβίαση του δικαιώματος του πληροφοριακού αυτοκαθορισμού, η χρήση προσωπικών στοιχείων πελατών απ' τις επιχειρήσεις, εγκυμονεί έναν ακόμη κίνδυνο. Συχνά, οι εταιρίες συλλέγοντας στοιχεία πελατών, εκμεταλλεύονται αρνητικές γι' αυτούς πληροφορίες για επιχειρηματικούς σκοπούς, με αποτέλεσμα να περιορίζεται η αυτόνομη δράση τους και η ελεύθερη ανάπτυξη της προσωπικότητάς τους. Χαρακτηριστικό είναι το παράδειγμα του διατραπεζικού συστήματος "Τειρεσίας" που δημιουργήθηκε από τράπεζες το Σεπτέμβριο του 1997 και σκοπό έχει τη συλλογή στοιχείων για πολίτες που έχουν οφειλές από ακάλυπτες επιταγές, απλήρωτες συναλλαγματικές, έχουν πτωχεύσει κτλ. Η καταχώριση ενός ατόμου σ' αυτήν την τράπεζα πληροφοριών έχει ως συνέπεια να είναι αδύνατη η χορήγηση δανείου ή πίστωσης για όσο διάστημα διατηρούνται στο αρχείο οι πληροφορίες αυτές. Έτσι λοιπόν, η εσφαλμένη πληροφόρηση για την οικονομική συμπεριφορά ενός προσώπου, μπορεί να έχει δυσμενείς συνέπειες γι' αυτό π.χ. απόρριψη αίτησης για λήψη δανείου ή χορήγησης πίστωσης κτλ.^{49, 50}

Είναι αξιοσημείωτο το γεγονός ότι η παραβίαση της ιδιωτικής ζωής του ατόμου απ' τη χρήση προσωπικών του στοιχείων είναι ένας απ' τους πλέον σημαντικούς παράγοντες που του δημιουργεί φόβο και ανασφάλεια και αναστέλλει την ανάπτυξη του ηλεκτρονικού εμπορίου. Μάλιστα σε μια έρευνα που διενεργήθηκε απ' τη Eurostat το 2002⁵¹ στους Ευρωπαίους πολίτες, αποκαλύφθηκε ότι το 64% των ερωτηθέντων που χρησιμοποιούν το internet, είναι επιφυλακτικοί στην αποκάλυψη προσωπικών τους δεδομένων όπως π.χ. όνομα, διεύθυνση, ημερομηνία γέννησης κτλ, λόγω των κινδύνων που

⁴⁸Deborah Harley, "A whole world in one glance: Privacy as a key enabler individual participation in democratic governance", www.pco.org.com

⁴⁹ Τράπεζα Πληροφοριών "Τειρεσίας", www.teiresias.gr

⁵¹ The European Opinion Research Group, www.europa.eu.int

εγκυμονούν οι συναλλαγές τους μέσω internet για την ιδιωτική τους ζωή. Σε πολλές περιπτώσεις μάλιστα, γίνεται εμπόριο των προσωπικών δεδομένων καταναλωτών, φαινόμενο το οποίο έχει λάβει μεγάλες διαστάσεις στη χώρα μας και περιορίζει το δικαίωμα αυτοδιάθεσης των πληροφοριών του ατόμου. Συγκεκριμένα, στην Ελλάδα έχουν καταγραφεί περισσότερες από 15,000 εταιρίες που τηρούν αρχεία με προσωπικά δεδομένα πολιτών, για τις οποίες η Αρχή Προστασίας Προσωπικών Δεδομένων έχει υποψίες ότι εμπορεύονται τα στοιχεία αυτά χωρίς όμως να το έχει γνωστοποιήσει στην Αρχή. Τα πιο περιζήτητα στοιχεία είναι πληροφορίες που αφορούν την οικονομική κατάσταση και την υγεία των καταναλωτών, καθώς και λίστες με οικογένειες των οποίων τα παιδιά είναι μαθητές Β' Λυκείου όπως και αυτές με νεογέννητα παιδιά και διαχειριστές πολυκατοικιών. Τα στοιχεία αυτά επιθυμούν να αποκτήσουν συνήθως επενδυτικές, ασφαλιστικές και φαρμακευτικές εταιρίες. Σύμφωνα με τον τέως πρόεδρο της Αρχής Προσωπικών Δεδομένων κ. Δαφέρμο «οι εταιρίες που ενδιαφέρονται να αποκτήσουν αρχεία με τέτοιες πληροφορίες συνήθως προσφεύγουν σε δημόσιους φορείς ή σε τράπεζες. Υπάρχουν όμως και άλλες εταιρίες που ασχολούνται αποκλειστικά και μόνο με τη δημιουργία και τη διακίνηση ανάλογων δεδομένων. Τέτοιες εταιρίες ουσιαστικά ενεργούν μεταξύ νομιμότητας και παρανομίας και ο αριθμός σήμερα στη χώρα μας δεν υπερβαίνει το 10%.» Όσο πιο ενημερωμένο είναι ένα αρχείο με προσωπικά στοιχεία πολιτών, τόσο πιο υψηλή είναι κι η τιμή αγοράς. Για παράδειγμα, μια λίστα που περιλαμβάνει στοιχεία για την οικονομική κατάσταση 100 ή 200 πολιτών, με λεπτομέρειες γύρω απ' την περιοχή κατοικίας τους, το μισθό τους, τις καταθέσεις σε τράπεζες, το ή τα αυτοκίνητα που διαθέτουν, μπορεί να ξεπεράσει σε κόστος τα 90 ευρώ.⁵²

⁵² Λαμπρινή Σταμάτη, “Μας πουλάνε και μας αγοράζουν 15000 εταιρίες”, τεύχος 4/9/1999, [http:// ta-nea.dolnet.gr](http://ta-nea.dolnet.gr)

ΚΕΦΑΛΑΙΟ 4

Προστασία προσωπικών δεδομένων

4.1 Εισαγωγή

Όπως αναφέρθηκε στην προηγούμενη ανάλυση, αποτελεί πλέον κοινή διαπίστωση ότι η εξέλιξη της πληροφορικής επιφέρει μεν σημαντικές αλλαγές στην κοινωνική οργάνωση και την οικονομική δραστηριότητα, ταυτόχρονα όμως γεννά κινδύνους κατά των θεμελιωδών ελευθεριών και της ιδιωτικής ζωής του ατόμου. Ειδικότερα, αναγνωρίζεται ευρέως ότι τα συστήματα πληροφορικής συνιστούν ένα απαραίτητο εργαλείο για τη διαχείριση πληροφοριών ιδίως στον ιδιωτικό τομέα, λόγω των δυνατοτήτων της σχεδόν απεριόριστης και σε ελάχιστο χρόνο συσσώρευσης, λογικής επεξεργασίας και συσχετισμού πληροφοριών που παρέχουν. Παράλληλα όμως, η συστηματική επεξεργασία προσωπικών πληροφοριών έχει επιπτώσεις για τον πολίτη, στο βαθμό που ο τελευταίος μεταβάλλεται σε «καθαρό πληροφοριακό αντικείμενο» και αποτελεί αντικείμενο χειραγώγησης. Γεγονός είναι δε, ότι οι κίνδυνοι απ' τη χρήση της πληροφορικής διευρύνονται συνεχώς με την πρόοδο της τεχνολογίας και τη γενίκευση της συλλογής και επεξεργασίας προσωπικών δεδομένων στις σύγχρονες λεωφόρους πληροφοριών, θέτοντας επιτακτικά το ζήτημα της προστασίας της ιδιωτικής ζωής του ατόμου δηλαδή της προστασίας των προσωπικών του δεδομένων. Παρακάτω θα γίνει μια αναφορά στο νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και ιδίως στα νομικά κείμενα διεθνών οργανισμών που αφορούν το ζήτημα αυτό.⁵³

4.2 Τα πρώτα διεθνή κείμενα προστασίας προσωπικών δεδομένων

Τα πρώτα ίχνη της ανάγκης προστασίας της ιδιωτικής ζωής του ατόμου, εντοπίζονται στη Σύμβαση της Ρώμης της 4^{ης} Νοεμβρίου 1950 για την προστασία των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών. Ειδικότερα σύμφωνα με το άρθρο 8 της Σύμβασης, κάθε πρόσωπο έχει δικαίωμα να γίνεται σεβαστή η ιδιωτική και οικογενειακή του ζωή, η κατοικία και η αλληλογραφία του.

⁵³Alfred Bullesbach, “Data protection and privacy at a global enterprise”, www.pco.org.com

Το δικαίωμα αυτό μπορεί να περιορισθεί εφόσον ο περιορισμός αυτός προβλέπεται απ' 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 αταξίας ή εγκλήματος, για την προστασία της υγείας ή των ηθών, ή για την προστασία των δικαιωμάτων και των ελευθεριών τρίτων προσώπων. Επίσης η διάταξη του άρθρου 10 της Σύμβασης καθιερώνει το δικαίωμα της ελευθερίας της έκφρασης, το οποίο περιλαμβάνει την ελευθερία της γνώμης και την ελευθερία λήψης ή μετάδοσης πληροφοριών ή ιδεών, χωρίς την επέμβαση δημόσιων αρχών και ανεξάρτητα απ' την ύπαρξη συνόρων. Το δικαίωμα αυτό υπόκειται σε περιορισμούς με σκοπό την προστασία της ιδιωτικής και οικογενειακής ζωής και απ' την ανάγκη να αποτραπεί η αποκάλυψη εμπιστευτικών πληροφοριών.^{54, 55}

Στην Ευρώπη η πρώτη εθνική νομοθεσία για την προστασία των προσωπικών δεδομένων ήταν ο νόμος του γερμανικού κρατιδίου της Έσσης του 1970. Ακολούθησε η Σουηδία το 1973, η Ομοσπονδιακή Δημοκρατία της Γερμανίας το 1977, η Αυστρία, η Γαλλία, η Δανία και η Νορβηγία το 1978, των οποίων τα νομοθετήματα εντάσσονται στην αποκαλούμενη «πρώτη γενιά νομοθεσιών». Τα νομοθετήματα αυτά όμως διακρίνονταν απ' τη δυσπιστία και το φόβο του νομοθέτη απέναντι σε κάθε μορφής ηλεκτρονική επεξεργασία προσωπικών δεδομένων. Περιείχαν γενικές και αόριστες ρήτρες, αυστηρό προληπτικό και κατασταλτικό έλεγχο και εξοντωτικές ποινικές, αστικές και διοικητικές κυρώσεις.⁵⁶

4.3 Κείμενα διεθνών οργανισμών για την προστασία προσωπικών δεδομένων

Αποτελεί κοινή διαπίστωση του επιστημονικού κόσμου ότι η ελευθερία της πληροφόρησης, τόσο στην ενεργητική της μορφή (ελευθερία του πληροφορείν),

⁵⁴ Απόστολος Γέροντας, *ό.π.*, σελ. 101-102

⁵⁵ Καράκωστας Ιωάννης, "Η προστασία του ιδιωτικού βίου των προσώπων της επικαιρότητας από τη σκοπιά του συγκριτικού δικαίου", ΔΕΕ, τεύχος Δεκεμβρίου 1999

⁵⁶ Ιγγλεζακης Ι., *ό.π.*, σελ.23

όσο και στην παθητική της μορφή (ελευθερία του πληροφορείσθαι), αποτελεί αναγκαία προϋπόθεση για την εύρυθμη λειτουργία της παγκοσμιοποιημένης οικονομίας, καθώς εξασφαλίζει την αδιάλειπτη διασυνοριακή ροή πληροφοριών. Επίσης η ελευθερία της πληροφόρησης συνιστά προϋπόθεση για τη διαμόρφωση γνώμης και συνεπώς για τη δυνατότητα συμμετοχής του πολίτη στα κοινά. Είναι άλλωστε αυτονόητο ότι η δημοκρατία προϋποθέτει ενημέρωση και διαφάνεια. Και πέρα απ' αυτό, το να παραμείνει δυνατή η αρχειοθέτηση και επεξεργασία πληροφοριών, ακόμη και εκείνων που έχουν προσωπικό χαρακτήρα, σημαίνει ενίσχυση της διατήρησης της μνήμης μιας κοινωνίας και της ιστορίας της. Τούτο μπορεί να συνειδητοποιηθεί καλύτερα, αν σκεφτούμε το ενδεχόμενο μιας ολοκληρωτικής καταστροφής των προσωπικών δεδομένων. Αλλά και η ιστορική έρευνα και γενικότερα η κοινωνία θα υφίστατο πλήγμα απ' την καταστροφή αυτή.

Βέβαια αξίζει να αναφερθεί, ότι η επεξεργασία δεδομένων με τη χρήση πληροφοριών είναι απαραίτητη, τόσο στο δημόσιο τομέα, όπου τα συστήματα πληροφορικής αποτελούν εργαλεία εκσυγχρονισμού της δημόσιας διοίκησης, όσο και στον ιδιωτικό τομέα, όπου είναι απαραίτητα για την ορθολογικότερη οργάνωση των λειτουργιών των επιχειρήσεων. Συνεπώς κάθε περιορισμός της επεξεργασίας θα λειτουργούσε ως εμπόδιο στη δράση της διοίκησης αλλά και ως περιορισμός της οικονομικής ελευθερίας των υπεύθυνων επεξεργασίας.⁵⁷

Ωστόσο, συχνά, τα συμφέροντα που ικανοποιούνται με την ακώλυτη ροή και χρήση των προσωπικών δεδομένων, δεν είναι πάντοτε ευγενή. Συχνά επιδιώκεται η ικανοποίηση περιέργειας ή η ικανοποίηση οικονομικών, επαγγελματικών ή άλλων θεμιτών ή αθέμιτων συμφερόντων των υπεύθυνων επεξεργασίας ή των τελικών αποδεκτών των στοιχείων αυτών. Η παρεμβολή των συμφερόντων των κατόχων δεδομένων μεγεθύνει τους κινδύνους, επειδή μετά το στάδιο της έστω θεμιτής συλλογής των προσωπικών δεδομένων, αυτά παραμένουν στην κατοχή εκείνου που τα συνέλεξε, διαθέσιμα για οποιαδήποτε

⁵⁷ Μ. Σταθόπουλος, "Τα συμφέροντα για την ακώλυτη ροή των προσωπικών δεδομένων", ΝοΒ, Ιανουάριος 2000, σελ.3

άλλη χρήση, διαφορετική από εκείνη για την οποία έγινε συλλογή. Σήμερα κάτοχοι τέτοιων πληροφοριών, που δεν είναι απαραίτητες για τους σκοπούς της συλλογής, είναι ιδιωτικοί φορείς π.χ. εργοδότες, τράπεζες κτλ που συγκεντρώνουν υπέρμετρη “πληροφοριακή” εξουσία και προβαίνουν σε κατάχρηση των πληροφοριών αυτών εις βάρος των υποκειμένων τους.

Γι’ αυτό λοιπόν είναι επιτακτική η νομοθετική προστασία του ατόμου. Ωστόσο απαιτείται συγκερασμός των δύο αντιτιθέμενων συμφερόντων δηλαδή της ελευθερίας της πληροφόρησης απ’ τη μια και της προστασίας των προσωπικών δεδομένων απ’ την άλλη. Στα πλαίσια της παγκοσμιοποιημένης πλέον οικονομίας μας, η αποκατάσταση της ισορροπίας ανάμεσα στις δύο αντίρροπες αυτές δυνάμεις είναι εν πολλοίς έργο των διεθνών οργανισμών, οι οποίοι θεσπίζοντας διεθνείς συμβάσεις και υιοθετώντας κατευθυντήριες οδηγίες προσπαθούν να εξασφαλίσουν την ελευθερία στη ροή των πληροφοριών, ενόσω παράλληλα προστατεύουν τα άτομα απ’ την κατάχρηση των προσωπικών τους δεδομένων.⁵⁸

Οι διεθνείς οργανισμοί αυτοί είναι οι εξής:

ΟΟΣΑ

Το Σεπτέμβριο του 1980 ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ) υπό την επιρροή του Privacy Act των ΗΠΑ, υιοθέτησε ένα κείμενο με τίτλο «Αρχές διέπουσες την προστασία της προσωπικής σφαίρας του ανθρώπου και τις διασυννοριακές ροές προσωπικών στοιχείων» με το οποίο προσκαλούσε τα κράτη μέλη του να ακολουθήσουν κοινή γραμμή για την προστασία προσωπικών δεδομένων, εφαρμόζοντας κάποιες κοινές αρχές. Ο λόγος για τον οποίο ο ΟΟΣΑ θέσπισε τις αρχές αυτές, είναι ο φόβος μήπως τα κράτη τα οποία συνιστούν τον οργανισμό, εισάγουν διαφορετικούς και αντικρουόμενους νόμους για την προστασία της ιδιωτικότητας του ατόμου. Το γεγονός αυτό θα αποτελούσε σοβαρό εμπόδιο στην ελευθερία της διασυννοριακής ροής πληροφοριών. Οι αρχές αυτές συγκλίνουν περισσότερο προς τη νομοθεσία των ΗΠΑ που είναι περισσότερο ελαστική όσον αφορά τη θέσπιση περιορισμών

⁵⁸ Ιγγλεζάκης Ι., ό.π., σελ.18

για την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Οι Αρχές αυτές είναι οι εξής^{59, 60}:

1. Αρχή της περιορισμένης συγκεντρώσεως/ συλλογής στοιχείων

Η αρχή αυτή αναφέρει ότι πρέπει να υφίστανται όρια στη συγκέντρωση προσωπικών στοιχείων και κάθε στοιχείο τέτοιου είδους πρέπει να συλλέγεται με νόμιμα και έντιμα μέσα και όπου παρίσταται αναγκαίο, με τη συναίνεση του υποκειμένου των στοιχείων.

2. Αρχή της ποιότητας των στοιχείων

Σύμφωνα με αυτή την αρχή, τα στοιχεία προσωπικού χαρακτήρα πρέπει να είναι σχετικά με τους σκοπούς για τους οποίους πρόκειται να χρησιμοποιηθούν και κατά την αναγκαία έκταση, για τους σκοπούς αυτούς, πρέπει να είναι ακριβή, πλήρη και ενημερωμένα.

3. Αρχή του προσδιορισμένου σκοπού

Στην αρχή αυτή ορίζεται ότι οι σκοποί για τους οποίους συλλέγονται προσωπικά στοιχεία πρέπει να είναι προσδιορισμένοι μέχρι το χρόνο συλλογής τους και η εν συνεχεία χρήση τους περιορισμένη στην εκπλήρωση αυτών των σκοπών ή τυχόν άλλων που δεν είναι ασυμβίβαστοι με αυτούς τους σκοπούς και όπως προσδιορίζονται σε κάθε περίπτωση αλλαγής σκοπού.

4. Αρχή περιορισμένης χρήσης

Η αρχή αυτή ορίζει ότι τα προσωπικά στοιχεία δεν πρέπει να αποκαλύπτονται, να καθίστανται διαθέσιμα ή αλλιώς να χρησιμοποιούνται για σκοπούς διαφορετικούς απ' αυτούς που προσδιορίστηκαν σύμφωνα με την προηγούμενη αρχή παρά εκτός αν α) έχει συναinéσει το υποκείμενο των στοιχείων ή β) το επιτρέπει ο νόμος.

⁵⁹ “Oecd guidelines on the Protection of privacy and transborder flows of personal data”, www.oecd.org

⁶⁰ Βασίλειος Θ. Αραβαντινός, “Η προστασία των στοιχείων προσωπικού χαρακτήρα από την αθέμιτη επεξεργασία τους με Η/Υ”, σελ.62

5. Αρχή μέτρων ασφαλείας

Τα προσωπικά στοιχεία πρέπει να προστατεύονται με εύλογα μέτρα ασφαλείας έναντι κινδύνων όπως είναι η απώλεια ή η μη εξουσιοδοτημένη πρόσβαση, καταστροφή, χρήση, μεταβολή ή αποκάλυψη των στοιχείων.

6. Αρχή της διαφάνειας

Πρέπει να υπάρχει μια γενική πολιτική διαφάνειας σε ό,τι αφορά την ανάπτυξη (συστημάτων), την πρακτική και την πολιτική έναντι των προσωπικών στοιχείων. Πρέπει να υπάρχουν μέσα που θα επιτρέπουν τη διαπίστωση της ύπαρξης και της φύσης των προσωπικών στοιχείων.

7. Αρχή ενημέρωσης

Ο ιδιώτης πρέπει να έχει το δικαίωμα:

Να λαμβάνει απ' τον υπεύθυνο της επεξεργασίας ή άλλον, έγκυρη βεβαίωση περί του αν ο υπεύθυνος της επεξεργασίας έχει στοιχεία που σχετίζονται με αυτόν ή όχι.

A) Να του κοινοποιούνται τα σχετικά με αυτόν στοιχεία

1^ο) εντός εύλογου χρόνου

2^ο) έναντι λογικού ανταλλάγματος ή και δωρεάν

3^ο) κατά εύληπτο τρόπο

4^ο) σε εμφάνιση τελείως κατανοητή απ' αυτόν

B) Να του εξηγείται, σε περίπτωση υποβολής σχετικού αιτήματος, η τυχόν άρνηση ικανοποίησης των παραπάνω δικαιωμάτων του και να του χορηγείται η δυνατότητα να προσβάλλει την άρνηση αυτή.

Γ) Να προσβάλλει στοιχεία που τον αφορούν και σε περίπτωση επιτυχούς προσβολής τους, να επιτυγχάνει τη διαγραφή, τη διόρθωση, τη συμπλήρωση ή τροποποίησή τους.

8. Αρχή υπευθυνότητας

Ο υπεύθυνος της επεξεργασίας βαρύνεται με την υποχρέωση να συμμορφωθεί με διατάξεις που υλοποιούν τις ανωτέρω αρχές.

Συμβούλιο της Ευρώπης

Το Συμβούλιο της Ευρώπης θέσπισε τη Σύμβαση υπ' αριθμόν 108, της 28.1.1981, για την "προστασία του ατόμου απ' την αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων", η οποία υπήρξε το πρότυπο για ορισμένο χρόνο στην Ευρώπη πριν από την ενεργοποίηση της Ε.Ε και τη θέσπιση σχετικής οδηγίας.⁶¹ Το νομικό αυτό κείμενο τέθηκε σε ισχύ την 1.10.1985 και είναι το πρώτο διεθνές δεσμευτικό νομικό κείμενο που παρέχει προστασία των προσωπικών δεδομένων των ατόμων από κατάχρηση κατά τη συλλογή και επεξεργασία τους και το οποίο ρυθμίζει ταυτόχρονα τη διασυνοριακή ροή δεδομένων. Πρόκειται για ένα κείμενο που θέτει τις γενικές κατευθύνσεις για την προστασία των προσωπικών στοιχείων κάθε προσώπου απ' την αυθαίρετη επεξεργασία τους, η οποία λαμβάνει χώρα με τη βοήθεια αυτοματοποιημένων μέσων και περιέχει μια σειρά εγγυήσεων και δικαιωμάτων υπέρ των προσώπων στα οποία αναφέρονται τα δεδομένα και προβλέπει την ίδρυση εθνικών αρχών, οι οποίες επιφορτίζονται με τον έλεγχο της εφαρμογής των διατάξεων της σύμβασης. Σύμφωνα με τη σύμβαση αυτή και συγκεκριμένα του άρθρου 4, τα μέλη του Συμβουλίου της Ευρώπης οφείλουν να προβλέψουν με την εσωτερική τους νομοθεσία όλα τα αναγκαία μέτρα για την υλοποίηση των βασικών αρχών που θεσπίζει η σύμβαση, όπως το δικαίωμα πρόσβασης στο αρχείο πληροφοριών, δικαίωμα διόρθωσης πληροφοριών, ρύθμιση σκοπών αρχειοθεσίας κτλ

Το άρθρο 1 της Σύμβασης ορίζει ως σκοπό την εξασφάλιση της προστασίας των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών για κάθε άτομο, ανεξάρτητα απ' την υπηκοότητα, την κατοικία και ειδικά το δικαίωμα στην ιδιωτική ζωή, έναντι της αυτοματοποιημένης επεξεργασίας των προσωπικών δεδομένων.

⁶¹ Στην Ελλάδα επικυρώθηκε με το ν. 2068/92, ΦΕΚ Α', Αρ.Φύλλου 118/9.7.92, και άρχισε να ισχύει την 1.1.1995 ενώ στις 8/11/2001 τέθηκε προς υπογραφή το Πρόσθετο Πρωτόκολλο αριθ. 181, το οποίο αποβλέπει στη βελτίωση των μεθόδων εφαρμογής της Σύμβασης. Ωστόσο ο ν. 2068/92 είχε μείνει ανεφάρμοστος έως την εισαγωγή του νέου νόμου για την προστασία προσωπικών δεδομένων δηλαδή του ν. 2472/97

Ως αυτοματοποιημένη επεξεργασία θεωρείται κάθε πράξη που εκτελείται στο σύνολό της ή εν μέρει με τη βοήθεια αυτοματοποιημένων μέσων (άρθρο 2 εδ. γ).

Κατά το άρθρο 2 της Σύμβασης, πληροφορίες προσωπικού χαρακτήρα θεωρείται κάθε πληροφορία η οποία αφορά συγκεκριμένο πρόσωπο. Η αυτόνομη επεξεργασία των προσωπικών δεδομένων πρέπει να γίνεται σύμφωνα με ορισμένες βασικές αρχές οι οποίες θεσπίζονται στη διάταξη του άρθρου 5. Σύμφωνα με αυτές, οι προσωπικές πληροφορίες που υπόκεινται σε αυτοματοποιημένη επεξεργασία πρέπει α) να έχουν αποκτηθεί και να υφίστανται επεξεργασία με νόμιμο και θεμιτό τρόπο β) να καταχωρίζονται και να αποθηκεύονται μόνον για ορισμένους και νόμιμους σκοπούς και να μην χρησιμοποιούνται κατά τρόπο που δεν συμβιβάζεται προς τους σκοπούς αυτούς γ) να είναι πρόσφορες, προσήκουσες και όχι υπέρμετρες σε σχέση με τους σκοπούς για τους οποίους έχουν καταχωρηθεί δ) να είναι ακριβείς και εφόσον κρίνεται αναγκαίο να ενημερώνονται κατά τακτά χρονικά διαστήματα ε) να διατηρούνται σε μορφή που επιτρέπει την εξακρίβωση της ταυτότητας των προσώπων τα οποία αφορούν οι πληροφορίες για χρονικό διάστημα που δεν υπερβαίνει εκείνο που είναι αναγκαίο για την εξυπηρέτηση των σκοπών για τους οποίους έχουν καταχωρηθεί. Κατά το άρθρο 7 τα κράτη μέλη οφείλουν να λαμβάνουν τα κατάλληλα μέτρα ασφάλειας για την προστασία των προσωπικών δεδομένων που έχουν καταχωρηθεί σε αυτοματοποιημένα αρχεία από συμπτωματική καταστροφή ή από συμπτωματική απώλεια, καθώς και από πρόσβαση σε αυτές, τροποποίηση ή μετάδοσή τους χωρίς την απαιτούμενη άδεια.

Σύμφωνα με το άρθρο 8 της Σύμβασης θεσπίζονται συγκεκριμένα δικαιώματα για το υποκείμενο των δεδομένων και ειδικότερα:

1) Να ενημερώνεται για την ύπαρξη αυτοματοποιημένων αρχείων προσωπικού χαρακτήρα, τους κυριότερους σκοπούς τήρησης του αρχείου καθώς και την ταυτότητα και τη συνήθη κατοικία ή την κύρια εγκατάσταση του κυρίου των αρχείων

2) Να επιτυγχάνει, εφόσον συντρέχει περίπτωση, τη διόρθωση ή τη διαγραφή πληροφοριών όταν έχουν αποτελέσει αντικείμενο επεξεργασίας κατά παράβαση των διατάξεων του εσωτερικού δικαίου που έχει υιοθετήσει τις βασικές αρχές επεξεργασίας των προσωπικών δεδομένων

3) Να έχει τη δυνατότητα της προσφυγής

Τα παραπάνω δικαιώματα μπορούν να περιορισθούν για στατιστικούς σκοπούς ή για επιστημονικές έρευνες, όταν δεν υπάρχει κίνδυνος προσβολής του ιδιωτικού βίου των προσώπων, τα οποία αφορούν οι πληροφορίες, ενώ κατά το άρθρο 9 είναι δυνατή η παρέκκλιση, όταν προβλέπεται από διάταξη νόμου του συμβαλλόμενου μέρους και αποτελεί απαραίτητο μέτρο σε μια δημοκρατική κοινωνία για την προστασία της ασφάλειας του κράτους, της δημόσιας ασφάλειας, των νομικών συμφερόντων του κράτους ή για την καταστολή των ποινικών παραβάσεων.

Η σύμβαση θεσπίζει την αρχή της ελεύθερης διασυνοριακής ροής των προσωπικών δεδομένων και κατά το άρθρο 12 τα συμβαλλόμενα μέρη δεν μπορούν, με μοναδικό σκοπό την προστασία του ιδιωτικού βίου, να απαγορεύουν ή να υποβάλλουν σε ειδική άδεια τη διασυνοριακή ροή των πληροφοριών προσωπικού χαρακτήρα, που προορίζονται για το έδαφος άλλου κράτους μέλους. Η αρχή αυτή υπόκειται όμως σε εξαιρέσεις και ειδικότερα α) στο μέτρο που η νομοθεσία του κράτους μέλους προβλέπει ειδική ρύθμιση για ορισμένες κατηγορίες πληροφοριών προσωπικού χαρακτήρα ή αυτοματοποιημένα αρχεία πληροφοριών, λόγω της φύσης των πληροφοριών ή των αρχείων αυτών, εκτός αν η ρύθμιση του άλλου συμβαλλόμενου μέρους προσφέρει ανάλογη ή ισοδύναμη προστασία και β) όταν η μετάδοση πραγματοποιείται απ' το έδαφος ενός κράτους μέλους προς το έδαφος μη συμβαλλόμενου μέρους μέσω εδάφους άλλου συμβαλλόμενου μέρους προκειμένου να αποφεύγεται να καταλήγουν τέτοιες μεταβιβάσεις σε περιγραφή της νομοθεσίας του συμβαλλόμενου μέρους.

Στα πλαίσια της εφαρμογής της Σύμβασης, τα κράτη μέλη αναλαμβάνουν την υποχρέωση να προσφέρουν αμοιβαία συνδρομή και για την επίτευξη αυτού του σκοπού κάθε συμβαλλόμενο μέρος ορίζει μια ή περισσότερες αρχές με συγκεκριμένες αρμοδιότητες και η αρχή αυτή οφείλει μετά από σχετική αίτηση της αρχής άλλου συμβαλλόμενου μέρους να παρέχει πληροφορίες για το δίκαιο και τη διοικητική πρακτική του σχετικά με την προστασία των πληροφοριών και να λαμβάνει, σύμφωνα με την εθνική του νομοθεσία, όλα τα κατάλληλα μέτρα για την παροχή πληροφοριών ουσίας, που αφορούν αυτοματοποιημένη επεξεργασία πραγματοποιούμενη στο έδαφός του, με εξαίρεση πληροφορίες οι οποίες αποτελούν αντικείμενο αυτής της επεξεργασίας (άρθρο 13).

Η Σύμβαση τέλος προβλέπει στο άρθρο 18 τη συγκρότηση Συμβουλευτικής Επιτροπής, η οποία αποτελείται από αντιπροσώπους των κρατών μελών και συγκαλείται απ' το Γενικό Γραμματέα του Συμβουλίου της Ευρώπης (άρθρο 20 παρ.1). Η συμβουλευτική επιτροπή επεξεργάζεται προτάσεις προκειμένου να διευκολυνθεί ή να βελτιωθεί η εφαρμογή της σύμβασης ή την τροποποίησή της και μπορεί να γνωμοδοτεί για θέματα, αν το ζητήσει συμβαλλόμενο μέρος, τα οποία συνδέονται με την εφαρμογή της Σύμβασης (άρθρο 19).⁶²

Αργότερα, στις 23.2.1999, το Συμβούλιο Υπουργών δημοσίευσε τη Σύσταση (99)5 : «Οδηγίες για την προστασία των ατόμων απ' τη συλλογή και επεξεργασία προσωπικών δεδομένων στις λεωφόρους των πληροφοριών, που μπορούν να συμπεριληφθούν ή να προστεθούν σε κώδικες δεοντολογίας». Η Σύσταση προέκυψε από ειδική ομάδα εργασίας με θέμα την προστασία δεδομένων, καλύπτει και τους χρήστες και τους Παρόχους Υπηρεσιών Internet και εκδόθηκε μετά από συνεργασία και με τα κράτη μέλη της Ευρωπαϊκής Ένωσης.

Πρόσφατα, το Συμβούλιο της Ευρώπης, υπέγραψε πρόσθετο Πρωτόκολλο στη Σύμβαση 108, με σκοπό τη βελτίωση των μεθόδων εφαρμογής της. Το Πρωτόκολλο προβλέπει ότι τα συμβαλλόμενα κράτη πρέπει να θεσπίσουν

⁶² Απόστολος Γέροντας, ό.π. ,σελ. 106-108

ανεξάρτητες αρχές της Σύμβασης 108 (άρθρο 1) και ότι η διασυνοριακή ροή δεδομένων προς κράτη που δεν έχουν υπογράψει τη Σύμβαση, επιτρέπεται μόνο αν το κράτος υποδοχής εξασφαλίζει «ικανοποιητικό επίπεδο προστασίας» (άρθρο 2). Προβλέπεται μάλιστα ειδική εξαίρεση, δηλαδή η μεταβίβαση επιτρέπεται, αν παρέχονται εγγυήσεις που βασίζονται σε προδιατυπωμένους όρους.⁶³

Γενικό Σύμφωνο Δασμών και Εμπορίου (GATS)

Η Γενική Συμφωνία για το Εμπόριο των Υπηρεσιών (GATS), η οποία αποτελεί τμήμα της GATT, στο άρθρο XIV παρέχει την ευχέρεια στα κράτη μέλη να υιοθετήσουν κατάλληλα μέτρα «για την προστασία του ιδιωτικού βίου σε σχέση με την επεξεργασία και τη διανομή προσωπικών δεδομένων και την προστασία του εμπιστευτικού χαρακτήρα ατομικών αρχείων και λογαριασμών». Παράλληλα, όμως, το ίδιο άρθρο περιορίζει τις δυνατότητες των κρατών, αφού τα ανωτέρω μέτρα δεν πρέπει να εφαρμόζονται ως συγκεκριμένο εμπόδιο του ελεύθερου εμπορίου υπηρεσιών ή με τρόπο που προκαλεί διακρίσεις.⁶⁴

Οργανισμός Ηνωμένων Εθνών (ΟΗΕ)

Ο ΟΗΕ στις 10 Δεκεμβρίου 1948 υπέγραψε την Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου, η οποία στο άρθρο 12 προστατεύει την ιδιωτική ζωή⁶⁵. Συγκεκριμένα ορίζει ότι: «Κανείς δεν επιτρέπεται να υποστεί αυθαίρετες επεμβάσεις στην ιδιωτική του ζωή, την οικογένεια, την κατοικία ή την αλληλογραφία του...Καθένας έχει το δικαίωμα να τον προστατεύουν οι νόμοι από επεμβάσεις και προσβολές αυτού του είδους». Η διάταξη δεν καθιερώνει μόνο δικαίωμα στον καθένα να ζητήσει έννομη προστασία για κάθε αυθαίρετη επέμβαση στο δικαίωμα του ιδιωτικού του βίου, αλλά παρέχει και κατευθυντήριες γραμμές στα κράτη για τη θέσπιση διατάξεων που προστατεύουν την ιδιωτική ζωή του ατόμου. Στην ίδια γραμμή με την Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου κινείται και το Διεθνές Σύμφωνο για τα Ατομικά και

⁶³ Σύμβαση για την προστασία του ατόμου απ' την αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων, διαθέσιμο στο <http://conventions.coe.int>

⁶⁴ C. Ragavan, "GATS-What is fact and what is fiction", www.citizen.org

⁶⁵ Η Οικουμενική διακήρυξη των δικαιωμάτων του ανθρώπου δεν έχει άμεση νομική δεσμευτικότητα

Πολιτικά Δικαιώματα του ΟΗΕ, το οποίο στο άρθρο 17 ορίζει ότι: «Κανένας δεν υπόκειται σε αυθαίρετη και παράνομη προσβολή της ιδιωτικότητάς του, της οικογένειάς, της κατοικίας, της αλληλογραφίας του, της τιμής ή της υπόληψής του». Τέλος, το 1990 ο ΟΗΕ δημοσίευσε τις Κατευθυντήριες Γραμμές (Οδηγίες ΟΗΕ) για τη ρύθμιση των μηχανογραφημένων προσωπικών αρχείων δεδομένων. Το πρώτο μέρος των Οδηγιών του ΟΗΕ υποδεικνύει τις «ελάχιστες εγγυήσεις» για την προστασία της ιδιωτικής ζωής που πρέπει να περιλαμβάνει η εθνική νομοθεσία των κρατών. Οι «αρχές ελάχιστης προστασίας» που προτείνονται για τις εθνικές νομοθεσίες, αντανακλούν τις βασικές αρχές των Οδηγιών του ΟΟΣΑ. Το άρθρο 8 προτείνει την ίδρυση ανεξάρτητων αρχών, οι οποίες θα επιβλέπουν την εφαρμογή των ρυθμίσεων. Προτείνεται επίσης να προβλεφθούν, σε περίπτωση παράβασης της σχετικής νομοθεσίας «εκτός από ατομικό δικαίωμα αποζημίωσης και ποινικές ή άλλες κυρώσεις».^{66, 67}

Ευρωπαϊκή Ένωση

Πρέπει να αναφερθεί ότι εκτός απ' τους παραπάνω διεθνείς οργανισμούς, και η Ευρωπαϊκή Ένωση έχει θεσπίσει μια σειρά από Οδηγίες για την προστασία της ιδιωτικής ζωής του ατόμου. Παράλληλα, το άρθρο 8 του Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης ορίζει τα εξής: «1. Κάθε πρόσωπο έχει δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν. 2. Η επεξεργασία αυτών των δεδομένων πρέπει να γίνεται νομίμως, για καθορισμένους σκοπούς και με βάση τη συγκατάθεση του ενδιαφερομένου ή για άλλους θεμιτούς λόγους που προβλέπονται απ' το νόμο. Κάθε πρόσωπο έχει δικαίωμα να έχει πρόσβαση στα συλλεγμένα δεδομένα που το αφορούν και να επιτυγχάνει τη διόρθωσή τους. 3. Ο σεβασμός των κανόνων αυτών υπόκειται στον έλεγχο ανεξάρτητης αρχής...». Επίσης η Ευρωπαϊκή Σύμβαση Ανθρωπίνων Δικαιωμάτων (ΕΣΔΑ) κατοχυρώνει το δικαίωμα της ιδιωτικής ζωής υπερ όλων των ατόμων, αφού στο άρθρο 8 τονίζει ότι «κάθε άτομο δικαιούται το σεβασμό της ιδιωτικής και οικογενειακής του ζωής». Τέλος η Οδηγία 97/7 ΕΚ, παρέχει

⁶⁶ Γιαννόπουλος Ν. Γιώργος, “Ροή πληροφοριών στο διαδίκτυο”,σελ.58

⁶⁷ Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου, διαθέσιμο στο www.lawnet.gr

προστασία της ιδιωτικής ζωής του καταναλωτή στις εξ αποστάσεως συμβάσεις , αφού στο άρθρο 10§1 ορίζει ότι « Απαιτείται η προηγούμενη συγκατάθεση του καταναλωτή για τη χρήση απ' τον προμηθευτή των ακόλουθων μέσων: α) αυτοματοποιημένου συστήματος κλήσεως χωρίς ανθρώπινη παρέμβαση (συσκευής αυτόματης κλήσεως) β) μηχανήματος τηλεμοιοτυπίας (φάξ). Στην §2 ορίζει ότι « Τα κράτη μέλη μεριμνούν ώστε τα μέσα εξ αποστάσεως επικοινωνίας, εκτός από εκείνα που αναφέρει η παράγραφος 1, εφόσον καθιστούν δυνατή μια ατομική επικοινωνία, να επιτρέπεται να χρησιμοποιηθούν μόνο αν ο καταναλωτής δεν έχει εκδηλώσει τη αντίθεσή του.»⁶⁸

Οδηγία 95/46 ΕΚ

Ένα αναμφισβήτητης σημασίας νομικό κείμενο για την προστασία της προσωπικής ζωής του ατόμου είναι η Οδηγία 95/46 ΕΚ την οποία εξέδωσε το Συμβούλιο της ΕΚ την 24.10.1995⁶⁹, περί της προστασίας των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και της ελεύθερης κυκλοφορίας των δεδομένων αυτών. Παρακάτω, θα γίνει μια αναφορά στα βασικά σημεία της Οδηγίας.

Στο άρθρο 1 ορίζεται ο στόχος της Οδηγίας που είναι η προστασία των θεμελιωδών δικαιωμάτων των φυσικών προσώπων και ιδίως της ιδιωτικής τους ζωής, έναντι της επεξεργασίας των προσωπικών τους δεδομένων. Με τον όρο «δεδομένα προσωπικού χαρακτήρα» νοείται «κάθε πληροφορία που αναφέρεται σε φυσικό πρόσωπο του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί, δηλαδή που μπορεί να προσδιοριστεί άμεσα ή έμμεσα, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός ή περισσότερων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από φυσική, βιολογική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική άποψη». Με τον όρο «επεξεργασία δεδομένων προσωπικού χαρακτήρα» νοείται «κάθε εργασία ή σειρά εργασιών που πραγματοποιούνται με ή χωρίς τη βοήθεια αυτοματοποιημένων διαδικασιών

⁶⁸ Άρθρο 10 Οδηγίας 97/7 ΕΚ

⁶⁹ ΕΕ L 281/31

και εφαρμόζονται σε δεδομένα προσωπικού χαρακτήρα, όπως η συλλογή, καταχώρηση, η οργάνωση, η αποθήκευση, η προσαρμογή ή η τροποποίηση, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η ανακοίνωση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η εναρμόνιση ή ο συνδυασμός, καθώς και το κλείδωμα, η διαγραφή ή η καταστροφή» (άρθρο 2)

Προϋποθέσεις θεμιτής επεξεργασίας

Σύμφωνα με το άρθρο 6 της οδηγίας, τα δεδομένα πρέπει να υφίστανται νόμιμη επεξεργασία και να συλλέγονται για καθορισμένους και νόμιμους σκοπούς. Επίσης πρέπει να είναι κατάλληλα, συναφή προς το θέμα και όχι υπερβολικά σε σχέση με τους σκοπούς για τους οποίους συλλέγονται. Ο υπεύθυνος επεξεργασίας οφείλει να τα ενημερώνει τακτικά και να λαμβάνει όλα τα απαραίτητα μέτρα ώστε δεδομένα ανακριβή ή ελλιπή να διαγράφονται ή να διορθώνονται. Τέλος πρέπει να διατηρούνται σε μορφή που να επιτρέπει τον προσδιορισμό της ταυτότητας των υποκειμένων μόνο κατά τη διάρκεια της επεξεργασίας, ενώ τα κράτη μέλη της Ε.Ε. οφείλουν να προβλέπουν κατάλληλες εγγυήσεις για τα δεδομένα που διατηρούνται πέραν της περιόδου αυτής για σκοπούς ιστορικούς, στατιστικούς ή επιστημονικούς.

Το άρθρο 7 της οδηγίας ορίζει τις αρχές της νόμιμης επεξεργασίας προσωπικών δεδομένων. Συγκεκριμένα ορίζει ότι το υποκείμενο πρέπει να δώσει προηγουμένως την συγκατάθεσή του προκειμένου να εκτελεστεί η επεξεργασία ή αλλιώς η επεξεργασία να:

1. είναι απαραίτητη για την εκτέλεση κάποιας σύμβασης στην οποία συμμετέχει ως συμβαλλόμενο μέρος το υποκείμενο
2. είναι αναγκαία για την τήρηση υποχρέωσης του υποκειμένου
3. είναι απαραίτητη για τη διαφύλαξη κάποιου ζωτικού συμφέροντός του
4. είναι απαραίτητη για την εκπλήρωση έργου δημοσίου συμφέροντος ή εμπόνητος στην άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο της επεξεργασίας

5. είναι απαραίτητη για την επίτευξη του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας υπό τον όρο ότι δεν προέχουν τα θεμελιώδη δικαιώματα ή τα συμφέροντα του υποκειμένου

Ο υπεύθυνος επεξεργασίας οφείλει να ενημερώνει το υποκείμενο των δεδομένων που προορίζονται για επεξεργασία, για τα εξής:

- την ταυτότητα τη δική του ή του εκπροσώπου του
- τους σκοπούς της επεξεργασίας για την οποία προορίζονται τα δεδομένα
- τους αποδέκτες των δεδομένων
- το κατά πόσο η παροχή των δεδομένων είναι υποχρεωτική ή όχι, καθώς και τις ενδεχόμενες συνέπειες της άρνησης της παροχής τους
- την ύπαρξη δικαιώματος πρόσβασης στα δεδομένα και δικαιώματος διόρθωσής τους (άρθρο 10)

Οι παραπάνω πληροφορίες πρέπει να παρέχονται στο υποκείμενο, και όταν ο υπεύθυνος επεξεργασίας αντλεί τα δεδομένα από τρίτο πρόσωπο, εκτός του υποκειμένου (άρθρο 11 παρ.1). Κατ' εξαίρεση, δεν απαιτείται ενημέρωση του υποκειμένου όταν τα προσωπικά δεδομένα συλλέγονται για στατιστικούς ή ιστορικούς σκοπούς και η ενημέρωση του ενδιαφερομένου καθίσταται αδύνατη ή απαιτεί δυσανάλογες προσπάθειες (άρθρο 11 παρ.2). Εκτός απ'το δικαίωμα ενημέρωσης, η οδηγία στο άρθρο 12 παρέχει στα υποκείμενα των δεδομένων το δικαίωμα πρόσβασης. Δηλαδή τα κράτη μέλη πρέπει να εγγυώνται στα υποκείμενα το δικαίωμα να λαμβάνουν:

- την επιβεβαίωση ότι υπάρχει ή όχι επεξεργασία καθώς και τις πληροφορίες σχετικά με τους σκοπούς της επεξεργασίας
- τη γνωστοποίηση των δεδομένων υπό επεξεργασία και των διαθέσιμων πληροφοριών για την προέλευσή τους
- την ενημέρωση σχετικά με τη λογική στην οποία στηρίζεται κάθε αυτοματοποιημένη επεξεργασία

Επίσης ο υπεύθυνος επεξεργασίας είναι υποχρεωμένος να προβεί σε διόρθωση, διαγραφή ή κλείδωμα των δεδομένων των οποίων η επεξεργασία δεν

είναι σύμφωνη με τις διατάξεις της οδηγίας, ιδίως λόγω ελλιπούς ή ανακριβούς χαρακτήρα των δεδομένων και να το κοινοποιήσει σε τρίτους στους οποίους έχουν ανακοινωθεί τα δεδομένα.

Το υποκείμενο των δεδομένων έχει επίσης το δικαίωμα αντίταξης, το οποίο αναλύεται στο άρθρο 14 της οδηγίας. Περιεχόμενο του δικαιώματος αυτού είναι η δυνατότητα που παρέχεται στο άτομο να αντιτάσσεται ανά πάσα στιγμή στην επεξεργασία δεδομένων που το αφορούν για επιτακτικούς και νόμιμους λόγους, εκτός αν στην εθνική νομοθεσία των κρατών ορίζεται διαφορετικά. Το υποκείμενο των δεδομένων έχει επίσης το δικαίωμα να αντιτάσσεται στην επεξεργασία των δεδομένων του που γίνεται για την εξυπηρέτηση σκοπών άμεσης εμπορίας και διαφήμισης.

Η οδηγία επιβάλλει στους υπεύθυνους επεξεργασίας να παρέχουν κάποια ασφάλεια στην επεξεργασία προσωπικών δεδομένων. Συγκεκριμένα στο άρθρο 17 ορίζει ότι τα κράτη πρέπει να λαμβάνουν όλα τα κατάλληλα μέτρα για την προστασία των δεδομένων από καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση. Τα μέτρα αυτά πρέπει να εξασφαλίζουν επίπεδο ασφάλειας ανάλογο προς τους κινδύνους που απορρέουν απ' την επεξεργασία και τη φύση των δεδομένων.

Στο άρθρο 18 ορίζεται η υποχρέωση των υπεύθυνων επεξεργασίας για κοινοποίηση των διαδικασιών επεξεργασίας προς κάποια Αρχή ελέγχου, η οποία πρέπει να γίνεται πριν απ' την εκτέλεση της επεξεργασίας. Η κοινοποίηση απλουστεύεται ή αποτελεί αντικείμενο εξαιρέσως στις ακόλουθες περιπτώσεις και υπό τους ακόλουθους όρους:

-εφόσον, για κατηγορίες επεξεργασιών οι οποίες, δεν μπορούν να θίξουν τα δικαιώματα και τις ελευθερίες των προσώπων στα οποία αναφέρονται τα δεδομένα, καθορίζουν τους σκοπούς της επεξεργασίας, τα δεδομένα υπό επεξεργασία, τα πρόσωπα στα οποία αναφέρονται τα δεδομένα, τον αποδέκτη των δεδομένων και τη διάρκεια αποθήκευσης των δεδομένων αυτών.

-εφόσον ο υπεύθυνος της επεξεργασίας ορίζει έναν υπεύθυνο για την προστασία των προσωπικών δεδομένων ο οποίος έχει κυρίως αποστολή να διασφαλίζει την εφαρμογή των εθνικών διατάξεων που θεσπίζονται κατ' εφαρμογή της παρούσας οδηγίας και να τηρεί μητρώο των επεξεργασιών που εκτελούνται απ' τον υπεύθυνο της επεξεργασίας.

Στην κοινοποίηση πρέπει να περιλαμβάνονται οι εξής πληροφορίες:

- το όνομα και η διεύθυνση του υπεύθυνου επεξεργασίας
- ο σκοπός της επεξεργασίας
- περιγραφή της κατηγορίας ή των κατηγοριών των προσώπων στα οποία αναφέρονται τα δεδομένα
- τους αποδέκτες στους οποίους ενδέχεται να ανακοινωθούν τα δεδομένα
- γενική περιγραφή που επιτρέπει να εκτιμηθεί προκαταρκτικά η σκοπιμότητα των μέτρων που έχουν ληφθεί ώστε να διασφαλίζεται η ασφάλεια της επεξεργασίας (άρθρο 19)

4.4 Η προστασία των δεδομένων προσωπικού χαρακτήρα στην Ελλάδα

4.4.1 Συνταγματικό πλαίσιο προστασίας της ιδιωτικής ζωής

Στην Ελλάδα, η προστασία της ιδιωτικότητας του ατόμου κατοχυρώνεται κατ' αρχάς από μια σειρά συνταγματικών διατάξεων, οι οποίες αποτελούν και τα θεμέλια της νομοθετικής προστασίας. Κατ' αρχήν το άρθρο 2§1 Σ ορίζει ότι «ο σεβασμός και η προστασία της αξίας του ανθρώπου αποτελούν πρωταρχική υποχρέωση της Πολιτείας». Το άρθρο αυτό παρέχει τη γενική συνταγματική προστασία της ανθρώπινης αξίας και εγγυάται την προστασία ειδικών εκδηλώσεων ή αγαθών, τα οποία ανήκουν στην προσωπικότητα του ατόμου και αποτελούν αναπόσπαστο τμήμα της αξίας του. Το δικαίωμα του ιδιωτικού βίου συνιστά πρωταρχική εκδήλωση της προσωπικότητας του ατόμου.

Επίσης το άρθρο 5§1 Σ⁷⁰ ορίζει ότι «Καθένας έχει δικαίωμα να αναπτύσσει ελεύθερα την προσωπικότητά του και να συμμετέχει στην κοινωνική, οικονομική

⁷⁰ Η παράγραφος αυτή προστέθηκε με την αναθεώρηση του συντάγματος το 2001

και πολιτική ζωή της χώρας, εφόσον δεν προσβάλλει τα δικαιώματα των άλλων και δεν παραβιάζει το Σύνταγμα ή τα χρηστά ήθη». Η διάταξη αυτή προστατεύει την ελευθερία του πληροφορείν, η οποία κατοχυρώνεται και απ' το άρθρο 14§1 που ορίζει ότι «Καθένας μπορεί να εκφράζει και να διαδίδει προφορικά, γραπτά και δια του τύπου τους στοχασμούς του, τηρώντας τους νόμους του Κράτους». Απ' την άλλη, το άρθρο 5^Α Σ προστατεύει την ελευθερία του πληροφορείσθαι ορίζοντας ότι «1. Καθένας έχει δικαίωμα στην πληροφόρηση, όπως ο νόμος ορίζει. Περιορισμοί στο δικαίωμα είναι δυνατόν να επιβληθούν με νόμο μόνο εφόσον είναι απολύτως αναγκαίοι και δικαιολογούνται για λόγους εθνικής ασφάλειας, καταπολέμησης του εγκλήματος ή προστασίας δικαιωμάτων και συμφερόντων τρίτων.2 Καθένας έχει δικαίωμα συμμετοχής στην Κοινωνία της Πληροφορίας. Η διευκόλυνση της πρόσβασης στις πληροφορίες που διακινούνται ηλεκτρονικά, καθώς και της παραγωγής, ανταλλαγής και διάδοσής τους αποτελεί υποχρέωση του κράτους».

Το πλέγμα των σχετικών διατάξεων συμπληρώνεται με το άρθρο 9 του Συντάγματος, που κατοχυρώνει με τη σειρά του το απαραβίαστο της ιδιωτικής και οικογενειακής ζωής του ατόμου. Σύμφωνα με το άρθρο 9§1εδ.2 Σ, «η ιδιωτική και οικογενειακή ζωή του ατόμου είναι απαραβίαστη». Η διακήρυξη του απαραβίαστου της ιδιωτικής ζωής του ατόμου σημαίνει ουσιαστικά την απαγόρευση δημοσιοποίησης της ζωής του. Απαγορεύεται δηλαδή κάθε επέμβαση που αποσκοπεί στην παρακολούθηση ή με οποιονδήποτε τρόπο ή μέσο καταγραφή της ιδιωτικής ζωής. Η διάταξη του άρθρου 9§1 Σ συμπληρώνεται απ' την ειδικότερη διάταξη του άρθρου 9^Α, η οποία ορίζει ότι «Καθένας έχει δικαίωμα προστασίας απ' τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, όπως νόμος ορίζει.» Η διάταξη αυτή όπως και η διάταξη του άρθρου 9§1 Σ, περιλαμβάνεται στις διατάξεις που εξειδικεύουν το περιεχόμενο της §1 του άρθρου 5Σ, το οποίο παρέχει γενική προστασία στην προσωπικότητα. Κατοχυρώνει το αμυντικό δικαίωμα προστασίας απέναντι στη συλλογή, επεξεργασία και χρήση με συμβατικό ή ηλεκτρονικό τρόπο, των

προσωπικών δεδομένων. Αυτό όμως δε σημαίνει ότι απαγορεύεται η συλλογή και επεξεργασία στοιχείων προσωπικού χαρακτήρα, ούτε δίνεται στο νομοθέτη η δυνατότητα να καθιερώνει τέτοια απόλυτη απαγόρευση. Αντιθέτως, ο νομοθέτης υποχρεώνεται να διαμορφώσει ένα περιοριστικό θεσμικό πλαίσιο μέσα στο οποίο καθίσταται θεμιτή η επεξεργασία τέτοιων δεδομένων.^{71, 72}

4.4.2 Νομοθετικό πλαίσιο προστασίας προσωπικών δεδομένων

Νόμος 2472/1997 «για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα»

Εισαγωγή

Η ψήφιση νόμου για την προστασία των προσωπικών δεδομένων στην Ελλάδα-η οποία υπήρξε ουραγός στον τομέα αυτό σε σχέση με τις υπόλοιπες ευρωπαϊκές χώρες- καθυστέρησε πολύ. Η σχετική διαδικασία διήρκεσε σχεδόν 14 χρόνια και μόλις το 1997 ψηφίστηκε ο νόμος 2472/97⁷³ για την «προστασία του ατόμου απ' την επεξεργασία δεδομένων προσωπικού χαρακτήρα» που είναι και ο κορμός της προστασίας δεδομένων στη χώρα μας. Αρχικά η Ελλάδα κύρωσε τη Σύμβαση 108/1981 με το νόμο 2068/1992, δεν έθεσε όμως ειδικούς κανόνες για την προστασία των προσωπικών δεδομένων σε εφαρμογή της διεθνούς αυτής ρύθμισης. Τελικώς μετά τη δημοσίευση της κοινοτικής οδηγίας 95/46 ΕΚ, ψηφίστηκε και δημοσιεύθηκε στις 10.4.1997 ο νόμος 2472/97⁷⁴. Ο νόμος αυτός μετά τη θέση σε ισχύ του αναθεωρημένου Συντάγματος του 2001 και τη νέα διάταξη του άρθρου 9^Α, αποτελεί εκτελεστικό του Συντάγματος νόμο, που σημαίνει ότι ενδεχόμενη κατάργηση ή ελάττωση της προστασίας που παρέχεται ήδη απ' το νόμο αυτό, θα αντέβαινε στο άρθρο 2§1 και θα ήταν ανίσχυρη ως αντισυνταγματική. Στη συνέχεια θα παρατεθούν τα βασικά σημεία του νόμου αυτού.⁷⁵

⁷¹ Ιγγλεζάκης Ι., ό.π., σελ.50,56

⁷² Καράκωστας Κ. Ιωάννης, “Δίκαιο και Internet”, σελ.85

⁷³ Νόμος 2472/97, διαθέσιμο στο www.dpa.gr

⁷⁴ ΦΕΚ 50 Α'/10.4.1997

⁷⁵ Ιγγλεζάκης Ι., ό.π., σελ.178

Στο άρθρο 1 του νόμου προσδιορίζεται το αντικείμενό του που είναι η «θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα προς προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής». Κατά τη διατύπωση του άρθρου αυτού αλλά και από τη βούληση του νομοθέτη προκύπτει ότι στόχος είναι η προστασία όχι μόνο της ιδιωτικής ζωής αλλά γενικά της προσωπικότητας, όπως αυτή συγκεκριμενοποιείται από τις επιμέρους διατάξεις του νόμου, απ' τις οποίες προκύπτει η γενική κατ' αρχήν απαγόρευση της επεξεργασίας, οι λόγοι νομιμοποίησής της και η αναγκαιότητα της συγκατάθεσης του υποκειμένου των δεδομένων. Σύμφωνα με το πνεύμα του νόμου λοιπόν, η επεξεργασία των προσωπικών δεδομένων επιτρέπεται μόνο υπό αυστηρές και πολύ συγκεκριμένες προϋποθέσεις. Μάλιστα ο εν λόγω νόμος προσφέρει ευρύτερη προστασία της προσωπικότητας του ατόμου σε σχέση με τις συνταγματικές διατάξεις (άρθρο 9 παρ. 1,2 και 5, άρθρο 19Σ) και τη διάταξη 57 ΑΚ, αφού καλύπτει και τις νέες προσβολές της προσωπικότητας απ' τη δυναμική εισβολή της ηλεκτρονικής τεχνολογίας.

Απ' τις σχετικές διατάξεις του νόμου προβλέπεται η διχοτόμηση των πληροφοριών σε απλά δεδομένα τα οποία θεωρούνται «κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων» (άρθρο 1) και σε ευαίσθητα δεδομένα, τα οποία αφορούν τη φυλετική ή εθνική προέλευση, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις κτλ. Η διχοτόμηση αυτή των πληροφοριών κρίθηκε απαραίτητη, ώστε να επιτευχθεί ο στόχος του νόμου που συνίσταται στην αποτελεσματική προστασία του ατόμου απ' την ανέλεγκτη συλλογή και χρήση προσωπικών δεδομένων κατά τρόπο ρεαλιστικό χωρίς δηλαδή να προκαλέσουν οι φραγμοί που θέτει το νομοθέτημα δυσλειτουργίες στην οικονομική, επαγγελματική και κοινωνική δραστηριότητα. Η υιοθέτηση της διάκρισης αυτής δεν εξασφαλίζει την αποτελεσματική προστασία του ατόμου, αφού στα πλαίσια των δυνατοτήτων της σύγχρονης ηλεκτρονικής επεξεργασίας όλες οι πληροφορίες είναι εν δυνάμει επικίνδυνες, όταν βρεθούν στα χέρια ατόμων που μπορεί να τις χρησιμοποιήσουν με επιβλαβή τρόπο για το άτομο.

Υποκείμενο των δεδομένων θεωρείται το φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί, δηλαδή μπορεί να προσδιορισθεί αμέσως ή εμμέσως με βάση συγκεκριμένα στοιχεία, που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική ή οικονομική (άρθρο 2γ). Η επεξεργασία των δεδομένων προσωπικού χαρακτήρα αναφέρεται σε κάθε εργασία ή σειρά εργασιών που πραγματοποιείται απ' το δημόσιο ή από νομικό πρόσωπο δημοσίου δικαίου ή ιδιωτικού δικαίου ή ένωση προσώπων ή φυσικό πρόσωπο με ή χωρίς τη βοήθεια αυτοματοποιημένων μεθόδων, όπως η συλλογή, καταχώριση, οργάνωση, διατήρηση, αποθήκευση, τροποποίηση, εξαγωγή, χρήση, διαβίβαση, διάδοση ή κάθε άλλης μορφής διάθεση, συσχέτιση ή ο συνδυασμός, η διασύνδεση, η δέσμευση, η διαγραφή, η καταστροφή (άρθρο 2δ). Σύμφωνα με το άρθρο 2^α, ως “δεδομένα προσωπικού χαρακτήρα”, νοείται κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων, εκτός απ' τα στατιστικής φύσεως συγκεντρωτικά στοιχεία απ' τα οποία δεν μπορούν να προσδιορισθούν τα υποκείμενα των δεδομένων. Η εξαίρεση αυτή τίθεται στο νόμο, επειδή ο σκοπός της επεξεργασίας δεδομένων για στατιστικούς σκοπούς δεν μπορεί να υπερβαίνει τα όρια εκείνα που θα οδηγούσαν στον προσδιορισμό της ταυτότητας των υποκειμένων.⁷⁶

Κανόνες και αρχές της επεξεργασίας προσωπικών δεδομένων

Η επεξεργασία των προσωπικών δεδομένων υπόκειται σε συγκεκριμένους κανόνες θεμιτής επεξεργασίας με σκοπό αφενός τη μείωση του κινδύνου προσβολής της προσωπικότητας του υποκειμένου των στοιχείων και αφετέρου στη διασφάλιση της δυνατότητας διαρκούς ελέγχου της επεξεργασίας απ' την πλευρά των υποκειμένων των δεδομένων και του κράτους. Κυρίαρχη αρχή θεωρείται η θεμιτή και νόμιμη συλλογή των δεδομένων και προκειμένου να υποβληθούν τα δεδομένα σε νόμιμη επεξεργασία πρέπει να συλλέγονται με θεμιτό και νόμιμο τρόπο και η επεξεργασία πρέπει να επιδιώκει εκ των προτέρων καθορισμένους σκοπούς, οι οποίοι είναι σαφείς και νόμιμοι (άρθρο 4 παρ.1). Η

⁷⁶ Απόστολος Γέροντας, ό.π., σελ.182-183

συλλογή των δεδομένων αναφέρεται στην προμήθεια πληροφοριών με τη μορφή των ερωτήσεων, υποβολή δικαιολογητικών, ακρόαση. Σε κάθε περίπτωση δε, οι πληροφορίες πρέπει να συλλέγονται μετά από προηγούμενη ενημέρωση ή συγκατάθεση του ενδιαφερομένου (άρθρο 5 παρ.1). Η Αρχή Προσωπικών Δεδομένων στην απόφαση 350-20.1.2000 θεωρεί νόμιμη τη συλλογή δεδομένων για σκοπούς απ' ευθείας διαφήμισης και απ' ευθείας προώθησης πωλήσεων προϊόντων ή υπηρεσιών είτε γίνεται εξ επαγγέλματος είτε όχι με την προϋπόθεση της συγκατάθεσης του υποκειμένου, η οποία είναι απαραίτητη στις περιπτώσεις της έρευνας καταναλωτικής συμπεριφοράς με σκοπό την άμεση ή έμμεση διαφήμιση προϊόντων ή την παροχή υπηρεσιών και στην περίπτωση μη χορήγησης της συγκατάθεσης η επεξεργασία είναι νόμιμη σύμφωνα με το άρθρο 5 παρ.2 εδ. ε, γιατί θεωρείται απολύτως αναγκαία για την ικανοποίηση του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας και το έννομο συμφέρον αυτού υπερέχει προφανώς του συμφέροντος του υποκειμένου, ενόψει του ότι τα συμφέροντα των υποκειμένων των δεδομένων των οποίων επιτρέπεται η επεξεργασία δεν θίγονται ουσιωδώς. Κατά τη διάταξη του άρθρου 11 παρ.1 του νόμου ο υπεύθυνος επεξεργασίας οφείλει, κατά το στάδιο της συλλογής δεδομένων προσωπικού χαρακτήρα, να ενημερώνει με τρόπο πρόσφορο και σαφή το υποκείμενο για την ταυτότητά του, και την ταυτότητα του τυχόν εκπροσώπου του, το σκοπό της επεξεργασίας τους, τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων και την ύπαρξη του δικαιώματος πρόσβασης του ενδιαφερομένου στα συλλεγμένα προσωπικά δεδομένα προκειμένου να είναι σε θέση να ασκήσει τα προβλεπόμενα απ' το νόμο δικαιώματα, όπως της διόρθωσης, της διαγραφής ή της υποβολής αντιρρήσεως.⁷⁷

Οι σκοποί που συνδέονται με τη συλλογή των δεδομένων προσωπικού χαρακτήρα πρέπει να αποτελούν αντικείμενο ειδικού προσδιορισμού το αργότερο τη στιγμή της συλλογής τους, η δε σχετική ρύθμιση προσανατολίζεται στην επεξεργασία των δεδομένων με βάση τους αρχικά καθορισμένους σκοπούς, χωρίς βέβαια να αποκλείεται η διαφοροποίηση των σκοπών, εφόσον συνδέονται

⁷⁷ Δεν πρέπει να θεωρηθεί νόμιμη και θεμιτή η συλλογή δεδομένων απ' τον καταναλωτή με παραπλανητικούς τρόπους ή η χρήση τους για σκοπούς που δεν καλύπτονται απ' τους αρχικούς (δευτερεύουσα χρήση των πληροφοριών)

λογικά με τους αρχικούς σκοπούς, με την προϋπόθεση της έγκαιρης ενημέρωσης του ενδιαφερομένου.

Τα δεδομένα προσωπικού χαρακτήρα πρέπει να συνδέονται άμεσα με τον επιδιωκόμενο σκοπό, να θεωρούνται πρόσφορα για την επιδίωξη του σκοπού και η συλλογή τους να περιορίζεται στα απολύτως απαραίτητα σε σχέση με τον επιδιωκόμενο σκοπό (άρθρο 4 παρ.1) Επομένως δεν συμβιβάζεται με το δικαίωμα της αυτοδιάθεσης των πληροφοριών ούτε η σώρευση πληροφοριών για την αντιμετώπιση μελλοντικών αναγκών, ούτε η συγκέντρωση πληροφοριών που δεν θεωρούνται πρόσφορες για την επίτευξη του ειδικά καθορισμένου σκοπού. Καθιερώνεται έτσι ως θεμελιώδης προϋπόθεση για τη νόμιμη λειτουργία κάθε αρχείου η αρχή του σκοπού της επεξεργασίας και η αρχή της αναγκαιότητας και προσφορότητας των δεδομένων σε σχέση πάντα με το σκοπό της επεξεργασίας. Κάθε επεξεργασία προσωπικών δεδομένων που γίνεται πέραν του επιδιωκόμενου σκοπού ή η οποία δεν είναι πρόσφορη και αναγκαία για την επίτευξή του δεν είναι νόμιμη.

Τα προσωπικά στοιχεία πρέπει να ανταποκρίνονται προς την πραγματικότητα, δηλαδή να είναι επίκαιρα και ακριβή (αρχή ποιότητας) (άρθρο 4 παρ.1) και προκειμένου να μπορούν να αξιοποιηθούν θα πρέπει να υποβάλλονται σε ενημέρωση, πράγμα που προϋποθέτει τη συμμετοχή του ενδιαφερόμενου, ώστε να είναι εφικτή η διόρθωσή τους. Τα δυσμενή με το υποκείμενο προσωπικά δεδομένα που διαβιβάζονται κάθε φορά στον αποδέκτη πρέπει να είναι ακριβή και ενημερωμένα μέχρι το χρόνο της διαβίβασης. Η ακρίβεια και ενημέρωση των στοιχείων αποτελεί βάρος του υπεύθυνου επεξεργασίας και σε καμιά περίπτωση του υποκειμένου, το οποίο σε αντίθετη περίπτωση διατηρεί τα δικαιώματα που προκύπτουν από τις σχετικές διατάξεις του νόμου και τις γενικές διατάξεις για την προστασία της προσωπικότητας.

Τα προσωπικά στοιχεία πρέπει να διατηρούνται σε μορφή που επιτρέπει τον προσδιορισμό της ταυτότητας των υποκειμένων τους μόνο κατά τη διάρκεια της περιόδου που απαιτείται κατά την κρίση της Αρχής, για την πραγματοποίηση των

σκοπών της συλλογής τους και της επεξεργασίας τους.⁷⁸ Όταν π.χ. η καταχώριση των προσωπικών στοιχείων αποσκοπεί στη σύναψη σύμβασης, τότε αυτά διατηρούνται μέχρι την επίτευξη του συγκεκριμένου σκοπού και διαγράφονται μετά την εκπλήρωση της αποστολής τους. Η αρχή της περιορισμένης διατήρησης στο χρόνο των προσωπικών δεδομένων συνδέεται με το δικαίωμα του υποκειμένου να αποφύγει οριστικούς προσδιορισμούς της ταυτότητάς του, πράγμα που θα έπληττε την ικανότητά του για αλλαγή και επαναπροσδιορισμό. Η απεριόριστη χρονικά διατήρηση των δεδομένων συνεπάγεται προφανείς κινδύνους: η πάροδος του χρόνου μπορεί να καταστήσει τα δεδομένα ανακριβή. Επιπλέον, τα ανακριβή δεδομένα συνδεδεμένα με υποκείμενα ή με περιόδους της ζωής του παρωχημένες, κινδυνεύουν να οδηγήσουν σε μια ισόβια «υπενθύμιση» της συμπεριφοράς και στη δημιουργία τεράστιων βάσεων δεδομένων, όπου θα βρίσκονται ανάμικτα, χωρίς συστηματική δομή και για μη καθορισμένους επακριβώς σκοπούς, δεδομένα που αφορούν όλα τα στάδια ζωής του υποκειμένου.⁷⁹

Μετά την πάροδο της περιόδου, η Αρχή μπορεί με αιτιολογημένη απόφαση να επιτρέψει τη διατήρηση δεδομένων προσωπικού χαρακτήρα, εφόσον κρίνονται αναγκαία για την επίτευξη ιστορικών, επιστημονικών ή στατιστικών σκοπών και υπό την προϋπόθεση να καταστούν απρόσωπα, ώστε να διασφαλιστεί η ανωνυμία των συγκεκριμένων προσώπων και εφόσον δεν προσβάλλονται τα δικαιώματα των υποκειμένων τους ή και τρίτων. Με την τήρηση αυτών των διατάξεων επιφορτίζεται ο υπεύθυνος επεξεργασίας, ο οποίος οφείλει στην περίπτωση αυτή να προβεί στην καταστροφή των δεδομένων προσωπικού χαρακτήρα και δεν νομιμοποιείται πλέον να συνεχίσει τη συλλογή και την επεξεργασία τους. Η αρχή της υπευθυνότητας, η οποία συμβάλλει και στη διαφάνεια της συλλογής και επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, συνίσταται στην υποχρέωση του υπεύθυνου επεξεργασίας για τήρηση και εφαρμογή των κανόνων και των αποφάσεων που αναφέρονται στην

⁷⁸ Σύμφωνα με την απόφαση 109-31.3.1999 της Αρχής Προστασίας Προσωπικών Δεδομένων, ο υπεύθυνος επεξεργασίας πρέπει να επεξεργάζεται μια διαβάθμιση των δεδομένων κατά κατηγορίες και ανάλογα με τη βαρύτητά τους, να υπαγάγει κάθε κατηγορία σε διαφορετική διάρκεια διατήρησης στο αρχείο και να γνωστοποιεί τη νέα ρύθμιση στην Αρχή

⁷⁹ Γέροντας Απόστολος, ό.π., σελ.196

προστασία της προσωπικότητας (άρθρο 4 παρ.1δ και παρ.2). Η Αρχή Προστασίας Προσωπικών Δεδομένων, όταν εξακριβώσει αυτεπαγγέλτως ή μετά από σχετική καταγγελία ότι έχουν παραβιασθεί οι σχετικές διατάξεις, επιβάλλει τη διακοπή της συλλογής ή της επεξεργασίας και την καταστροφή τους.

Προϋποθέσεις επεξεργασίας

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα επιτρέπεται μόνο όταν το υποκείμενο των δεδομένων έχει δώσει τη συγκατάθεσή του (άρθρο 5 παρ.1). Συγκατάθεση του υποκειμένου των δεδομένων, είναι κάθε ελεύθερη, ρητή και ειδική δήλωση βούλησης, που εκφράζεται με τρόπο σαφή και με πλήρη επίγνωση και με την οποία, το υποκείμενο των δεδομένων, αφού προηγουμένως ενημερωθεί⁸⁰, δέχεται να αποτελέσουν αντικείμενο επεξεργασίας τα προσωπικά δεδομένα που το αφορούν. Η συγκατάθεση μπορεί να ανακληθεί οποτεδήποτε, χωρίς αναδρομικό αποτέλεσμα.⁸¹ Η διάταξη αναφέρεται μόνο στην επεξεργασία των προσωπικών δεδομένων και δεν φαίνεται να καλύπτει και τη φάση της χρήσης τους, ενώ η απαγόρευση αυτή δεν ισχύει για τη φάση της συλλογής δεδομένων. Η συγκατάθεση του υποκειμένου αναφέρεται στην προηγούμενη συναίνεση του ενδιαφερομένου και αυτή η έννοια ανταποκρίνεται στο άρθρο 236 του Αστικού Κώδικα.

Η επεξεργασία είναι κατ'εξάιρεση επιτρεπτή και χωρίς τη συγκατάθεση του υποκειμένου των δεδομένων όταν:

1. Η επεξεργασία είναι αναγκαία για την εκτέλεση σύμβασης, στην οποία συμβαλλόμενο μέρος είναι υποκείμενο δεδομένων ή για τη λήψη μέτρων κατόπιν αιτήσεως του υποκειμένου κατά το προσυμβατικό στάδιο.

⁸⁰ Στην περίπτωση επεξεργασίας δεδομένων για σκοπούς άμεσης διαφήμισης, με την πρώτη επαφή του αποδέκτη με το υποκείμενο των δεδομένων, ο πρώτος είναι υποχρεωμένος να ενημερώσει το υποκείμενο για την πηγή απ' την οποία άντλησε τα προσωπικά του δεδομένα καθιστώντας σαφές ότι πρόκειται για διαφήμιση ή προώθηση πωλήσεων και να του δίνει τη δυνατότητα εξαίρεσης των προσωπικών του δεδομένων από κάθε περαιτέρω χρήση. Η μη απάντηση του υποκειμένου μετά την πρώτη επαφή δεν θεωρείται συγκατάθεση

⁸¹ Υποστηρίζεται ότι η αρχή της ρητής συγκατάθεσης δημιουργεί προβλήματα στην άμεση διαφήμιση και ότι αρκεί και η σιωπηρή συγκατάθεση, αν έχει προηγηθεί σχετική ενημέρωση του ενδιαφερομένου, Γέροντας Απόστολος, ό.π., σελ.210

2. Η επεξεργασία είναι αναγκαία για την εκπλήρωση υποχρέωσης του υπεύθυνου επεξεργασίας, η οποία επιβάλλεται από το νόμο.

3. Η επεξεργασία είναι αναγκαία για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου, αν αυτό τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του.

4. Η επεξεργασία είναι αναγκαία για την εκτέλεση έργου δημοσίου συμφέροντος ή έργου που εμπίπτει στην άσκηση δημόσιας εξουσίας και εκτελείται από δημόσια αρχή ή έχει ανατεθεί από αυτή είτε στον υπεύθυνο επεξεργασίας είτε σε τρίτο, στον οποίο γνωστοποιούνται τα δεδομένα. Η χρήση ή η επεξεργασία των δεδομένων πρέπει να ανταποκρίνεται στην αναγκαία αξίωση πληροφόρησης των δημόσιων αρχών που είναι απαραίτητη για την αποτελεσματική εκπλήρωση της αποστολής τους.

5. Η επεξεργασία είναι απολύτως αναγκαία για την ικανοποίηση του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας ή ο τρίτος ή οι τρίτοι στους οποίους ανακοινώνονται τα δεδομένα και υπό τον όρο ότι τούτο υπερέχει προφανώς των δικαιωμάτων και συμφερόντων των προσώπων στα οποία αναφέρονται τα δεδομένα και δεν θίγονται οι θεμελιώδεις ελευθερίες αυτών (άρθρο 5 παρ.2)

Η γνωστοποίηση

Ο υπεύθυνος επεξεργασίας υποχρεούται να γνωστοποιεί εγγράφως στην Αρχή τη σύσταση και λειτουργία αρχείου ή την έναρξη της επεξεργασίας (άρθρο 6 παρ.1). Κατά τη διάταξη του άρθρου 2γ της οδηγίας 95/46 ΕΚ ως "αρχείο δεδομένων προσωπικού χαρακτήρα" θεωρείται «κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα προσώπων με γνώμονα συγκεκριμένα κριτήρια, είτε το σύνολο αυτό είναι συγκεντρωμένο είτε αποκεντρωμένο είτε καταμεμημένο σε λειτουργική ή γεωγραφική βάση». Η διάταξη του άρθρου 2ε του νόμου 2472/1997 ορίζει το αρχείο δεδομένων προσωπικού χαρακτήρα ως «το σύνολο προσωπικών δεδομένων, τα οποία αποτελούν ή μπορεί να αποτελέσουν αντικείμενο επεξεργασίας και τα οποία τηρούνται είτε απ' το Δημόσιο ή από νομικό πρόσωπο δημοσίου δικαίου ή ιδιωτικού δικαίου ή ένωση προσώπων ή

φυσικό πρόσωπο». Από τη διαφοροποίηση αυτή όσον αφορά τη διάρθρωση του αρχείου συνάγεται ότι το ρυθμιστικό πεδίο του νόμου καταλαμβάνει κάθε μορφής επεξεργασία, αυτοματοποιημένη ή μη, ανώ κατά την κοινοτική οδηγία αρχεία που δεν είναι διαρθρωμένα σύμφωνα με ειδικά κριτήρια, όπως π.χ. ένας φάκελος ή σύνολο φακέλων δεν υπόκειται σε αυτή.

Σύμφωνα με το άρθρο 6 παρ.2, με τη γνωστοποίηση, ο υπεύθυνος επεξεργασίας πρέπει να δηλώσει απαραίτητα:

A. Το ονοματεπώνυμο ή την επωνυμία ή τον τίτλο του, και τη διεύθυνσή του.

B. Τη διεύθυνση που είναι εγκατεστημένο το αρχείο ή ο κύριος εξοπλισμός που υποστηρίζει την επεξεργασία των προσωπικών δεδομένων

Γ. Την περιγραφή του σκοπού της επεξεργασίας των δεδομένων που περιέχονται ή πρόκειται να περιληφθούν στο αρχείο

Δ. Το είδος των δεδομένων που υφίστανται ή πρόκειται να υποστούν επεξεργασία ή περιέχονται στο αρχείο.

Ε. Το χρονικό διάστημα για το οποίο προτίθεται να εκτελεί την επεξεργασία ή να διατηρήσει τα αρχεία.

Z. Τους αποδέκτες στους οποίους ανακοινώνει τα δεδομένα

H. Τις ενδεχόμενες διαβιβάσεις και το σκοπό της διαβίβασης δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες.

Θ. Τα βασικά χαρακτηριστικά του συστήματος και των μέτρων ασφάλειας του αρχείου ή της επεξεργασίας.

Τα δικαιώματα του υποκειμένου των δεδομένων

Με αφετηρία τη διαπίστωση ότι ο νόμος για την προστασία του ατόμου από την επεξεργασία προσωπικών δεδομένων έχει ως σκοπό την προστασία του δικαιώματος της προσωπικότητας, τότε πρέπει να θεωρηθεί αναγκαία η δυνατότητά του να ελέγχει τα στοιχεία που το αφορούν και τα οποία έχουν συλλεγεί και καταχωρηθεί στον Η/Υ. Η δυνατότητα αυτή εκδηλώνεται με την κατοχύρωση τεσσάρων θεμελιωδών δικαιωμάτων και συγκεκριμένα του δικαιώματος ενημέρωσης, πρόσβασης, αντίρρησης και παροχής προσωρινής

δικαστικής προστασίας, τα οποία αποτελούν μια αναπόσπαστη λειτουργική ενότητα και ρυθμίζονται λεπτομερώς σε ιδιαίτερο κεφάλαιο του νόμου 2472/1997. Τα δικαιώματα αυτά θεσπίζονται τόσο για το συμφέρον του υποκειμένου όσο και για τη διασφάλιση ενός αποτελεσματικού ελέγχου, της διαφάνειας και της νομιμότητας της επεξεργασίας και επομένως εισάγονται και οι αντίστοιχες θεσμικές εγγυήσεις με σκοπό την προάσπισή τους. Παραίτηση απ' τα δικαιώματα που θεσπίζει ο νόμος πρέπει να θεωρηθεί άκυρη, ενώ η άσκησή τους δεν μπορεί να έχει δυσμενείς επιπτώσεις, αφού έτσι θα αναιρούνταν ο σκοπός του νόμου, δηλαδή η άσκηση του δικαιώματος πρόσβασης ή και η προσφυγή στην Αρχή για να παράσχει τη συνδρομή της στην άσκηση των δικαιωμάτων του ατόμου.⁸²

Δικαίωμα ενημέρωσης

Το δικαίωμα της ενημέρωσης του ατόμου που απορρέει απ' το δικαίωμα της αυτοδιάθεσης των πληροφοριών, αποτελεί την προϋπόθεση για την αποτελεσματική άσκηση των άλλων δικαιωμάτων που θεσπίζει ο νόμος, αφού μόνο όταν το άτομο έχει ενημερωθεί υπεύθυνα σχετικά με τις πληροφορίες οι οποίες έχουν αντληθεί και καταχωρηθεί στα αρχεία πληροφοριών, είναι σε θέση να επέμβει διορθωτικά. Κατά τη διάταξη του άρθρου 11 παρ.1, ο υπεύθυνος επεξεργασίας οφείλει να ενημερώνει το υποκείμενο κατά τη διάρκεια συλλογής των δεδομένων. Η ενημέρωση πρέπει να γίνεται με τρόπο πρόσφορο και σαφή, δηλαδή να είναι εύληπτη και κατανοητή για το υποκείμενο των δεδομένων, ενώ στην περίπτωση κατά την οποία το υποκείμενο αδυνατεί να δώσει τη συναίνεσή του, ο υπεύθυνος επεξεργασίας οφείλει να ενημερώσει με τρόπο σαφή και πρόσφορο το νόμιμο αντιπρόσωπο του υποκειμένου.⁸³

Κατά τη διάταξη του άρθρου 11 παρ.1 όταν ο υπεύθυνος επεξεργασίας προβαίνει στη συλλογή των δεδομένων χωρίς τη σύμπραξη του υποκειμένου, οφείλει να ενημερώσει το υποκείμενο για τα εξής στοιχεία:

⁸² Απόστολος Γέροντας, *ό.π.*, σελ.221

⁸³ Τουντόπουλος Β., "Το δικαίωμα ενημέρωσης του υποκειμένου των δεδομένων", ΔΕΕ, 1999, σελ. 576

1. Την ταυτότητά του και την ταυτότητα του τυχόν εκπροσώπου του με προσδιορισμό της επωνυμίας, της έδρας, διεύθυνσης και αριθμού τηλεφώνου. Στο υποκείμενο των δεδομένων πρέπει να γνωστοποιούνται όλα τα στοιχεία που κρίνονται αναγκαία για τη διαπίστωση της ταυτότητας του υπεύθυνου επεξεργασίας, δηλαδή να καθιστούν συγκεκριμένο το πρόσωπο του υπεύθυνου επεξεργασίας, ώστε να αποφεύγονται οι κίνδυνοι σύγχυσης και ελλιπούς ενημέρωσης. Έτσι η αναγραφή π.χ. της ταχυδρομικής θυρίδα, δεν επαρκεί για τη διαπίστωση της ταυτότητας του υπεύθυνου επεξεργασίας και δεν διασφαλίζει τη διαφάνεια της επεξεργασίας.⁸⁴

2. Το σκοπό της επεξεργασίας η αναφορά του οποίου είναι καθοριστική, γιατί αφενός παραχωρεί στο υποκείμενο των δεδομένων τη δυνατότητα να ελέγξει αν και κατά πόσο τα δεδομένα έχουν συλλεγεί για καθορισμένους σκοπούς και αφετέρου διασφαλίζεται η αρχή της προσφορότητας των δεδομένων.

3. Τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων με προσδιορισμό της επωνυμίας, διεύθυνσης και αριθμού τηλεφώνου. Η ενδεικτική ανακοίνωση κατηγοριών αποδεκτών δεν είναι αποδεκτή, αλλά ενόψει της διαβίβασης των δεδομένων σε τρίτους, η ανακοίνωση πρέπει να είναι ειδική και συγκεκριμένη.

4. Την ύπαρξη του δικαιώματος πρόσβασης, αφού η άσκησή του προϋποθέτει την ενημέρωση και επομένως τη γνώση του.

Αν και ο τίτλος του σχετικού άρθρου αναφέρεται στο δικαίωμα της ενημέρωσης, απ' το περιεχόμενο προκύπτει ότι πρόκειται για υποχρέωση του υπεύθυνου επεξεργασίας. Δεν πρόκειται για παραχώρηση δικαιώματος προς το υποκείμενο των δεδομένων, με σκοπό να επιλέξει αυτό αν προβεί στην άσκησή του, αλλά για κατοχύρωση αξίωσης του υποκειμένου για συμμετοχή στη διεργασία της επεξεργασίας των δεδομένων που το αφορούν. Η δέσμευση του υπεύθυνου επεξεργασίας είναι διαρκής και σταθερή, τουλάχιστον όσον αφορά τα στοιχεία που αναφέρει η σχετική διάταξη.

⁸⁴ Στην περίπτωση των συνδεδεμένων εταιριών, η ανακοίνωση πρέπει να περιλαμβάνει το σύνολο των επιχειρήσεων, εφόσον οι εταιρίες τηρούν ενιαία αρχεία και αν οι επιχειρήσεις τηρούν αυτοτελή αρχεία, δεν κρίνεται απαραίτητη η αναγραφή των άλλων εταιριών του ομίλου

Ο ενδιαφερόμενος πρέπει να ενημερώνεται πριν από την έναρξη της επεξεργασίας, έτσι ώστε να είναι σε θέση να ασκήσει αποτελεσματικά τα δικαιώματά του, χωρίς αυτό να σημαίνει ότι αίρεται στη συνέχεια η υποχρέωση ενημέρωσης, αλλά για οποιαδήποτε μεταβολή των δεδομένων, ο υπεύθυνος επεξεργασίας υποχρεούται να προβαίνει στην ενημέρωση, γιατί διαφορετικά στερείται ο ενδιαφερόμενος του δικαιώματος άσκησης του δικαιώματος αντίρρησης.

Κατά την κανονιστική πράξη 1/1999 της Αρχής, όταν τα δεδομένα συλλέγονται απ' ευθείας απ' το υποκείμενο, η ενημέρωση γίνεται ταυτόχρονα με τη συλλογή. Όταν συλλέγονται από άλλες πηγές, η ενημέρωση γίνεται αμελλητί και πάντως πριν από οποιαδήποτε περαιτέρω χρησιμοποίηση ή επεξεργασία των δεδομένων μετά την καταχώριση. Σε περίπτωση επιγενόμενης μεταβολής των στοιχείων της παρ.1 του άρθρου 11, η ενημέρωση του υποκειμένου για τη μεταβολή γίνεται αμελλητί και πάντως πριν από οποιαδήποτε περαιτέρω επεξεργασία των δεδομένων. Επίσης σύμφωνα με την κανονιστική πράξη, όταν το υποκείμενο παρέχει τη συγκατάθεση ή τη συνδρομή του η ενημέρωση γίνεται εγγράφως. Προς τούτο, ο υπεύθυνος επεξεργασίας χρησιμοποιεί διπλότυπο έντυπο, το ένα αντίτυπο του οποίου υπογράφεται απ' το υποκείμενο, παραδίδεται στον υπορύθνο επεξεργασίας και διατηρείται απ' αυτόν καθ'όλη τη διάρκεια της επεξεργασίας. Η Αρχή μπορεί να απαλλάσσει εν όλω ή εν μέρει τον υπεύθυνο της επεξεργασίας απ' την υποχρέωσή του να ενημερώνει το υποκείμενο, εαν η καταχώριση, ο σκοπός της επεξεργασίας, οι αποδέκτες και το δικαίωμα πρόσβασης, αποτελούν κοινή γνώση του επιμελούς πολίτη.⁸⁵

Η ενημέρωση γίνεται με τη δημοσίευση σε δύο εφημερίδες της Πρωτεύουσας και μια της έδρας του υπεύθυνου επεξεργασίας. Όταν για τη συλλογή και επεξεργασία δεδομένων, δεν απαιτείται, ούτε ζητείται η συγκατάθεση του υποκειμένου, η ενημέρωσή του γίνεται με τον πιο πρόσφορο

⁸⁵ Κανονιστική πράξη 1/99 για την ενημέρωση υποκειμένου των δεδομένων κατ'άρθρο 11 Ν. 2472/1997, διαθέσιμη στο www.dpa.gr

τρόπο, ώστε να εξασφαλίζεται η όσο το δυνατόν απρόσκοπτη και επαρκής πληροφόρηση του υποκειμένου. Ενδεικτικά, η ενημέρωση μπορεί να γίνει:

- A) με ανάρτηση ευδιάκριτης προειδοποιητικής πινακίδας στο χώρο συναλλαγής
- B) με διάθεση έντυπου υλικού
- Γ) με αναγραφή σε λογαριασμούς, τιμολόγια ή άλλα περιστατικά, εφόσον προϋπάρχει συναλλακτική σχέση
- Δ) με ευδιάκριτη επισημείωση στο ερωτηματολόγιο, έντυπο αιτήσεως, δελτίο παροχής πληροφοριών κτλ, εφόσον το υποκείμενο καλείται να το συμπληρώσει
- E) με ειδική, σαφή και ευδιάκριτη επισήμανση στην αρχική σελίδα της ιστοσελίδας εφόσον η συλλογή γίνεται μέσω διαδικτύου

Το δικαίωμα πρόσβασης

Η διάταξη του άρθρου 12 του νόμου παραχωρεί στον πολίτη το δικαίωμα πρόσβασης στα αρχεία και συγκεκριμένα να γνωρίζει αν προσωπικά δεδομένα που τον αφορούν αποτελούν ή αποτέλεσαν αντικείμενο επεξεργασίας και να πληροφορείται για ορισμένα βασικά στοιχεία της επεξεργασίας και υποχρεώνει τον υπεύθυνο επεξεργασίας να απαντήσει εγγράφως (δικαίωμα πληροφόρησης) (άρθρο 12 παρ.1). Η πρώτη αρχή που ενέπνευσε τη σύνταξη αυτού του άρθρου υπήρξε η αρχή της διαφάνειας, σύμφωνα με την οποία ο ενδιαφερόμενος έχει τη δυνατότητα να λαμβάνει γνώση ως προς τη συλλογή, την καταχώριση, τη χρήση και τη γνωστοποίηση σε τρίτους, πληροφοριών που τον αφορούν. Αλλά η αρχή αυτή θα ήταν ατελέσφορη, χωρίς τη δυνατότητα για τον ενδιαφερόμενο να έχει, χωρίς υπερβολική προσπάθεια και υπέρογκα έξοδα, πρόσβαση στα αρχεία, χωρίς τη δυνατότητα να επεμβαίνει για τη διόρθωση, τη συμπλήρωση, την τροποποίηση, τη διευκρίνιση και τη διαγραφή των πληροφοριών. Ειδικότερα σύμφωνα με το άρθρο 12 παρ.2, το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητεί και να λαμβάνει από τον υπεύθυνο επεξεργασίας και χωρίς καθυστέρηση τις ακόλουθες πληροφορίες⁸⁶:

⁸⁶ Απόστολος Γέροντας, ό.π., σελ.230

- i. τα δεδομένα προσωπικού χαρακτήρα που το αφορούν και την προέλευσή τους
- ii. τους σκοπούς της επεξεργασίας και τους αποδέκτες
- iii. την εξέλιξη της επεξεργασίας για το χρονικό διάστημα από την προηγούμενη ενημέρωσή του
- iv. τη λογική στην οποία στηρίζεται κάθε αυτοματοποιημένη επεξεργασία δεδομένων

Κατά το άρθρο 12 παρ.3, το υποκείμενο των δεδομένων ασκεί το δικαίωμα πρόσβασης με την υποβολή σχετικής αίτησης στον υπεύθυνο επεξεργασίας και την ταυτόχρονη καταβολή χρηματικού ποσού, το ύψος του οποίου, ο τρόπος καταβολής και κάθε άλλο συναφές θέμα ρυθμίζεται με απόφαση της Αρχής. Αν το αίτημα για διόρθωση ή διαγραφή των δεδομένων κριθεί βάσιμο, επιστρέφεται στον αιτούντα το ποσό απ'τον υπεύθυνο επεξεργασίας, ο οποίος υποχρεούται να χορηγήσει στον ενδιαφερόμενο, δωρεάν και σε γλώσσα κατανοητή, αντίγραφο του διορθωμένου μέρους της επεξεργασίας.

Το δικαίωμα αντίρρησης

Με τη διάταξη του άρθρου 13 ρυθμίζεται το δικαίωμα αντίρρησης του υποκειμένου για την επεξεργασία δεδομένων που το αφορούν. Ο ενδιαφερόμενος μπορεί να ζητήσει οποτεδήποτε, απ' τον υπεύθυνο επεξεργασίας, να προβεί σε συγκεκριμένη ενέργεια σχετικά με την επεξεργασία προσωπικών δεδομένων που τον αφορούν. Το δικαίωμα αυτό μπορεί να ασκηθεί τόσο κατά τη διάρκεια της συλλογής δεδομένων, που συνεπάγεται την άρνηση της χορήγησης συγκατάθεσης για την επεξεργασία τους, όσο και μετά την άντλησή τους. Σύμφωνα με το άρθρο 13 παρ.1, οι αντιρρήσεις απευθύνονται εγγράφως στον υπεύθυνο επεξεργασίας και πρέπει να αναφέρονται στην επεξεργασία των δεδομένων και να επιδιώκουν συγκεκριμένη ενέργεια, όπως τη διόρθωση, συμπλήρωση, προσωρινή μη χρήση, δέσμευση, μη διαβίβαση ή διαγραφή στοιχείων που το αφορούν. Το αίτημα του υποκειμένου μπορεί να αναφέρεται και στην καταστροφή, μη συσχέτιση των δεδομένων ή μη διασύνδεση

των αρχείων με δεδομένα που το αφορούν. Η επιλογή του αιτήματος εναπόκειται στη διακριτική ευχέρεια του υποκειμένου και πρέπει να εναρμονίζεται με την αρχή της αναλογικότητας, δηλαδή η υποβολή των αντιρρήσεων πρέπει να κρίνεται εύλογη, ώστε να αποφεύγεται ο κίνδυνος της υπερβολικής επιβάρυνσης του υπεύθυνου επεξεργασίας.

Στην περίπτωση της ανακρίβειας των δεδομένων αναγνωρίζεται στο υποκείμενο το δικαίωμα διόρθωσης, δηλαδή όταν τα δεδομένα δεν ανταποκρίνονται στην πραγματικότητα ή δημιουργούν μια εσφαλμένη εντύπωση για τους τρίτους όσον αφορά το υποκείμενο, ανεξάρτητα απ' το αν η ανακρίβεια οφείλεται στο ίδιο το υποκείμενο ή χαρακτηρίζεται ως επουσιώδης, ο υπεύθυνος επεξεργασίας έχει την υποχρέωση να προβεί στη διόρθωση των ανακριβών δεδομένων και κατά τη διάταξη του άρθρου 4 παρ.2 στην καταστροφή των δεδομένων, που έχουν συλλεγεί ή υπόκεινται σε επεξεργασία κατά παράβαση της αρχής ακρίβειας.

Το υποκείμενο των δεδομένων διαθέτει επίσης το δικαίωμα να ζητήσει την προσωρινή μη χρησιμοποίηση, τη δέσμευση ή τη μη διαβίβαση των δεδομένων ή τη διαγραφή τους και το σχετικό αίτημα πρέπει να τελεί σε σχέση αναλογικότητας με τα θιγόμενα έννομα συμφέροντα του υποκειμένου και ειδικότερα όταν τα συμφέροντά του μπορούν να ικανοποιηθούν με τη διόρθωση, δεν μπορεί να γίνει αποδεκτό το αίτημά του για δέσμευση ή για διαγραφή, η οποία ως το αποτελεσματικότερο μέτρο για την προστασία των δικαιωμάτων του υποκειμένου, συνίσταται στην οριστική καταστροφή μέρους ή του συνόλου των δεδομένων.

Κατά τη διάταξη του άρθρου 13 παρ.3 του νόμου, κατοχυρώνεται ένα ειδικότερο δικαίωμα αντίρρησης, το οποίο συνίσταται στη δυνατότητα του ατόμου να δηλώσει στην Αρχή ότι δεν επιθυμεί την επεξεργασία δεδομένων που τον αφορούν, όταν ο υπεύθυνος επεξεργασίας προτίθεται να τα χρησιμοποιήσει για την προώθηση πώλησης προϊόντων ή παροχής υπηρεσιών εξ αποστάσεως. Η Αρχή καταγράφει τα στοιχεία της ταυτότητας των ατόμων αυτών σ'ένα μητρώο,

το οποίο οι υπεύθυνοι επεξεργασίας οφείλουν να συμβουλευονται πριν από κάθε επεξεργασία και να διαγράφουν απ' το αρχείο τους τα πρόσωπα που συμπεριλαμβάνονται στο μητρώο αυτό. Πρόκειται για τις γνωστές Robinson Lists.

Το δικαίωμα προσωρινής διοικητικής και δικαστικής προστασίας

Κατά την παράγραφο 7^α, που προστέθηκε με το νόμο 2951/2001, όταν η προστασία του ατόμου από την επεξεργασία προσωπικών δεδομένων επιβάλλει την άμεση λήψη απόφασης, ο Πρόεδρος μπορεί, ύστερα από αίτηση του ενδιαφερόμενου να εκδίδει προσωρινή διαταγή για άμεση ολική ή μερική, αναστολή της επεξεργασίας ή λειτουργίας αρχείου.

Το υποκείμενο των προσωπικών δεδομένων έχει το δικαίωμα να προσφύγει στο αρμόδιο δικαστήριο και να ζητήσει την άμεση αναστολή ή μη εφαρμογή πράξης ή απόφασης που τον θίγει, η οποία έχει ληφθεί από διοικητική αρχή ή νομικό πρόσωπο δημοσίου ή ιδιωτικού δικαίου ή ένωση προσώπων ή φυσικό πρόσωπο και αποκλειστικά με αυτοματοποιημένη επεξεργασία στοιχείων, εφόσον η επεξεργασία αυτή αποβλέπει στην αξιολόγηση της προσωπικότητάς του και ιδίως της οικονομικής φερεγγυότητάς του, της αξιοπιστίας του και της εν γένει συμπεριφοράς του.⁸⁷

Αρχή Προστασίας Προσωπικών Δεδομένων

Με το νόμο 2472/97 προβλέπεται η σύσταση της Αρχής Προστασίας και κεντρικό όργανο για τον έλεγχο της εφαρμογής του νόμου και την προστασία απ' την επεξεργασία προσωπικών δεδομένων και συγκεκριμένα τα άρθρα 15 επ. του νόμου αναφέρονται στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και ειδικότερα στη σύσταση, αποστολή και νομική της φύση(άρθρο 15), τη συγκρότηση(άρθρο 16), τα κωλύματα και ασυμβίβαστα των μελών της(άρθρο 17) τις υποχρεώσεις και τα δικαιώματα αυτών(άρθρο 18), τις αρμοδιότητες, τη

⁸⁷ Απόστολος Γέροντας, ό.π., σελ.234

λειτουργία και τις αποφάσεις της Αρχής(άρθρο 19) και τέλος τη Γραμματεία αυτής(άρθρο 20). Παρακάτω θα γίνει αναλυτικότερη αναφορά στην Αρχή αυτή.

Νόμος 2251/1994

Εκτός απ' το νόμο 2472/97 που είναι ο κορμός προστασίας των προσωπικών δεδομένων στην Ελλάδα, υπάρχει και ο νόμος 2251/1994 για την Προστασία του Καταναλωτή, ο οποίος στο άρθρο 9§10-13 ορίζει τις προϋποθέσεις που πρέπει να πληρεί η επιχείρηση για την επεξεργασία προσωπικών στοιχείων του καταναλωτή για σκοπούς άμεσης διαφήμισης⁸⁸. Σύμφωνα με το άρθρο αυτό, απαιτείται η ρητή συναίνεση του καταναλωτή για τη λήψη διαφημιστικού μηνύματος μέσω τηλεφώνου, φαξ, ηλεκτρονικού ταχυδρομείου ή άλλου ηλεκτρονικού μέσου επικοινωνίας. Τα προσωπικά στοιχεία θα πρέπει να έχουν περιέλθει στη γνώση της επιχείρησης α) είτε από προηγούμενες συναλλακτικές σχέσεις με το συγκεκριμένο καταναλωτή β) είτε από άλλες πηγές που είναι όμως προσιτές στον καθένα (π.χ. τηλεφωνικό κατάλογο ή γενικώς δημοσιευμένα στοιχεία όπως αυτά που δημοσιεύονται στον τύπο γ) είτε από κάποιο τρίτο πρόσωπο, μόνο όμως υπό την προϋπόθεση ότι ο καταναλωτής εγκρίνει ρητά τη μεταβίβαση των προσωπικών στοιχείων του για το συγκεκριμένο σκοπό της διαφήμισης. Επίσης ο διαφημιστής οφείλει να αναφέρει στον καταναλωτή με ποιο τρόπο έλαβε γνώση των στοιχείων του.⁸⁹

Πάντως, σε περίπτωση που ο καταναλωτής ζητήσει τη διακοπή της άμεσης διαφήμισης, η επιχείρηση οφείλει να τη διακόψει αμέσως, διαγράφοντας συγχρόνως τα προσωπικά στοιχεία του καταναλωτή απ' το αρχείο της. Τέλος, αναφέρεται ότι η άμεση διαφήμιση θα πρέπει να γίνεται με τέτοιο τρόπο ώστε να μην προσβάλλεται η ιδιωτική ζωή του καταναλωτή.⁹⁰

⁸⁸ Ο νόμος 2251/1994 που ψηφίσθηκε απ την Ελληνική Βουλή το Νοέμβριο του 1994. υπήρξε ιδιαίτερα πρωτοποριακός σε σχέση με τον προγενέστερό του (Ν 1961/91), καθώς παρέχει πιο αποτελεσματική προστασία για τους καταναλωτές, αφού δίνει πλέον στους ίδιους τη δυνατότητα να προασπίζονται τα συμφέροντά τους, μέσω οργανώσεων καταναλωτών. Ο νόμος αυτός διευκολύνει την ίδρυση οργανώσεων καταναλωτών και διευρύνει τις αρμοδιότητές τους μέσω κυρίως της γενίκευσης της «συλλογικής αγωγής». Κορνηλία Δελοούκα-Ιγγλέση, «Έλληνικό και κοινοτικό δίκαιο του καταναλωτή», σελ. 49-50

⁸⁹ Αλεξανδρίδου Δ. Ελίζα, «Δίκαιο προστασίας του καταναλωτή», σελ. 71

⁹⁰ Κορνηλία Δελοούκα-Ιγγλέση,ό.π., σελ.170-171

ΚΕΦΑΛΑΙΟ 5

Ευαίσθητα προσωπικά δεδομένα

5.1 Εισαγωγή

Μέχρι τώρα εξετάσαμε τη συλλογή και επεξεργασία απ' τις επιχειρήσεις των απλών προσωπικών δεδομένων των καταναλωτών όπως π.χ. πληροφορίες για το όνομα, την επαγγελματική και οικονομική κατάσταση του ατόμου, την ηλικία του κτλ, καθώς και το νομοθετικό πλαίσιο, τόσο το ευρωπαϊκό όσο και το ελληνικό, που διέπει την επεξεργασία των δεδομένων αυτών. Ωστόσο υπάρχει και μια άλλη κατηγορία προσωπικών δεδομένων, τα οποία λόγω των αυξημένων κινδύνων που εγκυμονεί η επεξεργασία τους στην ιδιωτική ζωή του ατόμου, πρέπει να χρήζουν ιδιαίτερης προστασίας. Σύμφωνα με το άρθρο 2β του νόμου 2472/97, τα δεδομένα αυτά χαρακτηρίζονται ως "ευαίσθητα", και αφορούν τη φυλετική προέλευση (συμπεριλαμβανομένων πληροφοριών για το χρώμα του δέρματος), τις πολιτικές, θρησκευτικές, φιλοσοφικές ή ηθικές πεποιθήσεις (συμπεριλαμβανομένης της απουσίας οποιασδήποτε θρησκευτικής πίστης), την εθνική προέλευση, τη συμμετοχή σε συνδικαλιστική οργάνωση και πληροφορίες που αφορούν την υγεία και την ερωτική ζωή του ατόμου.

Τα "ευαίσθητα προσωπικά δεδομένα" απαιτούν αυξημένη προστασία σε σχέση με τα απλά, διότι λόγω του περιεχομένου τους, η αποκάλυψη των πληροφοριών αυτών μπορεί να έχει εξαιρετικά δυσχερείς συνέπειες για το άτομο και ιδίως την απομόνωση και τον κοινωνικό αποκλεισμό του. Επίσης δύναται να εκδηλωθούν αυθαίρετες διακρίσεις λόγω της φυλετικής ή εθνικής καταγωγής, των πολιτικών φρονημάτων του κτλ. Μάλιστα συχνά, η επεξεργασία ευαίσθητων προσωπικών στοιχείων λαμβάνει χώρα χωρίς να έχει δοθεί η συγκατάθεση του υποκειμένου ή και χωρίς να λαμβάνονται επαρκή μέτρα για τη διασφάλιση της προστασίας της ιδιωτικής ζωής του ατόμου. Ενδεικτικά είναι εδώ, τα στοιχεία που αφορούν την επεξεργασία δεδομένων στο περιβάλλον του διαδικτύου π.χ. στην πολιτεία του Michigan των ΗΠΑ. Πληροφορίες σχετικά με την υγεία που περιελάμβαναν ονόματα, αριθμούς κοινωνικής πρόνοιας και κωδικούς διάγνωσης χιλιάδων ασθενών, διατέθηκαν σε απευθείας σύνδεση μέσω του διαδικτύου απ'

το Σύστημα Υγείας του Πανεπιστημίου του Michigan και παρέμειναν διαθέσιμα επί δύο μήνες. Επίσης συχνά, νοσοκομεία συλλέγουν πληροφορίες που αφορούν την υγεία των ασθενών και τα επεξεργάζονται με σκοπό εν συνεχεία την προώθηση ιατρικών προϊόντων στα άτομα αυτά.^{91, 92}

Η συγκέντρωση ευαίσθητων πληροφοριών, ιδίως στον ιατρικό τομέα, γίνεται συχνά με τη βοήθεια των “έξυπνων καρτών”, στις οποίες αποθηκεύεται ένας μεγάλος αριθμός ιατρικών πληροφοριών για τον εκάστοτε κάτοχό τους. Το ζήτημα είναι ότι ο έλεγχος της επεξεργασίας των καταχωρημένων σε αυτές πληροφοριών είναι εξαιρετικά δυσχερής έως αδύνατος, γιατί το υποκείμενο των δεδομένων δεν είναι σε θέση να γνωρίζει ποιες πληροφορίες είναι καταχωρημένες στις κάρτες αυτές και ποιοι έχουν τη δυνατότητα καταχώρισης και πρόσβασης σ’ αυτές.

5.2 Νομοθετική προστασία ευαίσθητων προσωπικών δεδομένων

5.2.1 Απόφαση υπ’ αριθμόν (73)22 του 1973 του Συμβουλίου της Ευρώπης

Σε διεθνές επίπεδο, το πρώτο νομικό κείμενο που μνημονεύει την ανάγκη καθιέρωσης ειδικής ρύθμισης για τα ευαίσθητα προσωπικά δεδομένα είναι η απόφαση υπ’ αριθμόν (73)22 της 26^{ης} Σεπτεμβρίου 1973 του Συμβουλίου της Ευρώπης , που αφορά την προστασία δεδομένων στον ιδιωτικό τομέα. Στην απόφαση αυτή, περιέχεται σύσταση στα κράτη μέλη της Ευρωπαϊκής Ένωσης, να απαγορεύουν την αυτοματοποιημένη επεξεργασία πληροφοριών, η οποία αφορά την αυστηρά προσωπική σφαίρα της ιδιωτικής ζωής των ατόμων, καθώς και των πληροφοριών εκείνων που μπορεί να αποτελέσουν τη βάση για την καθιέρωση δακρίσεων.

5.2.2 Σύμβαση αρ. 108 του 1981

Στο ίδιο πνεύμα, αλλά με σαφέστερες ρυθμίσεις, κινήθηκε και η Σύμβαση αρ. 108 της 28.1.1981 του Συμβουλίου της Ευρώπης. Στο άρθρο 6 παραθέτει έναν

⁹¹ Ιγγλεζάκης Ι., ό.π., σελ. 15-16

⁹² James Cornell, “ Personal and sensitive information”?. www.crimereduction.gov.uk

κατάλογο των κατηγοριών δεδομένων, τα οποία επιτρέπεται να τύχουν επεξεργασίας, υπό την προϋπόθεση ότι η νομοθεσία των κρατών προβλέπει εγγυήσεις και τα οποία θεωρούνται ως ευαίσθητα ή ιδιαίτερος εμπιστευτικά στα κράτη μέλη του Συμβουλίου της Ευρώπης. Σε αυτά συμπεριλαμβάνονται οι πληροφορίες προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική προέλευση, τα πολιτικά φρονήματα, τις θρησκευτικές ή άλλες πεποιθήσεις όπως και αυτές που αφορούν την υγεία ή τη σεξουαλική ζωή. Η απαρίθμηση των παραπάνω κατηγοριών δεδομένων είναι ενδεικτική και συνεπώς ο κοινός νομοθέτης μπορεί να συμπεριλάβει και άλλα είδη δεδομένων στη σχετική ρύθμιση ενώ μπορεί να γίνει και η διαβάθμιση των προσωπικών δεδομένων ανάλογα με το βαθμό ευαισθησίας τους.

Η διάταξη του άρθρου 6 έχει όμως περιορισμένο πεδίο εφαρμογής, καθόσον εφαρμόζεται μόνο στην αυτοματοποιημένη επεξεργασία δεδομένων και όχι στη δια χειρός επεξεργασία. Ακόμα, σύμφωνα με την εν λόγω διάταξη, η επεξεργασία ειδικών κατηγοριών δεδομένων δεν απαγορεύεται εντελώς, αλλά τίθεται υπό την προϋπόθεση της θέσπισης ιδιαίτερων εγγυήσεων. Συνεπώς, τα συμβαλλόμενα κράτη έχουν τη δυνατότητα να θεσπίσουν ρυθμίσεις, οι οποίες είναι δυνατόν να διαφοροποιούνται σε μεγάλο βαθμό. Παρέκκλιση απ' την παραπάνω ρύθμιση επιτρέπεται σύμφωνα με το άρθρο 9 της Σύμβασης για: α) την προστασία της ασφάλειας του κράτους, τη δημόσια ασφάλεια, τα νομισματικά συμφέροντα του κράτους ή την καταστολή ποινικών παραβάσεων β) την προστασία του προσώπου το οποίο αφορούν οι πληροφορίες.

Πάντως η ρύθμιση της παραπάνω Σύμβασης είναι ιδιαίτερα σημαντική, καθώς συντέλεσε στο να αναγνωρίσουν τα κράτη στην εθνική τους νομοθεσία, τη διάκριση ανάμεσα σε απλά και ευαίσθητα προσωπικά δεδομένα και εδραίωσε την πεποίθηση για την αναγκαιότητα θέσπισης ιδιαίτερων προστατευτικών ρυθμίσεων για τα ευαίσθητα προσωπικά δεδομένα. Τα εθνικά νομοθετήματα που ακολούθησαν μετά την ψήφιση της Σύμβασης, συμπεριέλαβαν στην πλειοψηφία

τους ρητές διατάξεις για την επεξεργασία ευαίσθητων προσωπικών δεδομένων, όπως π.χ. ο ισλανδικός νόμος, ο φιλανδικός, ο βρετανικός και άλλοι.⁹³

5.2.3 Οδηγία 95/46 ΕΚ “για την προστασία των φυσικών προσώπων έναντι επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών”

Σχετική ρύθμιση για την προστασία των ευαίσθητων προσωπικών δεδομένων περιλαμβάνεται και στην κοινοτική Οδηγία 95/46 ΕΚ. Η Οδηγία, σε αντίθεση με τη Σύμβαση υπ’ αριθμόν 108, προβλέπει κατά κανόνα την απαγόρευση της επεξεργασίας δεδομένων προσωπικού χαρακτήρα που παρέχουν πληροφορίες για τη φυλετική ή εθνική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, τη συμμετοχή σε συνδικαλιστικές οργανώσεις, την υγεία και τη σεξουαλική ζωή (άρθρο 8§1). Η Οδηγία δεν περιορίζεται δηλαδή στο να αξιώνει απλώς την ύπαρξη κατάλληλων εγγυήσεων όπως η Σύμβαση 108/1981, αλλά απαγορεύει τη συλλογή και επεξεργασία ευαίσθητων δεδομένων. Πριν την ψήφιση της κοινοτικής Οδηγίας, υπήρχαν σημαντικές διαφοροποιήσεις στις εθνικές νομοθεσίες των κρατών ως προς τις κατηγορίες προσωπικών δεδομένων που θεωρούνταν ως ευαίσθητες. Π.χ. οι νομοθεσίες της Νορβηγίας και της Δανίας θεωρούσαν τις πληροφορίες που αφορούσαν τη σεξουαλική ζωή του ατόμου ως «ευαίσθητες», ενώ ο γαλλικός νόμος όχι. Ωστόσο, το άρθρο 8§1 της Οδηγίας παραθέτει αναλυτικά τις κατηγορίες των ευαίσθητων προσωπικών δεδομένων, προκειμένου να επιτευχθεί συναίνεση μεταξύ των κρατών μελών, λόγω της εναρμόνισης των εθνικών νομοθεσιών με τις διατάξεις της Οδηγίας. Το άρθρο 8§2 της Οδηγίας ορίζει ότι η επεξεργασία ευαίσθητων προσωπικών στοιχείων επιτρέπεται κατ’ εξαίρεση όταν:

A) το πρόσωπο στο οποίο αναφέρονται τα δεδομένα έχει δώσει ρητά τη συγκατάθεσή του

B) η επεξεργασία είναι απαραίτητη για τη διασφάλιση ζωτικού συμφέροντος του υποκειμένου, υπό την προϋπόθεση ότι αυτό αδυνατεί να δώσει τη συγκατάθεσή του

⁹³ Ιγγλεζάκης Ι.,ό.π., σελ.89

Γ) η επεξεργασία αφορά δεδομένα τα οποία δημοσιοποιούνται απ' το πρόσωπο στο οποίο αναφέρονται

5.2.4 Ο ελληνικός νόμος 2472/1997

Ο νόμος 2472/97, που προσαρμόζει την κοινοτική Οδηγία 95/46 ΕΚ στην ελληνική έννομη τάξη, στο άρθρο 7§1, απαγορεύει τη συλλογή και επεξεργασία ευαίσθητων προσωπικών δεδομένων απ' τις επιχειρήσεις. Κατ'εξαιρέση επιτρέπεται η παραπάνω διαδικασία και η ίδρυση σχετικού αρχείου, τηρουμένων κάποιων προϋποθέσεων και πάντοτε ύστερα από άδεια της Αρχής Προστασίας Προσωπικών Δεδομένων, για την οποία θα γίνει λόγος αμέσως παρακάτω. Η άδεια αυτή χορηγείται για ορισμένο χρονικό διάστημα και ύστερα από ακρόαση του υπεύθυνου επεξεργασίας. Η άδεια περιέχει τα εξής στοιχεία:

- το ονοματεπώνυμο και τη διεύθυνση του υπευθύνου επεξεργασίας
- τη διεύθυνση όπου είναι εγκατεστημένο το αρχείο
- το είδος των δεδομένων προσωπικού χαρακτήρα
- το χρονικό διάστημα χορήγησης της άδειας
- τους όρους και τις προϋποθέσεις που έχει επιβάλλει η Αρχή για την ίδρυση του αρχείου

ΚΕΦΑΛΑΙΟ 6

Αρχή προστασίας προσωπικών δεδομένων

6.1 Βασικές δραστηριότητες της Αρχής

Ο νόμος 2472/97 στο άρθρο 15 ορίζει τη σύσταση ανεξάρτητης δημόσιας αρχής με αποστολή την εποπτεία εφαρμογής του παρόντος νόμου και άλλων ρυθμίσεων που αφορούν την προστασία του ατόμου απ' την επεξεργασία δεδομένων προσωπικού χαρακτήρα και ονομάζεται "Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα". Οι βασικές δραστηριότητες της Αρχής είναι οι εξής:

Α) Διενέργεια διοικητικών ελέγχων

Η δραστηριότητα αυτή που προβλέπεται απ' το άρθρο 19§1 του νόμου 2472/97, αποσκοπεί στην εξακρίβωση της τήρησης της νομιμότητας κατά τη συλλογή και επεξεργασία προσωπικών δεδομένων απ' τους υπεύθυνους επεξεργασίας. Οι έλεγχοι διενεργούνται από ελεγκτές είτε αυτεπάγγελτα είτε ύστερα από καταγγελία, αφορούν αρχεία του δημόσιου και ιδιωτικού τομέα και εκτείνονται τόσο στη νομιμότητα της λειτουργίας του αρχείου, όσο και στη φύση και την κατηγορία των δεδομένων, το σκοπό της επεξεργασίας, την τυχόν διασύνδεση των αρχείων ή τη διαβίβαση δεδομένων σε χώρες εκτός Ευρωπαϊκής Ένωσης, τα μέτρα ασφαλείας της επεξεργασίας και τέλος τα προσόντα των προσώπων που εκτελούν την επεξεργασία.

Το έτος 2002 η Αρχή προέβη στη διενέργεια επτά διοικητικών ελέγχων ιδιωτικών αρχείων. Οι φορείς που ελέγχθησαν αφορούσαν στο μεγαλύτερο μέρος τον τραπεζικό τομέα (5 έλεγχοι), τον τομέα υγείας (1) και τον τομέα παροχής υπηρεσιών διαδικτύου και πληροφορικής. Οι τράπεζες που ελέγχθηκαν ήταν:

- η Αγροτική Τράπεζα
- η American Express Bank
- η Ασπς Τράπεζα
- η Τράπεζα Κύπρου

-η υπηρεσία "Open 24" της EFG Eurobank Ergasias A.E.

B) Εξέταση προσφυγών, γνωμοδοτήσεις, οδηγίες, αποφάσεις

Η εξέταση προσφυγών και η απάντηση ερωτημάτων είναι ίσως το πιο καίριο μέρος του έργου της Αρχής, αφού έχει άμεσο αντίκτυπο στην καθημερινότητα του πολίτη και την προστασία των δικαιωμάτων του. Η προστασία των δικαιωμάτων της προσωπικότητας και της ιδιωτικής ζωής, πραγματώνεται με τη μεσολάβησή της στην επίλυση προβλημάτων στα οποία καλείται να παίξει τον ανεξάρτητο ρόλο που της έχει ανατεθεί απ' το νόμο. Το 2002 η Αρχή εξέτασε 578 προσφυγές απ' τις οποίες 62, δηλαδή ποσοστό περίπου 10%, στρέφονταν κατά των εταιριών προώθησης προϊόντων.

Κατηγοριοποίηση προσφυγών/καταγγελιών	
προσφυγές κατά τραπεζών	22
προσφυγές για πρόσβαση σε αρχεία και παραβίαση δεδομένων	366
προσφυγές κατά εταιριών πιστοληπτικής ικανότητας-Τειρεσίας	41
προσφυγές κατά εταιριών σταθερής και κινητής τηλεφωνίας	38
προσφυγές κατά νοσοκομείων/μιαυτηρίων	21
προσφυγές για κλειστά κυκλώματα τηλεόρασης	28
προσφυγές εταιριών προώθησης προϊόντων και πωλήσεων	<u>62</u>
Σύνολο	578

Γ) χορήγηση αδειών

Σύμφωνα με το άρθρο 7 του Ν2472/97, απαιτείται άδεια της Αρχής για τη συλλογή και επεξεργασία ευαίσθητων δεδομένων, καθώς και άδεια ίδρυσης και λειτουργίας σχετικού αρχείου. Το άρθρο 8 καθιερώνει σύστημα προηγούμενης άδειας της Αρχής σε περιπτώσεις διασύνδεσης αρχείων, όταν ένα απ' τα αρχεία που πρόκειται να διασυνδεθούν περιέχει ευαίσθητα δεδομένα ή αν η διασύνδεση έχει ως αποτέλεσμα την αποκάλυψη ευαίσθητων δεδομένων ή αν για την πραγματοποίηση της διασύνδεσης, πρόκειται να γίνει χρήση ενιαίου κωδικού αριθμού. Ακόμα, το άρθρο 9 που ρυθμίζει τη διασυννοριακή ροή προσωπικών

δεδομένων προβλέπει προηγούμενη άδεια της Αρχής για τη διαβίβαση δεδομένων σε χώρες που δεν ανήκουν στην Ευρωπαϊκή Ένωση.

Τον Ιούνιο του 2000, η Αρχή εξέτασε για το έτος 2002, 58 αιτήσεις χορήγησης αδειών λειτουργίας αρχείων με ευαίσθητα δεδομένα, οι οποίες κατηγοριοποιήθηκαν σύμφωνα με τον παρακάτω πίνακα:

Κατηγορία	Πλήθος
Νοσοκομεία-κέντρα υγείας	5
Ιατρικά κέντρα-κλινικές	5
Κοινωνικές υπηρεσίες ιδιωτικού τομέα	5
Γυμναστήρια, ινστιτούτα αισθητικής και αδυνατίσματος	13
Ασφαλιστικές εταιρίες	8
Λοιπές εμπορικές εταιρίες και οργανισμοί	12
Διαβίβαση δεδομένων σε χώρες εκτός της Ε.Ε.	10
Σύνολο	58

Δ) Γνωστοποιήσεις αρχείων

Το άρθρο 6 του Ν 2472/97 αναφέρεται στη συνεχή υποχρέωση των υπεύθυνων επεξεργασίας για γνωστοποίηση των αρχείων τους. Κατά το έτος 2002 κατατέθηκαν στην Αρχή 238 γνωστοποιήσεις, πλήθος σημαντικά μικρότερο απ' αυτό των 990 του προηγούμενου έτους, που οφείλεται κυρίως στο ότι καινούρια αρχεία δεν γνωστοποιούνται πλέον στην Αρχή, αφού το πολύ μεγάλο ποσοστό των υπαρχόντων αρχείων γνωστοποιήθηκε ήδη τα προηγούμενα έτη. Απ' το σύνολο των παραπάνω γνωστοποιήσεων μόνο 91 γίνονται από ιδιωτικές εταιρίες και χαρακτηρίζονται ως σημαντικές και αφορούν τους παρακάτω τομείς:

Κατηγορία	Αριθμός
Αεροπορικές εταιρίες	1
Ασφαλιστικά ταμεία	4
Ασφαλιστικές εταιρίες	10
Διαγνωστικά κέντρα, κλινικές	11
Εταρίες παροχής τηλεπικοινωνιακών υπηρεσιών, Internet service providers, ηλεκτρονικού εμπορίου	17
Εταιρίες προώθησης πωλήσεων, διαφημιστικές	18
Σύμβουλοι επιχειρήσεων	4
Τράπεζες, χρηματοοικονομικοί οργανισμοί	24
Φαρμακευτικές εταιρίες	2
Σύνολο	91

Παρατηρούμε ότι απ' τις παραπάνω σημαντικές γνωστοποιήσεις, οι 18, δηλαδή ποσοστό 20% περίπου, έγιναν από εταιρίες προώθησης προϊόντων.

6.2 Ηλεκτρονικό Κέντρο Εξυπηρέτησης του Πολίτη για την προστασία προσωπικών δεδομένων

Το Ηλεκτρονικό Κέντρο Εξυπηρέτησης έχει ως βασικό στόχο την καλύτερη εξυπηρέτηση των πολιτών σε θέματα προστασίας προσωπικών δεδομένων, αλλά και την υποστήριξη των υπεύθυνων επεξεργασίας για αποτελεσματική ανταπόκριση στις υποχρεώσεις τους. Στο έργο αυτό, το οποίο προσανατολίζεται στην αξιοποίηση του Διαδικτύου, ως βασικού τεχνολογικού μέσου, περιλαμβάνεται η βελτίωση των υπηρεσιών πληροφόρησης και επικοινωνίας από το δικτυακό τόπο της Αρχής, η ανάπτυξη υπηρεσιών ηλεκτρονικής υποβολής γνωστοποιήσεων και η βελτίωση της τηλεφωνικής εξυπηρέτησης των πολιτών μέσω της εγκατάστασης συστήματος ψηφιακού τηλεφωνικού κέντρου. Επίσης περιλαμβάνεται η δημιουργία εκπαιδευτικού και πληροφοριακού υλικού σε ηλεκτρονική μορφή, η δημιουργία ηλεκτρονικού κέντρου διαχείρισης

εσωτερικής πληροφορίας της Αρχής και η εκπαίδευση του προσωπικού της Αρχής.^{94, 95}

6.3 Οδηγία για τους όρους της νόμιμης επεξεργασίας δεδομένων προσωπικού χαρακτήρα νέων μητέρων για τους σκοπούς της άμεσης εμπορίας ή διαφήμισης στο χώρο των Μαιευτηρίων

Το 2000, η Αρχή Προστασίας Προσωπικών Δεδομένων εξέδωσε Οδηγία προς τα μαιευτήρια, σχετικά με την επεξεργασία προσωπικών δεδομένων νέων μητέρων για σκοπούς άμεσης προώθησης προϊόντων. Ύστερα από σχετική έρευνα, διαπιστώθηκε ότι εταιρείες συγκεντρώνουν προσωπικά στοιχεία από μητέρες με επισκέψεις στα δωμάτια των μαιευτηρίων μία ή δύο μέρες μετά τον τοκετό. Κατά την επίσκεψη η μητέρα δίνει τα στοιχεία της στον εκπρόσωπο της εταιρείας. Εδώ γεννάται το ερώτημα για το αν υπάρχει συγκατάθεση του υποκειμένου που έχει αποσπαστεί κατά τρόπο θεμιτό, αν δηλαδή η φυσική και ψυχολογική κατάσταση της μητέρας είναι τέτοια ώστε η συγκατάθεση που δίνεται πληροί τις προϋποθέσεις του άρθρ.2 παρ. ια του Ν.2472/97. Ανεξάρτητα από αυτό, πολλές φορές γίνεται επιλογή εκ μέρους των μαιευτηρίων, των εταιρειών που επιθυμούν την συγκέντρωση των στοιχείων.

Λαμβάνοντας υπόψη τα παραπάνω, η Αρχή σύμφωνα με το άρθρ.19 παρ 1 εδ.α του Ν.2472/97 εξέδωσε την παρακάτω **οδηγία**:

1. Για να είναι νόμιμη η συλλογή και η επεξεργασία στοιχείων, για τον σκοπό της προώθησης πωλήσεων, των νέων μητέρων που το επιθυμούν, τα μαιευτήρια ως υπεύθυνοι επεξεργασίας μπορούν να συντάσσουν ειδικό διπλότυπο εντύπο συμπλήρωσης στοιχείων. Το έντυπο αυτό θα δίνεται στην μητέρα κατά την διάρκεια της παραμονής της στο μαιευτήριο. Οι μητέρες που επιθυμούν να λαμβάνουν διαφημιστική αλληλογραφία θα συμπληρώνουν το έντυπο και θα το επιστρέφουν, κατά την έξοδο τους, στην αρμόδια υπηρεσία του μαιευτηρίου που θα ορίσει ο υπεύθυνος της επεξεργασίας, λογιστήριο κλπ..

⁹⁴ Ετήσια Έκθεση Αρχής Προστασίας Προσωπικών Δεδομένων 2002, www.dpa.gr

⁹⁵ Λίλιαν Μήτρου, Π. Δόνος, Φ.Μίτλεττον, Ευ. Παπακωνσταντίνου, ‘‘Η Αρχή προστασίας προσωπικών δεδομένων’’, σελ.11-14

2. Τα προσωπικά στοιχεία των μητέρων που συλλέγονται κατ' αυτόν τον τρόπο επιτρέπεται να δίνονται από τον υπεύθυνο επεξεργασίας, σε πρόσωπα ή εταιρείες που δραστηριοποιούνται στον τομέα της προώθησης πωλήσεων και άμεσης εμπορίας και διαφήμισης, που υποχρεούνται να τα χρησιμοποιήσουν αποκλειστικά για τους σκοπούς αυτούς.
3. Χρονικό διάστημα κατά το οποίο επιτρέπεται να διαβιβάζονται τα προσωπικά δεδομένα, ορίζονται οι τρεις (3) μήνες, από την έξοδο της μητέρας από το μαιευτήριο. Για επόμενο χρονικό διάστημα, προσωπικά στοιχεία θα δίνονται μόνο μετά από νέα ρητή συγκατάθεση της μητέρας.
4. Ο υπεύθυνος επεξεργασίας υποχρεούται να ενημερώνει τις μητέρες για τη διαδικασία που προβλέπεται στην παρούσα οδηγία και για τα δικαιώματά τους που απορρέουν από το Ν.2472/97, με σαφή και πρόσφορο τρόπο, όπως ιδίως με την επίδοση σχετικού ενημερωτικού εντύπου.
5. Είναι αυτονόητο ότι για την άμεση εμπορία προσωπικών δεδομένων ισχύουν οι περιορισμοί των άρθρων 9 παρ.10 και 14 παρ. 6 του Ν. 2251/94.⁹⁶

6.4 Όροι για την νόμιμη επεξεργασία δεδομένων προσωπικού χαρακτήρα για τους σκοπούς της άμεσης εμπορίας ή διαφήμισης και της διαπίστωσης πιστοληπτικής ικανότητας.

Η Αρχή εξέδωσε την απόφαση 26/2004, με την οποία κρίθηκαν οι όροι νόμιμης επεξεργασίας προσωπικών δεδομένων για σκοπούς άμεσης εμπορίας ή διαφήμισης και διαπίστωσης της πιστοληπτικής ικανότητας του προσώπου. Συγκεκριμένα θεωρείται νόμιμη η επεξεργασία δεδομένων για σκοπούς απ' αυθείας διαφήμισης και προώθησης προϊόντων και υπηρεσιών υπό τις εξής προϋποθέσεις:

Ι) Αν το υποκείμενο δώσει τη συγκατάθεσή του σύμφωνα με τα άρ. 2 εδ.ια) και 5 παρ.1 του Ν. 2472/97. Η συγκατάθεση είναι απαραίτητη στις περιπτώσεις της έρευνας καταναλωτικής συμπεριφοράς με σκοπό την άμεση ή έμμεση διαφήμιση προϊόντων η την παροχή υπηρεσιών.

⁹⁶ Απόφαση 523/18 της Αρχής Προστασίας Προσωπικών Δεδομένων, www.dpa.gr

II) Αν το υποκείμενο δεν δώσει την συγκατάθεσή του, τότε η επεξεργασία είναι νόμιμη κατ' εξαίρεση σύμφωνα με το άρθρο 5 παρ.2, εδ. ε, εφόσον α) είναι απολύτως αναγκαία για την ικανοποίηση του εννόμου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας β) το έννομο συμφέρον αυτού υπερέχει προφανώς του συμφέροντος του υποκειμένου, ενόψει του ότι τα συμφέροντα των υποκειμένων των δεδομένων των οποίων επιτρέπεται η επεξεργασία δεν θίγονται ουσιωδώς, δηλαδή δεν θίγονται σε τέτοιο βαθμό, ώστε να δικαιολογείται η απαγόρευση των εν λόγω δραστηριοτήτων γ) δεν θίγονται οι θεμελιώδεις ελευθερίες του υποκειμένου δ) τα δεδομένα προέρχονται από καταλόγους που απευθύνονται στο ευρύ κοινό (π.χ. τηλεφωνικός κατάλογος του ΟΤΕ) και υπάρχει η βεβαιότητα ότι τα υποκείμενα που έχουν συμπεριληφθεί σε αυτόν έχουν δώσει την συγκατάθεσή τους, ή από πηγές δημόσια προσβάσιμες που προορίζονται για την παροχή πληροφοριών στο ευρύ κοινό, εφόσον στην συγκεκριμένη περίπτωση έχουν τηρηθεί οι νόμιμες προϋποθέσεις για την πρόσβαση σ' αυτές, ή το ίδιο το υποκείμενο να δημοσιοποίησε τα προσωπικά του δεδομένα για συναφείς σκοπούς (π.χ διανομή διαφημιστικών φυλλαδίων, συμμετοχή σε καταλόγους εμπορικών εκθέσεων κ.λπ.)

Επιπλέον, ο υπεύθυνος επεξεργασίας πρέπει να έχει συμβουλευθεί το προβλεπόμενο από το άρθρο 19 παρ.4 εδ. δ) του Ν. 2472 Μητρώο της Αρχής στο οποίο καταχωρίζονται τα πρόσωπα που δεν επιθυμούν να περιλαμβάνονται σε αρχεία, τα οποία έχουν ως σκοπό την προώθηση προμήθειας αγαθών ή την παροχή υπηρεσιών εξ αποστάσεως και να μην συμπεριλάβει τα ανωτέρω πρόσωπα στα δημιουργούμενα αρχεία. Τέλος, οφείλει να περιορίζεται στα απολύτως αναγκαία δεδομένα (ονοματεπώνυμο, διεύθυνση και επάγγελμα) και ο σκοπός της επεξεργασίας να περιορίζεται στη διαφήμιση ή προώθηση πωλήσεως αγαθών και να μην αντίκειται στα χρηστά ήθη.

IV) Η υποχρέωση του υπεύθυνου επεξεργασίας να ενημερώσει το υποκείμενο κατά το στάδιο της συλλογής και της πρώτης διαβίβασης των δεδομένων ασκείται σύμφωνα με τις αποφάσεις και τους κανονισμούς της Αρχής, που αφορούν τους τρόπους ενημέρωσης των υποκειμένων από τον υπεύθυνο επεξεργασίας.

V) Αποδέκτες των προσωπικών δεδομένων, τα οποία συλλέγονται με σκοπό σχετιζόμενο με την άμεση εμπορία μπορούν να είναι πρόσωπα, τα οποία χρειάζονται τα δεδομένα για την άσκηση νόμιμης δραστηριότητας.

VI) Με την πρώτη επαφή του αποδέκτη με το υποκείμενο των δεδομένων, ο πρώτος είναι υποχρεωμένος να ενημερώσει το υποκείμενο για την πηγή από την οποία άντλησε τα προσωπικά του δεδομένα καθιστώντας σαφές ότι πρόκειται για διαφήμιση ή ενέργεια που αποσκοπεί στην προώθηση πωλήσεων αγαθών ή υπηρεσιών και να του δίνει την δυνατότητα εξαίρεσης των προσωπικών του δεδομένων από κάθε περαιτέρω χρήση αυτών για τον ανωτέρω σκοπό.

Διευκρινίζεται ότι η μη απάντηση του υποκειμένου μετά την πρώτη επαφή δεν θεωρείται συγκατάθεση. Σύμφωνα με το άρθρο 2 εδ.ια του Ν. 2472/97 η συγκατάθεση είναι ρητή και ειδική δήλωση βουλήσεως που εκφράζεται κατόπιν πλήρους ενημέρωσης του υποκειμένου απ' τον υπεύθυνο επεξεργασίας.

Σχετικά με τη διαπίστωση της πιστοληπτικής ικανότητας, η εξ επαγγέλματος συλλογή πληροφοριών από εταιρίες εμπορίας πληροφοριών χωρίς συγκατάθεση του υποκειμένου είναι νόμιμη όσον αφορά στα εξής μόνο "δυσμενή" δεδομένα: αιτήσεις πτωχεύσεων, αποφάσεις επί αιτήσεων πτωχεύσεων, διαταγές πληρωμής, προγράμματα πλειστηριασμού κινητών και ακινήτων, μεταβολές προσωπικών εταιριών, ΑΕ, ΕΠΕ και κοινοπραξιών, υποθήκες και προσημειώσεις υποθηκών, κατασχέσεις και επιταγές του ΝΔ 1923, ακάλυπτες επιταγές, διαμαρτυρόμενες συναλλαγματικές και γραμμάτια σε διαταγή.

Μετά τη συλλογή δεδομένων της ως άνω κατηγορίας και πριν από κάθε διαβίβαση, ο υπεύθυνος επεξεργασίας υποχρεούται να ενημερώσει ατομικά τα υποκείμενα, ώστε να ασκήσουν τα δικαιώματα πρόσβασης και αντίρρησης σύμφωνα με τα άρθρα 12 και 13 του νόμου 2472/97. Σε περίπτωση που το υποκείμενο ασκώντας το δικαίωμα αντίρρησης ζητήσει τη διαγραφή των

δεδομένων του, ο υπεύθυνος επεξεργασίας υποχρεούται να προχωρήσει στη διαγραφή ενημερώνοντας το υποκείμενο για τις τυχόν επιπτώσεις που θα έχει η διαγραφή στην εν γένει συναλλακτική του συμπεριφορά. Στην περίπτωση που το υποκείμενο αμφισβητήσει την νομιμότητα της εγγραφής και αφού ακολουθηθεί η διαδικασία των άρθρων 12 και 13, το βάσιμο του αιτήματος θα κρίνεται από την Αρχή.

Ο υπεύθυνος επεξεργασίας μπορεί να ενημερώσει τον αποδέκτη των δεδομένων για τυχόν άρνηση του υποκειμένου να δώσει συγκατάθεση για την συλλογή ορισμένων δεδομένων του.

Πρέπει να τονισθεί ότι όσα αναφέρθηκαν παραπάνω αφορούν τα λεγόμενα «δυσμενή» δεδομένα. Για την επεξεργασία των «ευμενών» (π.χ. κατοχή πιστωτικής κάρτας ή μπλόκ επιταγών, αναφορά σε υπάρχουσα ακίνητη περιουσία κλπ.) απαιτείται πάντοτε η συγκατάθεση του υποκειμένου.⁹⁷

⁹⁷ « Προσωπικά δεδομένα στο εμπόριο , τη διαφήμιση και τη συναλλακτική πίστη», Συνήγορος, τεύχος Σεπτεμβρίου-Οκτωβρίου 2004

ΚΕΦΑΛΑΙΟ 7

Διαβίβαση δεδομένων σε τρίτες χώρες

Ένα φαινόμενο που έχει λάβει μεγάλες διαστάσεις σήμερα, είναι η διασυνοριακή ροή δεδομένων, η οποία οφείλεται στην παγκοσμιοποίηση της οικονομίας. Διασυνοριακή διαβίβαση προσωπικών δεδομένων σε μεγάλη έκταση λαμβάνει χώρα ιδίως στο διαδίκτυο, όπως και συλλογή ακόμη και ευαίσθητων προσωπικών δεδομένων, με σκοπό την αξιοποίησή τους για τους σκοπούς της διαφήμισης και άμεσης προώθησης προϊόντων και υπηρεσιών.

Για τη ρύθμιση της διασυνοριακής ροής δεδομένων, εκδόθηκαν απ' το Συμβούλιο της Ευρώπης, Πρότυποι όροι συμβασης «για την εξασφάλιση ισοδύναμης προστασίας στο πλαίσιο διασυνοριακής ροής»⁹⁸. Πρόκειται για συλλογή πρότυπων όρων σύμβασης προορισμένων να εξασφαλίζουν «ισοδύναμη» προστασία, κατά τη διασυνοριακή ροή πληροφοριών με βάση τις εγγυήσεις της σύμβασης 108 του Συμβουλίου της Ευρώπης. Με βάση τους όρους αυτούς, ο αποστολέας διαβεβαιώνει ότι τηρεί σχεδόν το σύνολο των γενικών αρχών που διέπουν τον τομέα δραστηριότητας, δηλαδή ότι τα δεδομένα έχουν συλλεγεί και υποστεί επεξεργασία σύμφωνα με το εσωτερικό δίκαιο της χώρας στην οποία αυτός δραστηριοποιείται. Ιδιαίτερη αναφορά γίνεται στη θεμιτή και νόμιμη συλλογή των δεδομένων, τον σκοπό τήρησης, την επάρκεια, τη σχετικότητα και την ακρίβεια των δεδομένων καθώς και το χρόνο για τον οποίο επιτρέπεται η τήρησή τους. Ο παραλήπτης με τη σειρά του, αναλαμβάνει την υποχρέωση να τηρήσει τις ίδιες αρχές που δεσμεύουν τον αποστολέα στη χώρα του. Επιπρόσθετα, ο παραλήπτης δεσμεύεται συμβατικώς α) να χρησιμοποιεί τα δεδομένα μόνο για τους σκοπούς που περιέχονται στη σύμβαση β) να προστατεύει τα ευαίσθητα δεδομένα σύμφωνα με τα όσα ορίζει το εσωτερικό δίκαιο της χώρας του αποστολέα γ) να μην αναμεταβιβάζει τα δεδομένα σε τρίτους, εκτός αν υπάρχει αντίθετη συμβατική πρόβλεψη και δ) να διορθώνει,

⁹⁸ Οι όροι αυτοί δημοσιεύθηκαν ως αποτέλεσμα κοινής μελέτης του Συμβουλίου της Ευρώπης, της Επιτροπής των Ευρωπαϊκών Κοινοτήτων και του Διεθνούς Εμπορικού Επιμελητηρίου

διαγράφει και ενημερώνει τα δεδομένα σύμφωνα με τις επιθυμίες του αποστολέα. Οι πρότυποι όροι ρυθμίζουν επίσης την ευθύνη του παραλήπτη σε περίπτωση αθέμιτης ή παράνομης χρήσης, τα δικαιώματα των υποκειμένων, τον τρόπο επίλυσης των διαφορών και το δικαίωμα καταγγελίας. Το 1998, οι ανωτέρω πρότυποι όροι αναθεωρήθηκαν απ' το Διεθνές Εμπορικό Επιμελητήριο υπό το φως της Οδηγίας 95/46 ΕΚ προκειμένου να καλυφθεί η απαίτηση του άρθρου 25 για «ικανοποιητικό επίπεδο προστασίας» κατά την εξαγωγή δεδομένων προς τρίτες χώρες.

Επίσης με πρωτοβουλία της Γενικής Διεύθυνσης XV και σύμφωνα με το άρθρο 26§4 της Οδηγίας 95/46 ΕΚ⁹⁹ εκδόθηκαν δύο αποφάσεις της Ευρωπαϊκής Επιτροπής με τις οποίες προωθείται η λύση των συμβατικών ρητρών, πρώτον για την απλή διαβίβαση δεδομένων προς τρίτες χώρες και δεύτερον για τη διαβίβαση προς υπεύθυνους επεξεργασίας. Εφόσον αυτές οι τυποποιημένες ρήτρες ενσωματωθούν σε συμβατικά κείμενα, θεωρείται ότι προσφέρονται επαρκείς εγγυήσεις και ότι εξασφαλίζεται ικανοποιητικό επίπεδο προστασίας. Επομένως επιτρέπεται η διαβίβαση δεδομένων από υπεύθυνο επεξεργασίας εγκατεστημένο σε ένα κράτος της Ε.Ε. προς υπεύθυνο επεξεργασίας εγκατεστημένο σε τρίτο κράτος ακόμη και αν στο τρίτο κράτος δεν εξασφαλίζεται ικανοποιητικό επίπεδο προστασίας.¹⁰⁰

Τέλος το άρθρο 9 του νόμου 2472/1997 για τη διασυννοριακή ροή δεδομένων, ορίζει ότι η διαβίβαση προσωπικών δεδομένων προς τρίτη χώρα, τα οποία έχουν υποστεί ή πρόκειται να υποστούν επεξεργασία μετά τη διαβίβασή τους, επιτρέπεται ύστερα από άδεια της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Η Αρχή παρέχει την άδεια μόνο αν κρίνει ότι η τρίτη χώρα εξασφαλίζει ικανοποιητικό επίπεδο προστασίας, εξετάζοντας τη φύση των δεδομένων, τους σκοπούς και τη διάρκεια της επεξεργασίας, τους σχετικούς γενικούς και ειδικούς κανόνες δικαίου, τους κώδικες δεοντολογίας, τα μέτρα

⁹⁹ Το άρθρο 26 παρ.4 της Οδηγίας 95/46 ΕΚ ορίζει ότι «Εάν η Επιτροπή αποφανθεί, με τη διαδικασία που αναφέρεται στο άρθρο 31 παράγραφος 2, ότι ορισμένες τυποποιημένες συμβατικές ρήτρες παρέχουν τις επαρκείς εγγυήσεις που αναφέρονται στην παράγραφο 2, τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να συμμορφωθούν προς την απόφαση της Επιτροπής».

¹⁰⁰ Γιαννόπουλος Ν. Γιώργος,ό.π., σελ.143

ασφάλειας για την προστασία των προσωπικών δεδομένων καθώς και το επίπεδο προστασίας των χωρών προέλευσης και τελικού προορισμού των δεδομένων.

Η διαβίβαση δεδομένων προς τρίτη χώρα, η οποία δεν εξασφαλίζει ικανοποιητικό επίπεδο προστασίας, επιτρέπεται κατ' εξαίρεση με άδεια της Αρχής, εφόσον συντρέχει μια ή περισσότερες απ' τις κατωτέρω προϋποθέσεις:

A) Το υποκείμενο των δεδομένων έδωσε τη συγκατάθεσή του για τη διαβίβαση των δεδομένων και η συγκατάθεση έχει αποσπασθεί με τρόπο που να αντίκειται στο νόμο ή τα χρηστά ήθη

B) Η διαβίβαση είναι απαραίτητη i) για τη διασφάλιση ζωτικού συμφέροντος του υποκειμένου των δεδομένων, εφόσον αυτό τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του ή ii) για τη συνομολόγηση και εκτέλεση σύμβασης μεταξύ αυτού και του υπεύθυνου επεξεργασίας ή μεταξύ του υπεύθυνου επεξεργασίας και τρίτου προς το συμφέρον του υποκειμένου των δεδομένων, εφ' όσον το υποκείμενο τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του, ή iii) για την εκτέλεση προσυμβατικών μέτρων που έχουν ληφθεί κατ' αίτηση του υποκειμένου των δεδομένων.

Γ) Η διαβίβαση είναι απαραίτητη για την αντιμετώπιση εξαιρετικής ανάγκης και τη διαφύλαξη υπέρτερου δημόσιου συμφέροντος, ιδίως για την εκτέλεση συμβάσεων συνεργασίας με δημόσιες αρχές της άλλης χώρας, εφόσον ο υπεύθυνος επεξεργασίας παρέχει επαρκείς εγγυήσεις για την προστασία της ιδιωτικής ζωής και των θεμελιωδών ελευθεριών και την άσκηση των σχετικών δικαιωμάτων.

Δ) Η διαβίβαση είναι αναγκαία για την αναγνώριση, άσκηση ή υπεράσπιση δικαιώματος ενώπιον του δικαστηρίου.

E) Η μετάδοση πραγματοποιείται από δημόσιο μητρώο, το οποίο κατά το νόμο προορίζεται για την παροχή πληροφοριών στο κοινό και είναι προσιπό στο κοινό ή σε κάθε πρόσωπο που αποδεικνύει έννομο συμφέρον, εφόσον στη

συγκεκριμένη περίπτωση πληρούνται οι νόμιμες προϋποθέσεις για την πρόσβαση στο μητρώο.

Στις περιπτώσεις των προηγούμενων παραγράφων η Αρχή ενημερώνει την Ευρωπαϊκή Επιτροπή και τις αντίστοιχες Αρχές των άλλων κρατών μελών, όταν θεωρεί ότι μία χώρα δεν εξασφαλίζει ικανοποιητικό επίπεδο προστασίας.¹⁰¹

¹⁰¹ Άρθρο 9 του νόμου 2472/1997 διαθέσιμο στο www.europa.eu.int

ΜΕΡΟΣ 2^ο - ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

ΚΕΦΑΛΑΙΟ 1

Εισαγωγή

1.1 Ηλεκτρονικό εμπόριο και οι συνέπειές του στην οικονομία

Στα προηγούμενα κεφάλαια αναλύθηκε ο τρόπος και τα μέσα που χρησιμοποιούν οι επιχειρήσεις για τη συλλογή και επεξεργασία προσωπικών δεδομένων καταναλωτών για σκοπούς άμεσης διαφήμισης, οι κίνδυνοι που εγκυμονεί η παραπάνω διαδικασία για την ιδιωτική ζωή και το δικαίωμα του πληροφοριακού αυτοκαθορισμού των ατόμων και, τέλος, αναλύθηκε το ελληνικό και κοινοτικό νομοθετικό πλαίσιο προστασίας των δεδομένων προσωπικού χαρακτήρα. Στα επόμενα κεφάλαια θα αναλυθεί η προστασία απ' την επεξεργασία προσωπικών δεδομένων καταναλωτών για σκοπούς άμεσης διαφήμισης, ειδικά στο χώρο του διαδικτύου.

Πριν από λίγα χρόνια το διαδίκτυο αποτελούσε ένα μέσο επικοινωνίας που απασχολούσε μόνο τους ειδικούς επιστήμονες και όσους ασχολούνταν με την τεχνολογία. Η καταλυτική ωστόσο παρουσία του διαδικτύου σε όλους τους τομείς της κοινωνικής και οικονομικής ζωής, δεν θα μπορούσε παρά να επηρεάσει και το εμπόριο. Έτσι σήμερα το διαδίκτυο χρησιμοποιείται ευρύτατα για το «επιχειρείν» σε ολόκληρο τον κόσμο. Με τον όρο “Ηλεκτρονικό Εμπόριο”, νοείται ένα σύνολο επιχειρηματικών στρατηγικών που μπορούν να υποστηρίξουν συγκεκριμένους τομείς επιχειρηματικής δραστηριότητας και συγκεκριμένες επιχειρηματικές πρακτικές οι οποίες επιτρέπουν, μέσω της χρήσης νέων τεχνολογιών, τη διεκπεραίωση εμπορικών διαδικασιών με ηλεκτρονικά μέσα¹⁰². Το ηλεκτρονικό εμπόριο καλύπτει κυρίως δύο τύπους δραστηριοτήτων και διακρίνεται σε **έμμεσο** (offline) και **άμεσο** (online). Έμμεσο είναι όταν πρόκειται

¹⁰² Δουκίδης Γεώργιος, ό.π., σελ. 15

για ηλεκτρονική παραγγελία ενσώματων-υλικών αγαθών που μπορούν να παραδοθούν με παραδοσιακούς τρόπους όπως π.χ. ταχυδρομικά. Άμεσο είναι το ηλεκτρονικό εμπόριο που περιλαμβάνει παραγγελία, πληρωμή και παράδοση άυλων αγαθών και υπηρεσιών όπως λογισμικό, οπτικοακουστικό υλικό, υπηρεσίες πληροφόρησης κτλ.

Όλοι οι τομείς εμπορικής δραστηριότητας επηρεάζονται απ' το διαδίκτυο και η ανάπτυξη τα τελευταία χρόνια είναι ιδιαίτερα μεγάλη. Αρκεί να αναφερθεί ότι απ' τις μικρομεσαίες ευρωπαϊκές επιχειρήσεις το 84% αυτών έχουν πρόσβαση στο διαδίκτυο και το 70% έχουν δική τους ιστοσελίδα. Πάνω απ' τα δύο τρίτα των εταιριών στην Ευρώπη χρησιμοποιούν το διαδίκτυο ως επιχειρηματικό εργαλείο. Η νέα αυτή αγορά και ταυτόχρονα νέα τηλεπικοινωνιακή υπηρεσία προσφέρει νέους τρόπους διαφήμισης και διάθεσης προϊόντων, όπως π.χ. banners, pop-up ads, keyword searches, e-mail κτλ, οι οποίοι θα αναλυθούν παρακάτω. Μάλιστα έχει παρατηρηθεί ότι η ποσοστιαία αύξηση των δαπανών για διαφημίσεις μέσω διαδικτύου είναι μεγαλύτερη απ' αυτή των υπόλοιπων διαφημιστικών μέσων. Συγκεκριμένα οι συνολικές διαφημιστικές δαπάνες αυξήθηκαν κατά 2% το 2002 σε σχέση με τον προηγούμενο χρόνο, ενώ το κόστος για online διαφημίσεις αυξήθηκε κατά 20%, δηλαδή δέκα φορές περισσότερο.¹⁰³ Μέσω του διαδικτύου μπορεί να γίνει και διακίνηση χρηματοοικονομικών προϊόντων. Παραδείγματος χάριν το διαδίκτυο συμβάλει στην ταχύτερη διεκπεραίωση των τραπεζικών συναλλαγών, καθώς είναι πλέον δυνατή η άμεση μεταφορά κεφαλαίων σε οποιοδήποτε σημείο του πλανήτη. Επίσης με το telebanking ή electronic banking είναι δυνατό να δαβιβάζονται από πελάτες τραπεζών μέσω ηλεκτρονικών υπολογιστών, εντολές χρέωσης ή πίστωσης του λογαριασμού τους. Ο πελάτης μπορεί μέσω του διαδικτύου να παρακολουθεί τις κινήσεις και τα υπόλοιπα των λογαριασμών του, να ζητά έκδοση εγγυητικών επιστολών, να πληρώνει λογαριασμούς πιστωτικών καρτών ή να ενημερώνεται για τις τιμές συναλλάγματος. Το διαδίκτυο παράλληλα αποτελεί και μέσο διεκπεραίωσης χρηματιστηριακών συναλλαγών. Προσφέρει

¹⁰³ Αναφορά της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο για την εφαρμογή της Οδηγίας 2000/31 ΕΚ, "για ορισμένες νομικές πτυχές της Κοινωνίας της Πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά", COM(2003)702 final σελ.5

δυνατότητες επένδυσης σε ξένα χρηματιστήρια και μειώνει τους κινδύνους διενέργειας προσυννεοημένων συναλλαγών. Επιπρόσθετα, μέσω του διαδικτύου ο πελάτης μπορεί να παίζει ένα περισσότερο ενεργητικό ρόλο όσον αφορά την επιλογή πληροφοριών και την αναζήτηση κατάλληλων γι' αυτόν προϊόντων και μπορεί επίσης να συμμετέχει σε συζητήσεις για αγοραζόμενα προϊόντα και να καταθέτει τις δικές του απόψεις για τα υπό συζήτηση αγαθά.¹⁰⁴

Όσον αφορά τη διείσδυση του διαδικτύου στην Ευρωπαϊκή Ένωση, τα κράτη μέλη το Μάρτιο του 2000 έθεσαν ως στόχο, να γίνει η Ευρώπη η πιο ανταγωνιστική αγορά μέχρι το 2010. Υιοθέτησαν λοιπόν το πρόγραμμα "eEurope 2002", το οποίο έχει ως κύριο στόχο όχι μόνο την αύξηση της ανταγωνιστικότητας της ευρωπαϊκής αγοράς, αλλά και να εξασφαλίσει ότι όλοι οι Ευρωπαίοι πολίτες και ιδίως τα άτομα με ειδικές ανάγκες, θα έχουν πρόσβαση στο διαδίκτυο προκειμένου να βελτιωθεί η ποιότητα ζωής τους. Κάθε πολίτης με την κατάλληλη εκπαίδευση θα έχει τη δυνατότητα με ένα "κλικ" να έχει πρόσβαση στη γνώση, την εκπαίδευση, τις υπηρεσίες υγείας, τις χρηματοοικονομικές υπηρεσίες, την ψυχαγωγία κτλ.¹⁰⁵

Μέχρι το 2000 που αποφασίστηκε η εφαρμογή του προγράμματος αυτού, η χρήση του διαδικτύου παρεμποδιζόταν απ' τους εξής παράγοντες:

- Ακριβή, ανασφαλή και αργή πρόσβαση στο internet
- Ανεπαρκής αριθμός κατάλληλα εκπαιδευμένων χρηστών
- Αμέλεια απ' την πλευρά του κράτους για την ανάπτυξη νέων τεχνολογικών εφαρμογών

Προκειμένου να ξεπεραστούν τα παραπάνω εμπόδια, το eEurope 2002 έθεσε τους εξής στόχους:

- Εξασφάλιση γρήγορης, φθηνής και ασφαλούς πρόσβασης στο internet

Μια απ' τις κύριες προτεραιότητες του eEurope 2002 είναι η αναθεώρηση των κανόνων που αφορούν την πρόσβαση στο internet και η δημιουργία μιας ενιαίας

¹⁰⁴ Καράκωστας Κ. Ιωάννης, "Δίκαιο και internet", σελ. 1-2

¹⁰⁵ Κατσουλάκος Ιωάννης, "Νέα οικονομία, Διαδίκτυο και Ηλεκτρονικό εμπόριο", σελ. 148

αγοράς για τις τηλεπικοινωνίες. Η απελευθέρωση των τηλεπικοινωνιών ξεκίνησε τη δεκαετία του '80, ωστόσο δεν προχώρησε αρκετά. Γι' αυτό, το Μάρτιο του 2002 η Ευρωπαϊκή Ένωση αποφάσισε την απλοποίηση της υπάρχουσας νομοθεσίας που διέπει την πρόσβαση στο διαδίκτυο, μειώνοντας τους νόμους που διέπουν τις τηλεπικοινωνίες από είκοσι τρεις σε οκτώ και δημιουργώντας έτσι μια απελευθερωμένη τηλεπικοινωνιακή αγορά, όπου ο ανταγωνισμός οδηγεί σε μείωση των τιμών και βελτίωση της ποιότητας των παρεχόμενων υπηρεσιών. Το αποτέλεσμα είναι φθηνότερη και γρηγορότερη πρόσβαση στο internet για πολίτες και επιχειρήσεις. Ενδεικτικά αναφέρεται, ότι σύμφωνα με έρευνα που πραγματοποίησε η Ευρωπαϊκή Επιτροπή το Νοέμβριο 2001, το κόστος πρόσβασης στο internet για έναν ευρωπαίο χρήστη ήταν 10-20 ευρώ μηνιαίως (η χαμηλότερη προσφορά).

- Εκπαίδευση πολιτών για τη χρήση του internet

Σκοπός του eEurope 2002 είναι η εξασφάλιση επαρκούς εκπαίδευσης για όλους τους ευρωπαίους πολίτες στις νέες τεχνολογίες πληροφορικής και ειδικότερα στη χρήση του internet, έτσι ώστε να αυξηθεί η παραγωγικότητα των εργαζομένων στις επιχειρήσεις, να έχουν τη δυνατότητα οι καταναλωτές ν' αγοράζουν τα προϊόντα τους online και να αποκτήσουν οι μαθητές γνώσεις πληροφορικής. Χαρακτηριστικά, το 2002 το 93% των σχολείων στην Ευρωπαϊκή Ένωση απέκτησαν πρόσβαση στο internet σε σύγκριση με 89% το 2001. Επίσης το 2001 για κάθε 25 μαθητές αντιστοιχούσε ένας υπολογιστής, αναλογία η οποία μειώθηκε το 2003 σε 15 μαθητές ανά υπολογιστή.

Όσον αφορά το χώρο εργασίας, το 2002 πάνω απ' το 50% των εργαζομένων στην Ευρωπαϊκή Ένωση χρησιμοποιούσαν Η/Υ στην εργασία τους και τρεις στους τέσσερις υπαλλήλους γραφείων ήταν χρήστες Η/Υ. Ωστόσο η εκπαίδευση στο χώρο εργασίας ήταν ελλιπής, καθώς μόνο το 1/3 των εργαζομένων είχαν εκπαιδευτεί στη χρήση υπολογιστών για τη δουλειά τους. Στόχος του eEurope 2002 είναι να βελτιωθούν οι γνώσεις των εργαζομένων όσον αφορά τη χρήση του διαδικτύου και να αυξηθεί η πρόσβαση σχολείων σ' αυτό.^{106 107}

¹⁰⁶ “Towards a knowledge-based Europe”, 2002, www.europa.eu.int

1.2 Πεδία εφαρμογής του Ηλεκτρονικού Εμπορίου

Το ηλεκτρονικό εμπόριο έχει εφαρμογή σε μια ευρεία γκάμα επιχειρηματικών λειτουργιών, όπως π.χ των εξής:

A) Υποστήριξη πελάτη: Πολλές επιχειρήσεις δημιουργούν ομάδες συζητήσεων και επαφών με τους πελάτες τους, οι οποίοι με τον τρόπο αυτό μπορούν να επικοινωνούν όχι μόνο με την επιχείρηση αλλά και μεταξύ τους, ανταλλάσσοντας ιδέες, ερωτήσεις, συμβουλές κτλ.

B) Ανταλλαγή πληροφοριών για προϊόντα και υπηρεσίες: Η ανταλλαγή πληροφοριών, η διαφήμιση και ενημέρωση για προϊόντα και υπηρεσίες είναι ίσως η πλέον διαδεδομένη χρήση του ηλεκτρονικού εμπορίου. Π.χ. πολλές επιχειρήσεις διαθέτουν ηλεκτρονικές σελίδες μέσω των οποίων διαφημίζουν στο διαδίκτυο τα προϊόντα και τις υπηρεσίες που παρέχουν

Γ) Ανάπτυξη κοινών επιχειρηματικών διαδικασιών μεταξύ επιχειρήσεων: Τέτοιες διαδικασίες φέρνουν σε στενή επαφή τους συμμετέχοντες στο εμπορικό κύκλωμα, συσφίγγοντας τους επιχειρηματικούς δεσμούς και δυσχεραίνοντας με αυτόν τον τρόπο την αλλαγή συνεργατών. Για παράδειγμα η αλυσίδα σουπερμάρκετ Tesco της Μεγάλης Βρετανίας έχει αναπτύξει ένα πολύπλοκο σύστημα ανατροφοδότησης των 540 καταστημάτων που διαθέτει στη χώρα αυτή. Κάθε πώληση προϊόντων που καταγράφεται στα ταμεία κάποιου καταστήματος μεταφέρεται ηλεκτρονικά στα κεντρικά γραφεία της εταιρίας. Εκεί γίνεται αυτόματος έλεγχος αποθεμάτων για το συγκεκριμένο κατάστημα και υπολογίζονται οι ανάγκες ανατροφοδότησης κάθε καταστήματος με βάση τα προϊόντα που εμφανίζονται με υπόλοιπο κάτω απ' το όριο ασφαλείας. Η πληροφορία τελικά στέλνεται ηλεκτρονικά στον αντίστοιχο αποθηκευτικό χώρο της εταιρίας. Εκεί, αν τα προϊόντα δεν υπάρχουν σε απόθεμα, παραγγέλνονται ηλεκτρονικά απ' τον κατάλληλο προμηθευτή. Μετά τη παραλαβή, τα προϊόντα

¹⁰⁷ David Lennon, "The future of free information in the age of the internet", www.emeraldinsight.com

στέλνονται στο κατάστημα που τα χρειάζεται. Το όλο σύστημα ανατροφοδότησης λειτουργεί με τη στενή συνεργασία των προμηθευτών, οι οποίοι ουσιαστικά συμμετέχουν σε μια κοινή επιχειρηματική διαδικασία ανατροφοδότησης των ραφιών στα καταστήματα του σουπερμάρκετ.

Δ) Ηλεκτρονικές Τράπεζες: Σήμερα οι τράπεζες έχουν δημιουργήσει ηλεκτρονικές υπηρεσίες παρέχοντας ένα σύνολο δυνατοτήτων στους πελάτες τους. Οι ηλεκτρονικές τράπεζες επιτρέπουν στους πελάτες να χρεωπιστώνουν τους λογαριασμούς τους μέσα απ' το διαδίκτυο, να μεταφέρουν κεφάλαια από ένα λογαριασμό σε άλλο ή ακόμη να κάνουν αίτηση για προέγκριση δανείου ή απόκτηση πιστωτικής ή άλλης κάρτας.

Ε) Δημιουργία ηλεκτρονικών επιχειρήσεων (ψηφιακά καταστήματα): Το ηλεκτρονικό εμπόριο παρέχει τη δυνατότητα δημιουργίας ηλεκτρονικών επιχειρήσεων στο δίκτυο. Επιπλέον πολλές εταιρίες δημιουργούν Ηλεκτρονικά Εμπορικά Κέντρα, δηλαδή ομάδες επιχειρήσεων που συνεργάζονται ηλεκτρονικά δημιουργώντας ένα Εμπορικό Κέντρο στο διαδίκτυο. Μια ηλεκτρονική επιχείρηση αποτελείται από δύο ή περισσότερα ηλεκτρονικά καταστήματα και παρέχεται η δυνατότητα στις επιχειρήσεις να δημιουργήσουν ισχυρούς και ανταγωνιστικούς ομίλους εταιριών.¹⁰⁸

Ζ) Ηλεκτρονική διανομή: Στα πλαίσια της ηλεκτρονικής διανομής, μπορούν να ενταχθούν υπηρεσίες on-line διάχυσης πληροφοριών με μηδαμινό, συνήθως κόστος χρήσης. Για παράδειγμα, η εταιρία πληροφορικής Oracle διαθέτει μια ηλεκτρονική σελίδα στο διαδίκτυο μέσω της οποίας οι πελάτες ενημερώνονται για τα προϊόντα της εταιρίας, μπορούν να μεταφέρουν στον υπολογιστή τους δωρεάν δοκιμαστικές εκδόσεις (demos) των προγραμμάτων της εταιρίας, και αν

¹⁰⁸ Η ηλεκτρονική επιχείρηση υπάρχει μόνο στο διαδίκτυο. Απ' την ιστοσελίδα της εταιρίας, οι πελάτες μπορούν να δουν πληροφορίες για τα προϊόντα της και να τα παραγγείλουν πληρώνοντας μέσω ηλεκτρονικών συστημάτων πληρωμών. Οι παραγγελίες των πελατών μεταφέρονται μέσω δικτύου στον κατάλληλο προμηθευτή και τα προϊόντα αποστέλλονται μέσω ταχυδρομείου. Ο πελάτης έχει τη δυνατότητα να παρακολουθεί το σημείο όπου βρίσκεται η παραγγελία του ανά πάσα στιγμή.

πληρώσουν μέσω πιστωτικής κάρτας, μπορούν να μεταφέρουν ολόκληρα προγράμματα.^{109 110}

1.3 Οφέλη του διαδικτύου για τις επιχειρήσεις

Είναι γενικώς παραδεκτό ότι η χρήση του διαδικτύου έχει παρουσιάσει παγκοσμίως σημαντική άνοδο απ' τη στιγμή της εμφάνισής του. Ο αριθμός των υπολογιστών που είναι μόνιμα συνδεδεμένοι με το διαδίκτυο έφθασε το 2001 τα 268εκ, το 2002 τα 591εκ, ενώ το 2004 άγγιξε τα 900εκ. Για να γίνει πιο εμφανής η ραγδαία αύξηση της χρήσης του διαδικτύου, αρκεί να αναφέρουμε ότι μέχρι το 1991 ο αριθμός των χρηστών δεν ξεπερνούσε καν τα 14,2εκ.¹¹¹ Παράλληλα με την αύξηση του αριθμού των συνδεδεμένων χρηστών έχει παρατηρηθεί και αύξηση της χρήσης του για εμπορικούς σκοπούς, γεγονός που δηλώνει τον ταχύτατο ρυθμό μετατροπής του διαδικτύου σε κανάλι επικοινωνίας και επιχειρηματικών συναλλαγών. Παρακάτω θα παρατεθούν κάποια στατιστικά στοιχεία για την εξέλιξη του ηλεκτρονικού εμπορίου παγκοσμίως τα τελευταία χρόνια. Όσον αφορά την αγορά της Αμερικής, το Αμερικανικό Υπουργείο Εμπορίου ανακοίνωσε ότι το 2003 ο τζίρος του ηλεκτρονικού εμπορίου σημείωσε άνοδο κατά 26% στις ΗΠΑ με τις ηλεκτρονικές πωλήσεις να φθάνουν το 1,5% του συνολικού όγκου λιανικών πωλήσεων και να διαμορφώνεται στα \$55 δις.¹¹²

Όσον αφορά την αγορά της Ευρωπαϊκής Ένωσης, σε μια αναφορά που συνέταξε το e-Business Watch το Μάιο του 2002 με τίτλο "Η ανάπτυξη του η-εμπορίου στην Ε.Ε", τονίζει μεταξύ άλλων τα εξής:

- ✓ Το 2001 στην Ευρώπη οι online πωλήσεις ανήλθαν στα 77 δις. ευρώ, ενώ το 2006 σύμφωνα με προβλέψεις θα ξεπεράσουν τα 2,2 τρις ευρώ, αριθμός που αντιστοιχεί στο 22% του συνολικού εμπορίου.¹¹³

¹⁰⁹Karakaya Fahri, Charlton T. Earl, "Electronic Commerce: Current and Future Practices", www.emeraldinsight.com

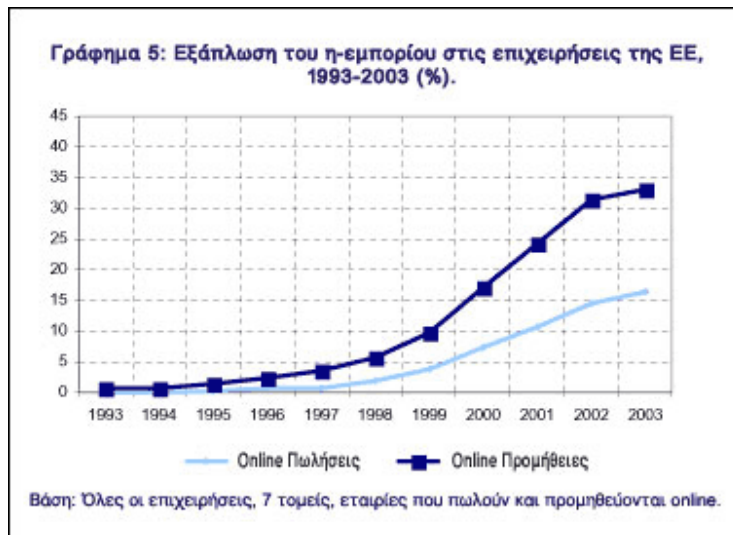
¹¹⁰ Δουκίδης Γεώργιος, ό.π., σελ.24-25

¹¹¹ Έκθεση του ΟΟΣΑ για το spam, ICCP(2003)10/Final, σελ. 4

¹¹² Ωστόσο στο ποσό αυτό δεν συμπεριλαμβάνονται οι πωλήσεις online της βιομηχανίας στοιχημάτων και τυχερών παιχνιδιών που φθάνουν το ποσό των \$6 δις, οι πωλήσεις φαρμάκων που ξεπερνούν τα \$0,7 δις, οι online πωλήσεις δημοπρασιών και B2B, καθώς και οι online πωλήσεις τουριστικών υπηρεσιών.

¹¹³ "Πενταετία ανάπτυξης για το ηλεκτρονικό εμπόριο", 2002, www.go-online.gr

✓ Οι ηλεκτρονικές προμήθειες έχουν αναπτυχθεί ραγδαία απ' τα τέλη της δεκαετίας του '90 και μετά, καθώς μια στις τρεις εταιρίες δήλωσαν ότι αγόρασαν online προϊόντα εξοπλισμού, συντήρησης και λειτουργίας της επιχείρησης.



Το 2002, οι επιχειρήσεις πραγματοποίησαν περίπου το 2% του συνολικού όγκου των πωλήσεών τους μέσω internet. Τα ποσοστά είναι υψηλότερα σε κάποιους τομείς, όπως ο τουρισμός (5%), τα ΜΜΕ, οι εκδόσεις-εκτυπώσεις, η πληροφορική (4%) και το λιανεμπόριο (3%). Το 2003, το ποσοστό του συνολικού όγκου των online πωλήσεων αυξήθηκε σε 2,3%. Ο κύριος παράγοντας της τόσο σημαντικής ανόδου του ηλεκτρονικού εμπορίου είναι η διάδοση των ευρυζωνικών συνδέσεων, δηλ. του "γρήγορου" internet, οι οποίες καθιστούν τις online αγορές ευκολότερες και πιο αξιόπιστες. Σύμφωνα με μελέτες μάλιστα, οι συνδρομητές ευρυζωνικής σύνδεσης εκτελούν διπλάσιες σε αριθμό εργασίες στο διαδίκτυο απ' τους κατόχους απλών συνδέσεων.¹¹⁴

Ο παρακάτω πίνακας δείχνει την εξέλιξη των online πωλήσεων στην Ελλάδα απ' το 2000 έως σήμερα, σύμφωνα με έρευνα της Forrester Research to 2004.

¹¹⁴ "Δραστηριότητες του η-εμπορίου: Ραγδαία ανάπτυξη των online αγορών", 2002, www.go-online.gr

Έτος	Πωλήσεις (σε εκατ)
2000	8
2001	17
2002	51
2003	125
2004	262

Σύμφωνα με προβλέψεις της ίδιας εταιρίας, το 2005 οι πωλήσεις θα ανέλθουν στα 476εκ. και το 2006 στα 772εκ. Η κατηγορία με τις περισσότερες πωλήσεις είναι τα είδη τουρισμού, και κυρίως τα εισιτήρια, ακολουθούν τα CDs, οι Η/Υ, τα βιβλία και η κινητή τηλεφωνία ¹¹⁵

Οι λόγοι που οδήγησαν τους καταναλωτές και τις επιχειρήσεις στο να εμπιστεύονται το διαδίκτυο για τις εμπορικές τους συναλλαγές είναι οι εξής:

-Ευρεία κάλυψη: Το διαδίκτυο είναι απ' τη φύση του ένα διεθνές δίκτυο και προσφέρει τη δυνατότητα παγκόσμιας και συνεχούς παρουσίας. Λειτουργεί εικοσιτέσσερις ώρες τη μέρα, επτά ημέρες την εβδομάδα.

-Χαμηλό κόστος: Το κόστος χρήσης του διαδικτύου είναι εξαιρετικά χαμηλό. Μάλιστα το κόστος προώθησης προϊόντων μέσω του διαδικτύου είναι πολύ χαμηλό, μόλις 0,01-0,5\$, ενώ το κόστος αποστολής μηνύματος μέσω συμβατικού ταχυδρομείου κυμαίνεται μεταξύ 0,5-1\$. Επίσης, το κόστος ανάπτυξης λειτουργίας και συντήρησης ενός κόμβου στο διαδίκτυο (website) είναι ιδιαίτερα χαμηλό. Μάλιστα η αύξηση του αριθμού των χρηστών ωθεί όλο και περισσότερες επιχειρήσεις να ασχοληθούν με τον τομέα της παροχής υπηρεσιών internet (Internet Service Providers-ISPs), με συνέπεια ο αυξανόμενος ανταγωνισμός να αποβαίνει σε όφελος του τελικού χρήστη (με τη μορφή χαμηλότερων συνδρομών και καλύτερων προσφορών).

-Ανάπτυξη σχέσεων με τους πελάτες: Το ηλεκτρονικό εμπόριο παρέχει τη δυνατότητα στις επιχειρήσεις να δημιουργούν πιο προσωπικές σχέσεις με τους πελάτες, χάρη στη δυνατότητα που έχουν να συγκεντρώνουν πληροφορίες για τη συμπεριφορά του καταναλωτή εύκολα και γρήγορα. Για παράδειγμα μια αεροπορική εταιρία μπορεί να καταγράφει πληροφορίες για τις προτιμήσεις κάθε πελάτη της (π.χ. πόσο συχνά ταξιδεύει, ποιες θέσεις προτιμά, αν ζητά γεύματα

¹¹⁵ Έρευνα της Forrester Research για το ηλεκτρονικό εμπόριο στην Ελλάδα, 2004, www.go-online.gr

για χορτοφάγους κτλ), και μ'αυτόν τον τρόπο να δημιουργήσει μια σχέση με τον πελάτη της, η οποία θα τον κάνει να αισθάνεται πιο άνετα και ότι απολαμβάνει της ιδιαίτερης προσοχής που αναζητά. Ακόμη ιστορική ανάλυση των προσωπικών αυτών δεδομένων που συλλέγονται, μπορεί να βοηθήσει την επιχείρηση να ανακαλύψει την ταυτότητα των πιο προσοδοφόρων πελατών της (συνήθως το 20% των πελατών αποτελεί το 80% των πηγών εσόδων) και να προσαρμόσει τις υπηρεσίες της και τα προϊόντα της στις προτιμήσεις αυτών των πελατών. Παράλληλα, με αυτόν τον τρόπο αυξάνει την εμπιστοσύνη των πελατών της και ισχυροποιείται η διαπραγματευτική της δύναμη.^{116, 117}

-εύκολη χρήση: Η χρήση του διαδικτύου, παρά το γεγονός ότι αποτελεί νέα τεχνολογία, δεν κρίνεται ιδιαίτερα δύσκολη. Είναι φιλικό προς το χρήστη και αυτό συμβάλει στη γρήγορη εξοικείωσή του.

1.4 Παραβίαση ιδιωτικότητας στο διαδίκτυο

Παρά τα οφέλη που αποκομίζουν τόσο οι επιχειρήσεις όσο και οι καταναλωτές απ' τη χρήση του διαδικτύου, εγκυμονούν σοβαροί κίνδυνοι για τους καταναλωτές. Ο πιο σημαντικός είναι η παραβίαση της ιδιωτικότητας των χρηστών, που είναι εύκολη υπόθεση καθώς το διαδίκτυο αποτελεί ένα διεθνές δίκτυο χωρίς εθνικά σύνορα ,δεν βρίσκεται υπό την επιτήρηση κάποιου οργανισμού και μέσω αυτού διακινείται ένας τεράστιος όγκος πληροφοριών. Η δημιουργία αρχείων προσωπικών δεδομένων χρηστών είναι εξαιρετικά εύκολη. Πληροφορίες για πελάτες σε ηλεκτρονικά καταστήματα, για “κυβερνοναύτες” που αφήνουν προσωπικές πληροφορίες υπογράφοντας βιβλία επισκεπτών σε σελίδες π.χ. IP address, αλλά και η απλή περιπλάνηση στο διαδίκτυο, γίνονται αντικείμενα συλλογής και ανάλυσης δημιουργώντας πρότυπα καταναλωτών, τα οποία διατίθενται έναντι μεγάλης αμοιβής στους ενδιαφερόμενους. Σε πολλές μάλιστα περιπτώσεις, οι χρήστες δεν γνωρίζουν ότι συλλέγονται προσωπικά τους στοιχεία, τι είδους στοιχεία είναι αυτά και για ποιο σκοπό συλλέγονται, γεγονός που συνιστά κατάφορη παραβίαση της ιδιωτικότητάς τους.¹¹⁸

¹¹⁶ Γεωργόπουλος Β. Νικόλαος, “Ηλεκτρονικό Επιχειρείν, προγραμματισμός και σχεδίαση”, σελ 25-26

¹¹⁷ Karakaya Fahri, Charlton T. Earl, “Electronic Commerce: Current and Future Practices”,

www.emeraldinsight.com

¹¹⁸ Dr. Armgard von Reden, “Data Protection Activities in the Private Sector”, www.pco.org.com

Στην εποχή του διαδικτύου, υπάρχει ένας επικεφαλής, ο “διαχειριστής”, ο οποίος έχει την άνεση και τη δυνατότητα να “κρυφοκοιπά” και να καταγράφει τις κινήσεις των χρηστών στο internet, ή να διαβάζει μηνύματα που στέλνει ή δέχεται κάποιος στο ηλεκτρονικό του ταχυδρομείο. Απ’ τη στιγμή που χιλιάδες άνθρωποι έχουν πρόσβαση στο ηλεκτρονικό ταχυδρομείο μέσω ενός website, ο κάθε χρήστης έχει αποδεχθεί πως οι ιδιοκτήτες και διαχειριστές του site αυτού θα γνωρίζουν λεπτομέρειες για τη ζωή του (όσες τουλάχιστον έχει γράψει ο ίδιος ο χρήστης συμπληρώνοντας την ειδική φόρμα εγγραφής, συνήθως ονοματεπώνυμο, διεύθυνση, ηλικία, επάγγελμα), ενώ τα e-mail του αποθηκεύονται σε έναν κεντρικό server που είναι προσβάσιμος στον καθένα.¹¹⁹ Ακόμα όμως και αν κάποιος χρήστης δεν επιθυμεί να εγγραφεί σε κάποιο website, ακόμα και τότε το διαδίκτυο μπορεί να παρακολουθεί τις κινήσεις του καθώς “σερφάρει” στο διαδίκτυο, καταγράφοντας τις διευθύνσεις των sites που επισκέπτεται, τη διεύθυνση του ηλεκτρονικού του ταχυδρομείου, τα τεχνικά χαρακτηριστικά του υπολογιστή του κτλ, χωρίς μάλιστα να το γνωρίζει ο ίδιος ο χρήστης.

Επίσης αξίζει να αναφερθεί, ότι συχνά πολλά ελληνικά και μη websites ζητούν απ’ τους επισκέπτες τους να συμπληρώσουν κάποια προσωπικά τους στοιχεία προκειμένου να λάβουν ως αντάλλαγμα κάποιες δωρεάν υπηρεσίες. Ορισμένοι απ’ τους ιδιοκτήτες των sites δηλώνουν εξαρχής την πρόθεσή τους να αξιοποιήσουν τα προσωπικά δεδομένα που θα συγκεντρώσουν για διαφημιστικούς, εμπορικούς ή στατιστικούς σκοπούς, ζητώντας την υπογραφή μιας «σύμβασης». Χαρακτηριστικό είναι το παράδειγμα του site της Vodafone, όπου για να αποκτήσει κανείς τη δυνατότητα δημιουργίας μιας προσωπικής σελίδας με τις ειδήσεις που τον ενδιαφέρουν, θα πρέπει να δεχθεί μεταξύ άλλων πως η εταιρία «θα διατηρεί σε αρχείο και θα επεξεργάζεται τυχόν προσωπικά δεδομένα στις συνδεδεμένες με αυτή επιχειρήσεις, εφόσον τούτο επιβάλλεται για λόγους λειτουργικής ή μηχανογραφικής εξυπηρέτησης της συναλλακτικής σχέσης

¹¹⁹ Mohsen Attaran, Ilja VanLaar, “Privacy and security on the internet: how to secure your personal information and company data”, www.emeraldinsight.com

μας ή για στατιστικούς ή ιστορικούς λόγους» και πως «τα προσωπικά δεδομένα, συμπεριλαμβανομένων των στοιχείων συναλλακτικής συμπεριφοράς, επιτρέπεται να ανακοινώνονται προς τρίτους, με σκοπό την εκτέλεση συναλλαγών μέσω διατραπεζικών συστημάτων, την προστασία της τραπεζικής πίστης καθώς και τη διαφημιστική προβολή των προϊόντων της εταιρίας ή συνδεδεμένων με αυτή επιχειρήσεων, την έρευνα αγοράς ή άλλη παρόμοια δραστηριότητα...».^{120 121} Απ' το παραπάνω παράδειγμα, γίνεται λοιπόν σαφές ότι ένας απ' τους λόγους που οι επιχειρήσεις συλλέγουν προσωπικά δεδομένα χρηστών, είναι για διαφημιστικούς σκοπούς και συχνά προσβάλλουν την ιδιωτική τους ζωή.

¹²⁰ Σταμάτη Λαμπρινή, «Σερφάροντας στο internet αφήνουμε ίχνη που αποκαλύπτουν μυστικά...», 22/04/2000, <http://ta-nea.dolnet.gr>

¹²¹ Godwin J. Udo, «Privacy and security concerns as major barriers for e-commerce: a survey study», www.emeraldinsight.com

ΚΕΦΑΛΑΙΟ 2

Διαφήμιση στο διαδίκτυο

2.1 Εισαγωγή

Το διαδίκτυο αποτελεί ένα νέο μέσο διαφήμισης που έρχεται να συμπληρώσει τα συμβατικά μέσα διαφήμισης. Ένας απ' τους λόγους ανάπτυξης του διαδικτύου ως μέσου διαφήμισης, είναι η μεγάλη και γρήγορη εξάπλωσή του παγκοσμίως. Ένας άλλος λόγος είναι το μειωμένο κόστος σε σχέση με αντίστοιχες διαφημίσεις σε τηλεόραση και ραδιόφωνο, η δυνατότητα να προβάλλονται συνέχεια σε έναν μεγάλο αριθμό χρηστών απ' όλο τον κόσμο, η εύκολη ανάπτυξη διαφημίσεων συνδυάζοντας κείμενο, ήχο και γραφικά, η γρήγορη και ανέξοδη ενημέρωσή τους και τέλος η δυνατότητα δημιουργίας σχέσεων one-to-one με τους καταναλωτές.

Σύμφωνα με στοιχεία της ερευνητικής εταιρίας TNS Media Intelligence/CMR, οι δαπάνες για online διαφημίσεις το πρώτο εξάμηνο του 2003 σημείωσαν αύξηση στα 3,2 δις. δολάρια, έναντι 2,8 δις. του αντίστοιχου διαστήματος του 2002. Οι ετήσιοι ρυθμοί αύξησης των διαφημίσεων μέσω διαδικτύου προβλέπονται στο 12,7%, ανερχόμενες στα 18,9 δις δολάρια το 2008. Σε αντιδιαστολή, οι παγκόσμιες διαφημιστικές δαπάνες αυξάνονται περίπου μόνο κατά 5,3% ετησίως, και αναμένεται να αγγίξουν τα 412 δις δολάρια το 2008, έναντι δαπανών ύψους 318 δις δολαρίων του 2003 με τις τηλεοπτικές διαφημίσεις να αυξάνονται μόλις κατά 6,8% στο ίδιο χρονικό διάστημα.^{122, 123}

2.2 Μέθοδοι διαφήμισης στο διαδίκτυο

Οι μέθοδοι που χρησιμοποιούν οι επιχειρήσεις για να διαφημιστούν στο διαδίκτυο είναι οι εξής:

¹²² “Σε άνοδο οι online διαφημίσεις”, 2004, www.go-online.gr

¹²³ “Σε νέες τεχνολογίες στρέφεται η διαφήμιση”, 2004, www.go-online.gr

2.1.1 Πινακίδες (Banners)

Τα banners αποτελούν το πιο συχνά χρησιμοποιούμενο μέσο διαφήμισης στο διαδίκτυο. Είναι εικόνες γραφικών που εμφανίζονται σε ένα σημείο της ιστοσελίδας, όπως μια διαφημιστική καταχώριση σε μια εφημερίδα και όταν κάνει “κλικ” ο χρήστης πάνω σ’αυτά, τότε παραπέμπεται μέσω ενός συνδέσμου στην ιστοσελίδα του διαφημιζόμενου.¹²⁴ Το banner συνήθως τοποθετείται στην αρχή ή στο τέλος της ιστοσελίδας και κυρίως επιλέγονται σημεία τα οποία κοιτάει περισσότερο ο επισκέπτης όπως κοντά σε κουμπιά εντολών, σε χώρους εισαγωγής κειμένου για έρευνα ή ακόμη στα πλαϊνά τμήματα ενός κειμένου που θα διαβαστεί με προσοχή. Τα πλεονεκτήματα που προσφέρουν τα banners σαν μέσα διαφήμισης είναι ότι αφενός βοηθούν στην υλοποίηση του one-to-one Marketing, καθώς μπορούν να προσαρμοστούν στις ανάγκες του καταναλωτή που επισκέπτεται την ιστοσελίδα, αφετέρου προσφέρουν τη δυνατότητα στην επιχείρηση να μετράει σε ελάχιστο χρόνο την επιτυχία μιας διαφημιστικής καμπάνιας. Είναι δυνατόν ένας χρήστης του διαδικτύου να αναγνωρίζεται απ’ την ιστοσελίδα που επισκέπτεται και την ίδια στιγμή να προβάλλεται σε αυτόν ένα ειδικά σχεδιασμένο banner, το οποίο θα του προσελκύσει την προσοχή.¹²⁵

Οι διαφημιστικές εταιρίες μετρούν την αποτελεσματικότητα των banners απ’ το λεγόμενο “click-through” ratio rate, που δείχνει, όπως έχει ειπωθεί, τον αριθμό των clicks που κάνει ένας χρήστης στο banner σε σύγκριση με τον αριθμό των εμφανίσεων του banner στην ιστοσελίδα. Το ποσοστό αυτό αγγίζει μόλις το 1%, που σημαίνει ότι αν ένα banner εμφανιστεί σε μια σελίδα 100 φορές, ο χρήστης θα κάνει μόνο μια φορά click πάνω σ’ αυτό. Το γεγονός αυτό καταδεικνύει την εξαιρετικά μικρή αποτελεσματικότητα αυτού του είδους της διαφήμισης. Μάλιστα ο χρήστης όταν αναζητά κάποια πληροφορία σε μια ιστοσελίδα, αναλώνει το 92%

¹²⁴ Σε ορισμένες συμβάσεις, η διαφήμιση μέσω banner αμοιβάται ανάλογα με τον αριθμό των παραπομπών στη σελίδα του διαφημιζόμενου, «πληρωμή ανά κλικ»

¹²⁵ Janet Ryan, Nancy Whiteman, “Defining the Medium”, www.clickz.com

του χρόνου του ψάχνοντας σε κάποιο κείμενο της ιστοσελίδας για να την βρει, παρά σε κάποιο banner.

Το 1998 ο Benway σε μια έρευνα που διεξήγαγε, διαπίστωσε ότι οι χρήστες δεν δίνουν σημασία στα banners που έχουν εξαιρετικά έντονα χρώματα. Επίσης συμπέρανε ότι τα banners που βρίσκονται στα κάτω μέρος της ιστοσελίδας έχουν μεγαλύτερη επισκεψιμότητα σε σχέση με αυτά που βρίσκονται στην κορυφή της, αφού το “click-through” rate είναι 77% υψηλότερο στην περίπτωση αυτή. Τέλος αποδείχτηκε ότι τα “κινούμενα” banners έχουν κατά 15% μεγαλύτερη επισκεψιμότητα σε σχέση με τα “στατικά”.¹²⁶

2.2.2 Διαφήμιση αναδυόμενων παραθύρων

Με την είσοδο σε μια ιστοσελίδα αυτόματα ανοίγει ένα διαφημιστικό μήνυμα, με τη μορφή μικρού παραθύρου (pop-up & pop-under advertising).¹²⁷

2.2.3 Διαδικτυακές Πύλες (portal)

Οι διαδικτυακές πύλες είναι ιστοσελίδες που τις επισκέπτονται καθημερινά εκατομμύρια χρήστες. Η μεγάλη δημοτικότητα των διαδικτυακών πυλών έχει προκαλέσει μια αυξημένη ζήτηση των ιστοσελίδων τους για τοποθέτηση διαφημίσεων απ’ τις επιχειρήσεις. Σημαντικό παράγοντα επιλογής μιας πύλης για την τοποθέτηση διαφημίσεων από μια εταιρία, αποτελεί ο μέσος χρόνος παραμονής του κάθε επισκέπτη στην ιστοσελίδα της πύλης. Στην Ελλάδα τη μεγαλύτερη επισκεψιμότητα έχει η πύλη του in.gr με δεύτερο το flash.gr.¹²⁸

2.2.4 Splash screens

Τα splash screen είναι διαφημιστικά μηνύματα τα οποία εμφανίζονται κατά το νεκρό χρονικό διάστημα που μεσολαβεί μέχρι να εμφανιστεί το περιεχόμενο της ιστοσελίδας που επισκέπτεται ο χρήστης. Ωστόσο, δεν έχουν υψηλούς αριθμούς

¹²⁶ Michelle Bayles, ‘‘ Just how blind are we to advertising banners on the web?’’, www.usabilityviwes.com

¹²⁷ Ιγγλεζάκης Δ. Ιωάννης, ‘‘Το νομικό πλαίσιο του ηλεκτρονικού εμπορίου’’, σελ. 97

¹²⁸ Νικόλαος Β. Γεωργόπουλος, ό.π., σελ. 242

επισκεψιμότητας, καθώς οι περισσότεροι χρήστες του διαδικτύου διακόπτουν τη λειτουργία τους πριν εμφανιστεί το μήνυμα διότι πιστεύουν ότι μειώνουν την ταχύτητα μεταφοράς των δεδομένων. Επίσης χαρακτηρίζονται από πολλούς χρήστες ενοχλητικά, κυρίως στην περίπτωση όπου η εμφάνισή τους συνοδεύεται από την αυτόματη ενεργοποίηση της διαφημιζόμενης ιστοσελίδας.

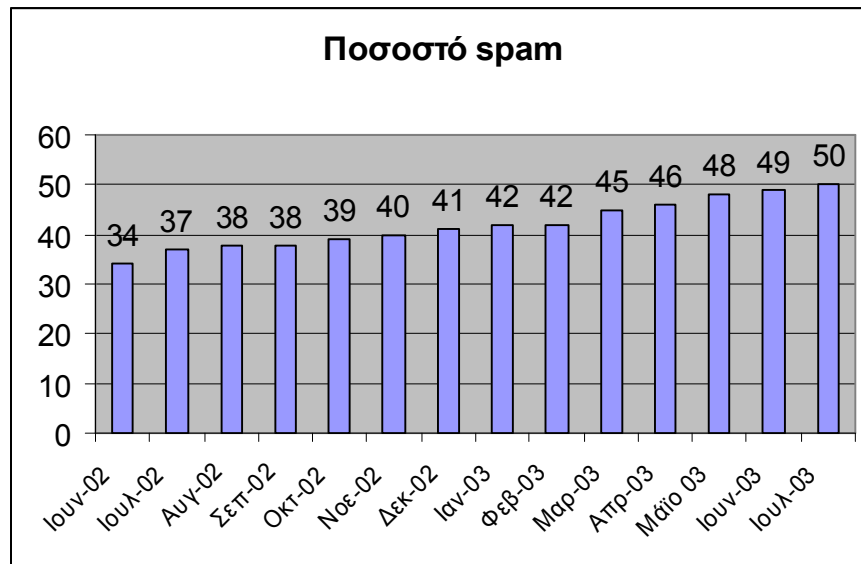
2.2.5 Χορηγία

Η σύγχρονη χορηγία δεν είναι ούτε δωρεά, ούτε φιλανθρωπία, ούτε ευεργεσία, αλλά είναι μια συνειδητή συναλλαγή κατά την οποία οι χορηγοί (εταιρείες) παρέχουν χρήματα, υπηρεσίες, και άλλα αγαθά, και σαν αντάλλαγμα περιμένουν από τους χορηγούμενους να τους υποστηρίξουν στους διάφορους σκοπούς τους, οι οποίοι κυρίως είναι επικοινωνιακοί με στόχο την προβολή του ονόματος, των προϊόντων, ή την προσέγγιση επαγγελματικών και κοινωνικών ομάδων.

2.2.6 Ηλεκτρονικό Ταχυδρομείο/ Μη αιτηθείσα εμπορική ηλεκτρονική επικοινωνία

Μια άλλη μορφή απ' ευθείας διαφήμισης και προώθησης προϊόντων, αποτελεί η αποστολή μη αιτηθέντων διαφημιστικών μηνυμάτων ηλεκτρονικού ταχυδρομείου, το επονομαζόμενο "spamming" ή "unsolicited bulk e-mail" ή αλλιώς "junk e-mail". Ειδικότερα, ως μη επιθυμητή ηλεκτρονική αλληλογραφία ορίζεται η μαζική συνήθως (συχνά άνω των 50,000 μηνυμάτων ηλεκτρονικού ταχυδρομείου) αποστολή του ίδιου (μη αιτηθέντος) μηνύματος ηλεκτρονικής αλληλογραφίας σε πολλούς αποδέκτες, για διαφημιστικούς σκοπούς. Αποδέκτες των μηνυμάτων αυτών μπορεί να είναι εκτός από μεμονωμένους χρήστες, και ομάδες συζητήσεων (newsgroup), στις οποίες συμμετέχει μεγάλος αριθμός χρηστών, ενώ ανεπιθύμητη αλληλογραφία αποστέλλεται πλέον και στα κινητά τηλέφωνα. Σήμερα η ανεπιθύμητη ηλεκτρονική αλληλογραφία αποτελεί το 50% των ηλεκτρονικών μηνυμάτων σε σύγκριση με το 7% το 2001 και το ποσοστό αυτό αυξάνεται συνεχώς. Το 2003 στάλθηκαν 4,9 τρις ηλεκτρονικά μηνύματα. Μάλιστα, το ποσοστό των πωλήσεων που είναι αποτέλεσμα «e-mail Mkt» κυμαίνεται μεταξύ 5-15% σε σύγκριση με αυτό των παραδοσιακών ταχυδρομικών

αποστολών που είναι μόνο 0,5-2%.¹²⁹ Ο παρακάτω πίνακας δείχνει το ποσοστό των ανεπιθύμητων ηλεκτρονικών μηνυμάτων ανά μήνα σε χρονική περίοδο ενός έτους. Παρατηρούμε λοιπόν ότι το ποσοστό αυτό βαίνει συνεχώς αυξανόμενο.¹³⁰



Η διαφημιζόμενη επιχείρηση δημιουργεί μια λίστα ηλεκτρονικών διευθύνσεων και μπορεί έτσι να στείλει μηνύματα στους καταναλωτές, ενημερώνοντάς τους για προσφορές ή νέα προϊόντα. Το ψηφιακό κατάστημα θα πρέπει να προσελκύσει τους καταναλωτές στην ιστοσελίδα του και στη συνέχεια να τους παρακινεί να εγγραφούν στη λίστα των επισκεπτών, προκειμένου να συλλέξει τις ηλεκτρονικές διευθύνσεις, καθώς επίσης και στοιχεία που θα το βοηθήσουν να σχεδιάσει τις μελλοντικές του διαφημιστικές καμπάνιες. Ένα κίνητρο που δίνουν οι εταιρίες στους χρήστες του διαδικτύου για να εγγραφούν στην ιστοσελίδα τους είναι η δωρεάν προσφορά πληροφοριακού υλικού ή ακόμη η παροχή εκπτώσεων σε προϊόντα/υπηρεσίες. Η προώθηση προϊόντων μέσω e-mail είναι πιο επιτυχής αν το περιεχόμενό τους είναι προσαρμοσμένο στις ανάγκες του κάθε καταναλωτή. Η εταιρία λοιπόν, μπορεί μέσω των στοιχείων που δίνει ο χρήστης κατά την εγγραφή του στην ιστοσελίδα (π.χ. καταναλωτικές προτιμήσεις, τρόπος ζωής, ηλικία, φύλο, εργασία ή ακόμα συγκεκριμένες περιοχές ενδιαφέροντος), να σκιαγραφήσει το προφίλ του κάθε εγγεγραμμένου και στη συνέχεια να

¹²⁹ Gauthronet Serge & Drouard Etienne, “Junk e-mail costs internet users euro 10 billion a year worldwide”, www.europa.eu.int

¹³⁰ Έκθεση του ΟΟΣΑ για το spam, ICCP(2003)10/Final,σελ. 5

διαμορφώσει το περιεχόμενο των μηνυμάτων σύμφωνα με τα ενδιαφέροντά του. Η εξατομίκευση των ηλεκτρονικών μηνυμάτων συμβάλλει στην επιτυχία της online διαφημιστικής καμπάνιας, εφόσον δημιουργείται κατά κάποιο τρόπο ένας διάλογος μεταξύ της εταιρίας και του καταναλωτή. Βέβαια είναι αδύνατον να γράφεται κάθε φορά ένα ξεχωριστό μήνυμα για κάθε πελάτη. Αυτό είναι εφικτό μόνο με τη χρήση του κατάλληλου λογισμικού. Ορισμένες τεχνικές που βοηθούν σε αυτή την κατεύθυνση είναι η εξατομίκευση του φακέλλου, δηλαδή το ηλεκτρονικό μήνυμα να μην έχει αποστολέα το όνομα της επιχείρησης αλλά κάποιο εργαζόμενο σε αυτή, ενώ επίσης να αναγράφεται το όνομα του παραλήπτη (π.χ. George@xyz.com και όχι Recipients of the abc newsletter). Επίσης πρέπει να αναφερθεί ότι η αποστολή μη αιτηθείσας ηλεκτρονικής αλληλογραφίας είναι ένα σημαντικό εργαλείο του σύγχρονου Mkt, καθώς το κόστος της αποστολής του είναι πολύ χαμηλό και μάλιστα είναι το ίδιο είτε η αποστολή γίνεται στο εσωτερικό είτε στο εξωτερικό.^{131, 132}

Έχει υπολογιστεί ότι κοστίζει σε μια επιχείρηση 0,05-1\$ η αποστολή spam και το κόστος αυτό δεν διαφοροποιείται ανάλογα με την απόσταση. Επίσης το οριακό κόστος αποστολής τέτοιων μηνυμάτων είναι πολύ χαμηλό, γεγονός που επιτρέπει στους spammers να έχουν υψηλά κέρδη, αφού ακόμη και ένα μόνο μήνυμα να έχει ανταπόκριση, ο spammer θα καλύψει το κόστος της διαφημιστικής του εκστρατείας και θα έχει κέρδος. Επομένως όσο πιο πολλά email στείλει μια επιχείρηση, τόσο μεγαλύτερο θα είναι το κέρδος της αφού το κόστος αποστολής των ηλεκτρονικών μηνυμάτων μένει σχεδόν σταθερό.

Παρ' όλο που το ποσοστό απόδοσης της ανεπιθύμητης ηλεκτρονικής αλληλογραφίας είναι αρκετά χαμηλό, περίπου 0,001%, το κέρδος είναι υψηλό. Αν υποθεθεί ότι η αποστολή 3,5 εκατ. μηνυμάτων έχει ως αποτέλεσμα 81 πωλήσεις και ότι η κάθε πώληση έχει αξία 19\$, τότε τα έσοδα είναι 1500\$ την πρώτη εβδομάδα. Το κόστος της αποστολής των μηνυμάτων εκτιμάται ότι είναι λιγότερο

¹³¹ Γεωργόπουλος Β. Γεώργιος, ό.π.,σελ. 238

¹³² Lilian Edward, "Consumer Privacy, On-line Business and the Internet: Looking for Privacy in all the Wrong Places", International Journal of Law and Information Technology, Vol.11 No3, Oxford University Press 2003

από 100\$ ανά εκατομμύριο μηνύματα. Έτσι, αν υποθεθεί ότι η εταιρία αποστέλλει 100 εκατ. μηνύματα, θα έχει κέρδος πάνω από 25,000\$.

Οι τρόποι με τους οποίους ένας spammer μπορεί να συλλέξει ηλεκτρονικές διευθύνσεις για την αποστολή ηλεκτρονικών μηνυμάτων είναι οι εξής¹³³:

- Το ίδιο το άτομο προμηθεύει τον spammer με την ηλεκτρονική του διεύθυνση
- Τρίτο μέρος προμηθεύεται τη διεύθυνση από το ίδιο το άτομο και στη συνέχεια την πουλάει στον spammer
- Οι spammers “ψαρεύουν” ηλεκτρονικές διευθύνσεις από ιστοσελίδες, καταλόγους ή ομάδες συζητήσεων
- Τρίτο μέρος που “ψαρεύει” ηλεκτρονικές διευθύνσεις από δημόσιους χώρους και τις πουλάει στους spammers
- Οι spammers χρησιμοποιούν μεθόδους τυχαίας εύρεσης ηλεκτρονικών διευθύνσεων

2.3 Γνώση του προφίλ των πελατών για αποτελεσματικό spamming

Όπως αναφέρθηκε προηγουμένως, για να είναι πιο αποδοτική και αποτελεσματική μια διαφήμιση, πρέπει να στοχεύει σε συγκεκριμένες ομάδες καταναλωτών καθώς οι καταναλωτές χρησιμοποιούν το διαδίκτυο κατά κύριο λόγο για τη δυνατότητά του να προσφέρει πληροφορίες και επομένως ανταποκρίνονται σε μεγαλύτερο βαθμό σε διαφημίσεις που καλύπτουν τις δικές τους ανάγκες. Για να ανταποκριθούν καλύτερα στις απαιτήσεις των καταναλωτών οι διαφημίσεις, οι εταιρίες συλλέγουν προσωπικά τους στοιχεία, τα επεξεργάζονται, φτιάχνουν το προφίλ τους και στη συνέχεια προσαρμόζουν το περιεχόμενο του διαφημιστικού μηνύματος στις ανάγκες και τις επιθυμίες τους. Οι εταιρίες χρησιμοποιούν διάφορα εργαλεία για τη συλλογή προσωπικών στοιχείων των “κυβερνοναυτών”, όπως είναι τα εξής:

A) Cookies

¹³³ Έκθεση του ΟΟΣΑ για το spam, ICCP(2003)10/Final σελ. 9

Το cookie είναι ένα απλό πρόγραμμα που αυτο-εγκαθίσταται στον τοπικό υπολογιστή του χρήστη κατά τη διάρκεια επίσκεψής του σε μια ιστοσελίδα. Πρόκειται ουσιαστικά για μηχανισμό “κατασκοπείας” που καταγράφει όλες τις κινήσεις του χρήστη. Τα προγράμματα αυτά παρέχουν τη δυνατότητα καταγραφής των δραστηριοτήτων του χρήστη απ’ ευθείας απ’ το σκληρό δίσκο του υπολογιστή του. Μπορούν δηλαδή να καταγράψουν τις σελίδες που έχει επισκεφθεί ο χρήστης, τις διαφημίσεις που διάβασε, τα προϊόντα που είναι τοποθετημένα στο καλάθι των αγορών του, τον αριθμό αναγνώρισής του κτλ.

Τα cookies βρίσκονται σε πολλά σχήματα και μεγέθη. Μπορούν να περιέχουν μεγάλη ποσότητα πληροφοριών, όπως όλα τα περιεχόμενα ενός εμπορικού καταστήματος ή απλώς ένα αυθαίρετο αριθμό αναγνώρισης που ο εξυπηρετητής του Ιστού μπορεί να χρησιμοποιήσει για να διαχωρίσει ένα χρήστη από κάποιον άλλο. Τα cookies έχουν ημερομηνία λήξης. Μπορούν να οριστούν ώστε να λήξουν μόλις παραιτηθεί ο χρήστης απ’ το φυλλομετρητή ή μπορεί να τους δοθεί ημερομηνία λήξης κάποια στιγμή στο μέλλον. Τα cookies που εξαφανίζονται μόλις παραιτηθεί ο χρήστης απ’ το φυλλομετρητή καλούνται “προσωρινά” ανώ αυτά που παραμένουν μεταξύ περιόδων φυλλομέτρησης καλούνται “επίμονα”.

Είναι επίσης τεχνικά δυνατόν ένας server να επιτρέψει την πρόσβαση στις πληροφορίες που συνέλεξε το “cookie” σε απεριόριστο αριθμό άλλων servers. Με αυτόν τον τρόπο οι διαφημιστικές εταιρίες έχουν τη δυνατότητα να παρακολουθήσουν τον επισκέπτη απ’ τη μια τοποθεσία στην άλλη, συλλέγοντας πληροφορίες για τις προσωπικές του συνήθειες, τις οποίες στη συνέχεια επεξεργάζονται, προκειμένου να σχεδιάσουν τα κατάλληλα διαφημιστικά μηνύματα. Ωστόσο τα cookies δεν μπορούν να καταγράψουν δεδομένα όπως το όνομα ή την ηλεκτρονική διεύθυνση του χρήστη. Οι εταιρίες όμως που ειδικεύονται στο χώρο όπως η Doubleclick και άλλες, μπορούν να συγκεντρώσουν τέτοιου είδους δεδομένα μέσω των ιστοσελίδων των μελών τους. Εάν λοιπόν, ένας χρήστης δώσει οικειοθελώς τα προσωπικά του στοιχεία σε site το οποίο ανήκει σε ένα δίκτυο των παραπάνω εταιριών, τότε είναι δυνατόν να ταυτιστεί το όνομα του χρήστη με τον αριθμό αναγνώρισης που έχει δοθεί απ’ το

διακομιστή και στη συνέχεια η πληροφορία αυτή να διαδοθεί προς όλα τα μέλη του δικτύου δυστυχώς εν αγνοία του χρήστη.¹³⁴

Επίσης οι εταιρίες άμεσης εμπορικής προώθησης θέτουν διαφημιστικές καταχωρίσεις στις ιστοσελίδες και με τη χρήση προγραμμάτων cookies που δεν γίνονται αντιληπτά από το χρήστη, παρακολουθούν τις κινήσεις του. Μόλις ο χρήστης διαβάσει τη διαφήμιση δίδεται εν αγνοία του εντολή στον browser να μεταβιβάσει αυτόματα διάφορα στοιχεία του χρήστη, τη διεύθυνση της ιστοσελίδας όπου βρίσκεται η διαφήμιση κ.α. Με συνδυασμό όλων αυτών των στοιχείων οι εταιρίες άμεσης εμπορικής προώθησης δημιουργούν όχι μόνο αρχεία πελατών αλλά και αρχεία με την πλήρη καταναλωτική συμπεριφορά του χρήστη. Σε πολλές περιπτώσεις μάλιστα, τα αρχεία αυτά είναι το μόνο περιουσιακό στοιχείο των επιχειρήσεων και συχνά γίνονται εξαγορές ή συγχωνεύσεις εταιριών με μόνο σκοπό την απόκτηση αυτών των πελατολογίων, εν αγνοία των υποκειμένων στα οποία αφορούν τα προσωπικά δεδομένα. Χαρακτηριστικό είναι το παράδειγμα της Doubleclick, η οποία το 1999 εξαγόρασε τη βάση δεδομένων Abacus Direct, στην οποία περιέχονται πληροφορίες για τη συναλλακτική συμπεριφορά του 90% των αμερικανικών νοικοκυριών και είχε σκοπό να συσχετίσει τα δεδομένα αυτά με τα δικά της αρχεία cookies. Ωστόσο μετά από προσφυγή, την οποία κατέθεσε η οργάνωση EPIC (Κέντρο προστασίας της ιδιωτικής ζωής) στην Αμερικάνικη Ομοσπονδιακή Επιτροπή Εμπορίου, ακολούθησε δημόσια κατακραυγή κατά των σχεδίων αυτών και έτσι η παραπάνω εταιρία ανακοίνωσε ότι ματαιώνει τα σχέδιά της.^{135, 136, 137}

B) Πρωτόκολλο HTTP

Με τη χρήση του πρωτοκόλλου αυτού, όταν ο χρήστης επιθυμεί να επισκεφθεί μια διεύθυνση ιστοσελίδας, καταγράφονται εκτός απ' τη διεύθυνση, και άλλες πληροφορίες που συνήθως καλούνται πληροφορίες επικεφαλίδας. Επίσης

¹³⁴ Stephen Walther, Jonathan Levine, "Εγχειρίδιο προγραμματισμού e-commerce με ASP", σελ.47

¹³⁵ Γιαννόπουλος Ν. Γιώργος, ό.π., σελ.127

¹³⁶ Godwin J. Udo, "Privacy and security concerns as major barriers for e-commerce: a survey study", www.emeraldinsight.com

¹³⁷ Σταμάτη Λαμπρινή, "Σερφάροντας στο internet αφήνουμε ίχνη που αποκαλύπτουν μυστικά", 22/04/2000 <http://ta-nea.dolnet.gr>

καταγράφονται οι ιστοσελίδες που επισκέφθηκε ο χρήστης, τα αρχεία που διάβασε ή αντέγραψε, οι διαδρομές έρευνας που ακολούθησε κλπ. Η ανωτέρω καταγραφή των ιχνών πραγματοποιείται σε όλα τα επίπεδα, δηλαδή, α)τοπικά στον προσωπικό υπολογιστή του χρήστη β) στους υπολογιστές των παρόχων υπηρεσιών διαδικτύου.

Γ) Έλεγχος της διεύθυνσης IP (Internet Protocol Address)

Με μια διεύθυνση IP, χαρακτηρίζεται κάθε υπολογιστικό μηχάνημα που είναι συνδεδεμένο στο διαδίκτυο, αποτελεί δηλαδή την ταυτότητα του μηχανήματος. Χάρη στην ταυτότητα αυτή ο πάροχος υπηρεσιών internet έχει τη δυνατότητα να γνωρίζει τις ακριβείς λεπτομέρειες όλων των πληροφοριών που διακινήθηκαν μέσω της διεύθυνσης IP (π.χ. ώρα και ημερομηνία σύνδεσης, ιστοσελίδες που αναζητήθηκαν, τα ηλεκτρονικά μηνύματα κτλ). Εάν η διεύθυνση αυτή ταυτιστεί με συγκεκριμένο χρήστη, ο πάροχος υπηρεσιών internet μπορεί να βρει τις ιστοσελίδες που επισκέφθηκε ο χρήστης, την ώρα και την ημερομηνία των επισκέψεων, τα αρχεία που ανέσυρε, τη συμμετοχή σε chat rooms και τέλος την αποστολή και λήψη e-mails. Μ' αυτόν τον τρόπο οι εταιρίες μπορούν να δημιουργήσουν το προφίλ του κάθε χρήστη και να του απευθύνουν συγκεκριμένα διαφημιστικά μηνύματα, κατάλληλα προσαρμοσμένα στις απαιτήσεις του.

Δ) Δημόσιοι Κατάλογοι

Επίσης οι εταιρίες μπορούν να συλλέξουν προσωπικά δεδομένα χρηστών από ιδιωτικούς και δημόσιους καταλόγους στο internet, χωρίς τη γνώση του υποκειμένου. Στη περίπτωση των ιδιωτικών καταλόγων, μια εταιρία μπορεί να αγοράσει το πελατολόγιο μιας άλλης εταιρίας προκειμένου να αποκτήσει τα προσωπικά στοιχεία των πελατών. Αντιθέτως, στην περίπτωση των δημοσίων καταλόγων, μια επιχείρηση μπορεί να έχει πρόσβαση σε δημόσια αρχεία όπως π.χ. τηλεφωνικούς καταλόγους ή καταλόγους φοιτητών κτλ.^{138, 139}

¹³⁸ Carlos Rodriguez Casal, 'Regulating Spam: opting in or opting out?', www.emeraldinsight.com

¹³⁹ Γιαννόπουλος Ν. Γιώργος,ό.π., σελ. 126

2.4 Επεξεργασία δεδομένων με μεθόδους εξόρυξης δεδομένων

Μετά τη συλλογή των προσωπικών δεδομένων των χρηστών ακολουθεί το στάδιο της επεξεργασίας τους. Μια καινούρια τεχνολογία που χρησιμοποιείται για το σκοπό αυτό, είναι η εξόρυξη δεδομένων (data mining). Τα εργαλεία εξόρυξης δεδομένων χρησιμοποιούνται απ' τις επιχειρήσεις όλων των επιχειρηματικών κλάδων, όπως π.χ. τηλεπικοινωνιακοί οργανισμοί, κατασκευαστές, αεροπορικές εταιρίες, λιανέμποροι κτλ, για να αποκαλύψουν ωφέλιμα υποδείγματα και συσχετίσεις των συλλεγμένων δεδομένων.. Συγκεκριμένα, στην περίπτωση των λιανέμπορων μια αποτελεσματική εφαρμογή εξόρυξης δεδομένων είναι η ανάλυση του καλαθιού αγοράς, όπου αναλύονται τα χαρακτηριστικά του καλαθιού αγορών των καταναλωτών και στη συνέχεια τα αποτελέσματα χρησιμοποιούνται για τη δημιουργία περισσότερο αποτελεσματικών προωθήσεων προϊόντων και διαφημιστικών εκστρατειών.

Οι μέθοδοι εξόρυξης δεδομένων μπορούν γενικά να διαχωριστούν σε δύο κατηγορίες. Η πρώτη χρησιμοποιεί στατιστικά μοντέλα με τη βοήθεια των οποίων τα εργαλεία εξόρυξης αποτιμούν στατιστικές υποθέσεις και στη συνέχεια ελέγχουν και παρουσιάζουν αποτελέσματα. Η δεύτερη κατηγορία κάνει χρήση μεθόδων τεχνητής νοημοσύνης, όπου τα εργαλεία εξόρυξης προσδιορίζουν τις παραμέτρους ενός μοντέλου με συνεχή εκπαίδευσή τους πάνω σε πραγματικά δεδομένα.

Οι επιχειρήσεις με τη βοήθεια της τεχνολογίας αυτής, χρησιμοποιούν αποτελεσματικότερα τις πολυέξοδες βάσεις δεδομένων τους, μετατρέποντας μη δομημένα στοιχεία σε πολύτιμες πληροφορίες. Κύρια παραδείγματα αυτών, αποτελούν η επίλυση προγνωστικών προβλημάτων και η έρευνα άγνωστων χαρακτηριστικών της καταναλωτικής συμπεριφοράς των πελατών. Επίσης, η εξόρυξη δεδομένων προσφέρει λύσεις σε προβλήματα διαφήμισης προϊόντων,

όπου η επιχείρηση με μεγαλύτερη ακρίβεια μπορεί να επιλέξει τους καταναλωτές που θα έχουν μεγαλύτερη ανταπόκριση.¹⁴⁰

2.5 Δυσμενείς συνέπειες του spamming - τεχνικά μέτρα αντιμετώπισης

Στην προηγούμενη ανάλυση, έγινε λόγος για τον τρόπο με τον οποίο οι επιχειρήσεις συλλέγουν και επεξεργάζονται προσωπικά δεδομένα χρηστών στο internet, προκειμένου να τους απευθύνουν προσωποποιημένα διαφημιστικά μηνύματα που θα έχουν μεγαλύτερη αποτελεσματικότητα. Αναφέρθηκε επίσης ότι ένα πολύ δημοφιλές για τις επιχειρήσεις μέσο διαφήμισης είναι το spamming καθώς και τα οφέλη που επιφέρει σ' αυτές. Ωστόσο η ανεπιθύμητη ηλεκτρονική αλληλογραφία δημιουργεί προβλήματα σε τρεις κυρίως κατηγορίες προσώπων¹⁴¹:

- 1) Στους απλούς χρήστες του ηλεκτρονικού ταχυδρομείου
- 2) Στους διαχειριστές δικτύου
- 3) Σε τρίτα πρόσωπα

Συγκεκριμένα, οι χρήστες e-mail υφίστανται κατ' αρχήν απώλεια χρόνου προκειμένου να ελέγξουν ανεπιθύμητα e-mail στην ηλεκτρονική τους θυρίδα και να διαχωρίσουν τα «γνήσια» μηνύματα απ' τις άχρηστες διαφημίσεις. Αν υποθέσουμε ότι οι χρήστες internet παγκοσμίως είναι περίπου 900εκ. και ότι 200 φορείς εμπορικής προώθησης μέσω ηλεκτρονικού ταχυδρομείου θα αποκτήσουν αργά ή γρήγορα μηχανές ικανές να διαβιβάζουν 100εκ. μηνύματα την ημέρα, τότε θα στέλνονται μέσω του διαδικτύου 20δισ. μηνύματα την ημέρα, που σημαίνει ότι αντιστοιχούν 22 μηνύματα ανά χρήστη. Αυτό αντιπροσωπεύει μισή ώρα τηλεφόρτωσης με την τρέχουσα τεχνολογία, χωρίς να ληφθεί υπόψη το γεγονός ότι τα εμπορικά ηλεκτρονικά μηνύματα εμπεριέχουν όλο και περισσότερο φωτογραφικό ή και οπτικοακουστικό υλικό. Το 65% των χρηστών δαπανούν περισσότερο από δέκα λεπτά την ημέρα προκειμένου να διαβάσουν και να

¹⁴⁰ Γεωργόπουλος Β. Νικόλαος,ό.π., σελ.247

¹⁴¹ Ιγγλεζάκης Δ. Ιωάννης, ό.π., σελ.112

διαγράφουν τα spam mail και το 24% των χρηστών αφιερώνει πάνω από είκοσι λεπτά την ημέρα.

Εκτός απ' το πρόβλημα της απώλειας χρόνου, οι χρήστες αντιμετωπίζουν και υψηλό κόστος. Αν υποθεθεί ότι ένας μέσος χρήστης ο οποίος έχει μια συνδρομή με κάποιον Παροχέα Υπηρεσιών Διαδικτύου (ISP) δώδεκα ευρώ για δέκα ώρες σύνδεσης το μήνα και συνήθη εξοπλισμό και ότι μπορεί να φορτώσει περίπου 180kb το λεπτό, φτάνουμε σε ένα κόστος το οποίο στη χειρότερη περίπτωση αντιπροσωπεύει τριάντα ευρώ το χρόνο για τη φόρτωση δεκαπέντε περίπου μηνυμάτων την ημέρα, δηλαδή συνολικού μεγέθους μεταξύ 500 και 800kb. Αν αυτό πολλαπλασιαστεί με τον αριθμό των χρηστών του διαδικτύου μιας δεδομένης χώρας, το συνολικό κόστος είναι ιδιαίτερα σημαντικό.¹⁴² Σε παγκόσμιο επίπεδο, αν ληφθεί υπόψη ότι ο συνολικός αριθμός των χρηστών είναι 900εκ, τότε η φόρτωση διαφημιστικών μηνυμάτων εκτιμάται ότι θα κοστίζει στους χρήστες είκοσιεπτά δις. ευρώ.¹⁴³

Επίσης, μια πολύ σημαντική δυσμενής συνέπεια του spamming για τους χρήστες, είναι η παραβίαση της ιδιωτικής τους ζωής, καθόσον με την εισβολή στην ιδιωτική σφαίρα παραβιάζεται το δικαίωμά τους στη μόνωση και το δικαίωμά τους να μην γίνονται αποδέκτες πληροφοριών εφόσον δεν το επιθυμούν. Ειδικότερα η συλλογή και η εμπορία ηλεκτρονικών διευθύνσεων χρηστών με σκοπό την αποστολή των μηνυμάτων, δημιουργεί ζήτημα προστασίας της ιδιωτικότητας, αφού η συλλογή ηλεκτρονικών διευθύνσεων που συνιστούν προσωπικά δεδομένα, παραβιάζει την ιδιωτική ζωή των χρηστών. Συχνά μάλιστα οι χρήστες, χάνουν την εμπιστοσύνη τους στο διαδίκτυο και αρνούνται να συμμετάσχουν σε forums ή Usenet groups, απ'το φόβο τους μήπως κάποιοι spammers "ψαρέψουν" τις ηλεκτρονικές τους διευθύνσεις.¹⁴⁴ Πρέπει να ειπωθεί ότι η συλλογή των διευθύνσεων των χρηστών γίνεται συνήθως χωρίς γνώση τους και κυρίως χωρίς να έχουν δώσει τη συγκατάθεσή τους. Τα

¹⁴² "Πόσο κοστίζει η ανεπιθύμητη ηλεκτρονική αλληλογραφία", www.go-online.gr

¹⁴³ Gauthronet Serge & Drouard Etienne, "Junk e-mail costs internet users euro 10 billion a year worldwide", www.europa.eu.int

¹⁴⁴ Κομνηνός Γ. Κόμνιος, "Η ανεπιθύμητη εμπορική ηλεκτρονική αλληλογραφία (spamming)", ΕπισκΕΔ Δ/2002, σελ.1009

προγράμματα συλλογής είναι αρκετά απλά στη χρήση τους. Λειτουργούν βάσει της αρχής της αυτόματης περιόδευσης σε ιστοχώρους και δημόσιους χώρους του Usenet χρησιμοποιώντας είτε ένα κατάλογο URL που έχει οριστεί εκ των προτέρων, είτε λέξεις κλειδιά σε μηχανές αναζήτησης που θα επιτρέψουν τη δημιουργία ενός καταλόγου συναφών URL. Στη συνέχεια, το λογισμικό συλλέγει συστηματικά όλες τις ηλεκτρονικές διευθύνσεις που βρίσκονται στις σελίδες αυτών των χώρων ή των ομάδων συζήτησης.

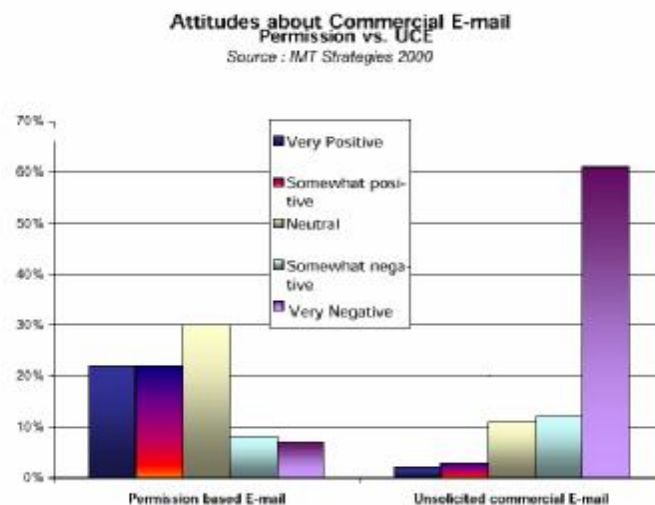
Απ'την άλλη πλευρά, η πρακτική αποστολής τεράστιου αριθμού e-mail δημιουργεί σοβαρό πρόβλημα στους διαχειριστές δικτύων. Σύμφωνα με εμπειριστατωμένες μελέτες, η αποστολή spam mail αυξάνει σημαντικά το κόστος διαχείρισης ενός δικτύου, αν μάλιστα σκεφτεί κανένας ότι περίπου το 14% των e-mails είναι spamming. Υπάρχει ανάγκη για διαρκείς αναβαθμίσεις, έξοδα συντήρησης του δικτύου καθώς και κόστος επένδυσης σε τεχνολογίες φιλτραρίσματος των ηλεκτρονικών μηνυμάτων (οι οποίες συχνά μπλοκάρουν μηνύματα που δεν συνιστούν spam mails). Επίσης, ο αυξημένος όγκος των μηνυμάτων μπορεί να μειώσει την ταχύτητα του internet και να υπερφορτώσει τους e-mail servers. Οι Παροχείς Υπηρεσιών Διαδικτύου χρειάζονται πόρους σε ανθρώπινο δυναμικό προκειμένου να αντιμετωπίσουν το spamming σε τεχνικό επίπεδο και να απαντήσουν στα παράπονα των συνδρομητών για τη λήψη ανεπιθύμητων μηνυμάτων. Συνολικά, το κόστος που αντιμετωπίζουν οι διαχειριστές του διαδικτύου υπολογίζεται πάνω από \$500εκ.¹⁴⁵

Μια τελευταία ομάδα προσώπων που προσβάλλονται απ' το spamming είναι οι τρίτοι, των οποίων οι ηλεκτρονικές διευθύνσεις πλαστογραφούνται και χρησιμοποιούνται συχνά στη θέση του αποστολέα προκειμένου να αποπροσανατολίσουν τον χρήστη και να συγκαλύψουν τα spam mails. Σε πολλές περιπτώσεις δηλαδή, οι spammers στέλνουν μηνύματα χρησιμοποιώντας τις διευθύνσεις άλλων επιχειρήσεων χωρίς να έχουν τη συγκατάθεσή τους, με αποτέλεσμα να προκαλείται ζημιά στη φήμη των εταιριών αυτών.¹⁴⁶

¹⁴⁵ Gauthronet Serge & Drouard Etienne, "Junk e-mail costs internet users euro 10 billion a year worldwide", www.europa.eu.int

¹⁴⁶ Έκθεση του ΟΟΣΑ για το spam, ICCP(2003)10/Final, σελ. 15

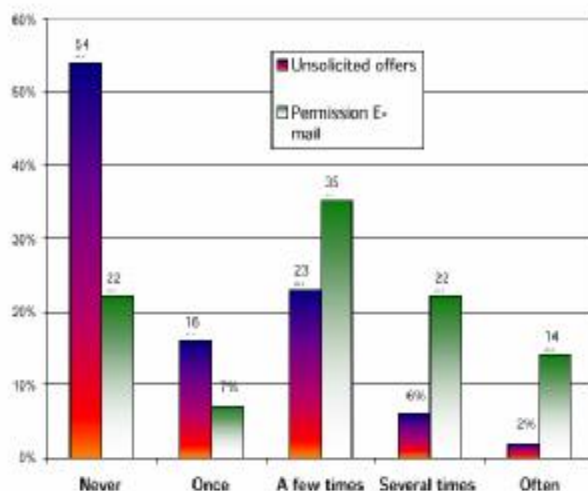
Χαρακτηριστική είναι η αντίδραση των χρηστών του διαδικτύου στην αποστολή spam. Σε μια έρευνα που πραγματοποιήθηκε απ' την αμερικάνικη εταιρία IMT (Integrating Marketing and Technology) σε 400 χρήστες internet, διαπιστώθηκε ότι οι αποδέκτες ανεπιθύμητης ηλεκτρονικής αλληλογραφίας δυσανασχετούν στη λήψη τέτοιων μηνυμάτων και πολύ λίγοι είναι αυτοί που ανταποκρίνονται. Τα παρακάτω σχήματα δείχνουν εμφανώς το συμπέρασμα της έρευνας.¹⁴⁷



Απ' το παραπάνω σχήμα βλέπουμε ότι πάνω απ' το 60% των αποδεκτών spam είναι δυσανεκτοί, ενώ μόλις ένα ποσοστό γύρω στο 2-3% έχουν διαμορφώσει μια πολύ θετική εντύπωση. Αντιθέτως, ένα αρκετά μεγάλο ποσοστό έχουν θετική άποψη για τη λήψη διαφημιστικών μηνυμάτων με προηγούμενη συναίνεσή τους (40%).

¹⁴⁷ Serge Gauthronet, Etienne Drouard, "Unsolicited Commercial Communications and Data Protection", www.europa.eu.int

Frequency of E-mail response



Δεν εκπλήσσει το γεγονός ότι οι καταναλωτές ανταποκρίνονται σε μεγαλύτερο βαθμό στα μηνύματα που δέχονται με τη συγκατάθεσή τους, καθώς το 70% των χρηστών κάνει “κλίκ” συχνά, ή ορισμένες φορές, ή λίγες φορές σε τέτοιου είδους μηνύματα, σε αντίθεση με το 30% στην περίπτωση των spams.¹⁴⁸

Για την αποτροπή των προβλημάτων που προκύπτουν απ’ την αποστολή μη επιθυμητής ηλεκτρονικής αλληλογραφίας, επιστρατεύονται διάφορα τεχνικά μέσα όπως π.χ. προγράμματα Η/Υ που διαθέτουν λειτουργίες “φιλτραρίσματος” των ανεπιθύμητων μηνυμάτων ή τα μπλοκάρουν. Ωστόσο όμως, οι λύσεις αυτές δεν είναι πάντοτε αποτελεσματικές, διότι οι αποστολείς μπορούν και παρακάμπτουν τους μηχανισμούς αυτούς. Ένα τέτοιο πρόγραμμα είναι το Outlook της Microsoft, το οποίο παρέχει τη δυνατότητα αποκλεισμού ορισμένων αποστολέων και μ’ αυτόν τον τρόπο ο χρήστης μπορεί να περιορίσει τον αριθμό των εισερχομένων spam mails και να τα διαχειριστεί καλύτερα, εφόσον γνωρίζει την ηλεκτρονική διεύθυνση του αποστολέα τους. Η λύση αυτή όμως δεν είναι ριζική καθότι οι spammers χρησιμοποιούν πλαστές ηλεκτρονικές διευθύνσεις αποστολέα ή διαφορετική ηλεκτρονική διεύθυνση για κάθε αποστολή (spoofing).

¹⁴⁸ IMT: "Permission E-mail: The Future of Direct Marketing", www.imtstrategies.com

Η πιο αποτελεσματική πρακτική ωστόσο είναι ο ίδιος ο χρήστης να αναφέρει τον spammer στην εταιρία παροχής υπηρεσιών internet που χρησιμοποιεί. Προτού φθάσει στα “Εισερχόμενα”, κάθε e-mail περνά από ένα διακομιστή (server). Οι περισσότεροι διακομιστές δεν επιθυμούν να χρησιμοποιούνται τα μηχανήματά τους για αποστολή spam. Συνήθως, η πολιτική των παροχών υπηρεσιών διαδικτύου απαγορεύει την αποστολή spam μέσω των λογαριασμών τους. Μόλις ενημερωθούν ότι γίνεται κακή χρήση συγκεκριμένου λογαριασμού, απενεργοποιούν το λογαριασμό του παραβάτη. Ο χρήστης πρέπει να μάθει το “domain” του αποστολέα (δηλαδή το κομμάτι της διεύθυνσης μετά το σύμβολο @) και στη συνέχεια να στείλει ολόκληρο το μήνυμα στη διεύθυνση abuse@kapoio-domain.com. Δεδομένου ότι οι spammers χρησιμοποιούν καταλόγους στους οποίους περιέχονται όσοι τους προκαλούν προβλήματα, αν ο χρήστης καταγγείλει 3-4 περιπτώσεις, ίσως διαπιστώσει μείωση του spam στο λογαριασμό του. Πολλές εταιρίες παροχής υπηρεσιών internet έχουν ήδη ενσωματώσει στα συστήματά τους ανάλογο λογισμικό προστασίας. Σε αυτές τις περιπτώσεις ο παραλήπτης παραλαμβάνει κανονικά το μήνυμα, με την ένδειξη “Possible Spam” πριν απ’ το θέμα του e-mail. Η Microsoft, το 2004, εξέδωσε νέα windows, τα οποία προλαμβάνουν τη λήψη spam mail, καθώς εγκρίνονται μόνο εκείνα τα μηνύματα που συμφωνούν με τις προδιαγραφές που έχει ορίσει ο ίδιος ο χρήστης.¹⁴⁹

2.6 Τρόποι ρύθμισης του spam: opt in - opt out

Ένας τρόπος ρύθμισης του spam, προκειμένου να μην παραβιάζει την ιδιωτική σφαίρα του αποδέκτη του, είναι τα συστήματα opt in & opt out. Το κριτήριο που διαχωρίζει τις δύο αυτές έννοιες, είναι το είδος συγκατάθεσης του ατόμου στην αποστολή spam mails απ’ τις επιχειρήσεις. Σε ένα opt in σύστημα, η εταιρία μπορεί να στέλνει μη αιτηθείσα ηλεκτρονική αλληλογραφία στον καταναλωτή, μόνο στην περίπτωση που αυτός έχει δώσει προηγουμένως τη ρητή συγκατάθεσή του. Στην περίπτωση αυτή, το site της επιχείρησης θα αναφέρει: “Αν επιθυμείτε να λαμβάνετε πληροφορίες για τα προϊόντα της εταιρίας

¹⁴⁹ “Η λύση της αναφοράς...Μάλλον η προτιμότερη”, www.go-online.gr

μας, βάλτε ένα “X” στο παρακάτω κουτί”. Αντιθέτως, σ’ένα opt out σύστημα, η εταιρία έχει το δικαίωμα να στέλνει spam στους καταναλωτές, μέχρι αυτοί να δηλώσουν την αντίρρησή τους. Αυτό σημαίνει ότι οι χρήστες του διαδικτύου έχουν το δικαίωμα να αντιταχθούν στην αποστολή ανεπιθύμητης αλληλογραφίας αν το επιθυμούν. Η εφαρμογή του συστήματος αυτού, απαιτεί την ύπαρξη δημόσιων ή ιδιωτικών καταλόγων. Οι δημόσιοι κατάλογοι περιλαμβάνουν τα ονόματα εκείνων που δεν επιθυμούν να λαμβάνουν spam. Έτσι αν μια εταιρία επιδιώκει στα πλαίσια της προώθησης των προϊόντων της να στείλει e-mail σε καταναλωτές με πληροφορίες για τα προϊόντα της, πρέπει πρώτα να συμβουλευτεί τις λίστες αυτές και να αποφύγει την αποστολή μηνυμάτων σε αυτούς που συμπεριλαμβάνονται στους καταλόγους αυτούς. Απ’ την άλλη, οι ιδιωτικοί κατάλογοι είναι κατάλογοι εταιριών με προσωπικά δεδομένα των πελατών τους οι οποίοι μπορεί να αποτελούν αντικείμενο πώλησης ή μεταβίβασης σε άλλες εταιρίες για την εξυπηρέτηση σκοπών άμεσου Mkt. Στις λίστες αυτές υπάρχει κατάλληλη ένδειξη γι’ αυτά τα υποκείμενα που δεν επιθυμούν να λαμβάνουν spam. Οι εταιρίες που χρησιμοποιούν τους καταλόγους αυτούς για να στέλνουν μη επιθυμητή ηλεκτρονική αλληλογραφία, πρέπει να εξαιρούν αυτούς που έχουν προηγουμένως εκφράσει την αντίρρησή τους. Στην περίπτωση που η εταιρία εφαρμόζει opt out σύστημα, το site της θα αναφέρει: “Αν δεν επιθυμείτε να λαμβάνετε πληροφορίες για τα προϊόντα της εταιρίας μας, βάλτε ένα “X” στο παρακάτω κουτί”.

Στο opt in σύστημα, οι εταιρίες άμεσης εμπορικής προώθησης, για να αποκτήσουν προσωπικά δεδομένα χρηστών, τοποθετούν ένα έντυπο «opt in» σε ένα δίκτυο 100 ή 200 πολυσύχναστων χώρων. Οι επισκέπτες θα πρέπει να συμπληρώσουν το έντυπο αυτό προκειμένου να γίνουν συνδρομητές σε ένα ενημερωτικό δελτίο, να συμμετάσχουν σ’ένα διαγωνισμό, να λάβουν ειδικές προσφορές σχετικές με τα ενδιαφέροντα που έχουν ορίσει κτλ. Στη συνέχεια τα δεδομένα αυτά τροφοδοτούν βάσεις 15 έως 20 εκατομμυρίων ηλεκτρονικών διευθύνσεων, το ένα τέταρτο των οποίων ανήκουν σε Ευρωπαίους χρήστες.

Στο πλαίσιο του συστήματος αυτού, ακολουθούνται πρακτικές οι οποίες ποικίλλουν από την άποψη της εντιμότητας δεδομένου ότι από τη μία πλευρά

υπάρχουν προσυμπληρωμένα τετραγωνίδια¹⁵⁰, ενώ απ' την άλλη υπάρχει το διπλό «opt in», δηλαδή επιβεβαίωση της εγγραφής με την αποστολή αυτόματου μηνύματος στο γραμματοκιβώτιο του επισκέπτη.¹⁵¹

Κάνοντας μια προσπάθεια να αναλύσουμε τα πλεονέκτηματα και τα μειονεκτήματα των δύο αυτών συστημάτων, πρέπει να αναφέρουμε ότι όσον αφορά το opt in σύστημα προσφέρει αποτελεσματικότερη προστασία στον ιδιωτικό βίο του καταναλωτή καθώς η αποστολή spam απ' τις επιχειρήσεις είναι δυνατή μόνο εφόσον ο αποδέκτης έχει δώσει τη συγκατάθεσή του και επίσης ο αποδέκτης αποφεύγει το κόστος της επικοινωνίας με την εν λόγω επιχείρηση, δηλαδή το κόστος λήψης των μηνυμάτων π.χ. τηλεφωνική σύνδεση, το κόστος ευκαιρίας απ' την απώλεια χρόνου για τη λήψη των μηνυμάτων κτλ. Απ' την πλευρά των εταιριών, ένα σημαντικό πλεονέκτημα είναι η αποφυγή σπατάλης πόρων για την αποστολή spam σε αποδέκτες που δεν ενδιαφέρονται για τα προϊόντα της επιχείρησης. Επίσης, σε αντίθεση με τα αρχεία «opt out», τα οποία δεν μπορούν να πωληθούν, τα αρχεία «opt in» μπορούν να αποτελέσουν αντικείμενο εμπορικής συναλλαγής. Έτσι, η συλλογή και η εμπορική χρήση δεδομένων για τα οποία τα ενδιαφερόμενα άτομα έχουν δώσει προηγουμένως τη συγκατάθεσή τους αποτελούν συγχρόνως μια πηγή κέρδους και ένα νέο τρόπο χρηματοδότησης του ηλεκτρονικού εμπορίου. Στο πλαίσιο αυτό, ο έμπορος ο

¹⁵⁰ Ορισμένα προγράμματα εμπορικής προώθησης βάσει άδειας περιέχουν πράγματι προσυμπληρωμένα τετραγωνίδια. Πρέπει να αναφερθεί ότι η πρακτική αυτή δεν συμφωνεί με το πνεύμα της εμπορικής προώθησης βάσει άδειας διότι δεν παρέχει καμιά εγγύηση για τη συγκατάθεση του πελάτη, εφόσον είναι πολύ πιθανόν οι επισκέπτες να προσπεράσουν την αντίστοιχη γραμμή χωρίς να την έχουν διαβάσει.

¹⁵¹ Όταν ένας χρήστης γράφεται συνδρομητής για παράδειγμα σε ένα ενημερωτικό δελτίο της ομάδας CNET, εμφανίζεται ένα παράθυρο με μια σειρά πλαισίων που πρέπει να σημειωθούν αν ο χρήστης επιθυμεί να λαμβάνει διαφημιστικά μηνύματα σε σχέση με καθορισμένους τομείς. Στο κάτω μέρος του καταλόγου αυτού υπάρχει ένας σύνδεσμος που επιτρέπει την πρόσβαση στη σελίδα «privacy policy» της ομάδας CNET. Η πολιτική αυτή είναι πλήρης και περιλαμβάνει μια ανακοίνωση η οποία αφορά την εγγραφή σ' ένα ενημερωτικό δελτίο που επεξηγεί σαφώς το ρόλο μιας τρίτης εταιρίας, εν προκειμένω της εταιρίας ηλεκτρονικής εμπορικής προώθησης Netcreations η οποία συλλέγει τα δεδομένα. Αφού συμπληρώσει το έντυπο και ορίσει τα θέματα για τα οποία επιθυμεί να ενημερώνεται, ο χρήστης επιβεβαιώνει την εγγραφή του και αυτό είναι το πρώτο «opt in». Αμέσως μετά λαμβάνει ένα μήνυμα επιβεβαίωσης εκ μέρους της Netcreations, με στόχο να εξασφαλιστεί ότι το «opt in» πραγματοποιήθηκε όντως απ' τον ενδιαφερόμενο και όχι εξ ονόματός του από κάποιον άλλο. Σε σχέση με το τελευταίο αυτό μήνυμα μπορούν να γίνουν τρεις παρατηρήσεις: η πρώτη είναι ότι γνωστοποιεί εκ νέου στον αποδέκτη την ύπαρξη ενός επώνυμου τρίτου μέρους στη σχέση του με τον ιστοχώρο μέσω του οποίου εγγράφεται στο ενημερωτικό δελτίο. Αυτό δεν είναι αμελητέο και καλύπτει το ενδεχόμενο ο χρήστης να μην έχει ενεργοποιήσει το σύνδεσμο προς τη σελίδα της «privacy policy». Η δεύτερη είναι ότι το μήνυμα περιέχει τα ενημερωτικά δελτία και τον κατάλογο διευθύνσεων στον οποίο έχει εγγραφεί ο χρήστης. Η Τρίτη είναι ότι δεν μπορεί να ξεκινήσει καμιά επικοινωνία αν δεν επιστραφεί e-mail επιβεβαίωσης. Μόλις η επιβεβαίωση του «opt in» φτάσει στον πάροχο, ο συνδρομητής λαμβάνει αυτόματα ένα τελευταία e-mail υποδοχής.

οποίος συνέλεξε μια πληροφορία λαμβάνει κάποια αμοιβή, όταν ένας απ' τους εταίρους του χρησιμοποιεί αυτή την πληροφορία στα πλαίσια μιας εκστρατείας εμπορικής προώθησης. Απ' την πλευρά του, αυτός που πραγματοποιεί την εκστρατεία είναι βέβαιος ότι απευθύνεται σε ένα πληθυσμό που ενδιαφέρεται να λαμβάνει εμπορικά μηνύματα και ως εκ τούτου αυξάνει την αποτελεσματικότητα των εμπορικών επικοινωνιών του. Ωστόσο το opt in σύστημα έχει και μειονεκτήματα. Το σημαντικότερο απ' αυτά είναι ο περιορισμός που θέτει στην επιχείρηση όσον αφορά την εφαρμογή της πολιτικής προώθησης των προϊόντων της, καθώς η επιχείρηση μπορεί να στείλει spam μόνο σε ένα περιορισμένο αριθμό ατόμων τα οποία δείχνουν ανάλογο ενδιαφέρον. Επίσης, με το «opt in» σύστημα, τίθεται το ερώτημα αν αύριο οι διαφημιζόμενοι δεν προσπαθήσουν να αναπτύξουν μια ευρεία αντίληψη της έννοιας «opt in». Σε εξαιρετικές περιπτώσεις, η ευρεία αυτή αντίληψη φαίνεται να στηρίζεται στο απλό γεγονός ότι, για παράδειγμα, ένας επισκέπτης ενός ιστοχώρου πίεσε από απροσεξία ένα εικονίδιο OK σε ένα παράθυρο διαλόγου που τον ρωτούσε αν θα επιθυμούσε να προσθέσει το χώρο αυτό στους σελιδοδείκτες του. Τίποτα δεν είναι πιο απλό πράγματι απ' το να συμπεριληφθεί μια ασαφής διάταξη σε μια δυσεύρετη σελίδα των όρων χρήσης ενός ιστοχώρου, όπου αναφέρεται με πολύ μικρούς χαρακτήρες ότι η συμπερίληψη του ιστοχώρου στους σελιδοδείκτες συνιστά αποδοχή της λήψης διαφημιστικών μηνυμάτων.¹⁵²

Όσον αφορά το opt out σύστημα, το πιο σημαντικό πλεονέκτημα για τις επιχειρήσεις, είναι ότι σε αντίθεση με το opt in σύστημα, έχουν τη δυνατότητα να προσεγγίζουν έναν μεγάλο αριθμό καταναλωτών χωρίς μεγάλο κόστος. Απ' την άλλη μεριά όμως, οι καταναλωτές είναι αυτοί που έχουν την ευθύνη λήψης των ανεπιθύμητων ηλεκτρονικών μηνυμάτων και πολλές φορές αγνοούν το δικαίωμα που έχουν να αρνηθούν τη λήψη τους ή είναι δύσκολη η όλη διαδικασία. Γι' αυτό οι επιχειρήσεις, κάθε φορά που στέλνουν spam στους χρήστες του διαδικτύου, θα πρέπει να ορίζουν και τη διαδικασία που πρέπει να ακολουθήσει ο χρήστης προκειμένου να συμπεριλάβει τον εαυτό του σε ένα δημόσιο κατάλογο.¹⁵³ Εύκολα

¹⁵² "Junk e-mail costs internet users euro 10 billion a year worldwide", www.europa.eu.int

¹⁵³ Carlos Rodriguez, "Regulating spam: opting in or opting out?", www.emeraldinsight.com

κατανοεί κανείς ότι η υιοθέτηση μιας βιώσιμης λύσης «opt out» θα απαιτούσε, για λόγους ασφάλειας δικαίου, την υιοθέτηση δεσμευτικών εθνικών ή κοινοτικών κανόνων με στόχο την καταχώριση, σε ένα ενιαίο διεθνές μητρώο, όλων εκείνων οι οποίοι έχουν εκφράσει την αντίθεσή τους. Μια τέτοια εξέλιξη θα είχε δρακόντεια αποτελέσματα: η αντίθεση ενός χρήστη του διαδικτύου στην λήψη εμπορικών μηνυμάτων από έναν ή ορισμένους εμπόρους θα μπορούσε να δεσμεύσει το σύνολο της επιχειρηματικής κοινότητας. Ως εκ τούτου, η λύση της προηγούμενης συγκατάθεσης φαίνεται να είναι η πλέον ενδεδειγμένη.

Ο παρακάτω πίνακας δείχνει ποια απ' τις δύο λύσεις έχουν υιοθετήσει στην εσωτερική τους νομοθεσία οι διάφορες χώρες της Ευρωπαϊκής Ένωσης.¹⁵⁴ Απ' τις παρακάτω χώρες μόνο η Πορτογαλία δεν έχει εφαρμόσει opt-in σύστημα, ωστόσο θα αναγκαστεί να το υιοθετήσει εξαιτίας της οδηγίας 2002/58 ΕΚ.

Χώρα	Μη επιθυμητά e-mails
Αυστρία	Opt-in
Βέλγιο	Opt-in
Δανία	Opt-in
Φινλανδία	Opt-in
Γαλλία	Opt-in
Γερμανία	Opt-in
Ελλάδα	Opt-in
Ιρλανδία	Opt-in
Ιταλία	Opt-in
Λουξεμβούργο	Opt-in
Κάτω Χώρες	Opt-in
Πορτογαλία	Opt-out
Ισπανία	Opt-in
Σουηδία	Opt-in
Ηνωμένο Βασίλειο	Opt-in

¹⁵⁴ Έκθεση του ΟΟΣΑ για το spam, ICCP(2003)10/Final, σελ. 21

2.7 Νομοθεσία για το spamming

2.7.1 Ευρωπαϊκή νομοθεσία

Σε προηγούμενη ανάλυση αναφέρθηκε ότι αν και το spamming αποτελεί ένα σημαντικό εργαλείο για τις επιχειρήσεις για την εφαρμογή πολιτικών άμεσης προώθησης των προϊόντων τους, ωστόσο προσβάλλει την ιδιωτική σφαίρα του αποδέκτη του, καθώς κατά πρώτον συνιστά ανεπιθύμητη ηλεκτρονική αλληλογραφία και κατά δεύτερον οι εταιρίες προκειμένου να στείλουν ηλεκτρονικά διαφημιστικά μηνύματα στους χρήστες του διαδικτύου, συγκεντρώνουν πληροφορίες για προσωπικά τους δεδομένα όπως π.χ. αγοραστικές συνήθειες, εισόδημα, ηλικία κτλ, με αποτέλεσμα να παραβιάζουν το απόρρητο της ιδιωτικής τους ζωής. Προκειμένου λοιπόν να προστατευθεί η ιδιωτική ζωή του ατόμου, τόσο ο Κοινοτικός όσο και ο Έλληνας νομοθέτης, έχουν θεσπίσει ρυθμίσεις για την αποστολή spam.

Απ' τα νομικά αυτά κείμενα, ιδιαίτερη βαρύτητα έχει η Οδηγία 2002/58 ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12^{ης} Ιουλίου 2002¹⁵⁵, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών, η οποία κατήργησε την Οδηγία 97/66¹⁵⁶ ΕΚ της 15^{ης} Δεκεμβρίου 1997 περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα. Η οδηγία αυτή αποτελεί εξειδίκευση της οδηγίας 95/46 ΕΚ σχετικά με τα προβλήματα που προκύπτουν στα σύγχρονα ψηφιακά δίκτυα επικοινωνιών. Η αναγκαιότητα αυτή βασίζεται στην εκτίμηση του ευρωπαϊού νομοθέτη ότι τα δημόσια προσβάσιμα δίκτυα ηλεκτρονικών επικοινωνιών παράγουν ιδιαίτερες ανάγκες προστασίας των διακινούμενων σε αυτά προσωπικών δεδομένων και αφού η οδηγία 95/46 ΕΚ αφορά τα μη δημόσια δίκτυα ηλεκτρονικής επικοινωνίας, ψηφίσθηκε η εν λόγω οδηγία για να καλύψει το κενό. Ωστόσο η οδηγία 95/46 ΕΚ καλύπτει και όποιο θέμα δεν ρυθμίζεται στην οδηγία 2002/58 ΕΚ.

¹⁵⁵ ΕΕ L 204 της 21/07/1998

¹⁵⁶ ΕΕ L 024 της 30/01/1998

Με το άρθρο 2 της οδηγίας εισάγονται οι ορισμοί των εννοιών «δεδομένα κίνησης», «δεδομένα θέσης», «επικοινωνία», «υπηρεσία προστιθέμενης αξίας» και «ηλεκτρονικό ταχυδρομείο». Ως «δεδομένα κίνησης» νοούνται τα δεδομένα που υποβάλλονται σε επεξεργασία για τους σκοπούς της διαβίβασης μιας επικοινωνίας σε δίκτυο ηλεκτρονικών επικοινωνιών ή της χρέωσής της, ενώ ως «δεδομένα θέσης» εκείνα που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών και που υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη μιας διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών. Ως «επικοινωνία» νοείται κάθε πληροφορία που ανταλλάσσεται ή διαβιβάζεται μεταξύ ενός πεπερασμένου αριθμού μερών, μέσω μιας διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών. Ως «υπηρεσία προστιθέμενης αξίας» νοείται κάθε υπηρεσία η οποία επιβάλλει την επεξεργασία των δεδομένων κίνησης ή θέσης πέραν εκείνων που απαιτούνται για τη μετάδοση της επικοινωνίας και της χρέωσής της. Τέλος, ως «ηλεκτρονικό ταχυδρομείο» ορίζεται κάθε μήνυμα με καίμενο, φωνή, ήχο ή εικόνα που αποστέλλεται μέσω δημόσιου δικτύου επικοινωνιών, το οποίο μπορεί να αποθηκευτεί στο δίκτυο ή στον τερματικό εξοπλισμό του παραλήπτη έως ότου ληφθεί απ' τον παραλήπτη.¹⁵⁷

Στο άρθρο 5 της νέας οδηγίας εισάγεται ο κανόνας της προστασίας του απορρήτου των ηλεκτρονικών επικοινωνιών αλλά και των δεδομένων κίνησης. Σύμφωνα με το άρθρο 5 παρ.1 «Τα κράτη μέλη κατοχυρώνουν, μέσω της εθνικής νομοθεσίας, το απόρρητο των επικοινωνιών που διενεργούνται μέσω δημόσιου δικτύου επικοινωνιών και των διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, καθώς και των συναφών δεδομένων κίνησης. Ειδικότερα, απαγορεύουν την ακρόαση, υποκλοπή, αποθήκευση ή άλλο είδος παρακολούθησης ή επιτήρησης των επικοινωνιών και των συναφών δεδομένων κίνησης από πρόσωπα πλην των χρηστών, εκτός αν υπάρχει σχετική νόμιμη άδεια. Η παρούσα παράγραφος δεν εμποδίζει την τεχνική αποθήκευση η οποία είναι αναγκαία για τη διαβίβαση επικοινωνίας» Στο ίδιο άρθρο επίσης, στην

¹⁵⁷ Γιώργος Νούσκαλης, «Η προστασία των προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες σύμφωνα με τις νέες κοινοτικές ρυθμίσεις της οδηγίας 2002/58 ΕΚ», ΠοιΧρ 2003

παράγραφο 3, διαγράφονται οι προϋποθέσεις της αποθήκευσης, πρόσβασης και επεξεργασίας των δεδομένων κίνησης του συνδρομητή ή χρήστη: «Τα κράτη μέλη μεριμνούν ώστε η χρήση των δικτύων ηλεκτρονικών επικοινωνιών για την αποθήκευση πληροφοριών ή την απόκτηση προσβάσεως σε πληροφορίες αποθηκευμένες στον τερματικό εξοπλισμό συνδρομητή ή χρήστη να επιτρέπεται μόνο εαν παρέχονται στον συγκεκριμένο συνδρομητή σαφείς και εκτεταμένες πληροφορίες σύμφωνα με την οδηγία 95/46 ΕΚ, μεταξύ άλλων για το σκοπό της επεξεργασίας, και ο υπεύθυνος ελέγχου των δεδομένων του παρέχει το δικαίωμα να αρνείται την επεξεργασία αυτή. Τούτο δεν εμποδίζει οιαδήποτε τεχνικής φύσεως αποθήκευση ή πρόσβαση, αποκλειστικός σκοπός της οποίας είναι η διενέργεια ή η διευκόλυνση της διαβίβασης μιας επικοινωνίας μέσω δικτύου ηλεκτρονικών επικοινωνιών ή που είναι αναγκαία μόνο για την παροχή υπηρεσίας στην κοινωνία των πληροφοριών την οποία έχει ζητήσει ρητά ο χρήστης ή ο συνδρομητής.»

Ασάφειες δημιουργεί, πάντως, το γεγονός ότι δεν γίνεται διάκριση μεταξύ ευαίσθητων και μη δεδομένων, σχετικά με τις προϋποθέσεις επεξεργασίας των δεδομένων στο άρθρο 5 παρ.3 της οδηγίας. Θα μπορούσε πάντως να υποθέσει κανείς ότι ισχύουν οι προϋποθέσεις επεξεργασίας των ευαίσθητων δεδομένων σύμφωνα με την οδηγία 95/46 ΕΚ.

Με τη νέα οδηγία επιβάλλεται στα κράτη μέλη να προστατεύσουν ως απόρρητες όλες τις πληροφορίες που προκύπτουν απ'τη χρήση δημόσιων δικτύων ηλεκτρονικών επικοινωνιών, εκτός αν υπάρχει συγκατάθεση των ενδιαφερομένων χρηστών. Η ρύθμιση αυτή ίσως επιβάλλει την επανεξέταση της άποψης που θεωρεί ότι το απόρρητο των επικοινωνιών προστατεύεται μόνο εαν η επικοινωνία διεξάγεται ιδιωτικά και όχι δημόσια. Με το νέο ευρωπαϊκό νομοθέτημα φαίνεται να θεωρούνται εξ ορισμού απόρρητες οι πληροφορίες που προκύπτουν απ' τη χρήση δημόσιων δικτύων ηλεκτρονικής επικοινωνίας.¹⁵⁸

¹⁵⁸ Γιώργος Νούσκαλης, «Ή προστασία των προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες σύμφωνα με τις νέες κοινοτικές ρυθμίσεις της οδηγίας 2002/58 ΕΚ», ΠοιΧρ 2003

Στα άρθρα 6 και 9 αναγνωρίζεται η δυνατότητα επεξεργασίας των δεδομένων κίνησης και θέσης καθώς και τα όρια της επιτρεπτής επεξεργασίας απ' τους παρόχους δημόσιου δικτύου ή διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών. Σύμφωνα με το άρθρο 6 παρ.1 της οδηγίας «τα δεδομένα κίνησης που αφορούν συνδρομητές και χρήστες, τα οποία υποβάλλονται σε επεξεργασία και αποθηκεύονται απ' τον πάροχο δημόσιου δικτύου ή διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών, πρέπει να απαλοίζονται ή να καθίστανται όταν δεν είναι πλέον απαραίτητα για το σκοπό της μετάδοσης μιας επικοινωνίας». Σύμφωνα με το άρθρο 9 της οδηγίας «Στις περιπτώσεις όπου δεδομένα θέσης εκτός των δεδομένων κίνησης, που αφορούν τους χρήστες ή συνδρομητές δικτύων ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, είναι δυνατόν να υποστούν επεξεργασία, η επεξεργασία αυτή επιτρέπεται μόνον όταν αυτά καθίστανται ανώνυμα ή με τη ρητή συγκατάθεση των χρηστών ή συνδρομητών στην απαιτούμενη έκταση και για την απαιτούμενη διάρκεια για την παροχή μιας υπηρεσίας προστιθέμενης αξίας. Ο φορέας παροχής υπηρεσιών είναι υποχρεωμένος να ενημερώνει τους χρήστες ή συνδρομητές, προτού δώσουν τη συγκατάθεσή τους, σχετικά με τον τύπο των δεδομένων θέσης εκτός των δεδομένων κυκλοφορίας που υποβάλλονται σε επεξεργασία, τους σκοπούς και τη διάρκεια της εν λόγω επεξεργασίας, καθώς και το ενδεχόμενο μετάδοσής τους σε τρίτους για το σκοπό παροχής της υπηρεσίας προστιθέμενης αξίας. Στους χρήστες ή συνδρομητές πρέπει να δίδεται η δυνατότητα να ανακαλούν οποτεδήποτε τη συγκατάθεσή τους για την επεξεργασία των δεδομένων θέσης, εκτός των δεδομένων κίνησης. Όταν ο χρήστης ή ο συνδρομητής έχει δώσει τη συγκατάθεσή του για την επεξεργασία δεδομένων θέσης εκτός των δεδομένων κίνησης, θα πρέπει να εξακολουθεί να έχει τη δυνατότητα, με απλά μέσα και ατελώς, να αρνείται προσωρινά την επεξεργασία των εν λόγω δεδομένων για κάθε σύνδεση με το δίκτυο ή για κάθε μετάδοση μιας επικοινωνίας. Η επεξεργασία των δεδομένων θέσης, εκτός των δεδομένων κίνησης, πρέπει να περιορίζεται σε πρόσωπα τα οποία ενεργούν υπό την εποπτεία του φορέα παροχής του δικτύου ή της διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών ή του τρίτου που παρέχει την υπηρεσία

προστιθέμενης αξίας, και πρέπει να περιορίζεται στα απολύτως απαραίτητα για τους σκοπούς της υπηρεσίας προστιθέμενης αξίας».

Το άρθρο 13 της εν λόγω Οδηγίας ορίζει ρητώς ότι η χρησιμοποίηση ηλεκτρονικού ταχυδρομείου για σκοπούς απευθείας εμπορικής προώθησης επιτρέπεται μόνο στην περίπτωση συνδρομητών, οι οποίοι έχουν δώσει εκ των προτέρων τη συγκατάθεσή τους (Opt-in σύστημα), με εξαίρεση την περίπτωση όπου ένας προμηθευτής αποκτά απ' τους πελάτες του στοιχεία επαφής ηλεκτρονικού ταχυδρομείου στο πλαίσιο προηγούμενων συναλλαγών, οπότε μπορεί να χρησιμοποιεί τα εν λόγω στοιχεία για την απευθείας εμπορική προώθηση των δικών του παρόμοιων προϊόντων ή υπηρεσιών, υπό την προϋπόθεση ότι οι πελάτες του έχουν σαφώς την ευκαιρία να αντιτάσσονται σε αυτή τη συλλογή των στοιχείων τους και αυτό με κάθε μήνυμα σε περίπτωση που ο χρήστης αρχικά δεν είχε διαφωνήσει με αυτή τη χρήση. Οπότε γίνεται αντιληπτό ότι η σχετική Οδηγία υιοθετεί σε γενικές γραμμές opt in σύστημα, με την εξαίρεση την οποία ορίζει. Ωστόσο η Ελλάδα και μαζί με αυτή και άλλες 7 Ευρωπαϊκές χώρες, δεν έχουν ενσωματώσει ακόμα στο εσωτερικό τους δίκαιο την εν λόγω Οδηγία με αποτέλεσμα τον Απρίλιο του 2004 η Επιτροπή να έχει ήδη κινήσει διαδικασία προσφυγής στο Ευρωπαϊκό Δικαστήριο.

Η Οδηγία 95/46 ΕΚ¹⁵⁹ για την προστασία προσωπικών δεδομένων αναφέρεται και στη νομιμότητα συλλογής ηλεκτρονικών διευθύνσεων και στις προϋποθέσεις που πρέπει να πληρούνται για την αποστολή spam mails. Σύμφωνα με το άρθρο 2^α της οδηγίας, οι διευθύνσεις e-mail αποτελούν προσωπικά δεδομένα αφού συνιστούν πληροφορία «που αναφέρεται σε φυσικό πρόσωπο του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί».

Σχετικά με τη νομιμότητα συλλογής των ηλεκτρονικών διευθύνσεων των χρηστών, η οδηγία αντιμετωπίζει διαφορετικά τις διάφορες καταστάσεις ανάλογα με το αν ο αποδέκτης του μηνύματος είναι¹⁶⁰:

¹⁵⁹ EE L 281 της 23/11/1995

¹⁶⁰ Gauthronet Serge & Drouard Etienne, 'Junk e-mail costs internet users euro 10 billion a year worldwide'', www.europa.eu.int

-ένας πελάτης ο οποίος έδωσε ο ίδιος την ηλεκτρονική του διεύθυνση στον αποστολέα

-ένα πρόσωπο την ηλεκτρονική διεύθυνση του οποίου έλαβε ο αποστολέας από τρίτον, ο οποίος με τη σειρά του είχε λάβει ο ίδιος την εν λόγω διεύθυνση απευθείας απ' το προαναφερόμενο πρόσωπο

-ένας χρήστης η ηλεκτρονική διεύθυνση του οποίου συνελέγη σε δημόσιο χώρο του διαδικτύου, χωρίς αυτός να το γνωρίζει

1. Στην περίπτωση που ο ίδιος ο χρήστης δίνει την ηλεκτρονική του διεύθυνση στον αποστολέα, ο αποστολέας μπορεί να του αποστείλει εμπορικά ηλεκτρονικά μηνύματα, με την επιφύλαξη του δικαιώματος του χρήστη να αντιταχθεί στη λήψη τέτοιων μηνυμάτων και/ή να αντιταχθεί στην κοινοποίηση της ηλεκτρονικής του διεύθυνσης σε τρίτους (άρθρο 14)
2. Στην περίπτωση που ο χρήστης παρέχει την ηλεκτρονική του διεύθυνση σε έναν έμπορο και αυτός στη συνέχεια την εκχωρεί σε τρίτον για σκοπούς εμπορικής προώθησης, η εκχώρησή αυτή είναι νόμιμη, αν ο συλλέκτης της ηλεκτρονικής διεύθυνσης ενημέρωσε προηγουμένως το χρήστη για το δικαίωμά του να αντιταχθεί δωρεάν σ' αυτήν. (άρθρο 11 παρ.1)
3. Όταν η ηλεκτρονική διεύθυνση συνελέγη από δημόσιους χώρους του διαδικτύου, τότε η πρακτική αυτή απ' τη φύση της δεν δίνει στα υποκείμενα των δεδομένων τη δυνατότητα να αντιταχθούν εκ των προτέρων στη συλλογή δεδομένων που τα αφορούν. Αυτή η πρακτική απαγορεύεται απ' την εν λόγω οδηγία γιατί παραβιάζει την αρχή του σκοπού (άρθρο 6) και είναι αμφισβητήσιμη ως προς την αρχή της νομιμότητας των επεξεργασιών (άρθρο 7)

Η οδηγία δίνει έναν αυστηρό ορισμό της συγκατάθεσης (άρθρο 2): πρόκειται για κάθε δήλωση βούλησης με την οποία το πρόσωπο στο οποίο αναφέρονται τα δεδομένα δέχεται να αποτελέσουν αντικείμενο επεξεργασίας τα προσωπικά δεδομένα που το αφορούν. Κατά συνέπεια, για να υπάρχει βεβαιότητα ότι ο

χρήστης του διαδικτύου έχει δώσει τη συγκατάθεσή του για τη λήψη εμπορικών μηνυμάτων, θα πρέπει να καταστεί υποχρεωτική η έκφραση της βούλησής του σχετικά με το θέμα αυτό. Η συγκατάθεση θα μπορούσε να εκφραστεί, όπως συμβαίνει συχνά στην πράξη, με τη συμπλήρωση ενός σχετικού τετραγωνιδίου στην ιστοσελίδα συλλογής πληροφοριών. Σε κάθε περίπτωση, αν ο χρήστης δεν συμπληρώσει ο ίδιος το τετραγωνίδιο που προβλέπεται για την έκφραση της συγκατάθεσής του, δεν είναι δυνατόν να θεωρείται ότι η συγκατάθεση έχει δωθεί. Η πρακτική να είναι το τετραγωνίδιο προσυμπληρωμένο με δυνατότητα του υποκειμένου να αντιπαχθεί στη συνέχεια, δεν συνάδει με τις επιλογές της οδηγίας, λόγω της ασάφειας που προκαλείται.¹⁶¹

Επίσης και η οδηγία 97/7 ΕΚ ρυθμίζει θέματα που αφορούν το spam. Συγκεκριμένα, η εν λόγω οδηγία, σε αντίθεση με την οδηγία 95/46 ΕΚ, ρυθμίζει μόνο τις προϋποθέσεις αποστολής μη αιτηθείσας εμπορικής αλληλογραφίας και δεν εξετάζει τη νομιμότητα συλλογής και επεξεργασίας των ηλεκτρονικών διευθύνσεων. Στο άρθρο 10 παρ.1 ορίζει ότι απαιτείται η προηγούμενη συγκατάθεση του καταναλωτή για τη χρήση από έναν προμηθευτή των ακόλουθων μέσων:

- αυτοματοποιημένου συστήματος κλήσεως χωρίς ανθρώπινη παρέμβαση
- μηχανήματος τηλεμοιότητας (fax)

Στο άρθρο 10 παρ.2 ορίζεται ότι τα κράτη μέλη μεριμνούν ώστε τα μέσα εξ αποστάσεως επικοινωνίας, συμπεριλαμβανομένου και του διαδικτύου, εφόσον καθιστούν δυνατή μια ατομική επικοινωνία, να επιτρέπεται να χρησιμοποιηθούν μόνο αν ο καταναλωτής δεν έχει εκδηλώσει την αντίθεσή του. Αυτό σημαίνει ότι η οδηγία υιοθετεί το καταρχήν επιτρεπτό της αποστολής διαφημιστικών e-mail, εκτός αν ο καταναλωτής εκδηλώσει ρητώς την αντίθεσή του.¹⁶²

¹⁶¹ Κομνηνός Γ. Κόμνιος, “Η ανεπιθύμητη εμπορική ηλεκτρονική αλληλογραφία (spamming), ΕπισκΕΔ/2002,σελ. 1013

¹⁶² Κομνηνός Γ. Κόμνιος, “Η ανεπιθύμητη εμπορική ηλεκτρονική αλληλογραφία (spamming), ΕπισκΕΔ/2002,σελ. 1015

Επιπρόσθετα πρέπει να αναφερθεί ότι και η Οδηγία 2000/31 ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8^{ης} Ιουνίου 2000 για “ορισμένες νομικές πτυχές της Κοινωνίας της Πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά”, παρέχει προστασία των καταναλωτών απ’την ανεπιθύμητη αλληλογραφία. Βέβαια η οδηγία αυτή, όπως και η οδηγία 97/7 ΕΚ, εξετάζει αποκλειστικά και μόνο τους όρους υπό τους οποίους είναι δυνατή η αποστολή ενός μη αιτηθέντος μηνύματος, και κατά συνέπεια δεν ασχολείται καθόλου με τη νομιμότητα του τρόπου με τον οποίο γίνεται η συλλογή ηλεκτρονικών διευθύνσεων, ζήτημα το οποίο διέπεται αποκλειστικά απ’ την οδηγία 95/46 ΕΚ. Συγκεκριμένα το άρθρο 7 παρ. 1 ορίζει ότι « Εκτός από άλλες προϋποθέσεις προβλεπόμενες από το κοινοτικό δίκαιο, τα κράτη μέλη τα οποία επιτρέπουν μη ζητηθείσα εμπορική επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου, εξασφαλίζουν ότι η εν λόγω εμπορική επικοινωνία από φορέα παροχής υπηρεσιών εγκατεστημένο στο έδαφός τους πρέπει να είναι αναγνωρίσιμη σαφώς και επακριβώς ευθύς ως περιέλθει στον παραλήπτη». Αυτό σημαίνει ότι ο παραλήπτης δεν θα πρέπει να υποχρεώνεται να «ανοίξει» το συγκεκριμένο e-mail για να αντιληφθεί ότι πρόκειται για διαφημιστική αλληλογραφία. Πριν απ’ το “κατέβασμα” του e-mail, ο παραλήπτης μπορεί να διακρίνει σαφώς αν πρόκειται για ανεπιθύμητη ή όχι αλληλογραφία, όταν στη στήλη του «θέματος (subject)» αναφέρεται ρητώς ότι πρόκειται για διαφήμιση. Θα μπορούσε ενδεχομένως να χρησιμοποιηθεί κάποια λεκτική ειδοποίηση ότι πρόκειται για διαφήμιση ή να προσαρτάται κάποιο τεχνικό φύσεως χαρακτηριστικό που θα προσδιορίζει σαφώς και επακριβώς το διαφημιστικό χαρακτήρα του e-mail. Με τον τρόπο αυτό το spamming δεν θα είναι απλώς εύκολα αναγνωρίσιμο αλλά θα μπορεί να εντοπίζεται ευκολότερα και αποτελεσματικότερα απ’ τις εφαρμογές φιλτραρίσματος, απαλλάσσοντας το χρήστη από απώλεια χρόνου και χρήματος.¹⁶³ Το άρθρο 7 παρ.2 ορίζει ότι «Με την επιφύλαξη της Οδηγίας 97/7 ΕΚ και της Οδηγίας 97/66 ΕΚ, τα κράτη μέλη λαμβάνουν μέτρα για να εξασφαλίζεται ότι οι φορείς παροχής υπηρεσιών που αναλαμβάνουν δραστηριότητες μη ζητηθείσών εμπορικών επικοινωνιών μέσω

¹⁶³ Κομνηνός Γ. Κόμνιος, ‘‘Η ανεπιθύμητη εμπορική ηλεκτρονική αλληλογραφία (spamming), ΕπισκεΔ/2002,σελ.1016

ηλεκτρονικού ταχυδρομείου συμβουλεύονται τακτικά και τηρούν τα μητρώα “επιλογών” (opt-out lists), στα οποία μπορούν να εγγράφονται τα φυσικά πρόσωπα που επιλέγουν να μην λαμβάνουν τέτοιες εμπορικές επικοινωνίες». Απ’ ότι φαίνεται η οδηγία υιοθετεί το σύστημα opt-out για την Ευρωπαϊκή Ένωση. Ενώ η ταυτότητα του αποστολέα μη αιτηθείσας ηλεκτρονικής αλληλογραφίας πρέπει να προκύπτει σαφώς απ’ το e-mail, δεν προβλέπεται σαφής νομική υποχρέωση του αποστολέα να αφαιρέσει την ηλεκτρονική διεύθυνση του παραλήπτη απ’ το αρχείο του. Εξάλλου, η οδηγία δεν προβλέπει ότι οι φορείς που αποστέλλουν ανεπιθύμητη αλληλογραφία πρέπει να συμβουλεύονται τα «μητρώα επιλογών» κάθε φορά που λαμβάνει χώρα η αποστολή διαφημιστικής αλληλογραφίας, αλλά ότι η έρευνα αυτή πρέπει απλώς να είναι τακτική.¹⁶⁴ Η οδηγία δεν κάνει καμιά αναφορά σε σχέση με τη δομή του λεγόμενου μητρώου επιλογών. Απ’ την οδηγία δεν προκύπτει αν πρόκειται για ένα κοινό μητρώο για ολόκληρη των Ευρώπη ή πολλαπλά μητρώα τα οποία θα πρέπει να συμβουλεύονται οι φορείς και στα οποία θα πρέπει να εγγράφονται οι χρήστες. Τέλος, η εν λόγω οδηγία δεν απαιτεί απ’ τα κράτη μέλη η αίτηση του παραλήπτη για εγγραφή του στο μητρώο να είναι ανέξοδη, γεγονός που συνιστά παράλειψη.^{165, 166}

Αναφορά για το spamming κάνει και η οδηγία 2002/65 ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την εξ αποστάσεως εμπορία χρηματοοικονομικών υπηρεσιών προς τους καταναλωτές. Συγκεκριμένα το άρθρο 10 ορίζει ότι «1. Η χρησιμοποίηση των ακόλουθων τεχνικών επικοινωνίας εξ αποστάσεως από έναν προμηθευτή απαιτεί την προηγούμενη συγκατάθεση του καταναλωτή: α) αυτοματοποιημένα συστήματα κλήσης χωρίς ανθρώπινη παρέμβαση και β) φαξ. 2. Τα κράτη μέλη μεριμνούν ώστε τα μέσα επικοινωνίας εξ αποστάσεως εκτός από εκείνα που αναφέρονται στην παρ.1, όταν παρέχουν δυνατότητα προσωρινής επικοινωνίας: α) να μην επιτρέπονται εάν δεν υπάρχει συγκατάθεση του ενδιαφερόμενου καταναλωτή ή β) να χρησιμοποιούνται μόνο

¹⁶⁴ Έκθεση του ΟΟΣΑ για το spam, ICCP(2003)10/Final, σελ. 25

¹⁶⁵ Αναφορά της Ευρωπαϊκής Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο για την εφαρμογή της οδηγίας 2000/31 ΕΚ, COM(2003)702 Final, σελ. 9

¹⁶⁶ Gauthronet Serge & Drouard Etienne, “Junk e-mail costs internet users euro 10 billion a year worldwide”, www.europa.eu.int

εφόσον δεν υπάρχει έκδηλη αντίθεση του καταναλωτή 3. Τα μέτρα που προβλέπονται απ' τις παρ. 1 και 2 δεν πρέπει να συνεπάγονται έξοδα για τους καταναλωτές».

2.7.2 Ελληνική νομοθεσία

Επίσης ρύθμιση για τη μη αιτηθείσα εμπορική επικοινωνία περιλαμβάνεται και στο π.δ. 131/2003, που αποτελεί την πράξη προσαρμογής της ελληνικής νομοθεσίας προς την οδηγία 2000/31 ΕΚ για το ηλεκτρονικό εμπόριο. Αναφέρεται στο άρθρο 6§1, ότι εμπορική επικοινωνία με παραλήπτη που δεν την έχει ζητήσει, αν γίνεται με ηλεκτρονικό ταχυδρομείο και εφόσον δεν απαγορεύεται, πρέπει να αναγνωρίζεται σαφώς και επακριβώς ευθύς ως περιέλθει σ' αυτόν. Τούτο σημαίνει ότι πρέπει να αναφέρεται το θέμα του ηλεκτρονικού μηνύματος, όπως και τα ακριβή στοιχεία του αποστολέα, ώστε να είναι αναγνωρίσιμη η (εμπορική ή επαγγελματική) ιδιότητα του αποστολέα. Επίσης για τη διασφάλιση της απαραίτητης διαφάνειας θα πρέπει να αναφέρεται η πραγματική ηλεκτρονική διεύθυνση του αποστολέα, καθώς ενίοτε οι ηλεκτρονικές διευθύνσεις των αποστολέων ανεπιθύμητης ηλεκτρονικής αλληλογραφίας δεν αντιστοιχούν σε μια πραγματική διεύθυνση. Βεβαίως, η παραπάνω ρύθμιση έχει ως προϋπόθεση να μην απαγορεύεται η αποστολή μη αιτηθείσας εμπορικής αλληλογραφίας από άλλες διατάξεις. Επίσης, το π.δ. 131/2003 ορίζει ότι οι φορείς υπηρεσιών που αναλαμβάνουν δραστηριότητες μη ζητηθείσας εμπορικής επικοινωνίας μέσω ηλεκτρονικού ταχυδρομείου οφείλουν να τηρούν και να συμβουλεύονται τακτικά, μητρώα «επιλογών», όπου μπορούν να εγγράφονται τα φυσικά πρόσωπα που επιλέγουν να μην λαμβάνουν τέτοιες επικοινωνίες. Δηλαδή η ρύθμιση αυτή έχει εφαρμογή μόνο στην περίπτωση που ισχύει το σύστημα opt out, δηλαδή α) όταν ο προμηθευτής κάνει χρήση στοιχείων που περιήλθαν σε γνώση του από προηγούμενες συναλλακτικές σχέσεις με τον καταναλωτή, από γενικά προσιτές πηγές ή από άλλο φυσικό ή νομικό πρόσωπο β) εφόσον ο καταναλωτής εγκρίνει ρητά τη μεταβίβαση των προσωπικών του στοιχείων για το σκοπό της άμεσης διαφήμισης (άρθρο 9§11 ν. 2251/1994) ή γ) κατά το άρθρο 13§2 της Οδηγίας 2002/58 ΕΚ, όταν ένας προμηθευτής αποκτά

απ' τους πελάτες του στοιχεία επαφής ηλεκτρονικού ταχυδρομείου στο πλαίσιο προηγούμενων συναλλαγών.¹⁶⁷

Επίσης, ο νόμος 2251/1994 στο άρθρο 9 παρ. 10 επιτρέπει τη μετάδοση διαφημιστικού μηνύματος απευθείας στον καταναλωτή μέσω ηλεκτρονικού ταχυδρομείου μόνο αν συναινεί ρητώς ο καταναλωτής. Στο άρθρο 4 παρ.6 ορίζεται ότι απαγορεύεται χωρίς τη συναίνεση του καταναλωτή η χρησιμοποίηση τεχνικών μέσων επικοινωνίας για την πρόταση σύναψης σύμβασης, όπως τηλεφώνου, αυτόματης κλήσης, φαξ, ηλεκτρονικού ταχυδρομείου ή άλλου ηλεκτρονικού μέσου επικοινωνίας. Τις παραπάνω διατάξεις συμπληρώνουν οι παρ. 11 και 12 του άρθρου 9 του ν.2251/1994.¹⁶⁸ Η μετάδοση διαφημιστικού μηνύματος απευθείας στον καταναλωτή με οποιοδήποτε τρόπο άμεσης επικοινωνίας, επιτρέπεται μόνο αν ο προμηθευτής κάνει χρήση στοιχείων ή προσωπικών δεδομένων του καταναλωτή που περιήλθαν σε γνώση του από προηγούμενες συναλλακτικές σχέσεις του με τον καταναλωτή από γενικά προσιτές πηγές, από κατάλογο ή άλλα δημοσιευμένα στοιχεία ή από άλλο φυσικό ή νομικό πρόσωπο, εφόσον ο καταναλωτής εγκρίνει ρητά τη μεταβίβαση των προσωπικών του στοιχείων για το σκοπό της άμεσης διαφήμισης. Ο νόμος μάλιστα παρέχει αξίωση στον καταναλωτή: 1. να υποχρεώσει το διαφημιστή σε αναφορά του τρόπου με τον οποίο περιήλθαν σε γνώση του τα προσωπικά στοιχεία του καταναλωτή 2. να ζητήσει τη διακοπή κάθε μορφής άμεσης διαφήμισης και τη διαγραφή των προσωπικών στοιχείων του καταναλωτή. Όσον αφορά την ένδικη προστασία του παραλήπτη μηνυμάτων, ο μεμονωμένος καταναλωτής νομιμοποιείται στην άσκηση των δικαιωμάτων του τόσο με την αγωγή παραλείψεως όσο και με την αξίωση για αποζημίωση, παρόλο που κάτι τέτοιο δεν προβλέπεται ρητώς απ' το άρθρο 9 του ν. 2251/1994.¹⁶⁹

¹⁶⁷ Ιγγλεζάκης Δ. Ιωάννης, "Το νομικό πλαίσιο του ηλεκτρονικού εμπορίου", σελ. 103

¹⁶⁸ Σιδηρόπουλος Θεόδωρος, "Το δίκαιο του διαδικτύου", σελ. 200

¹⁶⁹ Κομνηνός Γ. Κόμνιος, "Η ανεπιθύμητη εμπορική ηλεκτρονική αλληλογραφία (spamming)", ΕπιστΕΔ 2002, σελ. 1023

2.7.3 Νομοθεσία ΗΠΑ

Αναφορά πρέπει να γίνει και στη νομοθεσία των ΗΠΑ για την προστασία απ' το spamming, και ιδιαίτερα στον CAN-SPAM Act (Controlling the assault of Non-Solicited Pornography and Marketing Act), ο οποίος τέθηκε σε ισχύ την 1η Ιανουαρίου του 2004. Ο νόμος αυτός καθιερώνει opt-out σύστημα, καθώς επιτρέπει κατ'αρχήν την αποστολή spamming χωρίς προηγούμενη συγκατάθεση του χρήστη, ωστόσο όμως ο χρήστης έχει το δικαίωμα να αντιταχθεί εκ των υστέρων στην περαιτέρω αποστολή τέτοιων μηνυμάτων. Σχετικά με την απαγόρευση της αποστολής ανεπιθύμητης ηλεκτρονικής αλληλογραφίας ύστερα από άρνηση του παραλήπτη, στο άρθρο 5(4) (section 5(4)) ορίζει ότι αν ο παραλήπτης ενός διαφημιστικού μηνύματος εκφράσει στον αποστολέα την αντίθεσή του για την αποστολή τέτοιων ηλεκτρονικών μηνυμάτων, τότε είναι παράνομο:

1. για τον αποστολέα να συνεχίζει την αποστολή διαφημιστικών μηνυμάτων ακόμη και αφού περάσουν 10 εργάσιμες ημέρες μετά την εκδήλωση της αντίθεσης του παραλήπτη.

2. για οποιοδήποτε πρόσωπο ενεργεί για λογαριασμό του αποστολέα και συνεχίζει να αποστέλλει spam mails στον παραλήπτη, εφόσον έχει λάβει γνώση ή θα έπρεπε να γνωρίζει για την αντίθεση του αποστολέα στην λήψη τέτοιων μηνυμάτων.

3. για τον αποστολέα ή οποιοδήποτε άλλο πρόσωπο που γνωρίζει για την αντίθεση του παραλήπτη στην αποστολή spam, να παρέχει σε τρίτους την ηλεκτρονική διεύθυνση του παραλήπτη, εκτός αν υπάρχει προηγούμενη συγκατάθεση του χρήστη.

Επίσης στο άρθρο 5(5) ορίζεται ότι προκειμένου ο αποστολέας να αποστείλλει ένα ηλεκτρονικό διαφημιστικό μήνυμα στον παραλήπτη, πρέπει α) να αναφέρεται στο μήνυμα ότι πρόκειται για διαφήμιση β) να ενημερωθεί ο παραλήπτης για το δικαίωμά του να αντιταχθεί στην αποστολή τέτοιων μηνυμάτων γ) να αναφέρεται η φυσική διεύθυνση του αποστολέα στο μήνυμα. Ωστόσο, αν ο παραλήπτης έχει δώσει προηγουμένως τη συγκατάθεσή του στην

αποστολή ηλεκτρονικών μηνυμάτων, τότε δεν υποχρεούται ο αποστολέας να αναφέρει στο μήνυμα ότι πρόκειται για διαφήμιση.

Επίσης στο άρθρο 5(1) αναφέρεται ότι απαγορεύεται ο αποστολέας να αποκρύπτει ή να παραποιεί τα στοιχεία της επικεφαλίδας του e-mail που πιστοποιούν την ταυτότητα του (header information) και την προέλευση του μηνύματος. Ωστόσο δεν νομιμοποιείται ο παραλήπτης να μηνύσει τον spammer για παραβίαση του νόμου σύμφωνα με το άρθρο 7. Το δικαίωμα αυτό το έχουν οι κρατικές αρχές και το Federal Trade of Commission, το οποίο μπορεί να διερευνήσει κάθε περίπτωση παράβασης, να επιβάλλει πρόστιμα στους παραβάτες και να τους παραπέμψει στη δικαιοσύνη. Αντιθέτως οι Παροχείς Υπηρεσιών Διαδικτύου (ISPs) έχουν το δικαίωμα να υποβάλλουν μήνυση στους spammers.¹⁷⁰

2.8 Νομολογία για spamming

2.8.1 Απόφαση ΜΠρΑΘ 2110/2002

Παρακάτω παραθέτουμε μια περίπτωση απ' τη ελληνική νομολογία για να γίνει πιο κατανοητή η εφαρμογή της νομοθεσίας. Η υπόθεση αφορά συλλογή εκ μέρους τρίτου ηλεκτρονικών διευθύνσεων χωρίς τη συγκατάθεση των δικαιούχων, με σκοπό την αποστολή στις διευθύνσεις αυτές διαφημιστικών ηλεκτρονικών μηνυμάτων για το περιεχόμενο μιας ηλεκτρονικής εφημερίδας. Ο παρέχων τις σχετικές υπηρεσίες διαδικτύου, διέκοψε τη λήψη των παραπάνω ηλεκτρονικών μηνυμάτων καθώς οι αποδέκτες τους εξέφρασαν παράπονα πως παρέλαβαν την εφημερίδα υπό μορφή αλληλογραφίας χωρίς τη θέλησή τους. Ο εκδότης της ηλεκτρονικής εφημερίδας στις 9/10/2001 κατέθεσε ασφαλιστικά μέτρα κατά του παροχέα υπηρεσιών διαδικτύου με τα οποία απαιτούσε την άρση της απαγόρευσης λήψης της εφημερίδας του.

Αναλυτικά το ιστορικό της υπόθεσης έχει ως εξής: Ο αιτών είναι δημοσιογράφος, εκδότης της ηλεκτρονικής εφημερίδας «Το Ε.», το όνομα της

¹⁷⁰ Nixon Peabody LLP, ‘‘The CAN-SPAM Act of 2003: Overview and Analysis’’, www.nixonpea.com

οποίας έχει επισήμως καταχωρηθεί στη Διεύθυνση Σημάτων του Υπουργείου Ανάπτυξης και στο διαδίκτυο έχει καταχωρηθεί η ηλεκτρονική διεύθυνση της εφημερίδας που είναι η εξής: «www.emmeles.gr». Η εφημερίδα κυκλοφορεί απ' τις αρχές Μαΐου 2001 με πολιτικά και άλλα σχόλια, η επικοινωνία δε με το αναγνωστικό κοινό γίνεται με δύο τρόπους: 1) με την ανάρτηση της εφημερίδας στο διαδίκτυο και την ελεύθερη πρόσβαση σε κάθε χρήστη του διαδικτύου σ' αυτή και 2) με την αποστολή της στις ηλεκτρονικές διευθύνσεις των χρηστών του διαδικτύου με περιεχόμενο ανακοίνωση θεμάτων της και την πρόσκληση επίσκεψης της συγκεκριμένης ιστοσελίδας μέσω ηλεκτρονικού ταχυδρομείου. Η καθής που δραστηριοποιείται στον τομέα παροχής υπηρεσιών διαδικτύου, συνδρομητής της οποίας είναι και ο αιτών, κατόπιν επανειλημμένων διαμαρτυριών συνδρομητών της για λήψεις μαζικώς μη ζητηθείσας αλληλογραφίας απ' την ιστοσελίδα www.emmeles.gr κατά το χρονικό διάστημα από 27/6/2001 έως 8/7/2001 προέβη σε διακοπή λήψης ηλεκτρονικών μηνυμάτων από την πιο πάνω ιστοσελίδα. Στην διακοπή αυτή, η εταιρία προέβη μετά από διαμαρτυρίες συνδρομητών της οι οποίοι δεν επιθυμούσαν να λαμβάνουν το μήνυμα και άλλοι οι οποίοι ζήτησαν τη διαγραφή αλλά συνέχισαν να το λαμβάνουν και παρά τις προειδοποιήσεις του αιτούντος εκ μέρους της καθής για μη σύμφωνη χρήση του δικτύου προς τους γενικούς όρους σύνδεσης-σύμβασης στο δίκτυο της καθής. Σύμφωνα με τους όρους αυτούς ο συνδρομητής υποχρεούται να κάνει καλή χρήση του δικτύου σύμφωνα με τους όρους χρήσης. Κακή χρήση συνιστά η αποστολή μεγάλου αριθμού μηνυμάτων για τη διαφημιστική προβολή του αποστολέα, χωρίς οι παραλήπτες να έχουν ζητήσει να λαμβάνουν τέτοια μηνύματα. Σε περίπτωση κακής χρήσης του δικτύου η καθής δικαιούται να διακόψει την πρόσβαση στο Δίκτυο. Ακόμη, στους γενικούς όρους χρήσης των υπηρεσιών της -net, ορίζεται ότι η καθής μπορεί να αρνηθεί σε οποιονδήποτε την υπηρεσία όταν κατά την κρίση της γίνει γνωστή παραβίαση όρων του παρόντος. Στην προκειμένη περίπτωση ο αιτών, προκειμένου να βρει τις ηλεκτρονικές διευθύνσεις των συνδρομητών της καθής, δεδομένου ότι αυτή τηρεί αλφαβητικό ευρετήριο ονομάτων πρόσβασης των συνδρομητών της που είχαν επιλέξει να κατασκευάσουν τη δική τους σελίδα χρήστη, και χωρίς τη συγκατάθεση των συνδρομητών, προέβη σε συλλογή των ονομάτων αυτών απ'

τον πιο πάνω αλφαβητικό κατάλογο της καθής. Στη συνέχεια πρόσθεσε σ' αυτά «@otenet» και απέκτησε την ηλεκτρονική διεύθυνση των συνδρομητών της καθής, στους οποίους απέστειλε μαζικώς χωρίς να ζητηθεί αλληλογραφία απ' την ιστοσελίδα «www.emmeles», παραβιάζοντας τους όρους χρήσης που αναφέρθηκαν.

2.8.2 Σκεπτικό απόφασης

Με την απόφαση 2110/2002, το Μονομελές Πρωτοδικείο Αθηνών, λαμβανομένων υπ' όψη των πιθανολογούμενων περιστατικών 1) ότι ουδέποτε διακόπηκε η ελεύθερη πρόσβαση στην ιστοσελίδα του αιτούντος, αλλά αντίθετα αυτή είναι ελεύθερα προσβάσιμη σε κάθε χρήστη του διαδικτύου, είτε γίνεται μέσω του μηνύματος που αποστέλλει ο αιτών είτε γίνεται με απευθείας πρόσβαση στην ιστοσελίδα του, χωρίς έτσι να εμποδίζεται το δικαίωμα έκφρασης και διάδοσης των στοχασμών του αιτούντος, 2) ότι με την αποστολή του μηνύματος του αιτούντος επιβαρύνονται οικονομικά οι παραλήπτες του μηνύματος, οι οποίοι αναλώνουν και χρόνο για τη διαγραφή τους απ' τον ταχυδρομικό κατάλογο στον οποίο συμπεριλήφθηκαν παρά τη θέλησή τους, ενώ πολλές φορές η επιλογή τους αυτή δε λειτουργεί 3) ότι μεγάλος αριθμός συνδρομητών της καθής διαμαρτυρήθηκε σ' αυτή για την κατά τον προαναφερόμενο τρόπο λήψη μηνύματος από τον αιτούντα 4) ότι η καθής πριν την κατά τα άνω διακοπή προειδοποίησε τον αιτούντα για κακή χρήση του δικτύου και 5) ότι η συλλογή των κωδικών πρόσβασης των συνδρομητών της καθής χωρίς τη συγκατάθεσή της και η αποστολή μη ζητηθέντος μηνύματος, αντίκειται στα άρθρα 4 και 5 ν. 2472/1997 και γι' αυτό η υπό κρίση αίτηση απορρίπτεται.

Το κυρίως ζήτημα που τίθεται με βάση την παραπάνω απόφαση είναι αν είναι σύλληπη η διακοπή της δυνατότητας λήψης και αποστολής ηλεκτρονικής αλληλογραφίας, εκ μέρους του παροχέα υπηρεσιών πρόσβασης στο διαδίκτυο. Αλλά πρώτα θα πρέπει να εξετασθεί αν επιτρέπεται η συλλογή και αξιοποίηση των ηλεκτρονικών διευθύνσεων των χρηστών του διαδικτύου για τους σκοπούς της διαφημιστικής αποστολής μηνυμάτων. Ο ν. 2472/1997 έχει εφαρμογή στην

επεξεργασία δεδομένων προσωπικού χαρακτήρα με ή χωρίς τη βοήθεια αυτοματοποιημένων μεθόδων. Οι ηλεκτρονικές διευθύνσεις χρηστών θεωρούνται κι αυτές προσωπικά δεδομένα διότι συνιστούν πληροφορίες που αναφέρονται σ' ένα υποκείμενο δεδομένων (άρθρο 2 ν. 2472/97).

Όσον αφορά τη νομιμότητα της συλλογής ηλεκτρονικών διευθύνσεων με σκοπό την αποστολή spamming, αυτή θα είναι νόμιμη, εφόσον το υποκείμενο των δεδομένων έδωσε τη συγκατάθεσή του, σύμφωνα με τις διατάξεις των άρθρων 2 και 5 ν. 2472/1997. Όταν δεν έχει δώσει τη συγκατάθεσή του, τότε η επεξεργασία θα είναι νόμιμη κατ' εξαίρεση, όταν συντρέχει η περίπτωση που αναφέρεται στη διάταξη του άρθρου 5§2 ν. 2472/97, δηλαδή όταν η επεξεργασία είναι απολύτως αναγκαία για την ικανοποίηση του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος της επεξεργασίας και τούτο υπερέχει προφανώς του συμφέροντος του υποκειμένου των δεδομένων. Στη συγκεκριμένη περίπτωση, δεν ισχύει η εξαίρεση αυτή διότι δεδομένου του κόστους που έχει για τους χρήστες του ηλεκτρονικού ταχυδρομείου η λήψη μηνυμάτων δεν υπερέχει προφανώς των δικαιωμάτων και συμφερόντων των προσώπων στα οποία αναφέρονται τα δεδομένα.¹⁷¹

2.8.2 Απόφαση ΜΠρΑΘ 1988/29.8.2002

Με την απόφαση αυτή εφαρμόστηκε για πρώτη φορά το άρθρο 23 του νόμου 2472/1997 περί αστικής ευθύνης απ' την παράνομη επεξεργασία των προσωπικών δεδομένων α) του ονοματεπώνυμου β) της διεύθυνσης κατοικίας ατόμου που έχει περιληφθεί στο μητρώο «προσώπων που δεν επιθυμούν να περιλαμβάνονται σε αρχεία, τα οποία έχουν ως σκοπό την προώθηση προμήθειας αγαθών ή την παροχή υπηρεσιών εξ αποστάσεως». Το Μονομελές Πρωτοδικείο έκρινε ότι συντρέχει ηθική βλάβη από την αποστολή διαφημιστικών επιστολών στο όνομα και στη διεύθυνση κατοικίας του ενάγοντος, παρά την εκ μέρους του άσκηση του δικαιώματος αντίρρησης. Η εναγόμενη εταιρία απέστειλε τις εν λόγω επιστολές, παρά τις υποχρεώσεις της:

¹⁷¹ Απόφαση Μονομελούς Πρωτοδικείου Αθηνών 2110/2002, ΕπισκεΔ Α/2003, Ιγγλεζάκης Δ. Ιωάννης

1. να συμβουλευτεί το τηρούμενο απ 'την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μητρώο προσώπων που δεν επιθυμούν την επεξεργασία των δεδομένων τους για σκοπούς προώθησης προϊόντων
2. να διαγράψει το όνομα και τη διεύθυνση κατοικίας του ενάγοντος απ' το αρχείο προσώπων προς τα οποία αποστέλλει διαφημιστικές επιστολές
3. να παραλείπει την αποστολή τέτοιων επιστολών στον ενάγοντα (άρθρο 13 παρ.3)

Η παραπάνω πρακτική της εναγόμενης κρίθηκε απ' το δικαστήριο ότι συνιστά επεξεργασία των δεδομένων του ονόματος και της διεύθυνσης κατοικίας που ενέχει σκόπιμη άγνοια της πρόθεσης του ενάγοντος για προστασία του ιδιωτικού του χώρου. Η άγνοια αυτή και η σκόπιμη και παράνομη παραβίαση της προσωπικής σφαίρας του ενάγοντος κρίθηκε ότι του προκάλεσε ψυχική στενοχώρια και γι' αυτό του επιδικάστηκε χρηματική ικανοποίηση λόγω ηθικής βλάβης, κατά το άρθρο 23 παρ.1, η οποία επιμετρήθηκε στο ελάχιστο απ' το νόμο προβλεπόμενο ποσό των 5.869 ευρώ.¹⁷²

¹⁷² Βασίλης Α. Σωτηρόπουλος, "Ηθική βλάβη από παράνομη αποστολή διαφημιστικών εντύπων", περιοδικό Συνήγορος, Νοέμβριος-Δεκέμβριος 2002, σελ. 465

ΚΕΦΑΛΑΙΟ 3

Άλλα νομοθετήματα για την προστασία δεδομένων στο διαδίκτυο

3.1 Νομοθεσία για την προστασία του απορρήτου στο διαδίκτυο

Στην προηγούμενη ανάλυση, έγινε αναφορά στη νομοθεσία για την προστασία της ιδιωτικής σφαίρας των χρηστών του διαδικτύου από την αποστολή μη ζητηθείσας ηλεκτρονικής αλληλογραφίας. Στην παρούσα ανάλυση θα γίνει λόγος για τη νομοθεσία προστασίας του απορρήτου των ηλεκτρονικών μηνυμάτων καθώς η παραβίαση του απορρήτου από κάποιον τρίτο, συνιστά παραβίαση της ιδιωτικότητας του χρήστη. Επειδή μάλιστα το διαδίκτυο είναι ένας χώρος όπου η παρεχόμενη ασφάλεια είναι ανεπαρκής, είναι εύκολο για κάποιον χρήστη να έχει πρόσβαση στα ηλεκτρονικά μηνύματα άλλων χρηστών και γι' αυτό απαιτείται κατ'αρχήν συνταγματική προστασία. Συγκεκριμένα το άρθρο 19 του Συντάγματος προστατεύει το απόρρητο της επικοινωνίας και η προστασία αυτή επεκτείνεται σε όλα τα μέσα τηλεπικοινωνίας που υπάρχουν σήμερα, συνεπώς και στο διαδίκτυο. Υποκείμενα του δικαιώματος του απορρήτου είναι και ο αποστολέας του μηνύματος και ο αποδέκτης. Ως προς το περιεχόμενο του δικαιώματος πρέπει να τονιστεί ότι αντικείμενο προστασίας δεν είναι το μήνυμα καθεαυτό, αλλά το απόρρητο του μηνύματος. Γι'αυτό προστατεύεται και το απόρρητο των μηνυμάτων που απλά εκφράζουν συναισθήματα π.χ. «smileys». Το απόρρητο της επικοινωνίας μέσω του διαδικτύου δεν καλύπτει μόνο το περιεχόμενο του ηλεκτρονικού μηνύματος αλλά και τα εξωτερικά στοιχεία της επικοινωνίας δηλαδή τα δεδομένα που αφορούν το «αν» και το «πώς» μιας διαδικτυακής επικοινωνίας π.χ. η ταυτότητα των δύο χρηστών, ο τόπος και ο χρόνος επικοινωνίας κτλ. Η αυτόματη καταγραφή και αποθήκευση των δεδομένων αυτών απ' τον παροχέα υπηρεσιών διαδικτύου ή κάποιο τρίτο αποτελεί επέμβαση στο απόρρητο. Βέβαια στην Αμερική, όπου δε δίνεται ιδιαίτερη σημασία στην προστασία της ιδιωτικότητας, υποστηρίζεται η άποψη ότι το απόρρητο υπάρχει και προστατεύεται, αρκεί οι ενδιαφερόμενοι να έλαβαν τα κατάλληλα μέτρα για να διαφυλάξουν τη μυστικότητα του περιεχομένου της

επικοινωνίας. Δηλαδή, ένα ηλεκτρονικό μήνυμα το οποίο διαβιβάζεται χωρίς τη λήψη μέτρων ασφάλειας, δεν καλύπτεται από το απόρρητο και επομένως μπορεί να διαβαστεί από τρίτους.

Η συνταγματική προστασία του απορρήτου της επικοινωνίας, αρχίζει από τότε που το ηλεκτρονικό μήνυμα έχει γραφτεί αλλά δεν έχει διαβιβαστεί μέσω της τηλεφωνικής γραμμής στο λήπτη του έως τη στιγμή που ο λήπτης λαμβάνει γνώση του περιεχομένου του και για όσο διάστημα το μήνυμα παραμένει στο διακομιστή του (server). Η συνταγματική προστασία του απορρήτου, καθιστά ανίσχυρους ως αντισυνταγματικούς, οποιουσδήποτε νόμους επιτρέπουν τον έλεγχο της ηλεκτρονικής αλληλογραφίας. Συνεπώς, αντισυνταγματική θα ήταν η νομοθετικά επιβαλλόμενη υποχρέωση να έχει κάθε υπολογιστής το λεγόμενο «chirper chir» που επιτρέπει την υπό προϋπόθεση παρακολούθηση κάθε επικοινωνίας μέσω του διαδικτύου.¹⁷³

Το απόρρητο της επικοινωνίας προστατεύει επίσης και ο νόμος 2225/94 ο οποίος στο άρθρο 1 ορίζει την ίδρυση της «Εθνικής Επιτροπής Προστασίας του Απορρήτου των Επικοινωνιών» και η οποία έχει ως αποστολή την προστασία του απορρήτου κάθε μορφής τηλεπικοινωνιακής ανταπόκρισης συμπεριλαμβανομένης και της διαδικτυακής. Σύμφωνα με το άρθρο 2 του νόμου για την εκπλήρωση της αποστολής της η Επιτροπή προβαίνει σε κάθε απαραίτητη για την εκτέλεση των καθηκόντων της ενέργεια. Επιθεωρεί χωρίς προειδοποίηση τις σχετικές με το έργο της εγκαταστάσεις των ιδιωτικών επιχειρήσεων, που προσφέρουν υπηρεσίες σχετικές με ανταπόκριση ή επικοινωνία όπως π.χ. των παροχέων πρόσβασης στο διαδίκτυο, ζητά κάθε πληροφορία χρήσιμη για την επίτευξη της αποστολής της, ερευνά τα αρχεία των παροχέων πρόσβασης που αναφέρονται στο προστατευόμενο απόρρητο και τέλος ζητάει απ' την αρμόδια δικαστική αρχή την κατάσχεση μέσων παραβίασης του απορρήτου. Η ίδρυση της Αρχής αυτής βάσει του παραπάνω νόμου

¹⁷³ Άρθρο 19§1 Συντάγματος 2001, «Το απόρρητο των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο είναι απόλυτα απαραβίαστο. Νόμος ορίζει τις εγγυήσεις υπό τις οποίες η δικαστική αρχή δεν δεσμεύεται από το απόρρητο για λόγους εθνικής ασφάλειας ή για διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων».

στηρίζεται στην §2 του άρθρου 19Σ, η οποία ορίζει ότι «Νόμος ορίζει τα σχετικά με τη συγκρότηση, τη λειτουργία και τις αρμοδιότητες της ανεξάρτητης αρχής που διασφαλίζει το απόρρητο της §1».

Ειδική αναφορά πρέπει να γίνει και στον Κώδικα Δεοντολογίας Άσκησης Τηλεπικοινωνιακών Δραστηριοτήτων, ο οποίος ορίζει ότι απαγορεύεται αυστηρά στον παροχέα τηλεπικοινωνιακών υπηρεσιών (συμπεριλαμβανομένου και του παροχέα υπηρεσιών διαδικτύου) να παρακολουθεί, καταγράφει, ακροάζεται, αποκαλύπτει και αναμεταδίδει το περιεχόμενο οποιασδήποτε επικοινωνίας (άρθρο 1). Κατ'εξαίρεση επιτρέπεται τέτοιου είδους παρέμβαση, μόνο αν ο παρέχων τηλεπικοινωνιακές υπηρεσίες εξουσιοδοτείται να το πράττει απ' την ισχύουσα νομοθεσία ή αν μια τέτοια παρέμβαση καθίσταται αναγκαία στο πλαίσιο της τακτικής συντήρησης του δικτύου. Σύμφωνα με το άρθρο 2 του Κώδικα, ο παρέχων τηλεπικοινωνιακές υπηρεσίες δεν επιτρέπεται να δημοσιεύει προσωπικές πληροφορίες των χρηστών του, ούτε να τις χρησιμοποιεί για άλλους σκοπούς από εκείνους, για τους οποίους αυτές δόθηκαν απ' το χρήστη, εκτός αν ο χρήστης συναινεί εγγράφως.

Τέλος, προστασία του απορρήτου της ηλεκτρονικής επικοινωνίας προσφέρει και το άρθρο 370Γ ΠΚ, το οποίο στην παράγραφο 2, αποσκοπεί στην ποινική καταστολή κάθε περίπτωσης αυθαίρετης λήψης μεταδιδόμενων στοιχείων όπως π.χ. παγίδευση δικτύων μετάδοσης δεδομένων καθώς και στην καταστολή κάθε πρόσβασης σε ξένα συστήματα επεξεργασίας ή αποθήκευσης δεδομένων όπως π.χ. η χωρίς δικαίωμα πρόσβαση του δράστη σε τράπεζα πληροφοριών μέσω του διαδικτύου. Συγκεκριμένα, στην §2 ορίζει ότι "όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε Η/Υ ή μεταδίδονται με συστήματα τηλεπικοινωνιών, εφόσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα, ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφάλειας που είχε λάβει ο νόμιμος κάτοχός τους, τιμωρείται με φυλάκιση μέχρι 3 μήνες ή με χρηματική ποινή τουλάχιστον 30 €.¹⁷⁴

¹⁷⁴ Καράκωστας Κ. Ιωάννης, "Δίκαιο και internet", σελ.141

3.2 Αυτορρύθμιση στο διαδίκτυο

Στην μέχρι τώρα ανάλυση, έχει γίνει αναφορά στα νομικά κείμενα (ελληνικά και κοινοτικά) που διέπουν το πλαίσιο λειτουργίας του internet και έχουν ως στόχο την προστασία της ιδιωτικότητας των χρηστών στο χώρο αυτό. Ωστόσο σε ορισμένες χώρες κυρίως στην Αμερική το νομικό πλαίσιο προστασίας προσωπικών δεδομένων στο διαδίκτυο είναι ιδιαίτερα ελαστικό και επικρατεί η αντίληψη ότι η αυτορρύθμιση είναι προτιμότερη και πιο λειτουργική απ' την κρατική νομοθετική παρέμβαση. Η έννοια της αυτορρύθμισης συνίσταται σε κανόνες που θεσπίζουν οι ίδιες οι εταιρίες, με τους οποίους ρυθμίζεται η επιχειρηματική τους πρακτική όσον αφορά την προστασία της ιδιωτικότητας. Στην Αμερική υπάρχουν δύο προγράμματα αυτορρύθμισης, το "TRUSTe (2002)" και το "Better Business Bureau's BBBOnline Privacy Programme (2002)", τα οποία τέθηκαν σε ισχύ ύστερα από τις απειλές της αμερικανικής κυβέρνησης ότι θα θεσπίσει νόμους για την προστασία στο διαδίκτυο, αν δεν υπάρξει κάποια ιδιωτική πρωτοβουλία. Και τα δύο αυτά προγράμματα αξιολογούν τις πολιτικές συλλογής και επεξεργασίας προσωπικών δεδομένων καταναλωτών στο διαδίκτυο που εφαρμόζουν οι επιχειρήσεις που δραστηριοποιούνται στο χώρο αυτό, επιβλέπουν τη συμμόρφωση των εταιριών στους κανόνες της αυτορρύθμισης και τέλος επιβάλλουν ποινές στις εταιρίες που παραβιάζουν τις αρχές που έχουν θεσπιστεί με τα προγράμματα αυτά. Ωστόσο τα δύο αυτά προγράμματα δεν είναι αποτελεσματικά, γιατί δεν απαιτούν απ' τους υπεύθυνους επεξεργασίας δεδομένων να παίρνουν τη συγκατάθεση των υποκειμένων πριν προχωρήσουν στην επεξεργασία και επιπλέον δεν ορίζουν αποζημίωση σ' αυτούς που βλάπτονται απ' την επεξεργασία.¹⁷⁵

Σε γενικές γραμμές πρέπει να αναφέρουμε ότι οι συνθήκες επιτυχίας προγραμμάτων αυτορρύθμισης στο χώρο του διαδικτύου δεν είναι ιδιαίτερα ευνοϊκές. Ένας απ' τους λόγους είναι η ανάγκη ύπαρξης κινήτρων για τις επιχειρήσεις προκειμένου να συμμετέχουν στα προγράμματα αυτά, που όμως είναι ανύπαρκτα στο διαδίκτυο. Τα κίνητρα αυτά είναι οικονομικά, καθώς για να

¹⁷⁵ Nakra Prema, "Consumer privacy rights: CPR and the age of the internet", www.emeraldinsight.com

συμμετέχει μια εταιρία σ' ένα πρόγραμμα αυτορρύθμισης πρέπει να της αποφέρει κέρδη, διαφορετικά θα προτιμήσει να μη συμμετέχει. Ωστόσο μια εταιρία που συμμορφώνεται σε κανόνες προστασίας της ιδιωτικότητας των καταναλωτών έχει μεγαλύτερο κόστος για τη συλλογή και επεξεργασία των προσωπικών τους δεδομένων, από μια εταιρία που δε συμμορφώνεται και μάλιστα σε πολλές περιπτώσεις μπορεί να καταστεί ζημιογόνα και να εγκαταλείψει την επιχειρηματική της δραστηριότητα. Άλλωστε ο καταναλωτής δεν αντιλαμβάνεται εύκολα αν μια επιχείρηση συμμορφώνεται ή όχι σε κώδικες δεοντολογίας.

Επίσης προκειμένου να λειτουργήσει αποτελεσματικά ένας κώδικας δεοντολογίας απαιτούνται πόροι και χρόνος για την επιτήρηση της συμμόρφωσης των επιχειρήσεων με αποτέλεσμα να αυξάνεται και το κόστος εφαρμογής τέτοιων προγραμμάτων. Γι' αυτό χρηματοδοτούνται από χορηγούς που είναι μεγάλες εταιρίες, που συμμετέχουν και αυτές, αλλά είναι ευνόητο ότι δεν υφίσταται τιμωρία σε περίπτωση παραβίασης των κανόνων, επειδή ακριβώς είναι χρηματοδότες. Χαρακτηριστικό είναι το παράδειγμα της Microsoft η οποία χρηματοδοτεί το πρόγραμμα TRUSTe, χωρίς όμως να συμμορφώνεται στους κανόνες συλλογής και επεξεργασίας προσωπικών δεδομένων που αυτό επιβάλλει. Παρ' όλα αυτά όμως το TRUSTe δεν επέβαλε κυρώσεις στη Microsoft.

Επιπρόσθετα, πρέπει να αναφερθεί ότι ο αριθμός των web sites στο internet είναι τόσο μεγάλος, που είναι ιδιαίτερα δύσκολη η επίβλεψη των επιχειρήσεων για το αν συμμορφώνονται ή όχι στους κώδικες δεοντολογίας με αποτέλεσμα αυτοί να καθίστανται αναποτελεσματικοί. Τέλος το γεγονός ότι το πρόσωπο του οποίου τα προσωπικά δεδομένα συλλέγονται και χρησιμοποιούνται κατά τρόπο παράνομο δεν έχει τη δυνατότητα να ζητήσει επανόρθωση, δίνει τη δυνατότητα στις επιχειρήσεις να δρουν χωρίς περιορισμούς.¹⁷⁶

¹⁷⁶Lee, Ya-Ching, "Will self-regulation work in protecting online privacy?", www.emeraldinsight.com

3.3 Συγκριτική μελέτη για την πολιτική προστασίας της ιδιωτικότητας στα sites των ΗΠΑ-Αγγλία-Γαλλία

Προηγουμένως έγινε εμφανές ότι το νομοθετικό πλαίσιο στις ΗΠΑ είναι πιο ελαστικό όσον αφορά την προστασία της ιδιωτικής σφαίρας τόσο γενικώς όσο και στο διαδίκτυο ειδικότερα, σε σχέση με το νομοθετικό πλαίσιο της Ευρωπαϊκής Ένωσης. Συγκεκριμένα, ενώ στις ΗΠΑ το ρυθμιστικό πλαίσιο περιορίζεται σε κάποιους κώδικες δεοντολογίας (αυτορρύθμιση), στην Ευρώπη παρενέβη ο Κοινοτικός νομοθέτης ο οποίος θέσπισε την Οδηγία 2002/58, στην οποία είναι υποχρεωμένα να συμμορφωθούν όλα τα κράτη-μέλη. Εξαιτίας των διαφορών αυτών στο νομικό καθεστώς, είναι διαφορετική και η τακτική που ακολουθούν πολλά sites όσον αφορά την πολιτική προστασίας προσωπικών δεδομένων. Παρακάτω θα παρατεθούν τα αποτελέσματα μιας συγκριτικής έρευνας¹⁷⁷ που έγινε το χρονικό διάστημα Φεβρουαρίου-Μαΐου 2003, σε sites της Αγγλίας, Γαλλίας και των ΗΠΑ, προκειμένου να διαπιστωθεί τι είδους πολιτική προστασίας της ιδιωτικότητας εφαρμόζουν. Ο συνολικός αριθμός των sites που εξετάστηκαν ήταν 291, απ' τα οποία τα 93 ήταν γαλλικά, τα 106 βρετανικά και τα 92 αμερικάνικα και αντιπροσώπευαν διάφορους τομείς της οικονομίας όπως π.χ. τον τομέα τροφίμων, ενδυμάτων, ηλεκτρονικών, καλλυντικών και τουρισμού.

Στον παρακάτω πίνακα παρουσιάζονται οι πληροφορίες που ζητούν όλα τα sites απ' τους επισκέπτες τους, κυρίως για να διεκπεραιώσουν τις συναλλαγές μαζί τους, αλλά και για να τα επεξεργαστούν για σκοπούς άμεσου Μkt, φτιάχνοντας το προφίλ των πελατών τους. Η συντριπτική πλειοψηφία των sites ζητούν το όνομα, τον ταχυδρομικό κώδικα και τη διεύθυνση e-mail του συναλλασσόμενου(προφανώς για την αποστολή ηλεκτρονικής αλληλογραφίας). Πληροφορίες για τον αριθμό της πιστωτικής κάρτας των χρηστών, συλλέγουν σε μεγάλη πλειοψηφία τα sites των ΗΠΑ, ίσως γιατί στην Αμερική οι χρήστες

¹⁷⁷ Calin Gurau, Ashok Ranchhod, Claire Gauzente, " To legislate or not to legislate: a comparative exploratory study of privacy/ personalisation factors affecting French, UK and US web sites", www.emeraldinsight.com

πραγματοποιούν σε μεγαλύτερο βαθμό on-line αγορές σε σχέση με τις ευρωπαϊκές χώρες καθώς δείχνουν και μεγαλύτερη εμπιστοσύνη στο διαδίκτυο.

Προσωπικά δεδομένα που συλλέγονται	Γαλλία (%)	Μ.Βρετανία (%)	ΗΠΑ (%)
Όνομα	98,9	100	100
Διεύθυνση e-mail	94,6	94,3	100
Ταχυδρομικός κώδικας	98,9	100	100
Αριθμός τηλεφώνου	89,2	87,7	95,7
Αριθμός fax	39,8	34	20,7
Αριθμός πιστωτικής κάρτας	84,2	89,6	94,6

Αντίθετα, τα sites συλλέγουν πολύ λίγες δημογραφικές πληροφορίες απ' τους επισκέπτες τους, κυρίως γιατί οι πελάτες αρνούνται να δώσουν τέτοιου είδους πληροφορίες που τις θεωρούν άκρως προσωπικές και ευαίσθητες όπως π.χ. το φύλο, η μόρφωση ή το εισόδημα. Όπως φαίνεται άλλωστε απ' τον παρακάτω πίνακα τα μόνα δημογραφικά στοιχεία που συλλέγει η πλειοψηφία των sites είναι η ηλικία και σε μικρότερο βαθμό τα χόμπι. Πληροφορίες σχετικά με τα χόμπι είναι ιδιαίτερα χρήσιμες στις εταιρίες καθώς μπορούν να σκιαγραφήσουν την προσωπικότητα των πελατών. Μάλιστα, απ' ότι φαίνεται πληροφορίες για το εισόδημα δε συλλέγει κανένα αμερικάνικο ή βρετανικό site και μόνο το 2,4% των γαλλικών, καθώς το εισόδημα θεωρείται άκρως εμπιστευτική πληροφορία.

Δημογραφικά στοιχεία που συλλέγονται	Γαλλία	Μ.Βρετανία	ΗΠΑ
Ηλικία	88,1	85,1	74,3
Μέγεθος οικογένειας	9,5	10,6	15,3
Φύλο	4,8	6,4	7,6
Μόρφωση	2,4	4,3	7,6
Εισόδημα	2,4	0	0
Χόμπι	19	11	20,5
Επάγγελμα	7,1	8,5	10,2

Όσον αφορά την πολιτική προστασίας της ιδιωτικότητας, πρέπει να πούμε ότι τα περισσότερα sites έχουν τουλάχιστον μια υποτυπώδη αναφορά στην πολιτική που ακολουθούν. Απ' τον παρακάτω πίνακα φαίνεται ότι τα sites των ΗΠΑ, δεν κάνουν εκτενή αναφορά στην πολιτική προστασίας που εφαρμόζουν, σε αντίθεση με τα sites της Γαλλίας και της Μ.Βρετανίας που δίνουν περισσότερες πληροφορίες. Συγκεκριμένα, το 44,6% των αμερικανικών sites αφιερώνει μία μόνο παράγραφο για να ενημερώσει τους πελάτες για την πολιτική προστασίας προσωπικών δεδομένων και το 31,5% αφιερώνει μία μόνο πρόταση. Αντίθετα το 50% των βρετανικών sites και το 37,6% των γαλλικών έχει εκτενή και λεπτομερή αναφορά για το θέμα αυτό, ενώ μόνο το 2,8% των βρετανικών δεν έχει καμία αναφορά.

Έκταση αναφοράς για την πολιτική προστασίας της ιδιωτικότητας	Γαλλία	Μ.Βρετανία	ΗΠΑ
Καμία αναφορά	4,3	2,8	8,7
Μία πρόταση	17,2	17	31,5
Μία παράγραφο	40,9	30,2	44,6
Εκτενής αναφορά	37,6	50	15,2

Στη συνέχεια, η έρευνα επικεντρώθηκε στις πληροφορίες που παρέχουν τα sites στους επισκέπτες τους σχετικά με την πολιτική προστασίας των προσωπικών δεδομένων που εφαρμόζουν. Εδώ οι διαφορές είναι μεγάλες, καθώς τα sites των ΗΠΑ είναι πιο αόριστα και περιλαμβάνουν πολύ λιγότερες πληροφορίες απ' τα άλλα sites. Συγκεκριμένα, μόνο το 29,2% των αμερικανικών sites αναφέρει τι είδους προσωπικά στοιχεία συλλέγουν σε αντίθεση με το 52% των γαλλικών και το 50% των βρετανικών. Επίσης, ο αριθμός των αμερικανικών sites που ενημερώνουν τον καταναλωτή για το δικαίωμά του να αρνηθεί την αποστολή διαφημιστικών μηνυμάτων στα πλαίσια του άμεσου Mkt είναι μόλις 59,7%, σε αντίθεση με τα γαλλικά και βρετανικά sites που ο αριθμός αυτός είναι πολύ μεγαλύτερος. Όσον αφορά τη χρήση cookies, ενώ η συντριπτική πλειοψηφία των sites χρησιμοποιεί cookies για να παρακολουθεί την πλοήγηση του χρήστη στο διαδίκτυο, μόνο τα μισά περίπου ενημερώνουν τον καταναλωτή για τη χρήση της τεχνολογίας αυτής.

Κατηγορίες πληροφοριών	Γαλλία	Μ.Βρετανία	ΗΠΑ
Πληροφορίες που ζητούνται απ' το χρήστη	52	50	29,2
Χρήση πληροφοριών	58,7	58,1	51,4
Χρήση cookies	57,3	60,5	52,8
Επιλογή άρνησης προσφορών	73,3	76,7	59,7
Επιλογή άρνησης προσφορών τρίτων	61,3	60,5	56,9

Τέλος, σχετικά με τη μεταβίβαση και τη διατήρηση προσωπικών δεδομένων πελατών, πρέπει να αναφερθεί ότι τα sites των ΗΠΑ παρέχουν περισσότερη πληροφόρηση σχετικά με την ασφάλεια στη διαβίβαση προσωπικών δεδομένων, σε σχέση με τις άλλες δύο χώρες (54,4% ΗΠΑ, 38,9% Γαλλία, 41,2% Μ.Βρετανία). Απ' την άλλη, παρέχουν λιγότερη πληροφόρηση στους καταναλωτές για τη διάρκεια και τις συνθήκες διατήρησης των δεδομένων, αν και οι διαφορές δεν είναι μεγάλες. Δηλαδή, μόλις το 3,3% των αμερικανικών sites κάνουν αναφορά στη χρονική διάρκεια διατήρησης των προσωπικών στοιχείων των πελατών τους, ενώ τα αντίστοιχα ποσοστά σε Γαλλία και Μ.Βρετανία είναι διπλάσια. Τέλος, τα sites των ΗΠΑ δίνουν τη δυνατότητα στα υποκείμενα των δεδομένων να παραπονεθούν στις εταιρίες για τη χρήση των προσωπικών τους στοιχείων (91,1%), ενώ στη Γαλλία και Αγγλία τα ποσοστά αυτά είναι μικρότερα (85,6% και 87,3% αντίστοιχα).

ΚΕΦΑΛΑΙΟ 4

Τεχνικά μέτρα προστασίας των δεδομένων στο διαδίκτυο

4.1 Εισαγωγή

Εκτός απ' τις νομικές ρυθμίσεις που μπορεί να προσφέρουν προστασία των προσωπικών δεδομένων των χρηστών που δραστηριοποιούνται στο διαδίκτυο, υπάρχουν και τεχνικές λύσεις που έχουν ως στόχο την εξασφάλιση της ανωνυμίας τους. Εκτός απ' την εξασφάλιση της ανωνυμίας, οι τεχνικές λύσεις μπορούν να χρησιμοποιηθούν προκειμένου να εξομαλυνθούν οι διαφορές μεταξύ των εθνικών νομοθεσιών, όπως για παράδειγμα με αυτοματοποίηση των συστημάτων γνωστοποίησης προς τις κεντρικές ρυθμιστικές Αρχές και ενημέρωσης των ενδιαφερομένων. Ειδικότερα υπάρχουν τεχνικά εργαλεία, όπως τα αποκαλούμενα "ευφυή" προγράμματα Η/Υ (intelligent agents) που έχουν τη δυνατότητα να αυτοματοποιήσουν τη διαδικασία ελέγχου της γνωστοποίησης προς τις αρχές και της ενημέρωσης των ενδιαφερομένων. Επιπλέον, το λογισμικό αυτό έχει τη δυνατότητα, συνδυάζοντας πληροφορίες για τις πρακτικές κάποιας ιστοσελίδας, να ελέγχει αν ικανοποιούνται οι απαιτήσεις της νομοθεσίας. Παρακάτω παρατίθενται τα εργαλεία που μπορούν να χρησιμοποιηθούν προκειμένου να εξασφαλιστεί η προστασία της ιδιωτικότητας των χρηστών στο internet.

4.2 Συστήματα PET ¹⁷⁸ (Privacy Enhancing Technologies)

Η προστασία που προσφέρει αυτή η τεχνολογία είναι συμπληρωματική και εντοπίζεται στην επίλυση του προβλήματος που αναφέρθηκε, δηλαδή στην τήρηση ή μη της ανωνυμίας του χρήστη κατά τη δραστηριότητά του στο internet. Τα περισσότερα PET στηρίζονται στη δημιουργία ειδικής τεχνικής υποδομής που εξασφαλίζει αρχικά ότι συλλέγονται μόνο οι πληροφορίες που συμφωνούν με κάποιες ήδη υπάρχουσες γενικές αρχές ή κανόνες. Κατόπιν αποκλείεται κάθε περαιτέρω επεξεργασία ασυμβίβαστη με τον αρχικό σκοπό ή τις γενικές αρχές

¹⁷⁸Lorrie Faith Cranor, "The Role of Privacy Enhancing Technologies", www.cdt.org

της συλλογής πληροφοριών. Αρκετά γνωστό παράδειγμα είναι οι «ασφαλείς» φάκελλοι (cryptolore). Με τη χρήση τεχνικών κρυπτογραφίας οι πληροφορίες που διακινούνται μέσω αυτών δεν είναι δυνατόν να χρησιμοποιηθούν για χρήσεις διαφορετικές απ' αυτές που έχει προδιαγράψει ο αποστολέας.¹⁷⁹

4.3 Πρότυπο καταγραφής στοιχείων OPS¹⁸⁰ (Open Profiling Standard)

Το Πρότυπο αυτό επιτρέπει την ανταλλαγή προσωπικών πληροφοριών μεταξύ των προγραμμάτων φυλλομέτρησης (browsers) και των ιστοσελίδων (web sites). Οι χρήστες μπορούν να καταχωρίσουν τις προσωπικές τους πληροφορίες (καταναλωτικό προφίλ) στο πρόγραμμα φυλλομέτρησης και έχουν τη δυνατότητα να θέσουν ειδική ένδειξη, ώστε να απαγορεύσουν ή να επιτρέψουν συγκεκριμένες χρήσεις για ορισμένες από αυτές τις πληροφορίες. Ως αποτέλεσμα, το πρόγραμμα φυλλομέτρησης θα αποκαλύπτει προς την ιστοσελίδα, σε κάθε επίσκεψη, μόνο εκείνα τα στοιχεία, τα οποία έχει επιτρέψει ο χρήστης να αποκαλύπτονται.

4.4 Πρότυπο P3P¹⁸¹

Το P3P είναι αποτέλεσμα της κοινής συναίνεσης στον τομέα της βιομηχανίας για τη δημιουργία μίας γλώσσας XML μέσω της οποίας να εκφράζονται οι πολιτικές προσωπικού απορρήτου τοποθεσιών Ιστού (Web site privacy policies). Η δημοσίευση του P3P ως Σύσταση W3C υποδηλώνει ότι πρόκειται για έγγραφο με σταθερή ισχύ, το οποίο συμβάλλει στη διαλειτουργικότητα του Παγκόσμιου Ιστού και το οποίο έχει αναθεωρηθεί από τα Μέλη του W3C τα οποία και ευνοούν την ευρεία υιοθέτησή του. Η Ομάδα εργασίας που σχεδίασε το P3P αποτελείται από νομικούς ειδικούς σε θέματα προσωπικού απορρήτου, ηγετικούς φορείς τεχνολογίας Παγκόσμιου Ιστού,

¹⁷⁹ Ειδικότερα υπάρχουν PETs τα οποία μπορούν: α) να φιλτράρουν τα “cookies” ή παρέχουν στο χρήστη τη δυνατότητα να τα ελέγξει β) να επιτρέψουν ανώνυμη περιήγηση ή περιήγηση με ψευδώνυμο σε ιστοσελίδες γ) να κρυπτογραφήσουν δεδομένα δ) να επιτρέψουν ασφαλείς πληρωμές ε) να εμποδίσουν τη διαφήμιση ζ) να εντοπίσουν λογισμικό που επιχειρεί να “κατασκοπεύσει” τις δραστηριότητες του χρήστη η) να φιλτράρουν το ηλεκτρονικό ταχυδρομείο θ) να ελέγξουν την πρόσβαση σε υπολογιστές ι) να ελέγξουν την πολιτική της ιστοσελίδας ι) να εκπαιδεύσουν τον χρήστη σε θέματα προστασίας

¹⁸⁰ John MacKinsey, “Open profiling standards- white papers”, www.intresearch.forbes.com

¹⁸¹ Edwards Lilian, “Consumer Privacy, On-line Business and the Internet: Looking for Privacy in all the wrong places”, International Journal of Law Information Technology, Oxford University Press 2003

υπεύθυνους επιτρόπους για την προστασία δεδομένων και εταιρίες παγκόσμιου ηλεκτρονικού εμπορίου.

Το P3P έχει ως στόχο να επιτρέψει στους χρήστες να αποκτήσουν, με πρότυπο, απλό και αυτοματοποιημένο τρόπο, μεγαλύτερο έλεγχο κατά τη διαχείριση προσωπικών πληροφοριών στις τοποθεσίες Ιστού που επισκέπτονται. Διαβάζει αυτόματα το κείμενο της πολιτικής προστασίας που πρέπει ήδη να διαθέτει η υπό επίσκεψη ιστοσελίδα και το συγκρίνει με τις προτιμήσεις του χρήστη. Επιτρέπει έτσι ένα είδος εικονικής διαπραγμάτευσης μεταξύ χρήστη και ιστοσελίδας ως προς τις πληροφορίες που επιτρέπεται να συλλέξει και να μεταβιβάσει περαιτέρω η ιστοσελίδα. Με βάση το πρότυπο αυτό οι χρήστες έχουν τη δυνατότητα να ελέγχουν πλήρως τη διασπορά των πληροφοριών στο δίκτυο. Ο χρήστης θέτει στον Η/Υ του τις αρχικές παραμέτρους, ως προς το βαθμό αποκάλυψης των προσωπικών του πληροφοριών και στη συνέχεια η χρήση των πληροφοριών απ' τις ιστοσελίδες τις οποίες επισκέπτεται, περιορίζεται από αυτές τις αρχικές παραμέτρους.

Οι χρήστες του Web επιθυμούν να γνωρίζουν πώς χρησιμοποιούνται οι προσωπικές τους πληροφορίες από τους δικτυακούς τόπους που επισκέπτονται. Ορισμένες εταιρείες έχουν κάνει προσπάθειες να παρουσιάσουν δημόσια την πολιτική τους για την προστασία δεδομένων των δικτυακών τους τόπων, αλλά συχνά οι πληροφορίες αυτές δεν είναι εύκολα προσβάσιμες και κατανοητές. Οι χρήστες του Web χρειάζεται να μπορούν γρήγορα και με βεβαιότητα να πληροφορούνται αν μία εταιρεία εμπλέκεται σε πρακτικές διάθεσης πληροφοριών για από κοινού χρήση οι οποίες συμφωνούν ή αντιτίθενται στις επιθυμίες τους.

Το P3P παρέχει τη δυνατότητα σε όποιον έχει δικτυακό τόπο να μεταφράζει τις πρακτικές του για την προστασία δεδομένων σε εντολές / δηλώσεις του P3P βασισμένες στην XML , οι οποίες μπορούν να ανακτηθούν αυτόματα και να ερμηνευτούν χωρίς δυσκολία από έναν πλοηγό που υποστηρίζει το P3P.

Οι υπηρεσίες που υποστηρίζουν το P3P θα ενδυναμώσουν τον έλεγχο του χρήστη τοποθετώντας πολιτικές προστασίας δεδομένων εκεί όπου μπορούν να τις βρουν οι χρήστες, παρουσιάζοντας πολιτικές σε μορφή κατανοητή, και δίνοντας τη δυνατότητα στους χρήστες να παίρνουν ενημερωμένες αποφάσεις βασισμένοι σε αυτές τις πολιτικές. Για υπηρεσίες ηλεκτρονικού εμπορίου και δικτυακούς τόπους, η χρήση του P3P μπορεί να προσφέρει εξαιρετικές εμπειρίες πλοήγησης για πελάτες-χρήστες χωρίς να τους δημιουργεί αβεβαιότητα για την προστασία δεδομένων.

4.5 Λογισμικό για τη διαχείριση προγραμμάτων cookies

Σε προηγούμενη ανάλυση έγινε ιδιαίτερη αναφορά στα προγράμματα cookies τα οποία χρησιμοποιούνται συχνά για να “κατασκοπεύουν” το χρήστη όταν “σερφάρει” στο internet και επισκέπτεται κάποια ιστοσελίδα. Γι’ αυτό, προκειμένου να διασφαλιστεί η ανωνυμία του κατά τη διάρκεια χρήσης του διαδικτύου, πρέπει να έχει τη δυνατότητα να περιορίζει ή να αποκλείει τη δημιουργία cookies. Δύο μέθοδοι εφαρμόζονται στην πράξη : (i) τα σύγχρονα προγράμματα φυλλομέτρησης επιτρέπουν στους χρήστες να επιλέξουν είτε (α) να ειδοποιούνται κάθε φορά που κάποιος server επιχειρεί να τοποθετήσει cookies ώστε να μπορούν να ματαιώσουν τη δημιουργία τους είτε (β) να αρνούνται όλα τα cookies. (ii) Ειδικό λογισμικό αναλαμβάνει να διαγράφει όσα cookies έχουν εγκατασταθεί χωρίς έγκριση του χρήστη. Σε ορισμένες περιπτώσεις, το λογισμικό αυτό έχει τη δυνατότητα να περιορίσει και τις βασικές πληροφορίες (header information) που αποστέλλονται απ’ τον τοπικό υπολογιστή προς την ιστοσελίδα.

4.5 Αναταχυδρόμοι (re-mailers) ¹⁸²

Οι ανώνυμοι αναταχυδρόμοι ηλεκτρονικού ταχυδρομείου, έχουν τη δυνατότητα να προωθήσουν τα μηνύματα, χωρίς να αποκαλύπτεται η ταυτότητα του αποστολέα. Ορισμένοι λειτουργούν μέσω των ιστοσελίδων, στις οποίες δημιουργείται και αποστέλλεται το μήνυμα χωρίς καμιά αναφορά στις πληροφορίες (π.χ. διεύθυνση, στοιχεία τοπικού Η/Υ κτλ) που αποκαλύπτουν τον

¹⁸² “Remailers”, www.emailprivacy.info/remailers

αποστολέα. Σε άλλες περιπτώσεις, οι αναταχυδρόμοι αναλαμβάνουν να παραλάβουν το μήνυμα, να μεταβάλλουν τη διεύθυνση, να αφαιρέσουν τις πληροφορίες με τις οποίες μπορεί να εντοπιστεί ο αποστολέας και να το αποστείλουν στον παραλήπτη.

Οι υπηρεσίες των αναταχυδρόμων προσφέρουν διαφορετικούς βαθμούς προστασίας και συνήθως έχουν τη δυνατότητα να αντιμετωπίσουν ακόμα και την περίπτωση των «ωτακουστών». Αυτοί προσπαθούν να εντοπίσουν τον αποστολέα και τον παραλήπτη των μηνυμάτων, παρακολουθώντας τα εξερχόμενα και εισερχόμενα μηνύματα, που διακινεί ο αναταχυδρόμος, και πραγματοποιώντας διαδοχικές ταυτίσεις του μεγέθους και του χρόνου αποστολής του κάθε μηνύματος.

4.6 Ενδιάμεσοι εξυπηρετητές^{183, 184} (Proxy Servers)

Οι ενδιάμεσοι εξυπηρετητές μπορούν να χρησιμοποιηθούν προκειμένου ο χρήστης να αποκρύψει την ταυτότητά του ή ως φράγμα (firewall) για να εμποδίσουν ορισμένα προγράμματα (π.χ. cookies) να προσεγγίσουν τον Η/Υ του χρήστη. Παραλλαγή της ανωτέρω μεθόδου είναι ο «ενδιάμεσος ανωνυμοποιητής», ο οποίος αναλαμβάνει να παρεμποδίζει τις ιστοσελίδες να συλλέγουν πληροφορίες για το χρήστη, να τον συνδέουν με πληροφορίες που προκύπτουν «κατά την πληκτρολόγηση» και να εγκαθιστούν προγράμματα cookies.

Στην πράξη, «ο ενδιάμεσος» είναι proxy server που λειτουργεί ανάμεσα στον τοπικό υπολογιστή του χρήστη και το διαδίκτυο. Όταν ο χρήστης επιθυμεί να επισκεφθεί μια ιστοσελίδα, απευθύνει το αίτημα προς τον «ενδιάμεσο». Ο «ενδιάμεσος» την ανασύρει και τη μεταφέρει στον Η/Υ του χρήστη, χωρίς ο υπολογιστής να συνδέεται απευθείας με την ιστοσελίδα, με αποτέλεσμα να μην μεταφέρονται πληροφορίες για τον χρήστη και να μην υπάρχει δυνατότητα εγκατάστασης προγραμμάτων cookies.

¹⁸³ Mark David, ‘‘ What is a proxy server? A word definition from the webpedia’’, www.webopedia.com

¹⁸⁴ Γιαννόπουλος Ν. Γιώργος, ό.π., σελ.156

4.7 The Mail Abuse Prevention System (MAPS)

Οι πάροχοι υπηρεσιών πρόσβασης (ISPs), στην πλειονότητά τους, διώκουν τους αποστολείς των μη ζητηθέντων μηνυμάτων. Ένας απ' τους τρόπους δράσης τους, μεταξύ άλλων, είναι ότι έχουν οργανωθεί μέσω ενός δικτύου εθελοντών διαχειριστών, γνωστού ως The "Mail Abuse Prevention System" (MAPS), που έχει δημιουργήσει τη μαύρη λίστα Realtime Blackhole List. Η λίστα αυτή είναι ένας μηχανισμός μαζικού αποκλεισμού και επιτρέπει στους διαχειριστές του συστήματος των ISPs που ελέγχουν χιλιάδες συνδρομητές και επιτυχητητές ταχυδρομείου να αλληλοενημερώνονται τακτικά για τις «επιθέσεις», δηλαδή τις επιχειρήσεις αποστολής μη ζητηθέντων ηλεκτρονικών μηνυμάτων και να απομονώνουν τις διευθύνσεις και τα ονόματα τομέα των παρόχων υπηρεσιών που είναι γνωστές πηγές μη ζητηθεισών εμπορικών επικοινωνιών. Έτσι, όταν λήξει η συνδρομή ενός spammer, μεταφέρεται στον κατάλογο ώστε οι υπόλοιποι ISPs-εν προκειμένω οι 2000 ISPs σε ολόκληρο τον κόσμο που είναι συνδρομητές στην RLB, δηλαδή το 1/3 της αγοράς- τους οποίους θα μπορούσε να προσεγγίσει ο spammer, είναι αμέσως ενήμεροι για την πραγματική φύση της δραστηριότητας του πιθανού πελάτη τους και μπορούν να του αρνηθούν την παροχή υπηρεσιών. Εκτός απ' τη βασική αρχή λειτουργίας ανταλλαγής πληροφοριών, το σύστημα MAPS αποτελεί επίσης ένα φίλτρο που επιτρέπει με τη βοήθεια αλγορίθμων, το αυτόματο πάγωμα της αποστολής μηνυμάτων που προέρχονται από γνωστούς spammers καθώς και από ISPs που τους φιλοξενούν και οι οποίοι θεωρείται ότι δεν εκπληρώνουν το καθήκον εξυγίανσης του δικτύου το οποίο έχουν αναλάβει εξ ονόματος της διαφύλαξης των συλλογικών συμφερόντων του διαδικτύου.¹⁸⁵

4.7 Κρυπτογραφία

Έχει ήδη αναφερθεί σε προηγούμενα κεφάλαια, ότι το διαδίκτυο παρέχει ανεπαρκή ασφάλεια στους χρήστες που σημαίνει ότι οι πληροφορίες που μεταφέρονται μέσω του internet είναι πιθανό να υποκλαπούν από τρίτους και να αλλοιωθεί ή να τροποποιηθεί το περιεχόμενό τους όπως και να συλληχθούν κατά

¹⁸⁵ Gauthronet Serge & Drouard Etienne, "Junk e-mail costs internet users euro 10 billion a year worldwide", www.europa.eu.int

παράνομο τρόπο δεδομένα που αφορούν τον ιδιωτικό βίο των χρηστών του δικτύου με απώτερο στόχο να χρησιμοποιηθούν για σκοπούς άμεσου Μkt. Ειδικότερα, λόγω της τεχνικής διάρθρωσης των ανοικτών δικτύων, όπως είναι το διαδίκτυο, στο οποίο οι πληροφορίες, τα δεδομένα Η/Υ, διαχωρίζονται σε επιμέρους «πακέτα» και μεταφέρονται μέσω διαφορετικών οδών, από ένα κομβικό σημείο σε άλλο, μέχρι να καταλήξουν στον προορισμό τους, είναι εύκολο για έναν ειδικό να αποκτήσει πρόσβαση στα δεδομένα αυτά.¹⁸⁶ Σε έρευνα που διενεργήθηκε απ' τη Datamonitor για τους Ευρωπαίους χρήστες του διαδικτύου έδειξε ότι το 80% αυτών ερευνούν τα ψηφιακά καταστήματα για την εύρεση προϊόντων και μόλις το 15% προβαίνει σε online αγορές, θέτοντας σαν κύριο αίτιο την έλλειψη εμπιστοσύνης στην ασφάλεια που προσφέρει το διαδίκτυο. Επίσης η ίδια έρευνα κατέληξε στο συμπέρασμα ότι το 70% των Ευρωπαίων χρηστών του διαδικτύου υπέδειξε την αύξηση της ασφάλειας ως τον κύριο παράγοντα παρότρυνσης για πραγματοποίηση αγορών μέσω internet.¹⁸⁷ Για να αποφευχθούν λοιπόν τα παραπάνω προβλήματα, αναπτύχθηκαν από την κρυπτογραφία, ένα κλάδο των εφαρμοσμένων μαθηματικών, μέθοδοι κρυπτογράφησης που εξασφαλίζουν την ασφαλή μεταφορά δεδομένων Η/Υ μέσω ανοικτών δικτύων. Ως "κρυπτογράφηση" νοείται ο μετασχηματισμός δεδομένων Η/Υ σε μη αναγνωρίσιμη μορφή με τη χρήση κατάλληλων αλγορίθμων, έτσι ώστε να μπορούν να αναγνωσθούν μόνο με τη βοήθεια ενός κλειδιού αποκρυπτογράφησης. Ολα τα συστήματα κρυπτογράφησης βασίζονται σε τέσσερα μέρη:

A) Το απλό κείμενο (plaintext): Αποτελεί το αρχικό μήνυμα που δημιουργεί ο χρήστης, το οποίο μπορεί να είναι όχι μόνο κείμενο αλλά και video, ήχος ή οποιοσδήποτε άλλος τύπος αρχείου.

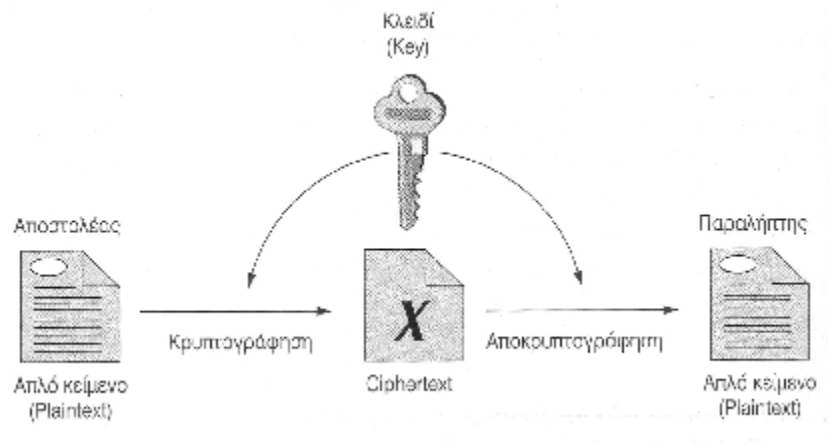
B) Κρυπτογραφημένο κείμενο (ciphertext): Αποτελεί το αρχικό απλό κείμενο το οποίο είναι όμως τροποποιημένο με τέτοιο τρόπο ώστε να μην μπορεί να διαβαστεί από τρίτους.

¹⁸⁶ Ιγγλεζάκης Δ. Ιωάννης, "Οι νομικές ρυθμίσεις για τις ψηφιακές υπογραφές, η οδηγία 1999/93 ΕΚ και οι εθνικές νομοθεσίες", ΕπισκΕΔ

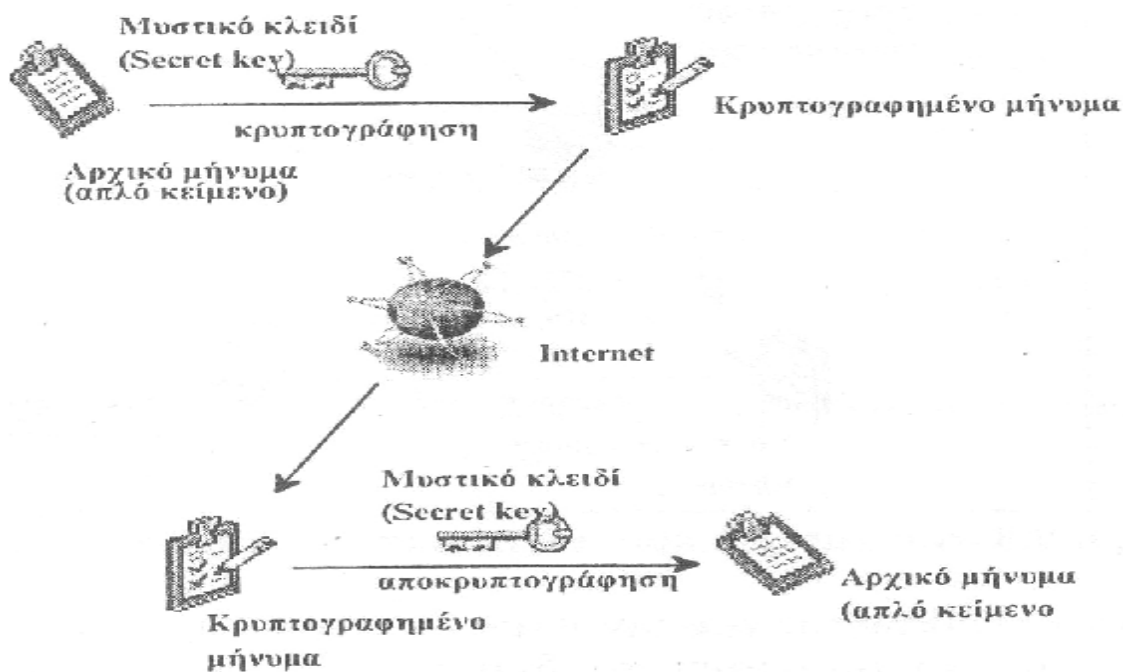
¹⁸⁷ Γεωργόπουλος Β. Νικόλαος,ό.π., σελ.251

Γ) Κρυπτογραφικός αλγόριθμος (cryptographic algorithm): Είναι μια μαθηματική λειτουργία, η οποία μετατρέπει το απλό κείμενο σε κρυπτογραφημένο και αντίστροφα.

Δ) Κλειδί (Key): Ένα μυστικό κλειδί χρησιμοποιείται για να κρυπτογραφήσει και αποκρυπτογραφήσει το μήνυμα. Κάθε κλειδί μετασχηματίζει το ίδιο απλό κείμενο σε διαφορετικό κρυπτογραφημένο κείμενο και μόνο οι κάτοχοι των κλειδιών μπορούν να διαβάσουν το κρυπτογραφημένο κείμενο.



Το βασικό χαρακτηριστικό των κρυπτογραφικών συστημάτων είναι ότι η ασφάλεια του συστήματος βασίζεται ολοκληρωτικά στη μυστικότητα του κλειδιού αποκρυπτογράφησης, καθώς εαν κάποιος λάβει το κρυπτογραφημένο κείμενο δεν μπορεί να το μετατρέψει στην αρχική του μορφή εφόσον δεν είναι κάτοχος του κλειδιού αποκρυπτογράφησης. Υπάρχουν δύο τύποι συστημάτων κρυπτογράφησης, το συμμετρικό κρυπτογραφικό σύστημα και το ασύμμετρο κρυπτογραφικό σύστημα. Τα συμμετρικά συστήματα, τα συστήματα δηλαδή που χρησιμοποιούν συμμετρικούς αλγόριθμους, έχουν ένα κοινό κλειδί για την κρυπτογράφηση και για την αποκρυπτογράφηση, το οποίο είναι γνωστό μόνο στον αποστολέα και τον παραλήπτη του μηνύματος και πρέπει να παραμένει μυστικό. Η τεχνολογία αυτή είναι κατάλληλη επομένως μόνο για κλειστές ομάδες χρηστών και όχι για συναλλαγές, στις οποίες μετέχει ένας μεγάλος αριθμός συναλλασσομένων όπως συμβαίνει στο διαδίκτυο.

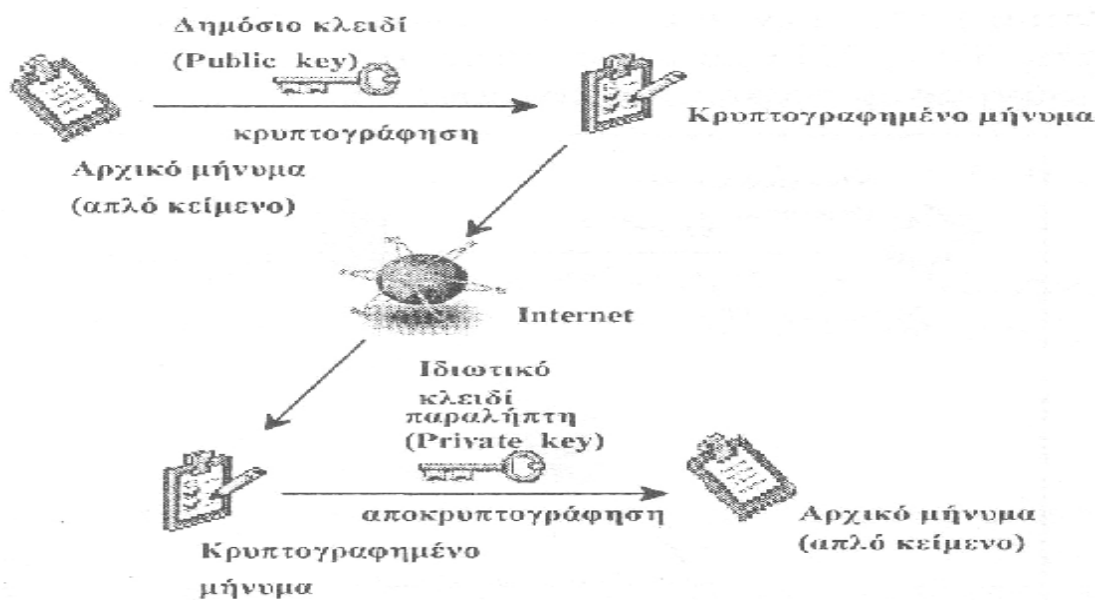


Για να ξεπεραστεί λοιπόν το πρόβλημα αυτό, ανακαλύφθηκε η ασύμμετρη κρυπτογράφηση. Στο σύστημα αυτό χρησιμοποιούνται ζευγάρια κλειδιών, το ένα για κρυπτογράφηση του μηνύματος και το άλλο για την αποκρυπτογράφησή του. Το ένα από τα δύο κλειδιά ονομάζεται δημόσιο κλειδί και διανέμεται δημοσίως, το άλλο ονομάζεται ιδιωτικό κλειδί και παραμένει μυστικό. Ο αποστολέας κρυπτογραφεί το κείμενο με το δημόσιο κλειδί του παραλήπτη μετατρέποντάς το σε ειδικής μορφής κείμενο και στη συνέχεια το στέλνει σε αυτόν. Ο κάτοχος του αντίστοιχου ιδιωτικού κλειδιού και παραλήπτης του μηνύματος είναι ο μόνος που μπορεί να αποκρυπτογραφήσει το απλό αυτό κείμενο. Το σύστημα κρυπτογράφησης με δημόσιο κλειδί αποτελεί ιδανική λύση για την επίτευξη ασφαλούς επικοινωνίας μέσω του διαδικτύου.^{188, 189, 190}

¹⁸⁸ “Ψηφιακή υπογραφή και νομοθεσία”, www.cgomag.gr

¹⁸⁹ Michel Gentot, “The privacy risks of public key infrastructures”, www.pco.org.com

¹⁹⁰ Δουκίδης Γεώργιος, ό.π., σελ.205



ΚΕΦΑΛΑΙΟ 5

Νομοθεσία άλλων χωρών για την προστασία δεδομένων

Στο σημείο αυτό κρίνεται σκόπιμο να γίνει μια περιληπτική αναφορά στη νομοθεσία ορισμένων μεγάλων ευρωπαϊκών και μη κρατών σχετικά με την προστασία των προσωπικών δεδομένων.

5.1 Γαλλία

Στη Γαλλία ισχύει ο νόμος 78/17 της 6^{ης} Ιανουαρίου 1978 για την πληροφορική, τα αρχεία και τις ατομικές ελευθερίες. Ο νόμος αυτός καθιερώνει ένα κεντρικό σύστημα καταχώρισης, το οποίο τηρείται και επιβλέπεται από ανεξάρτητη διοικητική αρχή, την CNIL. Η αρχή αυτή έχει καθήκον να ενημερώνει και να πληροφορεί το κοινό για τα δικαιώματα και τις υποχρεώσεις που προβλέπει ο νόμος, να εξετάζει τις προτάσεις του δημοσίου τομέα και να προτείνει τροποποιήσεις του νόμου εν όψει τεχνολογικών εξελίξεων. Επίσης έχει δικαίωμα να εκδίδει γνωμοδοτήσεις και να υποβάλλει σε προληπτικό έλεγχο τη διαβίβαση πληροφοριών στο εξωτερικό. Ενεργεί αυτεπαγγέλτως ή μετά από αίτηση, έχει δικαίωμα να διεξάγει ανακρίσεις και να εξασφαλίζει ότι τηρούνται τα δικαιώματα των πολιτών. Παράνομη επεξεργασία ή διακίνηση δεδομένων τιμωρείται με πρόστιμο ή φυλάκιση, ενώ ποινική δίωξη μπορεί να ασκηθεί από τις αρμόδιες εισαγγελικές αρχές.

Στα πλαίσια της αυτορύθμισης, η ένωση χρηστών διαδικτύου δημοσίευσε το 1997 τον «χάρτη του internet», ο οποίος προβλέπει τη δυνατότητα των χρηστών να διατηρούν την ανωνυμία τους και επιβάλλει στους παρόχους υπηρεσιών διαδικτύου να γνωστοποιούν στους χρήστες τα δεδομένα που συλλέγουν. Επίσης προβλέπει ως ανεξάρτητη επιβλέπουσα αρχή το «Συμβούλιο του internet», το οποίο έχει συμβουλευτικές και διαμεσολαβητικές αρμοδιότητες.

5.2 Γερμανία

Στη Γερμανία αναφέρεται για πρώτη φορά ειδική διάταξη για την προστασία δεδομένων στο Internet στο άρθρο 2§4 του Ομοσπονδιακού νόμου για τα Πολυμέσα της 22^{ης} Ιουλίου 1997. Με το νόμο αυτό επιβάλλεται υποχρέωση των παρόχων υπηρεσιών διαδικτύου να προσφέρουν στους χρήστες τη δυνατότητα ανώνυμης πρόσβασης και πληρωμής(με χρήση ψευδονύμου) όταν αυτό είναι εύλογο και τεχνικά επιτεύξιμο. Επιπλέον απαγορεύεται να μεταβιβασθούν σε τρίτους τα στοιχεία του χρήστη χωρίς τη συγκατάθεσή του ή να χρησιμοποιηθούν για εμπορικούς σκοπούς, για δημοσκοπήσεις καταναλωτών ή για έρευνα προκειμένου να εντοπισθεί η ανάγκη νέων μελλοντικών υπηρεσιών. Δεδομένα των χρηστών, εκτός απ' αυτά που απαιτούνται για να επιτευχθεί η σύνδεση, επιτρέπεται να τηρηθούν μόνο για την τιμολόγηση των υπηρεσιών και μόνο για διάστημα 80 ημερών. Προβλέπεται επίσης δικαίωμα πρόσβασης του χρήστη στα ανωτέρω δεδομένα σε απευθείας σύνδεση (online).¹⁹¹

5.3 Ηνωμένο Βασίλειο

Το 1998 εκδόθηκε ο Data Protection Act, ο οποίος αντικατέστησε τον προϊσχύσαντα νόμο προστασίας δεδομένων (Data Protection Act 1984) και προσαρμόζει τη βρετανική νομοθεσία προς την Οδηγία 95/46 ΕΚ. Ο νόμος αυτός θεσμοθετεί τον "Επιτρόπο πληροφοριών", ο οποίος έχει τη δυνατότητα να εξετάζει καταγγελίες, να εκδίδει οδηγίες συμμόρφωσης προς τους υπεύθυνους επεξεργασίας, να εκδίδει κώδικες συμπεριφοράς και τέλος να επιβλέπει τη νομοθεσία για την «ελευθερία στην πληροφόρηση». Επίσης ιδιαίτερα σημαντικό είναι ότι προβλέπει ειδική προστασία απ' την άμεση εμπορική προώθηση (άρθρο 11).

Όσον αφορά κανόνες αυτορρύθμισης, πρέπει να αναφερθεί ότι η βρετανική ένωση παρόχων υπηρεσιών internet, έχει εκδόσει Κώδικα συμπεριφοράς, υποχρεωτικό για όλα τα μέλη της, ο οποίος δίνει οδηγίες για τη μέθοδο γνωστοποίησης προς τον Επίτροπο και ενθαρρύνει τα μέλη να γνωστοποιούν

¹⁹¹ Γιαννόπουλος Ν. Γιώργος,ό.π., σελ.76

στους χρήστες τους σκοπούς συλλογής δεδομένων καθώς και το σχετικό δικαίωμα αντίρρησης. Επίσης η Συνομοσπονδία Βρετανικών Βιομηχανιών έχει δημοσιεύσει πρότυπους όρους σύμβασης για τη διαβίβαση δεδομένων προς τρίτες χώρες, τους οποίους υπέβαλε το 1998 προς έγκριση στη Γενική Διεύθυνση Εσωτερικής αγοράς της Ευρωπαϊκής Επιτροπής.

5.4 Ηνωμένες Πολιτείες Αμερικής

Παρ' ότι οι ΗΠΑ είναι ο κατ'εξοχήν υπέρμαχος της αυτορρύθμισης αρκετοί νόμοι επιβάλλουν σχετικές ρυθμίσεις. Ενδεικτικά:

1. Ο Ομοσπονδιακός Νόμος Εμπορίου του 1914, απαγορεύει τις αθέμιτες ή/ και απατηλές εμπορικές πρακτικές και επομένως καθιστά τις εταιρίες υπεύθυνες για τον τρόπο με τον οποίο παρουσιάζουν την πολιτική τους.
2. Ο νόμος του 1970 για την πιστοληπτική ικανότητα ρυθμίζει τη χρήση πληροφοριών που συλλέγονται από σχετικούς φορείς όπως οι εταιρίες ελέγχου πιστοληπτικής ικανότητας, οι εταιρίες ιατρικών δεδομένων και οι υπηρεσίες ελέγχου ενοικιαστών. Η εφαρμογή του νόμου ελέγχεται από την Ομοσπονδιακή Επιτροπή Εμπορίου. Ο νόμος προβλέπει δικαίωμα αστικής αποζημίωσης και επιβάλλει υποχρεώσεις ακόμη και στους προμηθευτές δεδομένων στις ανωτέρω εταιρίες.
3. Ο νόμος για τις ηλεκτρονικές επικοινωνίες του 1986 ρυθμίζει τη χρήση πληροφοριών που διαβιβάζονται με ηλεκτρονικό τρόπο. Ο νόμος προβλέπει ποινικές κυρώσεις και δικαίωμα αστικής αποζημίωσης.
4. Ο νόμος του 1991 για την προστασία των καταναλωτών τηλεπικοινωνιακών υπηρεσιών, που ρυθμίζει τις ανεπιθύμητες τηλεφωνικές κλήσεις.

Παρά την ύπαρξη κάποιων νόμων για την προστασία της ιδιωτικότητας στις ΗΠΑ, το κυρίως ρυθμιστικό πλαίσιο περιλαμβάνει κανόνες αυτορρύθμισης, όπως έχει αναλυθεί σε προηγούμενο κεφάλαιο. Ωστόσο η Ευρωπαϊκή Ένωση δε θεωρεί ότι μ' αυτόν τον τρόπο παρέχεται κατάλληλη προστασία σε όλες τις περιπτώσεις διαβίβασης προσωπικών δεδομένων από την Ε.Ε. και γι' αυτό

θεσπίστηκαν σε συνεργασία με τις αρχές των ΗΠΑ οι κανόνες του «ασφαλούς λιμένος». Σύμφωνα με τους κανόνες αυτούς, το Υπουργείο Εμπορίου των ΗΠΑ αναλαμβάνει την υποχρέωση να διατηρεί κατάλογο εταιριών οι οποίες αποδέχονται τις αρχές «ασφαλούς λιμένος», δηλαδή τηρούν ένα ελάχιστο σύνολο κανόνων προστασίας δεδομένων και αντίστοιχους μηχανισμούς ελέγχου. Η Ευρωπαϊκή Επιτροπή θεωρεί τη συμμετοχή μιας εταιρίας στον κατάλογο ως παροχή «ικανοποιητικού επιπέδου προστασίας» για τους σκοπούς της διασυνοριακής ροής δεδομένων προς τις ΗΠΑ. Οι Ευρωπαϊκές εταιρίες πλέον γνωρίζουν ότι μπορούν να πραγματοποιούν ελεύθερα συναλλαγές με εταιρίες στην άλλη πλευρά του Ατλαντικού, εφόσον οι τελευταίες έχουν προσχωρήσει στις αρχές «ασφαλούς λιμένος». Για τις εταιρίες που θα δηλώσουν συμμετοχή, αλλά δε θα συμμορφωθούν, προβλέπονται κυρώσεις με βάση την αμερικάνικη νομοθεσία. Ο «ασφαλής λιμήν», λειτουργεί από 1 Νοεμβρίου 2000, οπότε τέθηκε στη διάθεση των εταιριών ειδική ιστοσελίδα μέσω της οποίας μπορούν να καταχωρίσουν οι ίδιες σε απ' αυθείας σύνδεση τα στοιχεία τους ώστε να δηλώσουν συμμετοχή στο πρόγραμμα.¹⁹²

¹⁹² Γαννόπουλος Ν. Γιώργος,ό.π., σελ.80

ΣΥΜΠΕΡΑΣΜΑΤΑ

Απ' την παρούσα μελέτη έγινε εμφανές ότι οι σύγχρονες πρακτικές άμεσου μάρκετινγκ καθιστούν επιτακτική την ανάγκη για τις επιχειρήσεις να συλλέγουν και να επεξεργάζονται προσωπικά δεδομένα καταναλωτών προκειμένου να δημιουργούν πιο αποτελεσματικές πρακτικές μάρκετινγκ ικανοποιώντας πληρέστερα τις ανάγκες των καταναλωτών. Ωστόσο, συχνά οι επιχειρηματικές μονάδες προβαίνουν σε κατάχρηση των προσωπικών δεδομένων των υποκειμένων, παραβιάζοντας την ιδιωτικότητα του καταναλωτή και το δικαίωμα του πληροφοριακού αυτοκαθορισμού. Ιδιαίτερα στο διαδίκτυο η συλλογή προσωπικών πληροφοριών γίνεται ιδιαίτερα εύκολα, και μάλιστα συχνά χωρίς όχι μόνο τη συγκατάθεση αλλά ακόμα και τη γνώση του χρήστη, καθώς οι επιχειρήσεις χρησιμοποιούν εργαλεία για να παρακολουθούν την πλοήγηση του χρήστη στο διαδίκτυο και να συλλέγουν ποικίλες πληροφορίες γι' αυτόν.

Για την προστασία του πολίτη υπό την ιδιότητά του ως καταναλωτή, τα όργανα της Ευρωπαϊκής Ένωσης και οι εθνικές αρχές των κρατών μελών θέσπισαν σχετική νομοθεσία. Ωστόσο οι διαφορές στις νομοθεσίες των διαφόρων χωρών καθώς και η δυνατότητα των εταιριών να παραβιάζουν και να καταστρατηγούν τους νόμους, καθιστούν την αποτελεσματικότητα της νομοθεσίας περιορισμένη. Ιδιαίτερως η νομοθεσία που αφορά το spamming είναι αναποτελεσματική, καθώς είναι δύσκολη η εξεύρεση των spammers (συχνά αποκρύπτουν την ταυτότητά τους) και δεν μπορούν επομένως να τιμωρηθούν. Επίσης υπάρχει δυσκολία στη συλλογή αποδεικτικών στοιχείων διασυνοριακά καθώς το διαδίκτυο είναι ένα διεθνές μέσο επικοινωνίας και εμπορικών συναλλαγών.

Προκειμένου λοιπόν να αυξηθεί η προστασία των καταναλωτών απαιτείται ένας συνδυασμός της νομοθεσίας, της αυτορρύθμισης, της κατάλληλης τεχνολογίας και της εκπαίδευσης-ενημέρωσης των καταναλωτών για τα δικαιώματά τους, καθώς κάθε μία απ' τις παραπάνω λύσεις λειτουργώντας μεμονωμένα δεν επιφέρει το επιδιωκόμενο αποτέλεσμα. Όσον αφορά το

spamming πολλοί οργανισμοί προστασίας των καταναλωτών οργανώνουν ενίοτε προγράμματα ενημέρωσης των καταναλωτών για τις τεχνολογίες anti-spam και τους παρέχουν συμβουλές για την αποφυγή των ανεπιθύμητων ηλεκτρονικών μηνυμάτων.

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΕΛΛΗΝΙΚΗ

1. Αλεξανδρίδου Δ. Ελίζα, Δίκαιο προστασίας του καταναλωτή, Εκδόσεις Π.Ν. Σάκκουλας, Αθήνα-Θεσσαλονίκη, 1996
2. Αλεξανδρίδου Δ. Ελίζα, Δίκαιο Ηλεκτρονικού Εμπορίου, Εκδόσεις Π.Ν. Σάκκουλας, Θεσσαλονίκη 2004
3. Αραβαντινός Θ. Βασίλειος, Η προστασία των στοιχείων προσωπικού χαρακτήρα από την αθέμιτη επεξεργασία τους με Η/Υ, Εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα 1997
4. Βλαχοπούλου Μάρω, E-Marketing: πληροφοριακά συστήματα-νέες τεχνολογίες στο μάρκετινγκ, Εκδόσεις Rosili, 1999
5. Γαλάνης Π. Βασίλειος, Direct Marketing: η λογική του άμεσου μάρκετινγκ, Εκδόσεις Σταμούλης
6. Γέροντας Απόστολος, Πληροφορική και δίκαιο, Εκδόσεις Αντ.Ν. Σάκκουλας, Αθήνα –Κομοτηνή 1991
7. Γέροντας Απόστολος, Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία προσωπικών δεδομένων, Εκδόσεις Αντ.Ν. Σάκκουλας, Αθήνα-Κομοτηνή 2002
8. Γεωργόπουλος Β. Νικόλαος, Ηλεκτρονικό Επιχειρείν, προγραμματισμός και σχεδίαση, Εκδόσεις Ε. Μπένου, Αθήνα 2001
9. Γιαννόπουλος Ν. Γιώργος, Ροή πληροφοριών στο διαδίκτυο, Εκδόσεις Νομική Βιβλιοθήκη, 2002
10. Δελούκα-Ιγγλέση Κορνηλία, Ελληνικό και κοινοτικό δίκαιο του καταναλωτή, Εκδόσεις Σάκκουλα, Αθήνα 2003
11. Δουκίδης Ι. Γεώργιος, Ηλεκτρονικό Εμπόριο, Εκδόσεις Νέων Τεχνολογιών, Αθήνα 1998
12. Έκθεση Αρχής Προστασίας Προσωπικών Δεδομένων, 2002
13. Ιγγλεζάκης Ι. , Ευαίσθητα Προσωπικά Δεδομένα, Εκδόσεις Σάκκουλας, Αθήνα-Θεσσαλονίκη, 2003
14. Ιγγλεζάκης Δ. Ιωάννης, Το νομικό πλαίσιο του ηλεκτρονικού εμπορίου, Εκδόσεις Σάκκουλας, Αθήνα-Θεσσαλονίκη, 2003

15. Ιγγλεζάκης Δ. Ιωάννης , Απόφαση Μονομελούς Πρωτοδικείου Αθηνών 2110/2002, ΕπισκεΔ
16. Ιγγλεζάκης Δ. Ιωάννης, Οι νομικές ρυθμίσεις για τις ψηφιακές υπογραφές, η οδηγία 1999/93 ΕΚ και οι εθνικές νομοθεσίες, ΕπισκεΔ
17. Καράκωστας Κ. Ιωάννης, Δίκαιο και Internet, Εκδόσεις Π.Ν. Σάκκουλας, Αθήνα, 2003
18. Καράκωστας Ιωάννης, “Η προστασία του ιδιωτικού βίου των προσώπων της επικαιρότητας από τη σκοπιά του συγκριτικού δικαίου”, ΔΕΕ, τεύχος Δεκεμβρίου 1999
19. Κατσουλάκος Ιωάννης, “Νέα οικονομία, Διαδίκτυο και Ηλεκτρονικό εμπόριο”, Εκδόσεις Κέρκυρα, 2001
20. Κομνηνός Γ. Κόμνιος, Η ανεπιθύμητη εμπορική ηλεκτρονική αλληλογραφία (spamming), ΕπισκεΔ Δ/2002
21. Μήτρου Λίλιαν, Το δίκαιο στην Κοινωνία της Πληροφορίας, Εκδόσεις Αντ.Ν. Σάκκουλας , Αθήνα, 2002
22. Μήτρου Λίλιαν, Δόνος Π., Μίτλεττον Φ., Παπακωνσταντίνου Ευ., Η Αρχή προστασίας προσωπικών δεδομένων, Εκδόσεις Σάκκουλα, Αθήνα-Θεσσαλονίκη, 2002
23. Μπώκος Γ.Δ., Τεχνολογία και πληροφόρηση, Εκδόσεις Παπασωτηρίου, Αθήνα 2002
24. Νούσκαλης Γιώργος, Η προστασία των προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες σύμφωνα με τις νέες κοινοτικές ρυθμίσεις της οδηγίας 2002/58 ΕΚ, ΠοιΧρ 2003
25. Σιδηρόπουλος Θεόδωρος, “Το δίκαιο του διαδικτύου”, Εκδόσεις Σάκκουλας, Θεσσαλονίκη, 2003
26. Σκούρης Βασίλειος, Ιωάννου Κρατερός, Ελευθερία της διαφήμισης, Εκδόσεις Σάκκουλας, Θεσσαλονίκη 1996
27. Σταθόπουλος Μ., Τα συμφέροντα για την ακώλυτη ροή των προσωπικών δεδομένων, NoB, Ιανουάριος 2000
28. Σωτηρόπουλος Α. Βασίλης, Ηθική βλάβη από παράνομη αποστολή διαφημιστικών εντύπων, περιοδικό Συνήγορος, Νοέμβριος-Δεκέμβριος 2002
29. Τουντόπουλος Β., Το δικαίωμα ενημέρωσης του υποκειμένου των δεδομένων”, ΔΕΕ, Ιούνιος 1999

30. Περιοδικό ΧΡΗΜΑ, τεύχος 2^ο, Οκτώβριος 2001
31. Προσωπικά δεδομένα στο εμπόριο , τη διαφήμιση και τη συναλλακτική πίστη, Συνήγορος, τεύχος Σεπτεμβρίου-Οκτωβρίου 2004
32. Walther Stephen, Levine Jonathan, "Εγχειρίδιο προγραμματισμού e-commerce με ASP", Εκδόσεις Γκιούρδας, 2000

ΞΕΝΟΓΛΩΣΣΗ

1. Birkinshaw J., Why is knowledge Management so difficult?, Business Strategy Review, 2001
2. Cross Richard, Smith Janet, Customer Bonding, 5 steps to lasting customer loyalty, Prentice Hall, 1998
3. D. Peppers and Rogers M., Enterprise One to One: Tools for Competing in the Interactive Age, Doubleday Books, 1997
4. Edwards Lilian, Consumer Privacy, On-line Business and the Internet: Looking for Privacy in all the Wrong Places, International Journal of Law and Information Technology, Vol.11 No3, Oxford University Press 2003
5. Laudon C. Kenneth, Laudon P. Jane, Management Information Systems, Prentice Hall International editions, 6th edition
6. Murphy T. Daniel, Salinas Andres, Customer Relationship Management Technology and the Marina of the Near Future,
7. Perreault D. William, McCarthy E. Jerome, Basic Marketing, McGraw-Hill Irwin, 14th edition

ΔΙΚΤΥΑΚΟΙ ΤΟΠΟΙ

1. Armgard von Reden, "Data Protection Activities in the Private Sector", www.pco.org.com
2. Bayles Michelle, " Just how blind are we to advertising banners on the web?", www.usabilityiwes.com
3. Bullesbach Alfred, " Data protection and privacy at a global enterprise", www.pco.org.com
4. Carlos Rodriguez Casal, 'Regulating Spam: opting in or opting out?', www.emeraldinsight.com

5. Connell John ,“ Electronic Point of Sale”, www.techrepublic.com
6. Cooke Simon, “Database Marketing: Strategy or tactical tool?”, www.emeraldinsight.com
7. Cornell James,“ Personal and sensitive information”.
www.crimereduction.gov.uk
8. Dawn Anfuso, “Sales Revenue from DM and iMarketing On Rise”, 2002,
www.imediaconnection.com
9. Evans Martin, Lisa O’Malley and Maurice, “Direct Marketing: rise and rise or rise and fall?”, www.emeraldinsight.com
10. Feinberg A. Richards. and Mary Ann Eastlick, “Direct Marketing in the USA”,
www.emeraldinsight.com
11. Gauthronet Serge, Etienne Drouard, “Unsolicited Commercial Communications and Data Protection”, www.europa.eu.int
12. Gauthronet Serge & Drouard Etienne, “Junk e-mail costs internet users euro 10 billion a year worldwide”, www.europa.eu.int
13. Gentot Michel,“ The privacy risks of public key infrastructures’,
www.pco.org.com
14. Godwin J. Udo, “ Privacy and security concerns as major barriers for e-commerce: a survey study”, www.emeraldinsight.com
15. Gordon D. James, “ Geographic Information Systems”, www.qim.com
16. Gurau Calin, Ashok Ranchhod, Claire Gauzente, “ To legislate or not to legislate: a comparative exploratory study of privacy/ personalisation factors affecting French, UK and US web sites”, www.emeraldinsight.com
17. Harley Deborah, “ A whole world in one glance: Privacy as a key enabler individual participation in democratic governance”, www.pco.org.com
18. In Jazz J.Chen, Karen Popovich, “Understanding customer relationship management (CRM): people, process and technology”,
www.emeraldinsight.com
19. Karakaya Fahri, Charlton T. Earl, “Electronic Commerce: Current and Future Practices”, www.emeraldinsight.com
20. Lennon David, “The future of free information in the age of the internet”,
www.emeraldinsight.com

21. Light Ben, "CRM packaged software: a study of organizational experiences", www.emeraldinsight.com
- 22.. Lorrie Faith Cranor," The Role of Privacy Enhancing Technologies", www.cdt.org
23. MacKinsey John, "Open profiling standards- white papers", www.intresearch.forbes.com
24. Mark David," What is a proxy server? A word definition from the webpedia", www.webopedia.com
- 25.Mohsen Attaran, Ilja VanLaar,"Privacy and security on the internet: how to secure your personal information and company data", www.emeraldinsight.com
26. Nakra Prema,"Consumer privacy rights: CPR and the age of the internet", www.emeraldinsight.com
27. Ragavan C., "GATS-What is fact and what is fiction", www.citizen.org
28. Ryan Janet, Nancy Whiteman, "Defining the Medium", www.clickz.com
- 29.Schoenbachler D.Denise, Geoffrey L.Cordon, "Understanding consumer database marketing", www.emeraldinsight.com
30. Sharp Brenda, "Direct Marketing-the database", www.emeraldinsight.com
- 31.Thirlby P., "Geographic Information Systems in commercial property", www.emeraldinsight.com
32. Thornburg D. David, "Welcome to the communication age", www.emeraldinsight.com
- 33.Tombarge John, "Using management software for geographic information systems (GIS)", www.emeraldinsight.com
34. Waiman Cheung, "The use of the World Wide Web for commercial purposes", www.emeraldinsight.com
35. Wuorio Jeff, "7 Tips for keeping customers for life", www.microsoft.com
36. Yurong Xu, David C.Yen, Binshan Cin, "Adopting customer relationship management technology", www.emeraldinsight.com
37. Μαγιάση Έννυ,"Διαφήμιση και internet", www.lawnet.gr
38. Μπαλωμένου Χριστίνα, "Προσωπικά Δεδομένα", 2004, www.lawnet.gr

39. Σταμάτη Λαμπρινή, “Μας πουλάνε και μας αγοράζουν 15000 εταιρίες”, τεύχος 4/9/1999, [http:// ta-nea.dolnet.gr](http://ta-nea.dolnet.gr)
40. Σταμάτη Λαμπρινή, “Σερφάροντας στο internet αφήνουμε ίχνη που αποκαλύπτουν μυστικά...”, 22/04/2000, <http://ta-nea.dolnet.gr>
2. Έρευνα για τη χρήση του internet, www.europa.eu.int
3. “Towards a knowledge-based Europe”, 2002, www.europa.eu.int
6. “Δραστηριότητες του η-εμπορίου: Ραγδαία ανάπτυξη των online αγορών”, 2002, www.go-online.gr
11. “Vertical Market Trends in Direct Mail and the Impact on Production Service Providers”, FreshAddress Inc., www.the-dma.org
14. “CRM architecture for enterprise relationship Mkt in the new millenium”, White Paper, www7hp.com
25. Τράπεζα Πληροφοριών “Τειρεσίας”, www.teiresias.gr
26. The European Opinion Research Group, www.europa.eu.int
29. “Oecd guidelines on the Protection of privacy and transborder flows of personal data”, www.oecd.org
30. Σύμβαση για την προστασία του ατόμου απ’ την αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων, διαθέσιμο στο <http://conventions.coe.int>
32. Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου, διαθέσιμο στο www.lawnet.gr
36. Απόφαση 523/18 της Αρχής Προστασίας Προσωπικών Δεδομένων, www.dpa.gr
37. “Πενταετία ανάπτυξης για το ηλεκτρονικό εμπόριο”, 2002, www.go-online.gr
38. Έρευνα της Forrester Research για το ηλεκτρονικό εμπόριο στην Ελλάδα, 2004, www.go-online.gr
44. “Σε άνοδο οι online διαφημίσεις”, 2004, www.go-online.gr
45. “Σε νέες τεχνολογίες στρέφεται η διαφήμιση”, 2004, www.go-online.gr
50. “Πόσο κοστίζει η ανεπιθύμητη ηλεκτρονική αλληλογραφία”, www.go-online.gr

51. IMT: "Permission E-mail: The Future of Direct Marketing", www.imtstrategies.com
53. "Η λύση της αναφοράς...Μάλλον η προτιμότερη", www.go-online.gr
58. Nixon Peabody LLP, "The CAN-SPAM Act of 2003: Overview and Analysis", www.nixonpea.com
63. "Remailers", www.emailprivacy.info/remailers
65. "Ψηφιακή υπογραφή και νομοθεσία", www.cgomag.gr
68. DCI e-university, Your Resource for success in Customer Relationship Management, www.crmcommunity.com