Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Πληροφορική»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Η αντιμετώπιση του Spamming από την Ελληνική και τις Αλλοδαπές έννομες τάξεις**
Ονοματεπώνυμο Φοιτητή	**Vreko Shkelqim**
Πατρώνυμο	**Veis**
Αριθμός Μητρώου	**ΜΠΠΛ / 09071**
Επιβλέπων	**Αριστεα Σινανιωτη, Καθηγήτρια**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Αριστεα Σινανιωτη Καθηγήτρια	Θεμιστοκλής Παναγιωτόπουλος Καθηγητής	Δημήτριος Δ. Βέργαδος Επ. Καθηγητής

Αφιερωση

Θα ήθελα να αφιερώσω την παρούσα εργασία στους γονείς μου οι οποίοι μου παρείχαν όλα τα απαραίτητα εχέγγυα για την ολοκλήρωση των σπουδών μου, και στη σύντροφό μου Αννα Μαρια η οποία είναι δίπλα μου τα τελευταία δεκα χρόνια.

Ημερομηνία Παράδοσης : **18 Δεκέμβριου , 2012**

.....

Shkelqim V. Vreko

Διπλωματούχος Μεταπτυχιακών Σπουδών «Πληροφορική» και Μηχανικός Υπολογιστών συστημάτων Α.Τ.Ε.Ι Πειραιά.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Περίληψη – Λέξεις Κλειδιά 6
1. Εισαγωγή 7
2. Ηλεκτρονικό Εμπόριο 8
2.1 Εννοια του ηλεκτρονικού εμπορίου 8
2.2 Ηλεκτρονικό Εμπόριο και Ελληνική νομοθεσία 9
2.3 Βασικές κατηγορίες του ηλεκτρονικού εμπορίου 10
3. Έννοιες – Ορισμοί περί αυτόκλητων μηνυμάτων – Spam 10
3.1 Μορφές διαφήμισης 11
3.2 Διαφήμιση μέσω Internet 12
3.3 Τι είναι Spam 14
3.4 Γεωγραφικά ποσοστά των spammers 17
3.5 Ποιοι είναι οι spammers (Λίστα Ελλήνων Spammer) 18
3.6 Βασικά χαρακτηριστικά του Spam 19
3.7 Μορφές Spam μηνυμάτων 20
3.8 Τύποι Spam μηνυμάτων 21
3.8.1 Spam τύπου Phishing emails 21
3.8.2 Spam τύπου Chain emails 22
3.8.3 SPIT (Spam over Internet Telephony) μορφές 22
4. Ρυθμιστικό πλαίσιο αντιμετώπισης των Spam 24
4.1 Αρχή Προστασίας Προσωπικών Δεδομένων 24
4.2 Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών 24
4.3 Ο Ελληνικός Φορέας Πρόληψης Τηλεπικοινωνιακής Απάτης 25
4.3.1 Προσωπικά δεδομένα και spam 25
4.3.2 Το Spam ως παραβίαση των δικαιωμάτων προστασίας της ιδιωτικής ζωής και προστασίας των δεδομένων 27
4.4 Νομικοί Ορισμοί αναφορικά με το Spam 27
4.5 Υιοθέτηση των οδηγιών στην Ευρωπαική Ενωση 28
5. Νομοθεσία χωρών εντός Ευρωπαϊκής Ένωσης για την αντιμετώπιση του Spam 32
5.1 Η νομοθεσία για το Spam στην Ελλάδα 32
5.2 Η νομοθεσία για το Spam στο Ηνωμένο Βασίλειο 36
5.3 Η νομοθεσία για το Spam στην Ιταλία 36
5.4 Η νομοθεσία για το Spam στην Ομοσπονδιακή Δημοκρατία της Γερμανίας 37
5.5 Η νομοθεσία για το Spam στην Ισπανία 38
5.6 Η νομοθεσία για το Spam στην Δημοκρατία της Τσεχίας 38
6. Νομοθεσία χωρών εκτός Ευρωπαϊκής Ένωσης για την αντιμετώπιση του Spam 38
6.1 ΗΠΑ (Ηνωμένες Πολιτείες Αμερικής) 39
6.2 Καναδάς 41
6.3 Αυστραλία 43
6.4 Νέα Ζηλανδία 43
7. Σύγκριση νομοθετικών πλαισίων για την αντιμετώπιση των Spam 43
7.1 Επισκόπηση των μέτρων αντιμετώπισης του Spam βάση των Νομοθεσιών των Πολιτειών των ΗΠΑ 44
7.2 Διάκριση μεταξύ κοινοτικού δικαίου και δικαίου χωρών εκτός Ευρωπαϊκής Ένωσης όπως ΗΠΑ 45

8. Τρόποι προστασίας από τα Spam μηνύματα 46
8.1 Εφαρμογές αντι-phishing τακτικών 47
8.2 Εμπειρικοί τρόποι προστασίας από το Spam 47
8.3 Φόρμα Καταγγελίας κατά των spammers στο Εξωτερικό/Εσωτερικό 48
8.4 Πολέμιος των spammers 50
9. Ανάλυση τεχνικών μεθόδων και αρχιτεκτονικών των Spam 52
9.1 Μέθοδοι αντιμετώπισης ανεπιθύμητης αλληλογραφίας 53
9.1.1 Μέθοδοι από την πλευρά του αποστολέα (Sender Side (Pre-send) Methods) 54
9.1.2 Μέθοδοι από την πλευρά του παραλήπτη (Receiver Side (Pre-send) Methods) 56
9.2 Συνδυασμός μεθόδων – Ολοκληρωμένες λύσεις 64
9.2.1 SpamGuru 64
9.2.2 Filtron 66
9.2.3 Mailscanner χρησιμοποιώντας SpamAssassin 67
9.2.4 Φιλτράροντας εικόνα και κείμενο με το SPAMFighter 68
9.3 Συγκριτική μελέτη των χαρακτηριστικών κάθε μεθόδου 70
9.3.1 Money based solution 70
9.3.2 Προσέγγιση βασιζόμενη στην πηγή του ηλεκτρονικού μηνύματος 70
9.3.3 Προσέγγιση βασιζόμενη στο περιεχόμενο του μηνύματος 71
10. Γιατί το Spamming αποτελεί πρόβλημα 71
10.1 Αποφάσεις εναντίον του spamming 72
11. Συμπεράσματα 82
12. Πηγές & Πληροφορίες 84

Περίληψη

Κύριως στόχος της παρούσας διπλωματικής είναι η ανάλυση των νομικών διατάξεων, τεχνικών μεθόδων όπως και αναφορά στην αρχιτεκτονική διαφόρων φίλτρων προκειμένου να περιοριστεί ή να βρεθεί λύση στο πρόβλημα που αντιμετωπίζουν καθημερινά οι χρήστες του ηλεκτρονικού ταχυδρομείου, με την εμφάνιση της αυτόκλητης και μην ζητηθείσας εμπορικής επικοινωνίας. Η αυτόκλητη και μην ζητηθείσα εμπορική επικοινωνία γνωστή και ως Spam ήταν ανέκαθεν ένα αρκετά σοβαρό πρόβλημα των ηλεκτρονικών μηνυμάτων και έχει φτάσει πλέον σε ένα σημείο όπου δημιουργεί μείζον πρόβλημα στην ανάπτυξη του ηλεκτρονικού εμπορίου και της κοινωνίας των πληροφοριών. Σήμερα εκτιμάται ότι ένα αρκετά μεγάλο ποσοστό των ηλεκτρονικών μηνυμάτων είναι Spam. Ωστόσο, λόγω της δυσκολίας και της πολυπλοκότητας του προβλήματος, το ζήτημα της εφαρμογής και επιβολής του νόμου σε ένα παγκόσμιο περιβάλλον δεν έχει επιλυθεί. Η παρούσα διατριβή παρέχει μια επισκόπηση στο ηλεκτρονικό εμπόριο και των διαφόρων νόμων σχετικά με το πρόβλημα του Spamming επίσης γίνεται σύγκριση της αντι-spam νομοθεσίας των Ηνωμένων Πολιτειών και της Ευρωπαϊκής Ένωσης (Ε.Ε) και άλλων χωρών.

Λέξεις Κλειδιά:

Spamming, Ποινικό Δίκαιο και Η/Υ, Διαφήμιση στο διαδίκτυο, Μην ζητηθείσα εμπορική επικοινωνία, Προστασία των Δεδομένων Προσωπικού Χαρακτήρα στο Διαδίκτυο, Ηλεκτρονικό Εμπόριο.

Abstract

The main aim of this thesis is the analysis of the legal provisions, such as techniques and reference architecture of different filters in order to reduce or resolve the problem faced daily users of email, with the advent of unsolicited and not unsolicited commercial communications. Unsolicited and not requested advertising known as Spam has always been a fairly serious problem of emails and has now reached a point where it creates a major problem in the development of electronic commerce and information society. Today it is estimated that a sizable percentage of e-mails are Spam. However, because of the difficulty and complexity of the problem, the issue of implementation and enforcement in a global environment has not been resolved. The present thesis provides an overview of e-commerce and the various laws concerning the problem of Spamming also compare the anti-spam legislation in the United States and the European Union (EU) and other countries.

Key Words:

Spamming, Criminal Law and Computer, Advertising on the internet, Unsolicited and not requested advertising, Protection of Personal Data on the Internet, e-commerce.

1. Εισαγωγή

Η ιστορία της λέξης *spam* **[1]** ξεκινά από τη σύνθεση των λέξεων "Spiced Pork And Meat" και αρχικά αποτέλεσε κατοχυρωμένο εμπορικό σήμα της Hormel Foods Corporation ενός καινούριο είδος κρέατος που παρουσιάστηκε στην αγορά το 1937. Ήταν ένα καινοτομικό προϊόν καθώς προσέφερε «φρέσκο» κρέας χωρίς την ανάγκη κατάψυξης σε μια εποχή που το φρέσκο κρέας ήταν δυσεύρετο. Μετά τη λήξη του πολέμου όμως και το πέρασμα των χρόνων με τη βελτίωση του βιοτικού επιπέδου, το spam κατέληξε να είναι ένα αζήτητο προϊόν.

Το 1970 σ' ένα σκετς των *Μόντι Πάιθονς* **[1]**, εμφανίζεται μια κυρία με το σύζυγό της να δίνουν ή να προσπαθούν να δώσουν την παραγγελία τους στη σερβιτόρα ενός εστιατορίου. Η κυρία, έκπληκτη, αντιλαμβάνεται ότι στο διαθέσιμο μενού δεν υπάρχει ούτε ένα φαγητό χωρίς να περιέχει κάποια ποσότητα spam. Δίπλα στο προβληματισμένο ζεύγος, μια παρέα από… Βίκινγκς, ακούγοντας τα διαδραματιζόμενα, τραγουδούν την αγάπη τους για το spam, το εκλεκτό τους μεζεδάκι. Πρόκειται για μια ιστορική στιγμή, αναλογιζόμενοι ότι αυτός ή αυτοί που έδωσαν την ονομασία spam στην αυτόκλητη και ανεπιθύμητη διαφημιστική αλληλογραφία εμπνεύστηκαν από αυτή τη σκηνή.

Ήταν *3 Μαΐου του 1978* όταν ένας υπάλληλος από το τμήμα μάρκετινγκ της εταιρείας υπολογιστών DEC (Digital Equipment Corporation) έστειλε ένα μήνυμα για ένα νέο προϊόν της σε 400 χρήστες του *Arpanet* **[2]**, προκειμένου να διαφημίσει το καινούργιο προϊόν της εταιρίας του. Τριάντα χρόνια μετά το 80% των μηνυμάτων email θεωρείται ότι είναι spam, μία λέξη που προήλθε από ένα …σκετς των Μόντι Πάιθονς, όπως σημειώνει το BBC σε ένα ρεπορτάζ της.

Τα πρώτα spam στο *web* **[1]**, στη μορφή που είναι γνωστά σήμερα, εμφανίστηκαν στις ΗΠΑ γύρω στα μέσα της δεκαετίας του 90΄. Το πρώτο ήταν θρησκευτικού περιεχομένου και έφερε τον πολλά υποσχόμενο τίτλο: "*Ο Ιησούς έρχεται*!". Το επόμενο επίσης, από τις πιο γνωστές πρώτες προσπάθειες spamming είναι η αποστολή διαφήμισης μέσω του δικτύου USENET από δύο δικηγόρους του Phoenix σχετικά με τις παρεχόμενες από εκείνους νομικές υπηρεσίες σε θέματα μεταναστευτικής νομοθεσίας.

Έχοντας εξετάσει ιστορικά το θέμα των spam, παρακάτω γίνεται αναφορά για το spam στις μέρες μας και γιατί είναι ένα από τα σοβαρότερα και δύσκολα προβλήματα. Σε αρκετές χώρες το spam αποτελεί ένα από τα μεγαλύτερα προβλήματα στη διαδικτυακή ζωή πολλών χρηστών και στην πλειοψηφία των επιχειρήσεων. Πρόκειται για φαινόμενο παγκόσμιας κλίμακας, που εξαπλώνεται με εκθετικούς ρυθμούς, μέσω της σύγχρονης ψηφιακής τεχνολογίας **[3]**. Στην Ελλάδα το πρόβλημα αυτό βρίσκεται σε πολύ πιο περιορισμένο επίπεδο, σαφώς όμως δεν μπορεί να υπάρξει εφησυχασμός.

Δισεκατομμύρια spam ηλεκτρονικά μηνύματα κατακλύζουν τα ηλεκτρονικά ταχυδρομεία **[4]** των χρηστών και των επιχειρήσεων, παρότι επίσης δισεκατομμύρια είναι αυτά που φιλτράρονται από τους παρόχους υπηρεσιών πριν φτάσουν στους παραλήπτες τους. Έχει υπολογιστεί ότι καθημερινά, κατά μέσο όρο, αποστέλλονται ανά τον κόσμο δισεκατομμύρια spam ηλεκτρονικά μηνύματα, όπου ολοένα και αυξάνονται, οδηγώντας έτσι σε εξάντληση των διαθέσιμων πόρων του παγκόσμιου ιστού και στην υπερφόρτωση των συστημάτων. Για τους χρήστες ηλεκτρονικού ταχυδρομείου η ανεξέλεγκτη ροή απρόσκλητων διαφημιστικών εμπορικών μηνυμάτων, πέρα από ενόχληση συνιστά και απειλή. Το περιεχόμενο των μηνυμάτων αυτών συχνά είναι ακατάλληλο, ενώ δεν είναι σπάνιες οι καλά οργανωμένες απάτες. Οι ανήλικοι και οι αφελείς ενήλικοι κινδυνεύουν περισσότερο, χωρίς αυτό να σημαίνει ότι και πανέξυπνοι διαδικτυακοί περιηγητές δεν έχουν εξαπατηθεί.

Στις επιχειρήσεις υπάρχει μεγάλη απώλεια χρόνου για το ξεκαθάρισμα της αλληλογραφίας τους, κάτι που προκαλεί σημαντική επιβάρυνση στους δείκτες παραγωγικότητας των εργαζομένων. Οι εργαζόμενοι θα πρέπει, πολλές φορές την ημέρα, να ελέγχουν το ηλεκτρονικό τους ταχυδρομείο, θα πρέπει δηλαδή να ανοίγουν τα μηνύματα που αφορούν την επιχείρησή τους και να διαγράφουν τα μηνύματα spam (που αρκετές φορές αποτελούν την πλειοψηφία). Οι περισσότεροι κάνουν πλήρη και χρονοβόρο έλεγχο σε ολόκληρη την αλληλογραφία τους (ανοίγουν και εξετάζουν με

προσοχή όλα τα μηνύματά τους), κάποιες φορές από περιέργεια, συνήθως όμως για να σιγουρευτούν ότι δεν θα διαγράψουν από λάθος κάτι σημαντικό για την εταιρία τους. Επίσης, χρησιμοποιώντας ειδικά φίλτρα για το spam (όπου θα αναφερθούν στα επόμενα κεφάλαια), ώστε να περιορίσουν κάπως τις συνολικές ποσότητες spam ηλεκτρονικών μηνυμάτων που λαμβάνουν, κάποια από τα μηνύματα που θα ήθελαν να διαβάσουν διαγράφονται δίχως να έχουν κάποιο τρόπο να τα ανακτήσουν. Οι συνολικές απώλειες εργατοωρών και το κόστος στο σύνολο της οικονομίας φθάνουν σε πολύ υψηλά επίπεδα. Προβλήματα δημιουργεί επίσης και στους Παρόχους Υπηρεσιών Διαδικτύου (ΠΥΔ), καθώς μπορεί να μειώσει την ποιότητα των παρεχόμενων υπηρεσιών και τον χρόνο απόκρισης του δικτύου τους, πλήττοντας έτσι τη διαθεσιμότητα και αξιοπιστία τους.

Αν και οι χρήστες έχουν τη δυνατότητα συχνών αλλαγών των ηλεκτρονικών διευθύνσεών τους (μέσω webmail), αυτό δεν είναι εφικτό για τις επιχειρήσεις, οι οποίες για λόγους κύρους δεν μπορούν να χρησιμοποιήσουν webmail λογαριασμούς, ενώ παράλληλα η ηλεκτρονική διεύθυνση τους αποτελεί ένα ακόμα στοιχείο της επιχειρησιακής τους ταυτότητας. Μια αλλαγή της ηλεκτρονικής τους διεύθυνσης μπορεί να οδηγήσει σε αρκετά λειτουργικά προβλήματα.

Επιπλέον, τα μηνύματα spam, εκτός από ενοχλητικά, μπορεί να είναι προσβλητικά, απατηλά ή ακόμα και επικίνδυνου περιεχομένου. Για παράδειγμα αρκετά μηνύματα spam σήμερα διαφημίζουν πλαστά προϊόντα (π.χ. φαρμακευτικά προϊόντα ή προϊόντα λογισμικού) ως προϊόντα γνωστών εταιρειών, διαδίδουν παραπλανητικές ειδήσεις, ή / και προωθούν προϊόντα και υπηρεσίες σεξουαλικού ή / και πορνογραφικού χαρακτήρα. Επίσης, τα μηνύματα spam χρησιμοποιούνται συχνά και ως μέσα μετάδοσης ιών ή άλλων επιβλαβών ή / και κατασκοπευτικών λογισμικών.

Η δομή της διπλωματικής όπως παρουσιάζεται παρακάτω έχει ως εξής : το δεύτερο κεφάλαιο παρουσιάζουμε μια σφαιρική εικόνα και βασικών κατηγοριών του ηλεκτρονικού εμπορίου, στο τρίτο κεφάλαιο γίνεται αναλυτική αναφορά των εννοιών – ορισμών περί των αυτόκλητων μηνυμάτων (spam), αναφέρονται οι μορφές της διαφήμισης γενικώς και ειδικότερα οι κατηγορίες της διαφήμισης μέσω Internet. Γίνεται ανάλυση τι είναι spam, ποιοι είναι οι spammers, τα βασικά χαρακτηριστικά του spam και αναφέρονται περιληπτικά δύο μορφές spam μηνυμάτων και εστιάσουμε την προσοχή μας στο τι είναι τα φίλτρα. Στο τέταρτο κεφάλαιο αναλύεται το ρυθμιστικό πλαίσιο αντιμετώπισης των spam της Ευρωπαϊκής Ένωσης, των χωρών εντός της Ευρωπαϊκής Ένωσης και των χωρών εκτός της Ευρωπαϊκής Ένωσης. Εφόσον πρωτίστως έχουν ειπωθεί οι νομικές έννοιες και ορισμοί αναφορικά με το spam. Στο πέμπτο κεφάλαιο, βάση των όσον έχουν αναφερθεί στα προηγούμενα κεφάλαια γίνεται διάκριση μεταξύ του κοινοτικού δικαίου και δικαίου χωρών εκτός Ευρωπαϊκής Ένωσης όπως αυτό των ΗΠΑ. Στο έκτο κεφάλαιο αναλύονται μερικοί τρόποι προστασίας από τα spam μηνύματα, κυρίως εμπειρικοί τρόποι εφόσον στα προηγούμενα κεφάλαια έχουν αναφερθεί νομικοί τρόποι και μέθοδοι αντιμετώπισης τους. Στο έβδομο κεφάλαιο αναλύονται οι τεχνικές μέθοδοι και αρχιτεκτονικές φίλτρων για την αντιμετώπιση των spam μηνυμάτων. Στο όγδοο κεφάλαιο γίνεται μια αναφορά από έγκυρες πήγες το γιατί το Spamming αποτελεί πρόβλημα σήμερα και κάποιες καταδικάστηκες αποφάσεις κατά spamming από της ελληνικές έννομες τάξεις. Τέλος στο ένατο κεφάλαιο παρατίθενται τα συμπεράσματα από την παρούσα διπλωματική.

2. Ηλεκτρονικό Εμπόριο [5]

2.1 Έννοια του ηλεκτρονικού εμπορίου

Η ραγδαία ανάπτυξη της τεχνολογίας έχει αναμφισβήτητα επιφέρει σημαντικές αλλαγές στις παραδοσιακές οικονομικές δραστηριότητες. Η παγκοσμία οικονομία μετακινείται από μια κατεξοχήν μεταβιομηχανική οικονομία των υπηρεσιών σε μια ψηφιακή οικονομία, που ανήκει στην κοινωνία της πληροφορίας, όπου πρωταγωνιστικό ρόλο διαδραματίζει το ηλεκτρονικό εμπόριο.

Ως ηλεκτρονικό εμπόριο ορίζεται: «***το εμπορίου, η άσκηση του οποίου πραγματοποιείται με ηλεκτρονικά μέσα και αφόρα στην δυνατότητα σύναψης εμπορικών συναλλαγών μέσω τηλεπικοινωνιακών δικτύων και ιδίως μέσω του διαδικτύου*** **[6]**».

Το ηλεκτρονικό εμπόριο περικλείει ολόκληρο το φάσμα των οικονομικών δραστηριοτήτων που λαμβάνουν χώρα μεταξύ των επιχειρήσεων (Β 2 Β: *Business to Business*) η μεταξύ επιχειρήσεων και καταναλωτών (Β 2 C: *Business to Consumer*). Χωρίς αμφιβολία στη έννοια του ηλεκτρονικού εμπορίου περιλαμβάνονται ποίκιλες δραστηριότητες, όπως η ηλεκτρονική μεταφορά κεφαλαίου, οι ηλεκτρονικές φορτωτικές, η διαφήμιση και προώθηση προϊόντων, καθώς και άλλες οικονομικές δραστηριότητες. Τέλος, το ηλεκτρονικό εμπόριο μπορεί να αφόρα τόσο σε προϊόντα όσο και σε υπηρεσίες.

Άμεση συνεπεία των ανωτέρω εξελίξεων και της τεχνολογικής προόδου είναι ότι καθίσταται δυνατή η κατάρτιση των συμβάσεων της καθημερινής ζωής από απόσταση με αυτοματοποιημένο τρόπο στο πλαίσιο της χρήσεως των ηλεκτρονικών υπολογιστών **[7]** και του διαδικτύου, με αποτέλεσμα να κρίνεται ανεπαρκές το παραδοσιακό εμπόριο. Αντίθετα, το ηλεκτρονικό εμπόριο φαίνεται ιδανικότερο να ανταποκριθεί στης σύγχρονες ανήγες για συνεχή ανανέωση, ταχυτάτους ρυθμούς και δυνατότητα διαρκούς προσαρμογής στης καθημερινές απαιτήσεις των εμπορικών συναλλαγών.

2.2 Ηλεκτρονικό εμπόριο και Ελληνική νομοθεσία

Λαμβάνοντας υπόψη τα ανώτερα, γίνεται αντιληπτή η ιδιαίτερη σημασία του διαδικτύου για την άσκηση του ηλεκτρονικού εμπορίου. Για τον λόγο αυτό και η ελληνική νομοθεσία δεν μπορούσε να παρακολουθήσει τις νέες εξελίξεις, Ο κώδικας Βιβλίων και Στοιχείων προσαρμοστικέ με το ***πδ 186/1992*** (*τροποποιημένο από το* ***πδ 134/1996***) και έλαβε υπόψη τα νέα δεδομένα, τα οποία καθιστούν απαραίτητη την χρήση Η/Υ από εμπόρους για της ηλεκτρονικές εμπορικές συναλλαγές τους. Διατάξεις αφορούσες στη σύναψη εμπορικών συναλλαγών υπάρχουν σε διάφορους νομούς, στο ρυθμιστικό πεδίο των όποιον εμπίπτουν τομείς της οικονομικής ζωής. Παράδειγμα τα ***άρθρα 26 παρ. 2 και 27 παρ. 4 του ν. 2533/1997***, τα οποία εξισώνουν την ηλεκτρονική επικοινωνία της εταιρίας εκκαθάρισης συναλλαγών επί παραγώγων με την έγγραφη **[8]**. Παρόλη όμως την προσπάθεια που γίνεται σήμερα για την θέσπιση νομοθεσίας ικανής για την προστασία και ανάπτυξη του ηλεκτρονικού εμπορίου, εξακολουθούν να υφίσταται προβλήματα, τα οποία κατά κύριο λόγο πηγάζουν από τον χαρακτήρα του ιδίου του διαδικτύου ως παγκόσμιας αγοράς.

Στην προσπάθεια αυτή εισαγωγής αρχών για την διενεργεί του ηλεκτρονικού εμπορίου η Ευρωπαϊκή Ένωση εξέδωσε την ***Οδηγία 2000/31/ΕΚ*** «για ορισμένες πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά». Λειτουργεί κατά κάποιο τρόπο συμπληρωματικά σε σχέση με άλλες Οδηγίες όπως π.χ. με την Οδηγία για την προστασία των δεδομένων προσωπικού χαρακτήρα **[9]**. Έθεσε τις αρχές πάνω στης οποίες πρέπει να κινηθεί ο εθνικώς νομοθέτης για την εκπονήσει την εσωτερική νομοθεσία, για αυτό και χαρακτηρίζεται ως ***Οδηγία Αρχών*** **[10]**. Ο έλληνας νομοθέτης προσαρμόστηκε προς της ρυθμίσεις της Οδηγίας με την σχετική πράξη εφαρμογής (***πδ 131/2003*** **[8]**).

Βασική αρχή της Οδηγίας, σύμφωνα με το ***άρθρο 1 παρ.1***, είναι η εξασφάλιση της ελεύθερης κυκλοφορίας των υπηρεσιών της κοινωνίας της πληροφορίας μεταξύ των κρατών μελών της ΕΕ, ώστε να δημιουργηθεί ένας υπερεθνικός χώρος και να της απολαμβάνουν όλοι ανεξαιρέτως οι πολίτες της ΕΕ. Για να μη θίγει το κοινοτικό κεκτημένο, όσων αφόρα στην προστασία των καταναλωτών, ***άρθρο 1 παρ.3*** της Οδηγίας ορίζει ότι αυτή δεν θίγει το επίπεδο προστασίας ιδίως της δημοσίας υγείας και των συμφερόντων των καταναλωτή, όπως θεσπίζεται σε κοινοτικές πράξεις και στης εθνικές νομοθετικές πράξεις που εκδοθήκαν για την εφαρμογή τους, στο μετρό που δεν περιορίζεται έτσι η ελευθέρια παροχής υπηρεσιών της κοινωνίας της πληροφορίας.

Το ηλεκτρονικό εμπόριο διακρίνεται κύριος σε δυο κατηγορίες. Από την μια πλευρά υφίσταται το έμμεσο ηλεκτρονικό εμπόριο και από την άλλη το άμεσο. Η πρώτη περίπτωση αφόρα στην ηλεκτρονική παραγγέλλω υλικών αγαθών, για τα οποία παράλληλα υπάρχει η δυνατότητα παράδοσης τους με τους παραδοσιακούς τρόπους διανομής όπως π.χ. με το ταχυδρομείο. Το άμεσο ηλεκτρονικό εμπόριο άπτεται της παραδόσεως αυλών αγαθών και υπηρεσιών, όπως .χ. οπτικοακουστικό υλικό, υπηρεσίες πληροφόρησης, ψυχαγωγίας κλπ.**[10]**

2.3 Βασικές κατηγορίες του ηλεκτρονικού εμπορίου

Το ηλεκτρονικό εμπόριο διακρίνεται σε τέσσερεις κατηγορίες, ανάλογα με τα μετέχοντα σ΄αυτό μέρη.

1. Στην πρώτη κατηγορία (***B2B***), τα συμβαλλόμενα μέρη είναι επιχείρησης. Συγκεκριμένα μια επιχείρηση χρησιμοποίει το δίκτυο μιας άλλης επιχειρήσεις, προκείμενο να έρθει σε επαφή με τους πελάτες της η να αύξηση τον αριθμώ των πελατών της. Σ'αυτή την κατηγορία του ηλεκτρονικού εμπορίου υπάγεται και η ηλεκτρονική ανταλλαγή δεδομένων **[11]**. Ευνόητο είναι πως για την επιτυχή έκβαση των εφαρμογών αυτής της κατηγορίας απαιτείται συνεργασία και εναρμόνιση των επιχειρήσεων – συμβαλλομένων μερών.
2. Στη δεύτερη κατηγορία (***B2C***) συμβάλλονται η επιχείρηση από την μια πλευρά και ο καταναλωτής από την άλλη . Αποτελεί την πλέον συνήθη σήμερα εφαρμογή του ηλεκτρονικού εμπορίου. Εξάλλου η καταναλωτές αποτελούν και των κύριο στόχο τον διαφορών επιχειρήσεων. Ενημερώνονται για τα νέα προϊόντα και της παρεχόμενες υπηρεσίες μέσα από της ηλεκτρονικές σελίδες της κάθε επιχείρησης. Επιπλέων και αγοράζουν χρησιμοποιώντας ψηφιακό χρήμα.
3. Στην τρίτη κατηγορία (***B2A***: *Business to Administration* η ***B2G***: *Business to Government*).Τα μετέχοντα στο ηλεκτρονικό εμπόριο μέρη είναι η επιχείρηση και οι αρχές της Δημοσίας Διοίκησης. Τα τελευταία χρόνια έχει ενεργοποιηθεί ιδιαίτερα αυτός ο τομέας του ηλεκτρονικού εμπορίου. Σ΄αυτή την κατηγορία υπάγονται όλες οι πραγματοποιούμενες μεταξύ των δυο αυτών μερών συναλλαγές, με σκοπό την άντληση και παροχή πληροφοριών η ακόμη και την προώθηση απευθείας πληρωμών προς το δημόσιο **[12]**. Μεγάλη ανάπτυξη παρουσιάζει τα τελευταία χρόνια στην ΕΕ και η δημοσιά ηλεκτρονική προμήθεια (public e-procurement). Πρόκειται για την απόκτηση εκ μέρος της δημοσίας διοίκησης αγαθών και υπηρεσιών με ηλεκτρονικά μέσα.
4. Στην τέταρτη κατηγορία τα συμβαλλόμενα μέρη είναι η Δημοσιά Διοίκηση και η καταναλωτές. Στην κατηγορία αυτή ισχύουν τα προαναφερθέντα για την τρίτη κατηγορία.

3. Έννοιες – Ορισμοί περί αυτόκλητων μηνυμάτων (Spam)

Το spamming στο χώρο του Διαδικτύου συναντάται επίσης σε blogs ("blog spam"), σε chat rooms, σε άμεσα μηνύματα (instant messaging, IM, "spim") καθώς και με τη μορφή συνδέσμων ("link spamming"), ενώ η πρακτική αυτή τείνει πλέον να καταλάβει και άλλα μέσα, όπως το fax και τα κινητά τηλέφωνα ("sms spam", "mobile spam" ή "SpaSMS") πάντα όμως σε μικρότερη κλίμακα σε σχέση με την κύρια εκδήλωσή του.

Αν και ο όρος "*spam*" χρησιμοποιείται στα πολιτικά κείμενα, ή στις έρευνες δεν υπάρχει κάποιος υποστηριζόμενος νομικός καθορισμός του όρου . Από την αρχή της δεκαετίας του '90 ο όρος spam χρησιμοποιείται συνήθως για να περιγράψει «*οποιοδήποτε λαμβανόμενο μήνυμα που είναι ανεπιθύμητο από τον παραλήπτη*», συχνά αποτελούμενος από διαφημίσεις για προϊόντα και υπηρεσίες, μια προσέγγιση που επικρίθηκε από την ομάδα εργασίας *αντί-Spam* του Οργανισμού Οικονομικής Ανάπτυξης και Συνεργασίας ΟΟΣΑ (*OECD - Organization for Economic Cooperation and Development*).

Τα πρώτα spam η spamming (*οπού στην Ελλάδα μετονομάζεται σε μην ζητηθείσα εμπορική επικοινωνία*) στο web , στη μορφή που είναι γνωστά σήμερα, εμφανίστηκαν στις ΗΠΑ γύρω στα μέσα της δεκαετίας του 90΄.

3.1 Μορφές διαφήμισης

Είναι γνωστή η σημασία της διαφήμισης στις μέρες μας. Η ανταγωνιστικότητα των επιχειρήσεων αυξάνεται με ραγδαίους ρυθμούς με αποτέλεσμα κάποιες επιχειρήσεις να μένουν πίσω και άλλες να κλείνουν εντελώς. Κερδισμένες είναι οι επιχειρήσεις που αντιλαμβάνονται τα μηνύματα των καιρών και εφαρμόζουν νέες ανέξοδες **[13]** μεθόδους δημιουργίας και προώθησης των αγαθών τους.

"***Διαφήμιση είναι κάθε ανακοίνωση που γίνεται στα πλαίσια εμπορικής, βιομηχανικής, βιοτεχνικής ή επαγγελματικής δραστηριότητας με στόχο την προώθηση της διάθεσης αγαθών ή υπηρεσιών***" **[14]**.

Είναι μια προσπάθεια διάδοσης πληροφοριών με σκοπό να επηρεαστούν οι συναλλαγές αγοραστών-πωλητών. Στο παραδοσιακό μάρκετινγκ, η διαφήμιση είναι συνήθως απρόσωπη, μονόδρομη μαζική επικοινωνία, που πληρώνεται από χρηματοδότες. Το τηλεμάρκετινγκ και οι διαφημίσεις μέσω απευθείας αλληλογραφίας είναι προσπάθειες εξατομίκευσης της διαφήμισης ώστε να γίνει πιο αποτελεσματική. Αυτές οι προσεγγίσεις όμως είναι ακριβές και αργές. Επίσης σε γενικές γραμμές με τον παραδοσιακό τρόπο διαφήμισης είναι δύσκολη η μετρησιμότητα της απήχησής της.

Θα μπορούσε να ειπωθεί πως κάθε διαφήμιση είναι ένα μήνυμα που έχει ως πομπό την επιχείρηση και δέκτη το καταναλωτικό κοινό. Η εκτέλεση του διαφημιστικού μηνύματος μπορεί να γίνει με πολλούς και διαφορετικούς τρόπους. Κάθε διαφήμιση έχει διαφορετικό σκοπό ως προς τα αποτελέσματα που επιθυμεί να επιτύχει.

Παρακάτω αναφέρονται συνοπτικά οι μορφές που θα μπορούσε να έχει μια διαφήμιση:

Παραπλανητική διαφήμιση

"Παραπλανητική είναι κάθε διαφήμιση που με οποιονδήποτε τρόπο παραπλανά ή ενδέχεται να παραπλανήσει τους καταναλωτές εξαιτίας του απατηλού χαρακτήρα της και είναι ικανή να επηρεάσει την οικονομική τους συμπεριφορά, για τον λόγω αυτό, βλάπτει ή ενδέχεται να βλάψει έναν ανταγωνιστή. Η παραπλανητική διαφήμιση απαγορεύεται" **[14]**.

Συγκριτική διαφήμιση

"Η διαφήμιση που προσδιορίζει άμεσα ή έμμεσα την ταυτότητα συγκεκριμένου ανταγωνιστή ή των ομοειδών αγαθών ή υπηρεσιών που εκείνος προσφέρει. Επιτρέπεται εφόσον συγκρίνει με αντικειμενικό τρόπο τα ουσιώδη, συναφή, επαληθεύσιμα και επιλεγμένα με αμεροληψία χαρακτηριστικά ανταγωνιστικών αγαθών ή υπηρεσιών. Επιτρέπεται μόνο αν δεν είναι παραπλανητική, δεν προκαλεί σύγχυση στην αγορά μεταξύ του διαφημιζομένου και ενός ανταγωνιστή ή μεταξύ ανταγωνιστών του διαφημιζομένου ή μεταξύ άλλων διακριτικών γνωρισμάτων, αγαθών ή υπηρεσιών του διαφημιζομένου και ενός ανταγωνιστή ή περισσότερων ανταγωνιστών μεταξύ τους, δεν είναι υποτιμητική, δυσφημιστική ή περιφρονητική για έναν ανταγωνιστή ή για τα άλλα διακριτικά γνωρίσματα, αγαθά, υπηρεσίες ή δραστηριότητές του, δεν επιδιώκει κατά κύριο λόγο να επωφεληθεί από τη φήμη ή άλλου διακριτικού γνωρίσματος του ανταγωνιστή" **[14]**.

Αθέμιτη διαφήμιση

"Αθέμιτη διαφήμιση είναι κάθε διαφήμιση που προσβάλλει τα χρηστά ήθη, έχει στόχο ή ενδεχόμενο αποτέλεσμα την πρόκληση ή εκμετάλλευση αισθημάτων φόβου, προλήψεων ή δεισιδαιμονιών ή την εξώθηση σε εγκληματικές πράξεις, διακρίνει μειωτικά κοινωνικές ομάδες με βάση το φύλο, τη φυλή, την ηλικία, το θρήσκευμα, την εθνικότητα, την

καταγωγή, τις πεποιθήσεις και τις φυσικές ή ψυχικές ιδιαιτερότητες, δημιουργεί την εικόνα υπερβολικά δελεαστικής προσφοράς, ιδίως σε παιδιά, νέους και στις πιο ευάλωτες κατηγορίες του πληθυσμού, απευθύνει το διαφημιστικό μήνυμα κατευθείαν στο υποσυνείδητο, χωρίς να αφήνει στο δέκτη του μηνύματος τη δυνατότητα κριτικής, προβάλλει εμμέσως προϊόντα που αποτελούν το εμφανές περιεχόμενο του διαφημιστικού μηνύματος, χωρίς η προβολή αυτή να αποτελεί νοηματικά ουσιώδες και αναπόσπαστο τμήμα του. Η αθέμιτη διαφήμιση απαγορεύεται." **[14]**

Συγκαλυμμένη ή έμμεση διαφήμιση

"Η συγκαλυμμένη ή έμμεση διαφήμιση είναι η παρουσίαση σε προγράμματα, με λόγο ή εικόνα, εμπορευμάτων, υπηρεσιών, της επωνυμίας, του σήματος ή των δραστηριοτήτων ενός προσώπου που παράγει εμπορεύματα ή παρέχει υπηρεσίες, Μια τέτοια παρουσίαση θεωρείται ότι έχει διαφημιστικό σκοπό, όταν γίνεται έναντι αμοιβής ή αναλόγου ανταλλάγματος." **[14]**

Άμεση διαφήμιση

"Άμεση διαφήμιση είναι η μετάδοση διαφημιστικού μηνύματος απευθείας στον καταναλωτή μέσω τηλεφώνου, τηλεομοιοτυπίας (φαξ), ηλεκτρονικού ταχυδρομείου, αυτόματης κλήσης ή άλλου ηλεκτρονικού μέσου επικοινωνίας. Η άμεση διαφήμιση θα πρέπει να γίνεται με τρόπο που να μην προσβάλλει την ιδιωτική ζωή του καταναλωτή" **[14]**.

3.2 Διαφήμιση μέσω Internet

Η διαφήμιση στο Internet είναι μια ήσυχη δύναμη, που «καλπάζει», με πολύ γρήγορους ρυθμούς ανάπτυξης και διείσδυσης, τόσο στην αγορά (επιχειρήσεις, εταιρίες) αλλά και όσον αφορά τους ιδιώτες. Όλο και περισσότερες εταιρίες αυξάνουν το ποσοστό των χρημάτων που διαθέτουν για τη διαφήμιση των προϊόντων ή των υπηρεσιών τους στο Internet. Οι λόγοι είναι προφανείς. Η χρήση του Internet από όλο και περισσότερους ανθρώπους, αναγκαστικά οδηγεί τις εταιρίες να ενδιαφέρονται για τη διαφήμιση τους στο Internet.

Ο ρόλος και η δομή της διαφήμισης 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 έκφρασης ***(βλ. άρθρο 10 § 1 της Ευρωπαϊκής Σύμβασης Δικαιωμάτων του ανθρώπου και άρθρο 14 παράγραφος 1 του ελληνικού Συντάγματος)***.

Το Internet εισάγει επίσης και την έννοια του άμεσου μάρκετινγκ, το οποίο επιτρέπει στους διαφημιστές να αλληλεπιδράσουν απευθείας με τους πελάτες. Στο άμεσο μάρκετινγκ, ένας καταναλωτής μπορεί να κάνει κλικ σε μία διαφήμιση για να πάρει περισσότερες πληροφορίες ή να στείλει ένα ηλεκτρονικό μήνυμα και να κάνει μια ερώτηση.

Εκτός της αμφίδρομης επικοινωνίας και της δυνατότητας αποστολής ηλεκτρονικού μηνύματος που παρέχονται από το Internet, οι προμηθευτές μπορούν επίσης να στοχεύσουν σε συγκεκριμένες ομάδες και άτομα προς τα οποία θέλουν να κάνουν περισσότερη διαφήμιση.

Όσον αφορά την μετρησιμότητα της απήχησης της διαφήμισης, μια εταιρεία πριν αποφασίσει να διαφημιστεί σε μια ιστοθέση, μπορεί να επαληθεύσει τον αριθμό των προβολών των διαφημίσεων ή άλλων σχετικών δεδομένων που αναφέρονται από τους πωλητές του χώρου. Τέλος η διαφήμιση στο Internet είναι γρήγορη, φτηνή και εύκολα ανανεώσιμη.

Διερευνώντας αρκετές πηγές από το διαδίκτυο και σύμφωνα με την αναφορά **[15]**, εκτιμώ όπως αναφέρω συνοπτικά παρακάτω πως κάποιες από τις μορφές που θα μπορούσε να έχει μια διαφήμιση στο Internet είναι:

Αφίσα

Μια αφίσα είναι μια γραφική απεικόνιση που χρησιμοποιείται για διαφήμιση σε μία ιστοσελίδα. Συνδέεται με την ιστοθέση του διαφημιζομένου. Όταν οι χρήστες κάνουν «κλικ» στην αφίσα μεταφέρονται στην ιστοθέση του διαφημιζομένου. Οι διαφημιστικές εταιρείες καταναλώνουν πολύ χρόνο για να σχεδιάσουν μία αφίσα, που θα τραβάει την προσοχή του καταναλωτή.

Οι αφίσες συχνά περιλαμβάνουν βίντεο κλιπ και ήχο. Οι διαφημιστικές αφίσες είναι η συνηθέστερα χρησιμοποιούμενη μορφή διαφήμισης στο Internet.

E-mail

Ένας δημοφιλής τρόπος διαφήμισης στο Internet είναι η αποστολή πληροφοριών που αφορούν μια εταιρεία ή ένα προϊόν σε άτομα των οποίων η ηλεκτρονική διεύθυνση είναι καταχωρημένη σε λίστες αλληλογραφίας. Η αποστολή των πληροφοριών γίνεται μέσω ηλεκτρονικού ταχυδρομείου (e-mail). Τα μηνύματα μπορούν να συνδυάζονται με μικρά κλιπ ήχου ή βίντεο για να προωθήσουν ένα προϊόν και με δεσμούς επί της οθόνης, στους οποίους οι χρήστες μπορούν να κάνουν κλικ για να κάνουν μία αγορά.

Τα κυριότερα πλεονεκτήματα της διαφήμισης μέσω ηλεκτρονικού μηνύματος είναι το χαμηλό κόστος και η δυνατότητα προσέγγισης μιας μεγάλης ποικιλίας στοχευόμενων ακροατηρίων.

Διαφήμιση σε αίθουσες συζητήσεων

Μια αίθουσα συζητήσεων μπορεί να χρησιμοποιηθεί για να επιτρέψει σε ανθρώπους με ένα κοινό χόμπι να μοιραστούν τα ενδιαφέροντά τους. Μπορεί όμως να χρησιμοποιηθεί και για διαφημιστικούς σκοπούς. Οι προμηθευτές συχνά χρηματοδοτούν αίθουσες συζητήσεων. Ο χρηματοδότης προμηθευτής τοποθετεί ένα δεσμό συζήτησης στην ιστοθέση του. Οι διαφημίσεις συγχωνεύονται με τη δραστηριότητα της αίθουσας.

Η κύρια διαφορά ανάμεσα σε μια διαφήμιση που εμφανίζεται σε στατική ιστοσελίδα και σε μια διαφήμιση που εμφανίζεται σε αίθουσα συζητήσεων είναι ότι η τελευταία εμφανίζεται σε στοχευόμενο κοινό και μπορεί να έχει μεγαλύτερη απήχηση.

Webcasting

Αποτελεί μία δωρεάν υπηρεσία ειδήσεων του Internet που εκπέμπει εξατομικευμένες ειδήσεις και πληροφορίες. Ένας χρήστης εγγράφεται στο σύστημα webcasting και συλλέγει τις πληροφορίες που θέλει να δεχτεί, όπως αθλητικές ειδήσεις, πολιτικές ειδήσεις, τίτλους ειδήσεων, τιμές μετοχών ή προωθήσεις προϊόντων που θέλει. Ο χρήστης κατόπιν δέχεται τις πληροφορίες που ζήτησε, μαζί με εξατομικευμένες διαφημίσεις που βασίζονται στα εκφρασμένα ενδιαφέροντα του.

SMS & MMS

Τα τελευταία χρόνια έχει αυξηθεί και ο όγκος των διαφημιστικών μηνυμάτων spam **SMS** και **MMS** προς τους χρήστες σε όλο των κόσμο. Σε αυτή την απειλή δεν θα μπορούσε να μείνει από έξω και η ευρωπαϊκή κοινότητα συμπεριλαμβανόμενου και η Ελλάδα.

Σε αυτή την περιπτώσει και έχοντας στο νομικό οπλοστάσιο ***τους το άρθρο 6 § 1 του Π.Δ. 131/2003*** επιβάλλει συγκεκριμένες απαιτήσεις η παροχή κινητής και σταθερής τηλεφωνίας μερίμνησαν ώστε να έχουν τις μικρότερες απώλειες.

3.3 Τι είναι Spam;

Μεταξύ των δυνατοτήτων που παρέχονται από τα ηλεκτρονικά επικοινωνιακά μέσα, όπως για παράδειγμα το ηλεκτρονικό μήνυμα (e-mail), είναι το σχετικά χαμηλό κόστος μετάδοσης, η υψηλή αξιοπιστία και γενικά η γρήγορη παροχή υπηρεσιών.

Η υπηρεσία του ηλεκτρονικού ταχυδρομείου δεν είναι μόνο φθηνή και γρήγορη αλλά παρέχει επιπλέον και δυνατότητες αυτοματοποίησης. Αυτές οι ιδιότητες καθιστούν την υπηρεσία των ηλεκτρονικών μηνυμάτων πολύ ελκυστική για εμπορικούς διαφημιστικούς σκοπούς. Στο προηγούμενο κεφάλαιο αναφέρθηκε η γενική σημασία του spam, παρακάτω αναφέρεται ο κανονικός ορισμός του.

*"**Spam είναι η μαζική αποστολή μεγάλου αριθμού αυτόκλητων μηνυμάτων που απευθύνονται σε ένα σύνολο παραληπτών του διαδικτύου χωρίς αυτοί να το επιθυμούν και χωρίς να έχουν συνειδητά προκαλέσει την αλληλογραφία με τον εν λόγω αποστολέα**"* **[16]**.

Τα μηνύματα spam μπορεί να προωθούν κάθε είδους προϊόντα ή υπηρεσίες. Έτσι ως spam θεωρούνται και μηνύματα προώθησης υπηρεσιών, σκοπών φιλανθρωπικών ιδρυμάτων, σωματείων, ενώσεων, κλπ. Ο βασικός σκοπός του spam είναι η διαφήμιση μιας σειράς προσφερομένων αγαθών σχετιζόμενα με την πορνογραφία, το λογισμικό των ηλεκτρονικών υπολογιστών, τα ιατρικά προϊόντα, τους λογαριασμούς πιστωτικών καρτών, πτυχία πανεπιστημίων, κ.λ.π.

Έχοντας κάνει μια αναδρομή στα ιστορικά θέμα για τα spam, παρακάτω γίνεται αναφορά για το spam στις μέρες μας και γιατί είναι ένα από τα σοβαρότερα και δύσκολα προβλήματα.

Το spamming για τους spammer αποτελεί τη μεγαλύτερη ανακάλυψη μετά τον τροχό (…) κι αυτό γιατί μπορούν να κατακλύσουν ολόκληρη την υφήλιο με δισεκατομμύρια e-mail (spam-mail) μέσα σε ελάχιστο χρόνο, με ελάχιστα χρήματα! Η ανταποδοτική λειτουργία του spamming συνίσταται σε ποσοστό επί των ηλεκτρονικών μηνυμάτων που αποστέλλονται. Αυτό σημαίνει, απλούστερα, ότι η αποστολή περισσότερων spam e-mail ισοδυναμεί με περισσότερες πιθανότητες κέρδους. Βέβαια, ακόμη και η ελάχιστη ανταπόκριση στο μήνυμα ωφελεί τον spammer, καθώς αν έστω και ένας από τους δεκάδες χιλιάδες αποδέκτες του ίδιου μηνύματος spam ανταποκριθεί αγοράζοντας το διαφημιζόμενο προϊόν, καλύπτεται το κόστος της συνολικής αποστολής **[17]** spam από τα έσοδα **[18]** της διαφημιζόμενης επιχείρησης.

Σημειώνεται ότι εκτιμάται πως ετησίως αποστέλλονται δισεκατομμύρια spam μηνύματα κατακλύζουν τα ηλεκτρονικά ταχυδρομεία των χρηστών και των επιχειρήσεων, παρότι επίσης δισεκατομμύρια μηνύματα είναι αυτά που φιλτράρονται από τους παρόχους υπηρεσιών πριν φτάσουν στους παραλήπτες τους. Έχει υπολογιστεί ότι καθημερινά, κατά μέσο όρο, αποστέλλονται ανά τον κόσμο περί τα 100 δισ. spam ηλεκτρονικά μηνύματα, όπου ολοένα και αυξάνονται, οδηγώντας έτσι σε εξάντληση των διαθέσιμων πόρων του παγκόσμιου ιστού και στην υπερφόρτωση των συστημάτων.

Προϊόντα	25%
Χρηματοοικονομικά	20%
Υλικό απευθυνόμενο σε ενήλικες	19%
Απάτες	9%
Υγεία	7%
Διαδίκτυο	7%
Ελεύθερος χρόνος	6%
Θρησκευτικό περιεχόμενο	4%
Λοιπά	3%

Πίνακας 1: Κατηγορίες Spam

Πορνογραφία	91%
Υποθήκες και δάνεια	78%
Εφευρέσεις	68%
Ακίνητη περιουσία	61%
Λογισμικό	41%
Διαδίκτυο	7%
Ελεύθερος χρόνος	6%
Θρησκευτικό περιεχόμενο	4%
Λοιπά	3%

Πίνακας 2: Οι πιο ενοχλητικές κατηγορίες (% του συνόλου των spam [19])

E-mails που έχουν χαρακτηριστεί ως SPAM	40% του συνόλου των e-mail
Απεσταλμένα καθημερινά spam e-mails	12,4 δισεκατομμύρια
Ληφθέντα καθημερινά spam e-mails ανά άτομο	6
Ληφθέντα ετήσια spam e-mails ανά άτομο	2.200
Κόστος spam σε όλους τους χρήστες internet	$255 εκατομμύρια
Κόστος spam για επιχειρήσεις των ΗΠΑ το 2002	$8,9 εκατομμύρια
Καταστάσεις σχετιζόμενες με νομικά ζητήματα καταπολέμησης των spam	26
Αλλαγές διευθύνσεων ηλεκτρονικού ταχυδρομείου λόγω του SPAM	16%
Εκτιμώμενη αύξηση του spam για το 2007	63%
Ετήσιος αριθμός μηνυμάτων spam σε μια εταιρία 1000 εργαζομένων	2,1 εκατομμύρια
Χρήστες που απαντούν σε spam e-mails	28%
Χρήστες που αγόρασαν λόγω spam e-mail	8%
Εταιρικά e-mails που θεωρήθηκαν spam	15-20%
Εταιρικός χρόνος που καταναλώνεται ανά spam e-mail	4-5 δευτερόλεπτα

Πίνακας 3: Στατιστικά Spam 2006 [19].

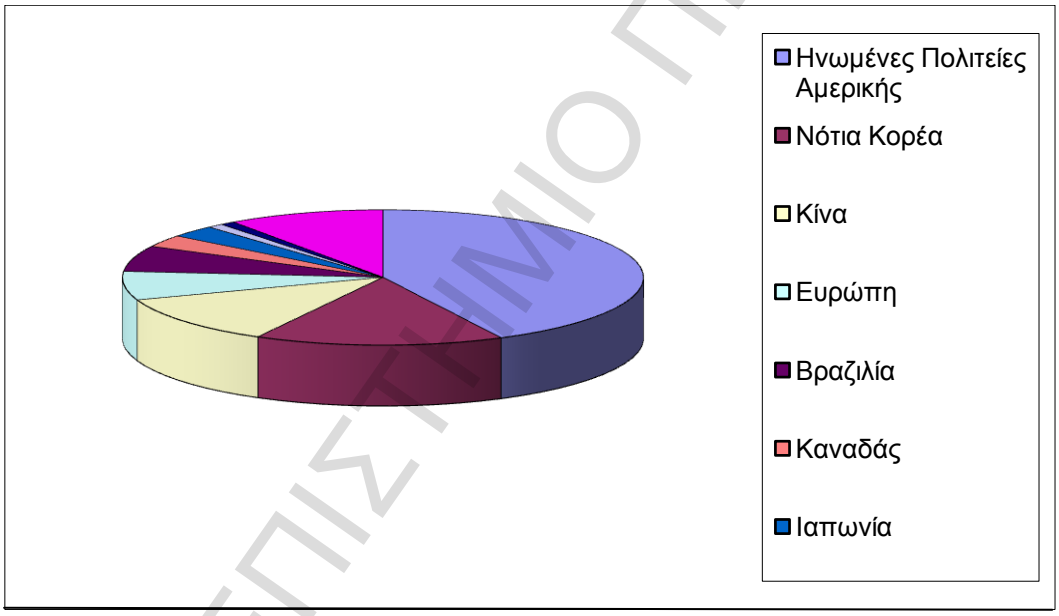
Στον Πίνακα 1 επισημαίνεται το ποσοστό επί τις εκατό των αναφερθέντων κατηγοριών που χρησιμοποιούνται ως μηνύματα spam, διαπιστώνεται λοιπόν όπως προανέφερα ότι τα περισσότερα μηνύματα spam έχουν εμπορικό περιεχόμενο, αλλά δεν έχουν πάντα εμπορικό περιεχόμενο.

Στον Πίνακα 2 επισημαίνεται το ποσοστό επί τις εκατό των πιο ενοχλητικών κατηγοριών του συνόλου των spam. Στις κατηγορίες αυτές φαίνεται πως την πρώτη θέση κατέχει η πορνογραφία με αρκετά μεγάλη διαφορά απ' όλες τις υπόλοιπες κατηγορίες.

Όπως προαναφέρθηκε, αποστολείς των μηνυμάτων αυτών είναι συνήθως εταιρίες που θέλουν ένα φτηνό τρόπο για να διαφημιστούν, ενώ παραλήπτες είναι λογαριασμοί ηλεκτρονικής αλληλογραφίας που έχουν γίνει γνωστοί στο διαδίκτυο, όπως για παράδειγμα ανοικτές λίστες αλληλογραφίας, διευθύνσεις καταγεγραμμένες σε δικτυακές σελίδες, είτε συνηθισμένα ονόματα χρηστών σε γνωστούς παρόχους ηλεκτρονικής αλληλογραφίας (π.χ. *john@hotmail.com*).

Στον Πίνακα 3 αναγράφονται τα στατιστικά στοιχεία των spam μηνυμάτων για το έτος 2006. Διαπιστώνεται πως τα ποσοστά των spam μηνυμάτων σε όλες τις κατηγορίες δεν είναι διόλου ευκαταφρόν.

Το spam ξεκίνησε ως κάτι άκακο και διασκεδαστικό, η ανάγνωση τέτοιων μηνυμάτων μπορούσε να θεωρηθεί και ως ευχάριστο διάλειμμα από τη δουλειά, αλλά κατέληξε να είναι ένα από τα μεγαλύτερα προβλήματα του διαδικτύου. Η αυξανόμενη ποσότητα spam έχει όλο και μεγαλύτερο αντίκτυπο σε χρόνο και χρήμα του τελικού χρήστη καθώς αυτός λαμβάνει περισσότερο όγκο δεδομένων από ότι χρειάζεται και θέλει.



Σχήμα 1: Ποσοστά εμφάνισης Spam 2006 ανά περιοχή [20]

Στον Σχήμα 1 απεικονίζονται τα ποσοστά εμφάνισης των spam μηνυμάτων για το έτος 2006 σε διάφορες χώρες. Διαπιστώνεται πως το ποσοστό εμφάνισης των spam μηνυμάτων κυρίως στις ΗΠΑ είναι αξιοσημείωτο, ακολουθούμενο από τα ποσοστά της Νότιας Κορέας, Κίνας και λοιπών χωρών.

Παρά τα εξωφρενικά μεγέθη της εξάπλωσης του φαινομένου, οι σημαντικότερες πηγές του είναι ολιγάριθμες. Σύμφωνα με τις αναφορές, μέχρι το 2006 περίπου το 90% του spam που παράγεται σε παγκόσμιο επίπεδο, προέρχεται από ομάδες spammer (κυρίως από τις ΗΠΑ, την Κίνα και την Νότιο Κορέα όπως φαίνεται στον Πίνακα 4). Οι ομάδες αυτές διαθέτουν άριστη τεχνογνωσία και χρησιμοποιούν προηγμένο λογισμικό για την υλοποίηση των στόχων τους. Το υπόλοιπο 10% δημιουργείται από μικρές επιχειρήσεις που δεν εφαρμόζουν τους κανόνες του ηλεκτρονικού μάρκετινγκ, από ανθρώπους που εκμεταλλεύονται την αφέλεια ή την άγνοια των χρηστών.

3.4 Γεωγραφικά ποσοστά των Spammers

Αναρωτηθήκατε ποτέ από πού προέρχονται τα δεκάδες ή εκατοντάδες ανεπιθύμητα μηνύματα που λαμβάνουμε καθημερινά στο e-mail μας, μηνύματα με διαφημίσεις για φάρμακα και προϊόντα, ακόμα και για υποτιθέμενες κληρονομιές προέρχονται από αρκετές χώρες του κόσμου, η πλειοψηφία τους όμως προέρχεται από την Ινδία.

Σύμφωνα με λίστα που δημοσίευσε η εταιρεία Sophos, για το τρίμηνο Ιουλίου – Σεπτεμβρίου του 2012 **[21]**, το ποσοστό μηνυμάτων spam που προέρχεται από την Ινδία είναι 16.1%. Ακολουθεί η Ιταλία με 9.4%, οι ΗΠΑ με 6.5% και η Σαουδική Αραβία με 5.1% ενώ στο ανάμεσα στις 13 χώρες της λίστας βρίσκεται ακόμα η Τουρκία με 3.8%, η Γερμανία με 2.7% και το Ηνωμένο Βασίλειο με 2.1%.

Αυτό δεν σημαίνει πως το σύνολο των μηνυμάτων αυτών προέρχονται μέσα από αυτές τις χώρες, ούτε πως οι περισσότεροι spammers είναι Ινδοί. Οι spammers οπουδήποτε και να βρίσκονται χρησιμοποιούν υπολογιστές που έχουν μολύνει ελέγχουν εξ αποστάσεως μέσω ειδικών προγραμμάτων **[22]** spyware και σύνδεση μεταξύ τους μέσω botnets για να διαδώσουν ανεπιθύμητα e-mail.

Όπως εξηγεί ο Graham Cluley της Sophos, «σημαντικός αριθμός υπολογιστών στην Ινδία έχουν μολυνθεί με malware». Αυτό επιτρέπει σε επιτήδειους να θησαυρίζουν στέλνοντας ανεπιθύμητα e-mail που προωθούν είδη αμφιβόλου ποιότητας καθώς και να μολύνουν ακόμα περισσότερους υπολογιστές για τον σκοπό αυτό.

The top 12 spam-relaying countries for July to September 2012:

1. India	16.1%
2. Italy	9.4%
3. USA	6.5%
4. Saudi Arabia	5.1%
5. Brazil	4.0%
6. Turkey	3.8%
7. France	3.7%
8. South Korea	3.6%
9. Vietnam	3.4%
10. China	3.1%
11. Germany	2.7%
12. United Kingdom	2.1%
Other	36.5%

Πίνακας 4: Ποσοστά εμφάνισης Spam 2012 ανά περιοχή

Η Ινδία κατέχει την τρίτη θέση στη λίστα των χωρών με τον υψηλότερο αριθμό χρηστών στο διαδίκτυο. Παρά το γεγονός αυτό όμως μόνο το 10.2% του πληθυσμού της έχει πρόσβαση σε αυτό. Το γεγονός αυτό προκαλεί την έλλειψη σημαντικών μέτρων για την προστασία των υπολογιστών της χώρας, κάτι που σύμφωνα με την εταιρεία Sophos μπορεί να οδηγήσει σε αύξηση όχι μόνο του spam αλλά και πιο επικίνδυνων μορφών επιθέσεων.

Όσον αφορά την προέλευση μηνυμάτων spam κατά ήπειρο τώρα, την πρώτη θέση έχει η Ασία με 48.7%, την δεύτερη η Ευρώπη με 28.2% και την τρίτη η Νότια Αμερική με 10.2%.

3.5 Ποιοι είναι οι Spammers (Λίστα Ελλήνων Spammer)

Σε αρκετές χώρες το spam αποτελεί ένα από τα μεγαλύτερα προβλήματα στη διαδικτυακή ζωή πολλών χρηστών και στην πλειοψηφία των επιχειρήσεων. Στην Ελλάδα το πρόβλημα αυτό βρισκόταν σε πολύ πιο περιορισμένο επίπεδο το 1995 όταν έκανε την εμφάνιση της . Την τελευταία δεκαετία όμως στην χώρα μας γνωρίζει τρομερή αύξηση όπως ανακοινώθηκε κατά την διάρκεια κάποιας ημερίδας από την ΑΔΑΕ το Ιανουάριο του 2007 **[23]** όπου αίσθηση είχε προκαλέσει και η εκτίμηση του στελέχους της Symantec, Ηλία Χάντζου (*ότι το 53% των e-mails που λαμβάνουν οι Έλληνες χρήστες*) είναι spam και παρά το νομοθετικό πλαίσιο που υπάρχει, σαφώς όμως δεν μπορεί να υπάρξει εφησυχασμός.

Οι ομάδες spammer και ένα ποσοστό από τους υπόλοιπους, για να αποφύγουν τις νομικές και οικονομικές συνέπειες των πράξεών τους, πλαστογραφούν τις ηλεκτρονικές διευθύνσεις τους ώστε να μην είναι δυνατός ή να είναι αρκετά δύσκολος ο εντοπισμός τους. Τις περισσότερες φορές, η ηλεκτρονική διεύθυνση και το όνομα που παρουσιάζεται ως ο αποστολέας των ποσοτήτων spam ηλεκτρονικών μηνυμάτων είναι κάποιος, εντελώς αθώος, χρήστης του διαδικτύου, του οποίου χρησιμοποιήθηκε εν αγνοία του η ηλεκτρονική διεύθυνσή του.

Η πιο συνηθισμένη τακτική των spammers είναι η αποστολή υπερβολικά μεγάλου αριθμού spam με συνεπεία να προκαλείται υπερφόρτωση της θυρίδας του ηλεκτρονικού ταχυδρομείου, με αποτέλεσμα να εμποδίζεται η είσοδος επιθυμητών και σημαντικών για το χρήστη μηνυμάτων. Εκτός αυτού, καλείται να ανεχθεί και χαμηλότερες ταχύτητες λειτουργίας του διαδικτύου λόγω της επιβάρυνσης του server **[24]**. Αυτό έχει σαν συνέπεια να μπλοκάρει ο λογαριασμός του από τις επιστροφές των ανεπίδοτων spam ηλεκτρονικών μηνυμάτων (κάθε αποστολή spam, περιλαμβάνει χιλιάδες ή και εκατομμύρια διευθύνσεις, πολλές από τις οποίες έχουν καταργηθεί) από τις εκατοντάδες και χιλιάδες διαμαρτυρίες των παραληπτών του spam.

Οι spammers επιστρατεύουν πλήθος τακτικών (harvesting) **[25]** για να αποκτήσουν διευθύνσεις ηλεκτρονικού ταχυδρομείου, όπως είναι η συλλογή διευθύνσεων από mailing lists ή από ιστότοπους κοινωνικής δικτύωσης (social networking sites) με τη χρησιμοποίηση ειδικού λογισμικού που ανιχνεύει στο σύμβολο «@» ή η μμέθοδος του "*dictionary attack*", όπου ο spammer προσπαθεί να μαντέψει και να συνθέσει πραγματικές ηλεκτρονικές διευθύνσεις συνδυάζοντας τυχαία γράμματα ή λέξεις που αντλεί από το λεξικό. Ένας ιδιαίτερα διαδεδομένος τρόπος απόκτησης ηλεκτρονικών διευθύνσεων είναι η εξαγορά τους από άλλο spammer ή από εταιρίες που διαθέτουν αντίστοιχες βάσεις δεδομένων **[26]**. Χαρακτηριστική είναι η ευκολία με την οποία μπορεί να γίνει μια τέτοια αγοραπωλησία ακόμη και μέσω διαδικτύου, αφού αρκεί να πληκτρολογήσει κανείς στη μηχανή αναζήτησης (π.χ. στο Google) τη φράση "bulk email" για να εμφανισθούν αμέσως καταχωρίσεις όπως "*Buy email lists - email addresses - email marketing*". Η εμπορευματοποίηση προσωπικών δεδομένων στο διαδίκτυο έχει εδραιωθεί ως πρακτική, ενώ ο χαρακτηρισμός της εν γένει διαδικασίας εξαγωγής πληροφοριών από μεγάλες βάσεις δεδομένων ως "*data mining*" **[27]** αποδεικνύει την αντιμετώπισή τους ως πολύτιμων «*κοιτασμάτων*» τα οποία «*εξορύσσονται*».

Οι τεχνικές των spam εξελίσσονται. Οι spammers που παρακινούνται από τα οικονομικά οφέλη και το χαμηλότερο κόστος για την ανάπτυξη των spam, μαθαίνουν πως λειτουργούν τα τρέχον αντι-spam εργαλεία και υιοθετούν συνεχώς νέες τεχνικές που μπορούν να τα παρακάμψουν.

Το ίντερνετ στην Ελλάδα αναπτύσσεται συνεχώς, ακόμα όμως δεν μπορεί, εκ των πραγμάτων, να συγκριθεί με το αμερικάνικο, το γερμανικό και το αγγλικό ίντερνετ. Όπως έχουν δείξει έρευνες που δημοσιεύονται κατά καιρούς στις αθηναϊκές εφημερίδες, το ποσοστό των ελλήνων που χρησιμοποιούν το διαδίκτυο είναι πολύ μικρό σε σχέση με την Ευρώπη. Πραγματικά δεν θα περίμενε κανείς να υπάρχουν έλληνες spammers, από ότι φαίνεται όμως υπάρχουν αρκετοί webmasters και άλλοι επαγγελματίες που καταφεύγουν σε μεθόδους spam για να διαφημίσουν την ιστοσελίδα και τα προϊόντα τους. Έχω βάσιμες υποψίες ότι ήδη υπάρχουν κάποια ελληνικά φόρουμ, τα οποία πουλάνε τις βάσεις δεδομένων τους και συνεργάζονται με spammers!

Πίστευα για πολύ καιρό ότι το email αποθηκεύεται κρυπτογραφημένο στις βάσεις δεδομένων των φόρουμ, όμως κάτι τέτοιο ισχύει μόνο για τους κωδικούς (passwords) και όχι πάντα (εξαρτάται από το λογισμικό).

Παρακάτω παραθέτω μια πραγματική λίστα ελλήνων spammer όπως αυτό ανακοινώθηκε από το site **[28]** με την *τελευταία ενημέρωση στης 30/07/2009.*

afrogo@ath.forthnet.gr
ajamfam@crosswind.net
bf@globalgreece.gr
bgca@otenet.gr
club@plus4u.gr
delphigroup@myfastmail.com
entypanetpromo@yahoo.gr
f.papapetrou@gmail.com
home@homed.gr
inbox@e-travelling.gr
info@autoscan.gr
info@futurebs.com
info@geegle.gr
info@networknews.gr
info@oikodomein.gr
info@onbusinessbook.com
info@refink.gr
info@safe-shop.gr
info@yourbaby.gr
intron112@yahoo.gr
jenios114@gmail.com
mani1@otenet.gr
marketing@desm.gr
mmantousis@praxi.gr
mshop@mshop.gr
news@e-poema.eu
newsletter@detoxcenter.gr
newsletter@my-space.gr
noreply@computron-ypologistes.com
noreply@economico.gr
noreply@mailinglist.gr
press@greekliberals.net
salesprivelife@gmail.com
seminars@aqsseminars.gr
sofo10@hol.gr
tiodastribuidores@lafloristeria.com
vagelisk@salesmanager.gr
veitas@alfredograf.com
ventlapaz@naturexbolivia.com

Τελευταία ενημέρωση: 30/07/2009

Για να υπάρχει εγκυρότητα στα e-mails που προσθέτουμε καθώς και να μην έχει νομικό πρόβλημα ο ιδιοκτήτης του forum, όσοι αναφέρουν ανεπιθύμητο e-mail να ανεβάζουν και ένα screenshot από το μήνυμα.

Κατά των Provider των ανωτέρω αποστολέων που δεν έκαναν καμία ενέργεια παρόλο που τους ενημερώσαμε και συνέχισαν την παράνομη αποστολή μηνυμάτων από πελάτες και χρήστες του δικτύου του

3.6 Βασικά χαρακτηριστικά του Spam

Συνοψίζοντας τις τεχνικές των spammer και τα προβλήματα που δημιουργούν τα spam μηνύματα, εκτιμούμε πως τα βασικά χαρακτηριστικά **[29]** των spam είναι τα ακόλουθα:

- Δεν υπάρχει καμία προηγούμενη σχέση του παραλήπτη με τον αποστολέα του διαφημιστικού ηλεκτρονικού μηνύματος, δηλαδή δεν έχει προηγηθεί αγορά προϊόντος ή εκδήλωση της επιθυμίας του παραλήπτη για παραλαβή της διαφημιστικής ηλεκτρονικής αλληλογραφίας. Σημειώνεται ότι το χαρακτηριστικό αυτό αποτελεί το βασικότερο στοιχείο για να χαρακτηριστεί ένα ηλεκτρονικό μήνυμα ως spam.

- Δεν υπάρχει η δυνατότητα της αυτόματης διαγραφής από τις λίστες των παραληπτών του αποστολέα, ή, ακόμα κι όταν αυτό συμβαίνει, λειτουργεί μόνο ως μέθοδος για επιβεβαίωση λειτουργίας της συγκεκριμένης ηλεκτρονικής διεύθυνσης.
- Στέλνεται με τη χρήση τεχνικών που αποκρύπτουν την ταυτότητα του αποστολέα.
- Δεν υπάρχει μια έγκυρη και λειτουργική διεύθυνση επικοινωνίας με τον αποστολέα του διαφημιστικού μηνύματος.
- Στέλνεται χωρίς διάκριση, με αυτοματοποιημένα μέσα.
- Περιλαμβάνει ή προωθεί παράνομο ή δυσάρεστο περιεχόμενο .
- Το περιεχόμενό του είναι ψευδές ή παραπλανητικό.

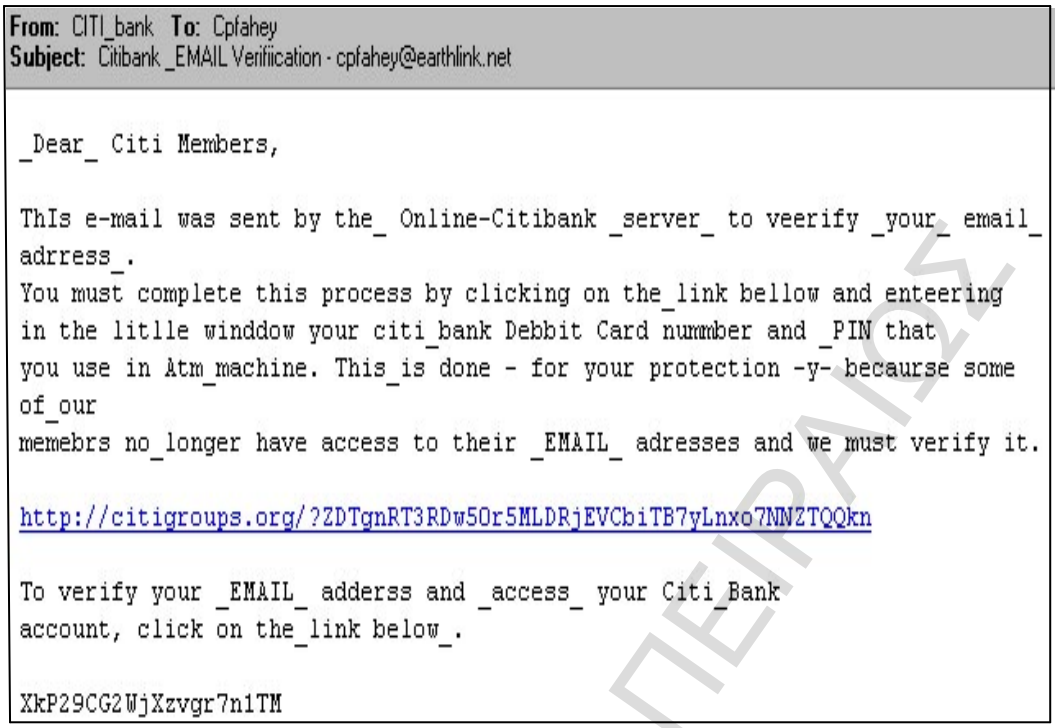
Οι διευθύνσεις των παραληπτών έχουν αποκτηθεί με λογισμικό ανίχνευσης του παγκόσμιου ιστού για συλλογή ηλεκτρονικών διευθύνσεων ("*αράχνες*") ή έχουν αγοραστεί από εταιρείες που παράγουν CD με αυτό το περιεχόμενο (εκατομμύρια διευθύνσεις ηλεκτρονικού ταχυδρομείου σε ένα CD, συνήθως έναντι πολύ μικρού κόστους).

3.7 Μορφές spam μηνυμάτων

Στο τμήμα αυτό παρουσιάζουμε σύγχρονα παραδείγματα **[30]** μορφών των ανεπίκλητων ηλεκτρονικών μηνυμάτων, με κάποια ανάλυση και σχετικές πληροφορίες.

Εικόνα 1:

Αυτό το μήνυμα σε spam εσταλη , 10 ημέρες μετά την σύγκρουση εκ προθέσεως από τρομοκράτες με αεροπλάνα στα κτίρια World Trade Center 2001.09.11 με αποτέλεσμα τα κτίρια να καταστραφούν από τις πυρκαγιές .



From: CITI_bank **To:** Cpfahey
Subject: Citibank _EMAIL Verifiication - cpfahey@earthlink.net

Dear Citi Members,

ThIs e-mail was sent by the_ Online-Citibank _server_ to veerify _your_ email_ adrress_.
You must complete this process by clicking on the_link bellow and enteering in the litlle winddow your citi_bank Debbit Card nummber and _PIN that you use in Atm_machine. This_is done - for your protection -y- becaurse some of_our
memebrs no_longer have access to their _EMAIL_ adresses and we must verify it.

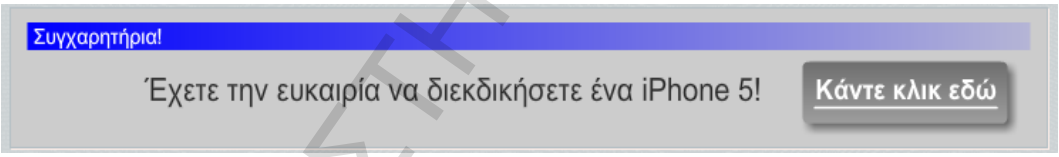
http://citigroups.org/?ZDTgnRT3RDw5Or5MLDRjEVCbiTB7yLnxo7NNZTQQkn

To verify your _EMAIL_ adderss and _access_ your Citi_Bank account, click on the_link below_.

XkP29CG2WjXzvgr7n1TM

Εικόνα 2:

Αυτή η απάτη "*κλοπής ταυτότητας*," masquerading ως μήνυμα από Citibank, που ελήφθη στις 2004.04.04, καθιστά άμεση αίτηση για τον προσωπικό αριθμό αναγνώρισης (PIN), το οποίο μπορεί να χρησιμοποιηθεί για την ανάληψη μετρητών με χρεωστική κάρτα



Εικόνα 3:

Σε αυτή την εικόνα έχουμε μια κλασική περίπτωση spam μηνύματος όπου καλείται ο εισερχόμενος σε μια σελίδα να διεκδίκηση μια συσκευή.

3.8 Τύποι spam μηνυμάτων

Μέχρι στιγμής έχει αναφερθεί η έννοια των spam μηνυμάτων και τα βασικά χαρακτηριστικά τους. Παρακάτω αναφέρονται αρκετά συνοπτικά δύο τύπους των spam μηνυμάτων που υπάρχουν.

3.8.1 Spam τύπου Phishing e-mails

Σύμφωνα με τις αναφορές **[31]**, το spam τύπου *Phishing*, το οποίο πρωτοεμφανίστηκε πριν από δύο χρόνια, αναφέρεται στην προσπάθεια απόσπασης προσωπικών στοιχείων, οικονομικού συνήθως χαρακτήρα που αφορούν τραπεζικούς λογαριασμούς και πιστωτικές κάρτες, χρησιμοποιώντας ως δόλωμα κάποιο ψεύτικο πρόσχημα.

Το Phishing επιχειρείται συνήθως με την αποστολή κάποιου spam μηνύματος, το οποίο ισχυρίζεται ψευδώς ότι αποστέλλεται από κάποια υπαρκτή και νόμιμη εταιρεία (τράπεζα, ηλεκτρονικό κατάστημα, υπηρεσία ηλεκτρονικών πληρωμών κλπ.), σε μία

προσπάθεια να παραπλανήσει τον παραλήπτη και να του αποσπάσει απόρρητα προσωπικά και οικονομικά δεδομένα. Στη συνέχεια, τα στοιχεία αυτά χρησιμοποιούνται από τους spammers για την πραγματοποίηση παράνομων οικονομικών συναλλαγών. Το *Phishing* έχει καταστεί ένα από τα ταχύτερα αναπτυσσόμενα εγκλήματα μέσω του διαδικτύου.

Το phishing δεν είναι επιζήμιο μόνο για τον αποδέκτη, αλλά και για την εταιρεία που μιμείται. Αρκετές εταιρείες, ιδρύματα και οργανισμοί μπορούν σίγουρα να επιβεβαιώσουν ότι οι ονομασίες των προϊόντων τους έχουν χρησιμοποιηθεί σε διάφορες απάτες. Μέσα σε σύντομο χρονικό διάστημα, οι ζημίες από φορείς ηλεκτρονικού "*phishing*" έχουν κάνει τους καταναλωτές ιδιαίτερα προσεκτικούς με τις εταιρείες, ιδρύματα και οργανισμούς που ήταν κάποτε αξιόπιστα. Για το λόγο αυτό, οι επιχειρήσεις και οι καταναλωτές έχουν ευαισθητοποιηθεί ως προς την πρόληψη αυτού του εγκλήματος.

3.8.2 Spam τύπου Chain e-mails

Πρόκειται για μηνύματα που προτρέπουν τους παραλήπτες να τα προωθήσουν κι αυτοί με τη σειρά τους σε άλλους παραλήπτες **[32]**.

Χαρακτηριστική είναι η περίπτωση που αφορά σε συγκέντρωση χρηματικού ποσού που θα βοηθήσει την αποκατάσταση κάποιου σημαντικού προβλήματος υγείας ενός παιδιού σε μία μακρινή χώρα. Το αξιοπερίεργο είναι ότι οι παραλήπτες δεν χρειάζεται να δώσουν αυτοί χρήματα, αλλά μόνο να προωθήσουν το μήνυμα σε όσο το δυνατό περισσότερους παραλήπτες ώστε να συγκεντρωθεί όσο το δυνατό μεγαλύτερο ποσό! . Πιο εντυπωσιακή είναι η περίπτωση όπου το υποτιθέμενο ποσό το παίρνουν αυτοί που προωθούν τα μηνύματα!.

Άλλες φορές υποτίθεται ότι το μήνυμα έχει κάνει το γύρο του κόσμου ***x*** φορές και πρέπει ο παραλήπτης να προωθήσει το μήνυμα σε ***y*** παραλήπτες για να μη σπάσει η αλυσίδα. Τέτοια μηνύματα εκμεταλλεύονται την αφέλεια, το φόβο, και τις δεισιδαιμονίες, που δυστυχώς ακόμα και στην εποχή μας διακατέχουν μεγάλο μέρος των ανθρώπων, αφού υποτίθεται πως αν οι παραλήπτες ακολουθήσουν τις οδηγίες τότε θα βγουν κερδισμένοι επαγγελματικά, οικονομικά, συναισθηματικά, κ.λπ.! Αλλιώς θα υπάρχουν τραγικές συνέπειες στην υγεία τους, ή θα καταστραφούν οικονομικά, ή θα χάσουν τη δουλειά τους, και άλλα τέτοια «διασκεδαστικά»!

Πάντως, πρέπει να τονίσουμε ότι δεν είναι τεχνικά εφικτό να εξακριβωθεί πόσες προωθήσεις έχουν γίνει σε κάποιο μήνυμα και ποιοι τις έκαναν ή δεν τις έκαναν

3.8.3 SPIT (Spam over Internet Telephony) μορφές

Πριν αναφερθούν οι μορφές SPIT, θα πρέπει να αναφερθούν συνοπτικά κάποια πράγματα για το πρωτόκολλο που χρησιμοποιείται από αυτές.

Το SIP **[33]** είναι ένα πρωτόκολλο επιπέδου εφαρμογής για τη διαχείριση των συνόδων πολυμέσων στο internet. Μια σύνοδος μπορεί να καθιερωθεί μεταξύ δύο ή περισσότερων τελικών χρηστών ή και μπορεί να εσωκλείει IP τηλεφωνικές κλήσεις, μηνύματα και συνδιαλέξεις. Το SIP διακινείται μέσω μηνυμάτων όπως INVITE για την έναρξη μιας περιόδου λειτουργίας και BYE για τον τερματισμό της. Ένα SIP μήνυμα μπορεί να εμπεριέχει μια περιγραφή της συνόδου των δυνατοτήτων των μέσων που θα επιτρέψουν τη διαπραγμάτευση μεταξύ των χρηστών. Οι αιτήσεις δρομολόγησης στο SIP επιτυγχάνονται, μέσω πληρεξούσιων, οι οποίες ανακτούν την τρέχουσα θέση των χρηστών.

Σύμφωνα με την αναφορά **[34]**, ως νέο αναδυόμενο πρότυπο IP τηλεφωνίας, το SIP σίγουρα θα είναι στόχος επιθέσεων spam. "Κατά συνέπεια, ένα πολύ κρίσιμο σημείο είναι ο προσδιορισμός εκ των προτέρων του SIP spam και των μηχανισμών αντιμετώπισης του, πριν δημιουργηθεί πρόβλημα ή γίνει σοβαρότερο. Οι διάφορες μορφές του SIP spam μπορούν να κατηγοριοποιηθούν ως εξής:

- **κλήση spam (*call spam*):** αυτή είναι η περίπτωση των αυτόκλητων μηνυμάτων για τη θέσπιση συνόδου φωνής ή βίντεο. Ο spammer μεταδίδει το μήνυμά τους με μέσα πραγματικού χρόνου. Η μορφή αυτή είναι ο συνήθης τρόπος που χρησιμοποιείται από τις τηλεπωλήσεις.
- **Άμεσα μηνύματα spam (*IM spam*):** αυτή η μορφή είναι παρόμοια με τα spam ηλεκτρονικά μηνύματα, αυτόκλητες συνομιλίες των οποίων το περιεχόμενο περιέχετε στο μήνυμα που ο αποστολέας επιδιώκει να μεταδώσει.
- **Παρουσία spam (*Presence spam*):** Άλλη μια μορφή spam παρόμοια με την IM spam ονομάζεται Presence spam. Το τελευταίο δημιουργείται από αυτόκλητες αιτήσεις παρουσίας (συνδρομές) οι οποίες στέλνονται για να περιληφθούν στον κατάλογο των φίλων του χρήστη και, στη συνέχεια, θα σταλθούν IMs σε αυτόν τον χρήστη ή ορισμένες άλλες μορφές επικοινωνίας θα ξεκινήσουν".

Μέχρι στιγμής, μόνο μερικές περιπτώσεις SPIT είναι γνωστές. Σύμφωνα με την αναφορά **[35]** αυτές οι περιπτώσεις αναφέρθηκαν από έναν μεγάλο ιαπωνικό πάροχο υπηρεσιών VoIP. Συνολικά 3 (τρεις) περιπτώσεις είχαν εντοπιστεί, αλλά όλες τους είχαν αποδοθεί στην ίδια εταιρεία. Αν και αυτές είναι οι μοναδικές αναφορές SPIT περιπτώσεων, αυτό δεν σημαίνει ότι αυτές είναι οι μόνες που έχουν παραχθεί, όμως αυτές οι SPIT περιπτώσεις έχουν απομονωθεί δίχως επίπτωση. Έτσι, φαίνεται ότι οι περισσότεροι από τους φορείς παροχής υπηρεσιών VoIP ακόμη θεωρούν ότι δεν υπάρχει κάποια SPIT περίπτωση στα VoIP δίκτυα τους ή δεν θέλουν να αποκαλύψουν τις πραγματικές SPIT στατιστικές, προκειμένου να καθησυχάσουν τους συνδρομητές τους.

Αυτή η έλλειψη SPIT στατιστικών μπορεί επίσης να εξηγηθεί από το γεγονός ότι η VoIP ανάπτυξη βρίσκεται ακόμη σε νηπιακό στάδιο (η κίνηση VoIP αυτή τη στιγμή εκτιμάται ότι θα είναι το 10% της PSTN κυκλοφορίας), οπότε δεν υπάρχουν επαρκής VoIP υποδομές έτσι ώστε το SPIT να είναι επικερδές για τους spammers. Επιπλέον, τα τρέχων VoIP δίκτυα μπορούν να συνεχίσουν να θεωρούνται ως νησιά που συνδέονται μέσω του δικτύου PSTN, και αυτό δεν έχει ως αποτέλεσμα την δημιουργία μεγάλων όγκων κλήσεων.

Παρά το μικρό αριθμό των περιπτώσεων SPIT που έχουν αναφερθεί, δεν υπάρχει αμφιβολία ότι το SPIT θα αυξηθεί ανάλογα με τα VoIP δίκτυα. Παραδοσιακά οι PSTN τηλεπωλήσεις σίγουρα θα μεταβιβαστούν σε VoIP την ίδια στιγμή που θα μεταβιβαστούν και οι χρήστες του PSTN. Κατά συνέπεια, το VoIP, θα υποφέρει από το SPIT πρόβλημα διότι οι στόχοι των "*spammers*" είναι οι ίδιοι και οι τεχνικές μπορούν να διατηρηθούν και στα δύο είδη δικτύων. Φυσικά οι PSTN τηλεπωλητές θα πρέπει να προσαρμοστούν με την χρήση του VoIP για τις δραστηριότητές τους, αλλά αυτό σίγουρα θα έχει ως αποτέλεσμα την αύξηση του αριθμού των ανεπιθύμητων κλήσεων VoIP συγκριτικά με την απόδοση του δικτύου PSTN αν και δεν είναι μεγαλύτερη.

Ο αριθμός των κλήσεων που γίνεται από τους τηλεπωλητές μπορεί να είναι υψηλό, ωστόσο, αυτό δεν είναι η χειρότερη περίπτωση. Το σενάριο της χειρότερης περίπτωσης θα προκύψει, εάν λάβουμε υπόψη ότι το ποσοστό των κλήσεων SPIT και άμεσων μηνυμάτων (IM) θα είναι όσο των spam στα μηνύματα ηλεκτρονικού ταχυδρομείου (περίπου 80-85%). Σε αυτή την περίπτωση, δεν θα πρέπει να θεωρήσουμε μόνο ότι οι πελάτες είναι οι μόνοι που πλήττονται άμεσα από το πρόβλημα αυτό, αλλά και οι πάροχοι υπηρεσιών VoIP θα έχουν ένα σοβαρό πρόβλημα διαστασιολόγησης των συστημάτων των δικτύων τους. Αν υπάρξει αυτή η περίπτωση τα αντι-SPIT εργαλεία θα είναι απαραίτητα για την χρηστικότητα των συστημάτων VoIP.

Μια SIP Spam Παραβίαση αναφέρεται στη διαβίβαση του όγκου, αυτόκλητων SIP μηνυμάτων κάθε μορφής. Μια SIP Spam απειλή είναι μια πιθανή ενέργεια ή εκδήλωση που εκμεταλλεύεται μια SIP Spam ευπάθεια για την ανάπτυξη μιας SIP Spam παραβίασης.

4. Ρυθμιστικό πλαίσιο αντιμετώπισης των Spam

Το spam είναι ένα θέμα, που άπτεται διαφορετικών πτυχών των υπηρεσιών ηλεκτρονικών επικοινωνιών, της προστασίας του καταναλωτή, της προστασίας της ιδιωτικότητας και της ασφάλειας, σε εθνικό και διασυνοριακό επίπεδο. Κατά συνέπεια, το νομικό πλαίσιο που έχει ήδη τεθεί σε εφαρμογή είναι πολύπλοκο, λόγω των διάφορων εθνικών δημόσιων και ιδιωτικών οργανισμών εκτέλεσης που ασχολούνται με αυτό το θέμα και την ανάγκη να καλύπτει διάφορα είδη αυτόκλητων μηνυμάτων.

Η συνηθέστερη μορφή διαφήμισης στο Διαδίκτυο η αυτόκλητων μηνυμάτων είναι η άμεση διαφήμιση, συνήθως μέσω της λεγόμενης «*μη αιτηθείσας εμπορικής επικοινωνίας*». Η αποστολή μη αιτηθέντων διαφημιστικών μηνυμάτων ηλεκτρονικού ταχυδρομείου, το λεγόμενο '*spamming*' ή '*unsolicited bulk e-mail'* ή '*junk mail'*. Στις μέρες μας έχει λάβει ενδημικό χαρακτήρα λόγω του χαμηλού της κόστους, αλλά και της δυνατότητας, που παρέχει σε διαφημιστές και διαφημιζομένους για άσκηση εξατομικευμένης πολιτικής μάρκετινγκ.

Παρακάτω θα αναφερθούν οι νομικές έννοιες και ορισμοί αναφορικά με το spam ώστε να μπορέσουν να γίνουν ευκολότερα κατανοητά τα νομοθετικά πλαίσια χωρών εντός και εκτός της Ευρωπαϊκής Ένωσης αλλά δεν θα παραλείψουμε να κάνουμε μια αναφορά στης εποπτικές και ρυθμιστικές αρχές στον τομέα των τηλεπικοινωνιών.

4.1 Αρχή Προστασίας Προσωπικών Δεδομένων

Για την αμεσότερη και ταχύτερη προστασία των πολιτών από την επεξεργασία προσωπικών δεδομένων θεωρήθηκε αναγκαία η ίδρυση μιας Αρχής που θα εποπτεύει και θα ασχολείται αποκλειστικά με αυτό το αντικείμενο. Η αρχή αυτή, που ιδρύθηκε το 1997 και ονομάστηκε Αρχή Προστασίας Προσωπικών Δεδομένων (ΑΠΠΔ) **[36]** είναι ποικίλες αρμοδιότητες σύμφωνα με τις διατάξεις του ***Ν.2472/1997*** (άρθρα 15–20) και έχει ως αποστολή την εποπτεία της τήρησης του προσωπικού απορρήτου και στο Διαδίκτυο, όπως ορίζεται και από τον μεταγενέστερο ***Ν.2774/1999*** για την *«Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα»*. μεταξύ των οποίων είναι να εκδίδει οδηγίες και αποφάσεις και να γνωμοδοτεί για κάθε ρύθμιση που αφορά την επεξεργασία και προστασία δεδομένων προσωπικού χαρακτήρα. Οι σημαντικότερες αποφάσεις της ΑΠΠΔ είναι :

- Η Απόφαση 50/2000 σχετικά με τους όρους για την νόμιμη επεξεργασία δεδομένων προσωπικού χαρακτήρα για τους σκοπούς της άμεσης εμπορίας ή διαφήμισης και της διαπίστωσης πιστοληπτικής ικανότητας.

- Η Απόφαση 8/2003 σχετικά με την πρόσβαση τρίτου σε δεδομένα εταιρείας κινητής τηλεφωνίας για άσκηση δικαιώματος υπεράσπισης ενώπιον δικαστηρίου.

4.2 Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών

Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) **[37]** λειτουργεί από το 2003 ως ανεξάρτητη αρχή σύμφωνα με τις διατάξεις του ***Ν.3115/2003***. Σκοπός της ΑΔΑΕ είναι η προστασία του απορρήτου των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο. Στην έννοια της προστασίας του απορρήτου των επικοινωνιών περιλαμβάνεται και ο έλεγχος της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου.

Στις αρμοδιότητες της ΑΔΑΕ περιλαμβάνεται το δικαίωμα διενέργειας ελέγχων, αποδοχής και εξέτασης καταγγελιών αλλά και έκδοσης κανονιστικών κειμένων, όπως είναι ο Κανονισμός για την Διασφάλιση του Απορρήτου Εφαρμογών και Χρήστη Διαδικτύου.

4.3 Ο Ελληνικός Φορέας Πρόληψης Τηλεπικοινωνιακής Απάτης

Ο (*ΕΦΤΑ*) **[38]** δημιουργήθηκε τις αρχές του 2000 από στελέχη των εταιρειών σταθερών και κινητών επικοινωνιών στην Ελλάδα (OTE, Vodafone, Cosmote, STETHELLAS), τα οποία δραστηριοποιούνται στον εντοπισμό και την πρόληψη τις Τηλεπικοινωνιακής Απάτης και του Ηλεκτρονικού Εγκλήματος γενικότερα.

Ως Τηλεπικοινωνιακή Απάτη θεωρείται :

a) Η πρόσβαση σε τηλεπικοινωνιακά δίκτυα για χρήση τηλεπικοινωνιακών υπηρεσιών, χωρίς να πληρώνεται το αντίστοιχο τέλος.
b) Η μη εξουσιοδοτημένη πρόσβαση σε δεδομένα με σκοπό την αποκόμιση οικονομικού οφέλους, ή για τις αθέμιτους σκοπούς, τις βιομηχανική κατασκοπεία.
c) Η απάτη τις ηλεκτρονικές συναλλαγές και το ηλεκτρονικό εμπόριο.

Ο ΕΦΤΑ δημιουργήθηκε με σκοπό :

1. Την ανταλλαγή πληροφοριών σχετικών με τις μεθόδους, με τις οποίες διενεργούνται Τηλεπικοινωνιακές Απάτες, εξαιτίας των οποίων χάνονται πολλά δις Ευρω για τις Ευρωπαϊκές Τηλεπικοινωνιακές εταιρίες, κάθε χρόνο.
2. Την από κοινού λήψη μέτρων των συνεργαζόμενων εταιριών, για την αντιμετώπιση νέων περιπτώσεων Τηλεπικοινωνιακής Απάτης, αλλά και του γενικότερου Ηλεκτρονικού Εγκλήματος, φαινόμενα που εντάθηκαν μετά και την πλήρη απελευθέρωση των τηλεπικοινωνιών στην Ελλάδα.
3. Την ανταλλαγή πληροφοριών (στα πλαίσια των ***Ν.2472/97*** *«για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα»* και του ***Ν.2774/99*** *«για την προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα»*), σχετικά με απατεώνες, οι οποίοι μετερχόμενοι διάφορες μεθόδους, χρεώνουν τις συνεργαζόμενες εταιρίες με τεράστια χρηματικά ποσά.

4.3.1 Προσωπικά δεδομένα και Spam

Η προστατευτική στάση απέναντι στα προσωπικά δεδομένα αντικατοπτρίζεται στο σχετικό νομοθετικό πλαίσιο που διαμορφώθηκε σε διεθνές, ευρωπαϊκό και εθνικό επίπεδο.

Ιστορικά το πρώτο εθνικό νομοθέτημα που αφορούσε παγκοσμίως στην προστασία των προσωπικών δεδομένων ήταν εκείνο του κρατιδίου της Έσσης της Γερμανίας το 1970. Στη συνέχεια ακολούθησε η θέσπιση αντίστοιχων νόμων από τη Σουηδία, την Αυστρία, τη Γαλλία, τη Δανία, τη Νορβηγία και το Λουξεμβούργου **[39]**, ρυθμίσεις άκρως αυστηρές, επηρεασμένες από το κλίμα της εποχής που αντιμετώπιζε με φόβο και δυσπιστία την τεχνολογία και τους ηλεκτρονικούς υπολογιστές.

Το 1980 ο Οργανισμός για Οικονομική Συνεργασία και Ανάπτυξη (Ο.Ο.Σ.Α.) εξέδωσε τη Σύσταση με τίτλο «Κατευθυντήριες γραμμές διέπουσες την προστασία της ιδιωτικής σφαίρας του ανθρώπου και τις διασυνοριακές ροές δεδομένων προσωπικού χαρακτήρα»**[40]**. Η έλλειψη νομικής δεσμευτικότητας της Σύστασης δεν μειώνει τη σημασία της, καθώς οι κατευθυντήριες γραμμές **[41]** τις οποίες εισήγαγε αποτέλεσαν σημείο αναφοράς για όλα τα νομοθετικά κείμενα που ακολούθησαν.

Από αυτές τις κατευθυντήριες γραμμές επηρεάστηκε και η Σύμβαση του Συμβουλίου της Ευρώπης «για την προστασία των ατόμων από την αυτόματη επεξεργασία των προσωπικών πληροφοριών» που υπογράφηκε στο Στρασβούργο στις 28.1.1981, περισσότερο γνωστή ως «Σύμβαση 108» **[42]**. Η Σύμβαση αυτή, το πρώτο νομικά δεσμευτικό κείμενο διεθνώς, παγίωσε τις αρχές που διέπουν την προστασία των προσωπικών δεδομένων και το κείμενό της υπήρξε πρότυπο για τις μετέπειτα ρυθμίσεις, κυρίως σε ευρωπαϊκό επίπεδο.

Το 1990 η Γενική Συνέλευση των Ηνωμένων Εθνών συνέταξε τις «*Κατευθυντήριες αρχές προστασίας προσωπικών δεδομένων σε αυτοματοποιημένα αρχεία*», κείμενο το

οποίο επαναλαμβάνει ουσιαστικά τις αρχές που έχουν ήδη διατυπωθεί από τον Ο.Ο.Σ.Α. και τη Σύμβαση 108.

Όπως αναφέρθηκε παραπάνω, στα spam κατατάσσονται κυρίως μηνύματα εμπορικού περιεχομένου, όπου ο καταναλωτής για να αγοράσει το προϊόν που τον ενδιαφέρει υποχρεούται να εισάγει κάποια στοιχεία του, τα οποία ονομάζονται προσωπικά δεδομένα (π.χ όνομα, επάγγελμα, διεύθυνση, τηλέφωνο, αριθμός τραπέζης κ.λ.π). Τα δεδομένα αυτά επεξεργάζονται από την εκάστοτε εταιρεία που έστειλε το μήνυμα είτε από τους spammers εάν πρόκειται για μήνυμα παραπλάνησης, απάτης. Επεξεργασία δεδομένων προσωπικού χαρακτήρα **[43]** αποτελεί η συλλογή, η αποθήκευση, η τροποποίηση, η χρήση, η διαβίβαση ή κάθε άλλης μορφής διάθεση, η συσχέτιση ή ο συνδυασμός, η διαγραφή.

Ορόσημο στην προστασία των προσωπικών δεδομένων αποτελεί η ***Οδηγία 95/46*** «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών», η οποία εναρμονίζει τις αντίστοιχες εθνικές νομοθεσίες, αφομοιώνοντας παράλληλα τις αρχές και το επίπεδο προστασίας που είχε διαμορφωθεί από τις προαναφερθείσες διεθνείς και ευρωπαϊκές ρυθμίσεις. Η ***Οδηγία 95/46*** καθιερώνει υψηλό επίπεδο προστασίας με τις αρχές που αναφέρονται ***στο άρθρο 6*** και είναι:

α) *η αρχή της νομιμότητας της επεξεργασίας*,

β) *η αρχή του σκοπού*,

γ) *η αρχή της αναλογικότητας*,

δ) *η αρχή της ακρίβειας και*

ε) η *αρχή της χρονικά περιορισμένης διατήρησης των δεδομένων*.

Παρόλο που η γενική ***Οδηγία 95/46*** ως τεχνολογικά ουδέτερη θα μπορούσε να εφαρμοσθεί στο διαρκώς μεταβαλλόμενο τεχνολογικά περιβάλλον (αιτιολογική σκέψη ***αριθμ. 46 Οδ. 2002/58***), εξειδικεύθηκε από την ***Οδηγία 97/66*** «για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα», η οποία καταργήθηκε **[44]** από την ***Οδηγία 2002/58*** «για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες».

Η δυνατότητα εφαρμογής των κανόνων προστασίας δεδομένων βασίζεται στη μεταχείριση «των προσωπικών δεδομένων». Ένας γενικός ορισμός **[45]** που μπορεί να δοθεί για τα προσωπικά δεδομένα είναι οποιαδήποτε πληροφορία η οποία προσδιορίζει ή εύκολα μπορεί να προσδιοριστεί με την βοήθεια της πληροφορίας αυτής ένα φυσικό πρόσωπο. Ένα ευπροσδιόριστο πρόσωπο είναι κάποιος που μπορεί να προσδιοριστεί, άμεσα ή έμμεσα, κυρίως αναφορικά σε έναν προσδιοριστικό ή σε έναν ή περισσότερους παράγοντες συγκεκριμένης φυσικής, φυσιολογικής, διανοητικής, οικονομικής, πολιτιστικής ή κοινωνικής ταυτότητάς του (οδηγία προστασίας δεδομένων). Αυτά τα κριτήρια αναφέρονται στον κατάλληλο παράγοντα του προσδιορισμού, της ευκολίας και της ακρίβειας του προσδιορισμού. Ένα πρόσωπο δεν θα θεωρηθεί «ευπροσδιόριστο» εάν ο προσδιορισμός απαιτεί έναν αριθμό ωρών, κόστους και ανθρώπινου δυναμικού.

Ο άμεσος προσδιορισμός είναι δυνατός εάν παραδείγματος χάριν μια διεύθυνση ηλεκτρονικού ταχυδρομείου περιέχει έναν ή περισσότερους από τους ευπροσδιόριστους παράγοντες, όπως ένα όνομα, έτσι ώστε το πρόσωπο που αφορούν τα στοιχεία μπορεί να προσδιοριστεί χωρίς τη χρήση μιας τρίτης πηγής. Οι αριθμοί τηλεφώνου επιτρέπουν τον έμμεσο προσδιορισμό των συνδρομητών μέσω της χρήσης των αντίστροφων καταλόγων καθώς επίσης και μέσω των ηλεκτρονικών φορέων επικοινωνίας παροχής υπηρεσιών. Ο έμμεσος προσδιορισμός επιτρέπει επίσης τις διευθύνσεις IP, οι οποίες μπορούν να επισημανθούν σε έναν υπολογιστή και κατά συνέπεια μέσω του προμηθευτή και σε έναν συνδρομητή.

4.3.2 Το Spam ως παραβίαση των δικαιωμάτων προστασίας της ιδιωτικής ζωής και προστασίας των δεδομένων

Η ευρωπαϊκή νομοθεσία προβλέπει εγγυήσεις σε σχέση με την παραλαβή των αυτόκλητων κλήσεων όχι μόνο επειδή δεν μπορεί να επιβάλλει επιβάρυνση ή / και του κόστους για το δικαιούχο, αλλά κυρίως επειδή οι αυτόκλητες επικοινωνίες επηρεάζουν τα θεμελιώδη δικαιώματα του ατόμου.

Το θέμα της προσβολής προσωπικών δεδομένων τίθεται έντονα στο spamming, καθώς γίνεται δεκτό από τη θεωρία και τη νομολογία **[46]** ότι η ηλεκτρονική διεύθυνση (e-mail address) συνιστά μορφή ηλεκτρονικής υπογραφής και, επομένως, απλό προσωπικό δεδομένο**[47]**.

Το spam θεωρείται παραβίαση της ιδιωτικής ζωής **[48]**. Κείμενο μη δεσμευτικό, αλλά εξίσου σημαντικό είναι το θεμελιώδες δικαίωμα της ιδιωτικής ζωής, που στηρίζεται στο *άρθρο 8* της Ευρωπαϊκής Σύμβασης των Δικαιωμάτων του Ανθρώπου, καθώς και στον Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης [***άρθ. 7*** *(ιδιωτικότητας) και* ***άρθ. 8*** *(προστασία δεδομένων)*] περιλαμβάνει ιδιωτικότητα της πληροφορίας, ιδιωτικότητα της συσχέτισης και της ελευθερίας της επικοινωνίας με την έννοια της ιδιωτικότητας / μυστικότητας των επικοινωνιών. Η ιδιωτικότητα της πληροφορίας σχετίζεται με το δικαίωμα του ατόμου να αποφασίζει μόνο του, εάν και ποια προσωπικά δεδομένα μπορούν να γνωστοποιούνται σε τρίτους ή / και να επεξεργαστούν από αυτούς. Επηρεάζει επίσης τη λεγόμενη σχεσιακή διάσταση της ιδιωτικότητας, δηλαδή το δικαίωμα να καθορίζει, ποιες επικοινωνίες επιθυμεί κάποιος να λαμβάνει ή όχι. **[49]**

Κατά κύριο λόγω, οι αυτόκλητες κλήσεις παραβιάζουν την ιδιωτικότητα με τη στενή και εμφανή έννοια του όρου, μέσω της παράνομης εισβολής στους ηλεκτρονικούς υπολογιστές, των διακομιστών και στην ιδιωτική σφαίρα του ατόμου [οδηγία περί ηλεκτρονικής ιδιωτικότητας]. Περαιτέρω, το spam καθώς και η αντίστοιχη παράνομη συλλογή και χρήση των προσωπικών δεδομένων στερεί από τα άτομα την ικανότητά τους να καθορίζουν τι πληροφορίες σχετικά με αυτούς, θα γίνουν γνωστές σε άλλους, επηρεάζει το δικαίωμα της αυτοδιάθεσης. **[50]**.

4.4 Νομικοί ορισμοί αναφορικά με το Spam

Αν και ο όρος spam χρησιμοποιείται στα πολιτικά κείμενα, ή στις έρευνες δεν υπάρχει κάποιος υποστηριζόμενος νομικός καθορισμός του όρου. Ο όρος spam χρησιμοποιείται συνήθως, όπως προανέφερα, για να περιγράψει «*οποιοδήποτε λαμβανόμενο μήνυμα που είναι ανεπιθύμητο από τον παραλήπτη*», συχνά αποτελούμενος από διαφημίσεις για προϊόντα και υπηρεσίες, μια προσέγγιση που επικρίθηκε από την ομάδα εργασίας αντι-Spam του Οργανισμού Οικονομικής Ανάπτυξης και Συνεργασίας ΟΟΣΑ (*OECD - Organization for Economic Co-operation and Development*) ως «*πάρα πολύ ευρύ και απλοϊκό*» **[51]** εφόσον δεν διευκρινίζει το μέσο μήνυμα ούτε διαφοροποιεί τα spam από τις νόμιμες μεθόδους.

Οι περισσότεροι παγκόσμιοι προτεινόμενοι ορισμοί για το spam αναφέρονται στα ακόλουθα στοιχεία:

- *εκούσιο,*
- *μαζικό,*
- *εμπορικό*

Στην ανακοίνωσή «*σχετικά με τις εκούσιες εμπορικές επικοινωνίες ή spam*» η Ευρωπαϊκή Επιτροπή καταλλήλως σημειώνει ότι ο όρος χρησιμοποιείται περισσότερο ως όρος που ούτε καθορίζεται ούτε χρησιμοποιείται από τις σχετικές οδηγίες. Στα επίσημα έγγραφα της Ευρωπαϊκής Ένωσης το spam ορίζεται ως:

"***η επαναλαμβανόμενη μαζική αποστολή των εκούσιων εμπορικών μηνυμάτων από έναν αποστολέα που μεταμφιέζει ή σφυρηλατεί την ταυτότητά του***" [52] ή "***η αποστολή σε μεγάλη ποσότητα του εκούσιου υλικού μάρκετινγκ-διαφήμισης μέσω του ηλεκτρονικού ταχυδρομείου"*** [53].

Ένα κρίσιμο συστατικό όλων των ορισμών φαίνεται να είναι ο όρος *«εκούσιο».* Σε ένα σύστημα επιλογής (*opt-in*), όπως το σύστημα που υιοθετήθηκε από την Ευρωπαϊκή Ένωση, οι εκούσιες επικοινωνίες, δηλαδή οι επικοινωνίες με σκοπό την προσέγγιση των χρηστών χωρίς την προγενέστερη συγκατάθεσή τους, είναι παράνομη. Σε ένα σύστημα αποχώρησης (*opt-out*), υπάρχουν εκούσιες νομικές επικοινωνίες (*πριν από την αποχώρηση του παραλήπτη*) και εκούσιες παράνομες επικοινωνίες (*μετά από την αποχώρηση του παραλήπτη*)**[50].**

Ως «***επικοινωνία***» καθορίζονται "***οποιεσδήποτε πληροφορίες που ανταλλάσσονται ή που μεταβιβάζονται μεταξύ ενός πεπερασμένου αριθμού συμβαλλόμενων μερών με τη βοήθεια μιας δημόσια διαθέσιμης ηλεκτρονικής υπηρεσίας επικοινωνιών***" **[48]**.

Η έννοια του «*ηλεκτρονικού ταχυδρομείου*» αξίζει την μέγιστη προσοχή: Σύμφωνα με την αναφορά **[48]**, μήνυμα ηλεκτρονικού ταχυδρομείου είναι "οποιοδήποτε μήνυμα κειμένου, φωνής, ήχου ή εικόνας που στέλνεται μέσω ενός δημόσιου δικτύου επικοινωνιών και μπορεί να αποθηκευτεί στο δίκτυο ή στον τερματικό εξοπλισμό του παραλήπτη έως ότου συλλεχθεί από τον παραλήπτη".

Με αυτή την έννοια καλύπτεται όχι μόνο το ηλεκτρονικό ταχυδρομείο, SMS ή MMS αλλά και οποιαδήποτε μορφή ηλεκτρονικής επικοινωνίας, όπου δεν απαιτείται η ταυτόχρονη συμμετοχή του αποστολέα και του παραλήπτη **[59],[48]**. Μεταξύ άλλων περιλαμβάνονται και τα μηνύματα που αφήνονται στους αυτόματους τηλεφωνητές, συστήματα υπηρεσίας προσωπικού τηλεφωνητή, που περιλαμβάνονται στις κινητές υπηρεσίες, επικοινωνίες που απευθύνονται άμεσα σε μια διεύθυνση IP **[54]**.

Η παραπομπή «*σε ένα πεπερασμένο αριθμό μερών*» πρέπει να ερμηνευθεί ως «*point to point* (από σημείο σε σημείο) *επικοινωνία*». Ακόμα και αν η χρήση του όγκου φαίνεται να είναι στοιχείο καθορισμού του spam, όπου συνήθως συνδέεται με την αποστολή μεγάλου αριθμού αυτόκλητων μηνυμάτων **[55]**, οι διατάξεις της οδηγίας [48] δεν προϋποθέτουν μια μέγιστη ή ελάχιστη ποσότητα σταλμένων μηνυμάτων. Αυτή η προσέγγιση είναι κατανοητή. Η Ευρωπαϊκή προσέγγιση βασίζεται στην αρχή της συγκατάθεσης και όχι στην ποσότητα ηλεκτρονικής αποστολής.

Μια ευρεία προσέγγιση υιοθετείται από την FEDMA (Federation of European Direct and interactive Marketing / ομοσπονδία του ευρωπαϊκού άμεσου μάρκετινγκ) ως προς την χρήση των προσωπικών δεδομένων στο άμεσο μάρκετινγκ **[56]**, όπου καθορίζει το άμεσο μάρκετινγκ ως

«***επικοινωνία μέσων οποιουδήποτε υλικού διαφήμισης ή μάρκετινγκ, το οποίο πραγματοποιείται από τον ίδιο άμεσο έμπορο ή εξ ονόματός του και κατευθύνεται σε συγκεκριμένα άτομα***».

4.5 Υιοθέτηση των Οδηγιών στην Ευρωπαϊκή Ένωση

Λόγω των προβλημάτων που σχεδόν όλες οι χώρες αντιμετώπιζαν και ακόμα αντιμετωπίζουν από τα spam μηνύματα, τα οποία στέλνονται από υπηκόους κάποιας χώρας προς υπηκόους της ίδιας χώρας ή εκτός αυτής, η Ευρωπαϊκή Ένωση αποφάσισε πως θα πρέπει να δημιουργήσει κάποιες οδηγίες.

Οι οδηγίες αυτές θα υιοθετηθούν από τις χώρες της Ευρωπαϊκής Ένωσης ή ακόμα και αν χρειαστεί να υποχρεωθούν να εντάξουν κάποιο νομικό πλαίσιο στο δίκαιο τους, όπου θα ρυθμίζεται το πρόβλημα των spam.

Σύμφωνα με την Επιτροπή, το νομικό πλαίσιο πρέπει να βεβαιώνει ότι οι υπηρεσίες ρυθμίζονται μέσω ενός ισότιμου τρόπου και οι καταναλωτές / χρήστες θα πρέπει να αποκτήσουν το ίδιο επίπεδο προστασίας, σε σχέση με την τεχνολογία που χρησιμοποιούν. Κατά συνέπεια, ο παραπάνω υιοθετημένος καθορισμός του spam είναι εφαρμόσιμος σε κάθε μορφή / μέσο του spamming. Οι νομικές διατάξεις, που παρουσιάζονται παρακάτω εφαρμόζονται τηρούμενων των αναλογιών σε παρόμοιες τεχνολογίες με διαφορετικές προδιαγραφές. Από τους βασικότερους στόχους της Ε.Ε. το

(***άρθρο 34 και 56 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης***)**[57]** προκειμένου να αποφευχθούν ανάλογα προσκόμματα στη λειτουργία της κοινοτικής αγοράς. Αποφεύγοντας τις απόλυτες απαγορεύσεις στο χώρο της πληροφορικής ως αντιστάθμισμα , εξοπλίζει τους καταναλωτές με αυξημένη πληροφόρηση, ώστε να μην καθίστανται θύματα των ποικίλων διαφημιστικών μεθόδων **[58]**.

Οι οδηγίες που έχουν εκδοθεί από την Ευρωπαϊκή Ένωση είναι οι εξής:

Η ***Οδηγία 2002/58/ΕΚ*** *του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου, της 12ης Ιουλίου 2002* **[48]**, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες) **[48]** αναφέρει τις αυτόκλητες κλήσεις του Ηλεκτρονικού ταχυδρομείου ”για τους σκοπούς του άμεσου εμπορίου”, οι οποίες - σύμφωνα με την Ευρωπαϊκή Επιτροπή “συνολικά καλύπτουν τα περισσότερα είδη spam”. **[59]**

Σύμφωνα με την αναφορά **[48]**, η οδηγία περιλαμβάνει τους ορισμούς των όρων **"*χρήστης", "δεδομένα κίνησης", "δεδομένα θέσης", "επικοινωνία", "κλήση", "υπηρεσία προστιθέμενης αξίας", "ηλεκτρονικό ταχυδρομείο"*** κ.α.

Αναφέρεται στα ενδεδειγμένα τεχνικά και οργανωτικά μέτρα που οφείλει να λαμβάνει ο φορέας παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών καθόσον αφορά την ασφάλεια του δικτύου, προκειμένου να προστατεύεται η ασφάλεια των υπηρεσιών του .Κατοχυρώνει το απόρρητο των επικοινωνιών που διενεργούνται μέσω δημόσιου δικτύου επικοινωνιών και των διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, καθώς και των συναφών δεδομένων κίνησης των κρατών μελών μέσω της εθνικής νομοθεσίας. Ορίζει ότι πρέπει να απαλείφονται ή να καθίστανται ανώνυμα όταν δεν είναι πλέον απαραίτητα για το σκοπό της μετάδοσης μιας επικοινωνίας τα δεδομένα κίνησης που αφορούν συνδρομητές και χρήστες, τα οποία υποβάλλονται σε επεξεργασία και αποθηκεύονται. Ρυθμίζει τα θέματα της αναλυτικής χρέωσης, της ένδειξης της ταυτότητας και του περιορισμού της αναγνώρισης καλούσας και συνδεδεμένης γραμμής, των δεδομένων θέσης, της αυτόματης προώθησης κλήσεων, των τηλεφωνικών καταλόγων συνδρομητών, των αυτόκλητων κλήσεων, των τεχνικών χαρακτηριστικών και τυποποίησης κ.α.

Όσον αφορά το spam η οδηγία αναφέρει στο ***άρθρο 13*** πως μπορεί να αντιμετωπιστεί ή περιοριστεί. Συνοπτικά δεν επιτρέπεται η χρήση αυτόματων συστημάτων κλήσης (φαξ, ηλεκτρονικό ταχυδρομείο, κλπ), και η χρήση των στοιχείων του πελάτη που αποκτήθηκαν από προηγούμενη αγορά ενός προϊόντος, γενικώς οι αυτόκλητες κλήσεις με σκοπό την άμεση εμπορική προώθηση δίχως να έχουν δώσει οι συνδρομητές εκ των προτέρων την συγκατάθεση τους. Θα πρέπει να τους έχει δοθεί σαφώς και ευδιάκριτα η ευκαιρία να αντιταχθούν στην χρησιμοποίηση των ηλεκτρονικών στοιχείων επαφής τους. Η συγκατάθεση μπορεί να δοθεί με κάθε τρόπο που επιτρέπει την ελεύθερη έκφραση ακόμα και με σήμανση τετραγωνιδίου κατά την σύνδεση με κάποια ιστοσελίδα στο Internet. Τα προσημειωμένα τετραγωνίδια δεν είναι συμβατά διότι εκεί υπάρχει υπονοούμενη συγκατάθεση, η οποία και δεν είναι συμβατή. Εμφανείς πρέπει να είναι στον συνδρομητή ο σκοπός του μηνύματος. Επίσης απαγορεύεται η αποστολή μηνυμάτων, άμεσης εμπορικής προώθησης, μέσω ηλεκτρονικού ταχυδρομείου δίχως να είναι εμφανή ή έγκυρη η διεύθυνση του αποστολέα.

Η ***Οδηγία 2002/58/ΕΚ*** δεν καλύπτει ρητά όλα τα ζητήματα που αφορούν την προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών, συμπεριλαμβανομένων των υποχρεώσεων του υπεύθυνου επεξεργασίας και των ατομικών δικαιωμάτων. Δεν θίγει την δυνατότητα των κρατών μελών να προβαίνουν σε νόμιμη παρακολούθηση των ηλεκτρονικών επικοινωνιών ή να λαμβάνουν άλλα μέτρα όταν αυτό είναι αναγκαίο για τους σκοπούς της δημόσιας ασφάλειας, της εθνικής άμυνας, της ασφάλειας του κράτους σύμφωνα με την Ευρωπαϊκή σύμβαση για την προάσπιση των δικαιωμάτων του ανθρώπου και των θεμελιωδών ελευθεριών.

Η ***Οδηγία 2000/31/ΕΚ*** *του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8ης Ιουνίου 2000* **[60]** σχετίζεται με ορισμένες πτυχές των υπηρεσιών της κοινωνίας

της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά («οδηγία για το ηλεκτρονικό εμπόριο»), έχει ως στόχο την ομαλή λειτουργία της εσωτερικής αγοράς, εξασφαλίζοντας την ελεύθερη κυκλοφορία των υπηρεσιών της Κοινωνίας της Πληροφορίας μεταξύ των κρατών μελών.

Σύμφωνα με την αναφορά ο νομος, ορίζει ***τις έννοιες "υπηρεσίες της κοινωνίας της πληροφορίας", "φορέας παροχής υπηρεσιών", "εγκατεστημένος φορέας παροχής υπηρεσιών","αποδέκτης της υπηρεσίας","καταναλωτής","εμπορικές επικοινωνίες" "νομοθετικώς κατοχυρωμένο επάγγελμα***" κ.α.

Κάθε κράτος μέλος μεριμνά ώστε οι υπηρεσίες της κοινωνίας της πληροφορίας που παρέχει ένας φορέας εγκατεστημένος στο έδαφός του να τηρούν τις ισχύουσες εθνικές διατάξεις του οι οποίες εμπίπτουν στο συντονισμένο τομέα.

Τα κράτη μέλη εξασφαλίζουν ότι η ανάληψη και η άσκηση δραστηριότητας φορέα παροχής υπηρεσίας της Κοινωνίας της Πληροφορίας δεν μπορεί να υπαχθεί σε καθεστώς προηγούμενης παροχής άδειας ή σε οποιαδήποτε άλλη προϋπόθεση ισοδυνάμου αποτελέσματος.

Εκτός από άλλες προϋποθέσεις 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 πληρούν τουλάχιστον τους αναφερόμενους όρους. Τα κράτη μέλη εξασφαλίζουν ότι η χρήση εμπορικών επικοινωνιών που συνιστούν υπηρεσία της Κοινωνίας της Πληροφορίας ή αποτελούν μέρος της, η οποία παρέχεται από μέλος νομοθετικώς κατοχυρωμένου επαγγέλματος, επιτρέπεται εφόσον τηρεί τους επαγγελματικούς κανόνες, μεριμνούν ώστε το νομικό τους σύστημα να επιτρέπει τη σύναψη συμβάσεων με ηλεκτρονικά μέσα, διασφαλίζουν ότι, σε περίπτωση παροχής μιας υπηρεσίας της Κοινωνίας της Πληροφορίας η οποία συνίσταται στη μετάδοση πληροφοριών που παρέχει ο αποδέκτης της υπηρεσίας σε ένα δίκτυο επικοινωνιών ή στην παροχή πρόσβασης στο δίκτυο επικοινωνιών, δεν υφίσταται ευθύνη του φορέα παροχής υπηρεσιών όσον αφορά τις μεταδιδόμενες πληροφορίες, όσον αφορά την αυτόματη, ενδιάμεση και προσωρινή αποθήκευση των πληροφοριών, για τις πληροφορίες που αποθηκεύονται μετά από αίτηση του αποδέκτη της υπηρεσίας.

Τα κράτη μέλη και η Επιτροπή ενθαρρύνουν την κατάρτιση κωδίκων δεοντολογίας σε κοινοτικό επίπεδο, από τις ενώσεις ή οργανώσεις επαγγελματιών και καταναλωτών και την εθελοντική διαβίβαση των σχεδίων των κωδίκων δεοντολογίας, μεριμνούν ώστε τα ένδικα μέσα του εθνικού δικαίου όσον αφορά τις υπηρεσίες της κοινωνίας της πληροφορίας, να επιτρέπουν την ταχεία λήψη μέτρων, συμπεριλαμβανόμενων προσωρινών μέτρων, προκειμένου να παύει οποιαδήποτε παράβαση και να προλαμβάνεται περαιτέρω ζημία.

Όσον αφορά το *spam* η οδηγία αναφέρει *στο **άρθρο 7*** πως μπορεί να αντιμετωπιστεί ή περιοριστεί. Συνοπτικά ορίζει πως η μη ζητηθείσα εμπορική επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου, όπου ο αποστολέας είναι εγχώριος φορέας παροχής υπηρεσιών, θα πρέπει να είναι σαφώς αναγνωρίσιμη και ευθύς όταν φτάσει στον παραλήπτη. Ο νομοθέτης θεωρεί πως αυτό μπορεί να επιτευχθεί με μια ετικέτα “ADV” (advertisement - διαφήμιση) στην αρχή της επικεφαλίδας του μηνύματος.

Αυτοί οι εγχώριοι φορείς παροχής υπηρεσιών θα πρέπει να τηρούν και να συμβουλεύονται τα μητρώα “αποχώρησης”, όπου είναι εγγεγραμμένοι όσοι επιλέγουν να μην λαμβάνουν τέτοιες εμπορικές επικοινωνίες.

Η ***Οδηγία 97/7/ΕΚ*** *του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 20ης Μαΐου 1997* για την προστασία των καταναλωτών κατά τις εξ αποστάσεως συμβάσεις **[40]** έχει ως αντικείμενο την προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών, οι οποίες αφορούν τις εξ αποστάσεως συμβάσεις μεταξύ καταναλωτών και προμηθευτών.

Σύμφωνα με την αναφορά **[40]**, ορίζει τις έννοιες "***Εξ αποστάσεως σύμβαση***", "***Καταναλωτής***", "***Προμηθευτής***", "***Μέσο επικοινωνίας εξ αποστάσεως***", "***Φορέας μέσου επικοινωνίας***".

Οι διατάξεις της οδηγίας δεν εφαρμόζονται στις συμβάσεις που αφορούν χρηματοοικονομικές υπηρεσίες, που συνάπτονται μέσω αυτόματων διανεμητών ή εμπορικών χώρων αυτόματης πώλησης, που συνάπτονται με τους φορείς των τηλεπικοινωνιών λόγω χρησιμοποιήσεως των δημόσιων τηλεφωνικών θαλάμων, που συνάπτονται για την κατασκευή και πώληση ακινήτων ή αφορούν άλλα δικαιώματα επί ακινήτων, εξαιρουμένης της μισθώσεως, και που συνάπτονται κατόπιν πλειστηριασμού. Ο καταναλωτής πρέπει να διαθέτει εγκαίρως πριν από την σύναψη οποιασδήποτε συμβάσεως εξ αποστάσεως κάποιες πληροφορίες όπως την ταυτότητα του προμηθευτή και το αργότερο κατά τη στιγμή της παράδοσης όσον αφορά τα αγαθά πρέπει να λαμβάνει γραπτή ενημέρωση σχετικά με τους όρους και τον τρόπο άσκησης του δικαιώματος αποχώρησης.

Η ***Οδηγία 97/7/ΕΚ*** ήταν το πρώτο ευρωπαϊκό νομικό κείμενο για την προστασία των καταναλωτών από ανεπιθύμητη επικοινωνία. Όσον αφορά το spam η οδηγία αναφέρει στο ***άρθρο 10*** πως μπορεί να αντιμετωπιστεί ή περιοριστεί. Συνοπτικά ορίζει πως απαιτείται η εκ των προτέρων συγκατάθεση του παραλήπτη για την χρήση μέσων αυτόματων συστημάτων κλήσης από τον αποστολέα. Τα μέσα για εξ αποστάσεως επικοινωνία επιτρέπεται να χρησιμοποιηθούν μόνο εάν ο παραλήπτης δεν έχει εκδηλώσει σαφώς την αντίθεση του. Θεωρώ πως με αυτό τον τρόπο θα εξαλειφθούν ή περιοριστούν αρκετά οι ανεπιθύμητες επικοινωνίες.

Η ***Οδηγία 95/46/ΕΚ*** **[41]** του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα κα για την ελεύθερη κυκλοφορία των δεδομένων αυτών παρέχει το πλαίσιο για την νόμιμη και θεμιτή επεξεργασία των δεδομένων προσωπικού χαρακτήρα. Δημιουργεί ένα κανονιστικό πλαίσιο που αποσκοπεί στην επικράτηση ισορροπίας μεταξύ ενός υψηλού επιπέδου προστασίας της ιδιωτικής ζωής των προσώπων και της ελεύθερης κυκλοφορίας δεδομένων προσωπικού χαρακτήρα εντός της Ευρωπαϊκής Ένωσης.

Σύμφωνα με την αναφορά **[41]**, ορίζει τις έννοιες "***Δεδομένα προσωπικού χαρακτήρα***", "***Επεξεργασία δεδομένων προσωπικού χαρακτήρα", "Αρχείο δεδομένων προσωπικού χαρακτήρα", "Υπεύθυνος επεξεργασίας", "Εκτελών την επεξεργασία", "Αποδέκτης", "Συγκατάθεση του προσώπου στο οποίο αναφέρονται τα δεδομένα"***

Η ***Οδηγία 2002/58/ΕΚ***, εφαρμόζεται σε όλα τα θέματα που αφορούν την προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών που δεν καλύπτονται ρητά από τις διατάξεις της οδηγίας της ιδιωτικότητας στις ηλεκτρονικές επικοινωνίες , συμπεριλαμβανομένων των υποχρεώσεων του υπεύθυνου επεξεργασίας και των ατομικών δικαιωμάτων.

Αναφέρει τις αρχές που πρέπει να τηρούνται ως προς την ποιότητα των δεδομένων, τις βασικές αρχές νόμιμης επεξεργασίας δεδομένων, ειδικές κατηγορίες επεξεργασίας, θα πρέπει να υπάρχει ενημέρωση του προσώπου σε περίπτωση συλλογής των δεδομένων του, το πρόσωπο αυτό θα πρέπει να ενημερωθεί για την ταυτότητα του υπεύθυνου επεξεργασίας, τους σκοπούς της επεξεργασίας. Το πρόσωπο στο οποίο αναφέρονται τα δεδομένα θα πρέπει να έχει δικαίωμα να αντιταχθεί άμεσα, κατ' αίτησης του και δωρεάν.

Οι προϋποθέσεις που ορίζονται στην οδηγία για την επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να είναι σεβαστές στο πλαίσιο της διαφήμισης.

Θεωρούμε πως με της οδηγίες αυτές, η Ευρωπαϊκή Ένωση έθεσε κάποιες αρκετά γερές βάσεις ως προς την αντιμετώπιση των spam μηνυμάτων. Αν και θα μπορούσε να ειπωθεί πως τις αδυναμίες και τα κενά μιας οδηγίας καλύπτονται από την άλλη οδηγία, δυστυχώς όμως συνεχίζουν να υπάρχουν κάποια εκμεταλλεύσιμα, από τους spammers, κενά. Κατά την γνώμη μου θα έπρεπε να υπάρχει μια οδηγία όπου θα ανέλυε διεξοδικά όλα τα θέματα που αφορούν τα spam μηνύματα, θα έθετε μέτρα αντιμετώπισης τους και θα συνέβαλε στην προστασία των χρηστών του ηλεκτρονικού ταχυδρομείου.

5. Νομοθεσία χωρών εντός Ευρωπαϊκής Ένωσης για την αντιμετώπιση του Spam

Παραπάνω αναφέρθηκαν οι οδηγίες όπου θα πρέπει να υιοθετηθούν από τις χώρες της Ευρωπαϊκής Ένωσης ή ακόμα και αν χρειαστεί να υποχρεωθούν να εντάξουν κάποιο νομικό πλαίσιο στο δίκαιο τους, όπου θα ρυθμίζεται το πρόβλημα των spam. Παρακάτω θα αναφερθούν οι νομοθεσίες των χωρών αυτών ως προς τα μέτρα που λαμβάνουν για το *spamming*.

5.1 Η νομοθεσία για το Spam στην Ελλάδα

Το φαινόμενο της "ανεπιθύμητης ηλεκτρονικής αλληλογραφίας" (spam) δεν είναι πλέον κάτι νέο στην χώρα μας. Οι spammers δεν γνωρίζουν σύνορα αφού πλήττουν αδιακρίτως ηλεκτρονικές διευθύνσεις σε παγκόσμιο επίπεδο. Εξάλλου, είναι αρκετά δύσκολο από την ηλεκτρονική διεύθυνση να γίνει κατανοητό αν ο αποστολέας ενός ηλεκτρονικού μηνύματος είναι Αγγλόφωνος, Ισπανόφωνος ή μιλάει Ελληνικά (π.χ μια ηλεκτρονική διεύθυνση της μορφής john@yahoo.com). Οπότε τα τελευταία χρόνια, όπου το φαινόμενο spamming έχει λάβει μεγάλες διαστάσεις στο διαδίκτυο, αναπόφευκτα και οι ελληνικές εταιρείες παροχής υπηρεσιών Internet (ISP) αναγκάζονται να εφαρμόσουν πολιτικές για την αντιμετώπιση του και την καταπολέμησή του, αλλά και το κράτος αναγκαστικά δημιούργησε νέους είτε τροποποίησε υπάρχον νόμος ώστε να μπορέσει να οριοθετήσει, να ελέγξει ή / και να αντιμετωπίσει το πρόβλημα του spamming, όπως υποχρεωτικά επέβαλε και η Ευρωπαϊκή Ένωση με τις οδηγίες.

Ο ***Νόμος 2251 του 1994*** **[42]** ρυθμίζει ζητήματα προστασίας των καταναλωτών. Σύμφωνα με την αναφορά ο νομος , ορίζει τις έννοιες *"**Καταναλωτής**", "**Προμηθευτής**", "**Σύμβασης από απόσταση**", "**Σταθερό μέσο**", "**χρηματοοικονομική υπηρεσία**", "**Μέσο επικοινωνίας εξ' αποστάσεως**"*.

Αναφέρει τους γενικούς όρους συναλλαγών και τη δεσμευτικότητά τους σε σχέση με τον καταναλωτή και ορίζει ποιοι όροι είναι καταχρηστικοί. Ορίζει όλα τα απαραίτητα για τις συμβάσεις εκτός εμπορικού καταστήματος, τις συμβάσεις από απόσταση και κάτω από ποιους όρους είναι έγκυρες. Ρυθμίζει τις υποχρεώσεις του πωλητή μετά την πώληση απέναντι στον καταναλωτή όπως είναι οι σαφείς οδηγίες για την ασφαλή χρήση, διατήρηση, συντήρηση και πλήρη αξιοποίηση του προϊόντος καθώς και ενημέρωση για τους κινδύνους κατά τη χρήση και διατήρησή του αλλά και την ευθύνη που έχει ο παραγωγός για τα ελαττωματικά προϊόντα.

Περιλαμβάνει διατάξεις για την διαφήμιση και τις διάφορες εκφάνσεις της και απαγορεύει κάποιες μορφές της όπως την παραπλανητική και την αθέμιτη. Αναφέρεται στις ενώσεις καταναλωτών που έχουν σαν αποκλειστικό σκοπό την προστασία των συμφερόντων του καταναλωτικού κοινού και στα συλλογικά μέσα προστασίας των καταναλωτών.

Ορίζει τη σύσταση επιτροπών φιλικού διακανονισμού σε κάθε νομαρχία για την εξώδικη επίλυση των διαφορών ανάμεσα σε προμηθευτές και σε καταναλωτές ή ενώσεις καταναλωτών αλλά και συστήνει το Εθνικό Συμβούλιο Καταναλωτών που έχει σαν σκοπό να εκφράζει τις θέσεις των καταναλωτών για θέματα προστασίας των καταναλωτών, υποβάλλει προτάσεις για την προώθηση των συμφερόντων τους και τη διασφάλιση των δικαιωμάτων τους και εκδίδει γνωμοδοτήσεις σε καταναλωτικά θέματα. Οι ενώσεις καταναλωτών νομιμοποιούνται επίσης σε άσκηση συλλογικής αγωγής, με την οποία μπορούν εκτός των άλλων να προβάλουν αξίωση χρηματικής ικανοποίησης λόγω ηθικής βλάβης και να ζητήσουν τη λήψη ασφαλιστικών μέτρων (***άρθρο 10§16 στοιχ. α΄, β΄, γ΄ ν. 2251/1994).***

Όσον αφορά το θέμα του spam ο νόμος αναφέρει **στο *άρθρο 9 § 11*** περί των διαφημίσεων, πως μπορεί να αντιμετωπιστεί ή περιοριστεί. Συνοπτικά ορίζει πως για να επιτραπεί η μετάδοση διαφημιστικού τηλεπικοινωνιακών ή άλλων ηλεκτρονικών μηνυμάτων θα πρέπει να έχει προηγουμένως συνεναίσει ρητά και ο παραλήπτης, είτε

εάν ο αποστολέας κάνει χρήση στοιχείων ή πληροφοριών προσωπικού χαρακτήρα του παραλήπτη όπου περιήλθαν στην διάθεση του από προηγούμενη συναλλαγή δηλαδή

«***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***».

τους θα πρέπει ο παραλήπτης να έχει προηγουμένως εγκρίνει τη μεταβίβαση των στοιχείων του για το σκοπό της άμεσης διαφήμισης, ο αποστολέας υποχρεούται να ενημερώσει τον παραλήπτη για τον τρόπο που περιήλθαν τα στοιχεία του αποστολέα στην διάθεση του. Εάν ο παραλήπτης αποφασίσει πως θέλει να διαγραφούν τα στοιχεία του από την βάση δεδομένων του αποστολέα, ο αποστολέας είναι υποχρεωμένος να τα διαγράψει αμέσως.

Στο άρθρο 9 § 12, 13 ο ίδιος νόμος ορίζει ρητά ότι σε κάθε περίπτωση η αποστολή διαφημιστικών ηλεκτρονικών επιστολών θα πρέπει να γίνεται με τρόπο που να μην προσβάλει την ιδιωτική ζωή του χρήστη.

Εκτιμώ πως με αυτό τον τρόπο θα περιοριστούν σε πολύ μεγάλο βαθμό τα αυτόκλητα μηνύματα (spam), έτσι δεν θα λαμβάνονται μηνύματα που δεν θα έχει επιλέξει ή συναινέσει ο παραλήπτης. Όμως δεν καλύπτει πλήρως το θέμα αντιμετώπισης των spam. Δεν αναφέρεται ποια θα είναι η ποινικοποίησης εάν ο αποστολέας δεν ακολουθήσει τον νόμο, δεν αναφέρεται πως θα ξεχωρίσει ο παραλήπτης εάν το μήνυμα αυτό κατατάσσεται στα spam ή όχι δίχως να χρειαστεί να το αποθηκεύσει και να ανατρέξει στο περιεχόμενο του μηνύματος, δηλαδή να είναι εμφανής ο σκοπός του μηνύματος. Δεν αναφέρεται τίποτα για την εγκυρότητα ή όχι και την ταυτοποίηση της ηλεκτρονικής διεύθυνσης του αποστολέα. Όπως ορίζουν οι οδηγίες που προαναφέρθηκαν της Ευρωπαϊκής Ένωσης.

Ο ***Νόμος 2472 του 1997*** **[61]** είναι μια εναρμόνιση με την ***Οδηγία 95/46/ΕΚ*** του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 ρυθμίζει ζητήματα προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, δηλαδή θεσπίζει τις προϋποθέσεις για την επεξεργασία δεδομένων προσωπικού χαρακτήρα με σκοπό την προστασία των δικαιωμάτων, των ελευθεριών και της ιδιωτικής ζωής φυσικών προσώπων. Σύμφωνα με την αναφορά **[61]**,

ορίζει τις έννοιες των *"**Ευαίσθητων δεδομένων**", "**Δεδομένων προσωπικού χαρακτήρα**", "**Επεξεργασία δεδομένων προσωπικού χαρακτήρα**", "**Υποκείμενο των δεδομένων**","**Αρχείο δεδομένων προσωπικού χαρακτήρα**", "**Τρίτος**", "**Συγκατάθεση**", "**Αποδέκτης**","**Διασύνδεση**", "**Υπεύθυνος επεξεργασίας**", "**Εκτελών την επεξεργασία**".*

Αναφέρει τα χαρακτηριστικά νόμιμης επεξεργασίας και συλλογής δεδομένων προσωπικού χαρακτήρα, αναπτύσσει και θεσπίζει την έννοια της Αρχής προστασίας δεδομένων προσωπικού χαρακτήρα όπου υποδεικνύει και τις κυρώσεις που εφαρμόζει στους παραβάτες της νομοθεσίας. Η συλλογή και επεξεργασία των δεδομένων θα πρέπει να γίνεται με τρόπο θεμιτό, νόμιμο, σαφές, να διατίθενται ακριβώς όσες πληροφορίες χρειάζονται για την επεξεργασία και όχι παραπάνω και για όσο χρονικό διάστημα ορίζεται. Για να μπορέσει να υπάρξει επεξεργασία δεδομένων προσωπικού χαρακτήρα θα πρέπει ο ιδιοκτήτης των δεδομένων να έχει πρωτίστως δώσει την συγκατάθεση του. Θα πρέπει να ενημερώνεται και η Αρχή από τον υπεύθυνο επεξεργασίας για την σύσταση και λειτουργία αρχείου ή την έναρξη επεξεργασίας.

Απαγορεύει την συλλογή και επεξεργασία ευαίσθητων δεδομένων, επιτρέπεται μόνον εάν έχει δοθεί άδεια από την Αρχή ή έχει δοθεί άδεια από τον ιδιοκτήτη των ευαίσθητων δεδομένων.

Η Αρχή παρέχει άδεια διαβίβασης δεδομένων προσωπικού χαρακτήρα (σε χώρες που δεν ανήκουν στην Ευρωπαϊκή Ένωση) που έχουν υποστεί ή πρόκειται να υποστούν επεξεργασία μόνο εάν η χώρα αυτή εξασφαλίζει ικανοποιητικό επίπεδο ασφαλείας είτε ο ιδιοκτήτης των δεδομένων έχει δώσει την συγκατάθεση του. Διαφορετικά για χώρες εντός της Ευρωπαϊκής Ένωσης η διαβίβαση είναι ελεύθερη. Καθένας έχει δικαίωμα να γνωρίζει

εάν δεδομένα προσωπικού χαρακτήρα που τον αφορούν αποτελούν ή αποτέλεσαν αντικείμενο επεξεργασίας.

Ο νόμος αυτός σε όλα σχεδόν τα άρθρα και τις παραγράφους του, καλύπτει το θέμα του spam σε μια γενική μορφή. Αναφέρεται περισσότερο στο θέμα της επεξεργασίας των δεδομένων και των υποχρεώσεων των παρόχων υπηρεσιών και όχι στα αυτόκλητα μηνύματα και των τρόπο αντιμετώπισης τους ή κανόνων αυτών.

Θεωρούμε πως με βάση τα προαναφερόμενα το θέμα των *spam* δεν καλύπτεται πλήρως, μια καλή προσέγγιση της αντιμετώπισης αυτού θα ήταν ο συνδυασμός των δύο νόμων ***2472/1997*** *και* ***2251/1994***, αλλά και πάλι θα μπορούσε να ειπωθεί πως υπάρχουν κενά σε αρκετά σημεία.

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.

Ωστόσο, σύμφωνα με ***το άρθρο 13 § 2*** της οδηγίας 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.

Πρόσφατα, η ***Οδηγία 2002/58*** τροποποιήθηκε σε ορισμένα σημεία της από την καινούργια ***Οδηγία 2009/136*****.**

Σύμφωνα με ***το άρθρο 6 § 2 του Π.Δ. 131/2003*** (*το οποίο αποτελεί εναρμόνιση με το άρθρο 7 § 2 της οδηγίας για το ηλεκτρονικό εμπόριο*), με την επιφύλαξη των ***διατάξεων της ΚΥΑ 21496/2000*** 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 συμβουλεύονται τέτοιου είδους τακτικά μητρώα 'επιλογών'. Το Μητρώο υποχρεούται να λειτουργεί σύμφωνα με τις αρχές της μη διάκρισης, της διασφάλισης της διαφάνειας και της αντικειμενικότητας **(*άρθρο 16 § 1***), αλλά και να διατηρεί κατάλληλη υποδομή (εξυπηρέτες ονομάτων, διαδικτυακό τόπο, λογισμικό) για την επαρκή πληροφόρηση και εξυπηρέτηση των καταχωρούμενων φορέων (***άρθρο 12 § 8-11***).

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 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 συμβουλεύονται πριν από κάθε επεξεργασία, ώστε να διαγραφούν τα πρόσωπα των οποίων τα δεδομένα απαγορεύεται να επεξεργαστούν.

Αντίθετα ο ***Νόμος. 3471/06*** *και το* ***Π.Δ. 131/2003*** προβλέπονται ρητά μητρώα '*επιλογών*' που 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.

Όποτε το Spam θεωρείται παραβίαση της ιδιωτικής ζωής.

«Το θεμελιώδες δικαίωμα της ιδιωτικής ζωής, που στηρίζεται στο άρθρο 8 της Ευρωπαϊκής Σύμβασης των Δικαιωμάτων του Ανθρώπου, καθώς και στον Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης [άρθ. 7 (ιδιωτικότητας) και άρθ. 8 (προστασία δεδομένων)] περιλαμβάνει ιδιωτικότητα της πληροφορίας, ιδιωτικότητα της συσχέτισης και της ελευθερίας της επικοινωνίας με την έννοια της ιδιωτικότητας / μυστικότητας των επικοινωνιών».

Η ιδιωτικότητα της πληροφορίας σχετίζεται με το δικαίωμα του ατόμου να αποφασίζει μόνο του, εάν και ποια προσωπικά δεδομένα μπορούν να γνωστοποιούνται σε τρίτους ή / και να επεξεργαστούν από αυτούς. Επηρεάζει επίσης τη λεγόμενη σχεσιακή διάσταση της ιδιωτικότητας, δηλαδή το δικαίωμα να καθορίζει, ποιες επικοινωνίες επιθυμεί κάποιος να λαμβάνει ή όχι .

Ο ***Νόμος 3471 του 2006*** **[62]** ρυθμίζει ζητήματα προστασίας δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών. Από τις διατάξεις του νομού προκύπτει ότι το υποκειμενικό πεδίο εφαρμογής του είναι ευρύτερο από εκείνο του ***ν. 2472/1997***, καθώς περιλαμβάνει και τα νομικά πρόσωπα. Ο εσωτερικός νομοθέτης εξασφάλισε υψηλότερο επίπεδο προστασίας σε σχέση με εκείνο της ***Οδηγίας 2002/58***, η οποία εφαρμόζεται μόνο στα φυσικά πρόσωπα, επιτρέποντας όμως στα κράτη μέλη να υιοθετήσουν διαφορετική ρύθμιση (***άρθρο 13§5 Οδ. 2002/58***). Η καινοτομία του εθνικού νόμου καθίσταται εμφανής ήδη από το ***άρθρο 2 αριθμ. 1***, όπου ως συνδρομητής ορίζεται κάθε φυσικό ή νομικό πρόσωπο. Επιπλέον, στο ***άρθρο 10 § 5*** του νόμου αναγνωρίζεται και στα νομικά πρόσωπα μια περιορισμένη μεν, αλλά υπαρκτή προστασία από την αποκάλυψη περισσότερων στοιχείων πέραν των άκρως απαραίτητων για τον προσδιορισμό και την εξατομίκευσή τους (επωνυμία ή διακριτικός τίτλος, έδρα, νομική μορφή, διεύθυνση). Πρόκειται για το λεγόμενο σύστημα "*no-opt*" **[63]**, η εφαρμογή του οποίου υπαγορεύθηκε από την ανάγκη εξασφάλισης ενός καθεστώτος διαφάνειας στα νομικά πρόσωπα. Επιπλέων ο νόμος αυτός τροποποιεί σε κάποια σημεία τον ***Νόμο 2472/1997***.
Σύμφωνα με την αναφορά **[62]**, ορίζει τις έννοιες του:

"Συνδρομητή", "Χρήστη", "Δεδομένων κίνησης", "Δεδομένων θέσης", "Επικοινωνίας", "Κλήσης", "Ηλεκτρονικού ταχυδρομείου", "Υπηρεσίες ηλεκτρονικών επικοινωνιών", "Υπηρεσίες προστιθέμενης αξίας", "Δημόσιου δικτύου", "Διαθέσιμες στο κοινό υπηρεσίες ηλεκτρονικών επικοινωνιών".

Κατοχυρώνει το απόρρητο των επικοινωνιών που διενεργούνται μέσω δημόσιου δικτύου επικοινωνιών και των διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, καθώς και των συναφών δεδομένων κίνησης των κρατών μελών μέσω της εθνικής νομοθεσίας. Αναφέρει τα χαρακτηριστικά και τους κανόνες νόμιμης επεξεργασίας και συλλογής δεδομένων προσωπικού χαρακτήρα, δεδομένων κίνησης και θέσης.

Ρυθμίζει τα θέματα της αναλυτικής χρέωσης, της ένδειξης της ταυτότητας και του περιορισμού της αναγνώρισης καλούσας και συνδεδεμένης γραμμής, της αυτόματης προώθησης κλήσεων, των τηλεφωνικών καταλόγων συνδρομητών, ασφάλειας, αρμοδιότητες της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών. Αναφέρει επίσης τις ποινικές κυρώσεις που θα δεχθούν όσοι παραβούν τον νόμο.

Όσον αφορά το θέμα του spam ο νόμος αναφέρει στο ***άρθρο 11 § 5,*** περί της μη ζητηθείσας επικοινωνίας, πως μπορεί να αντιμετωπιστεί ή περιοριστεί. Η νομοθετική επιλογή που εκφράζεται το άρθρο αυτό βρίσκει έρεισμα τόσο στον Αστικό Κώδικα όσο

και στο Σύνταγμα. Συνοπτικά ορίζει πως η πραγματοποίηση μη ζητηθείσας επικοινωνίας, αυτόκλητης επικοινωνίας επιτρέπεται μόνο αν ο συνδρομητής έχει εκ των προτέρων δώσει ρητή συγκατάθεση, ο φορέας παροχής υπηρεσιών υποχρεούται να τηρεί και να ενημερώνεται από τους καταλόγους όπου έχουν εγγεγραμμένους τους συνδρομητές που έχουν δηλώσει ότι δεν επιθυμούν να δέχονται τέτοιες επικοινωνίες. Ο αποδέκτης θα πρέπει να έχει την δυνατότητα να αντιτάσσεται εύκολα και δωρεάν στη συλλογή και χρησιμοποίηση των ηλεκτρονικών του στοιχείων. Θα πρέπει να αναφέρεται ευδιάκριτα και σαφώς η ταυτότητα του αποστολέα καθώς και η έγκυρη διεύθυνση στην οποία ο αποδέκτης θα μπορεί να ζητήσει τον τερματισμό της επικοινωνίας.

Δεν αναφέρεται πως θα ξεχωρίσει ο παραλήπτης εάν το μήνυμα αυτό κατατάσσεται στα spam ή όχι δίχως να χρειαστεί να το αποθηκεύσει και να ανατρέξει στο περιεχόμενο του μηνύματος, δηλαδή να είναι εμφανής ο σκοπός του μηνύματος, όπως αναφέρουν οι οδηγίες της Ευρωπαϊκής Ένωσης. Θεωρώ πως το θέμα των spam καλύπτεται καλύτερα σ' αυτόν τον νόμο αλλά όχι πλήρως.

Συμπερασματικά δεν υπάρχει στην χώρα μας κάποιος συγκεκριμένος νόμος πλήρης και αναλυτικός ως προς την αντιμετώπιση των spam μηνυμάτων. Θα μπορούσε να υπάρξει ένα καλό επίπεδο αντιμετώπισης ή περιορισμού τους με τον συνδυασμό των τριών νόμων που προαναφέρθηκαν. Θα μπορούσε να ειπωθεί πως ο κάθε νόμος από αυτούς τους τρεις καλύπτει τα κενά των άλλων δύο νόμων για το θέμα αυτό.

Παρακάτω θα αναφερθούν συνοπτικά οι νομοθεσίες αντιμετώπισης του spam των υπόλοιπων χωρών της Ευρωπαϊκής Ένωσης.

5.2 Η νομοθεσία για το Spam στο Ηνωμένο Βασίλειο

Σύμφωνα με την αναφορά **[64]**, η κυβέρνηση του Ηνωμένου Βασιλείου έθεσε σε εφαρμογή την *οδηγία 2002/58/ΕΚ της Ευρωπαϊκής Ένωσης, το Δεκέμβριο του 2003*. *Η νομοθεσία έχει προσελκύσει αρκετά κριτικά σχόλια για την υπερβολική αδυναμία της, για παράδειγμα, καθιστώντας νομικά την αποστολή αυτόκλητων μηνυμάτων ηλεκτρονικού ταχυδρομείου σε επιχειρήσεις που βασίζονται στο σύστημα αποχώρησης (opt-out).*

Για την αντιμετώπιση του spamming στο Ηνωμένο Βασίλειο υπάρχουν δύο νόμοι που είναι χρήσιμοι:

1. Ο νόμος περί προστασίας των δεδομένων του 1998, **[65]** και
2. Ο Κανονισμός της προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες του 2003 **[66]**

Οι οποίοι και αναφέρουν ρητά πως :

1. *Δεν επιτρέπεται να γίνεται επεξεργασία ή αποθήκευση των στοιχείων των χρηστών του ηλεκτρονικού ταχυδρομείου χωρίς να έχει προηγηθεί η συγκατάθεση τους.*

2. *Δεν επιτρέπεται να λαμβάνουν οι παραλήπτες εμπορικά μηνύματα ηλεκτρονικού ταχυδρομείου χωρίς τη ρητή συναίνεση τους εκτός αν υπάρχει μια προηγούμενη σχέση συναλλαγής με την εταιρεία και δεν έχουν αποσύρει την συναίνεση τους.*

Αυτοί οι νόμοι εφαρμόζονται σε ολόκληρο το Ηνωμένο Βασίλειο και έχουν χρησιμοποιηθεί για την καταπολέμηση των αυτόκλητων ηλεκτρονικών μηνυμάτων στο πλαίσιο της Αγγλικής έννομης τάξης και της Σκωτίας.

5.3 Η νομοθεσία για το Spam στην Ιταλία

Η κυβέρνηση της Ιταλίας τροποποίησε ή / και συμμόρφωσε το νομικό της δίκαιο βάση των οδηγιών της Ευρωπαϊκής Ένωσης, ως προς την αντιμετώπιση των spam. Σύμφωνα

με την αναφορά **[67]**, "στην Ιταλία υπάρχουν 3 διαφορετικές νομοθεσίες που "*προστατεύουν*" τους χρήστες του Internet από το spam:

1. Το ***DL 675/1996*** *σχετικά με την προστασία της ιδιωτικής ζωής*: *αναφέρει, κυρίως, ότι μια εταιρεία πρέπει να έχει άδεια από κάθε χρήστη του οποίου τα προσωπικά δεδομένα (όπως η ηλεκτρονική διεύθυνση) θέλει να χρησιμοποιήσει.*

*2. Το **DL 171/1998** (που απορρέει από την ευρωπαϊκή κοινοτική **οδηγία 97/66/ΕΚ**) για την προστασία του απορρήτου των τηλεπικοινωνιών: απαγορεύει όλα τα αυτόματα συστήματα κλήσης ενός χρήστη και λέει ότι όλα τα έξοδα διαφήμισης θα πρέπει να καταβάλονται από την εταιρεία και όχι από τον χρήστη.*

*3. Το **DL 185/1999** (που απορρέει από την ευρωπαϊκή κοινοτική **οδηγία 97/7/ΕΚ**) για την προστασία των πελατών σχετικά με τις συμβάσεις μεγάλων αποστάσεων: αν μια εταιρεία θέλει να πουλήσει κάτι για παράδειγμα μέσω του διαδικτύου ή του τηλεφώνου, για να διαφημίσει τα προϊόντα της θα πρέπει να έχει την άδεια του χρήστη.*

Ενεργώντας με αυτές τις 3 νομοθεσίες, είναι δυνατόν να υπάρξουν κυρώσεις επιστροφής από 500 ευρώ έως και 5000 ευρώ, η εταιρεία θα πρέπει να διερευνηθεί για την πολιτική προστασίας της ιδιωτικής ζωής και ο υπεύθυνος επεξεργασίας των προσωπικών δεδομένων μπορεί επίσης να φυλακιστεί. Όλα αυτά, για κάθε spam μήνυμα ηλεκτρονικού ταχυδρομείου. Ο χρήστης αρκεί να στείλει ένα υπογεγραμμένο μήνυμα στην εταιρεία ζητώντας εξηγήσεις σχετικά με τα spam και αν έχουν άδεια για την αποστολή των διαφημιστικών.

Ο νόμος υποχρεώνει την επιχείρηση να απαντήσει εντός 5 εργάσιμων ημερών. Μετά από αυτό, αν η εξήγηση της εταιρείας δεν είναι αρκετή, ο χρήστης μπορεί να στείλει ένα άλλο ηλεκτρονικό μήνυμα στην Ιταλική Αρχή Προσωπικών Δεδομένων, όπου θα διερευνήσει από μόνη της. Συνήθως η Αρχή Προσωπικών Δεδομένων καθιστά στην εταιρεία πρόστιμο περίπου 500 ευρώ όπου πρέπει να τα καταβάλει στον χρήστη.

5.4 Η νομοθεσία για το Spam στην Ομοσπονδιακή Δημοκρατία της Γερμανίας

Ιστορικά, η πρώτη απόφαση που αναφέρθηκε στο δικαίωμα αυτό ήταν η απόφαση της 15 Δεκεμβρίου 1983 του Ομοσπονδιακού Συνταγματικού Δικαστηρίου της Γερμανίας. Αυτή κήρυσσε ορισμένες διατάξεις του νόμου για την απογραφή του πληθυσμού ως αντισυνταγματικές, επειδή απαιτούσαν την παροχή περισσότερων πληροφοριών από ό,τι δικαιολογεί ο σκοπός της απογραφής. Επίσης εκφράσθηκε δυσπιστία ως προς τον τρόπο διαχείρισης των πληροφοριών αυτών από το κράτος εξαιτίας της χρήσης νέων τεχνολογιών **[68]**.

Σύμφωνα με την αναφορά **[34]**, στη Γερμανία, η ευθύνη για το ζήτημα των αυτόκλητων ηλεκτρονικών μηνυμάτων που περιέχουν ιούς ή σκουλήκια είναι ακόμη υπό συζήτηση. Ωστόσο, το γερμανικό δίκαιο του αθέμιτου ανταγωνισμού (*Gesetz gegen den unlauteren Wettbewerb - UWG*) συνιστά ότι ο αποδέκτη πρέπει να εγκρίνει την αποστολή των διαφημίσεων στην ταχυδρομική θυρίδα του. Ωστόσο, μόνο ένας ανταγωνιστής ο οποίος ασχολείται με την ίδια δραστηριότητα με του αποστολέα επιτρέπεται να καταθέσει ασφαλιστικά μέτρα για τον αποστολέα, όχι ο ίδιος ο αποδέκτης του spam.

Μεμονωμένα άτομα έχουν τη δυνατότητα να καταθέσουν αγωγή κατά ενός spammer στη βάση του κοινού γερμανικού ανθρώπινου δικαίου, σε συνδυασμό με την **§ *823*** *και* ***1004*** *του αστικού κώδικα.*

Η γερμανική κυβέρνηση συζήτησε το 2005 έναν ρητό αντι-spam νόμο, παρόλα αυτά δεν πέρασε τη φάση των συζητήσεων. Ένας νέος νόμος (*Telemediengesetz)* είχε προβλεφθεί να περάσει ως νομοσχέδιο, το 2007, το οποίο θα απαγόρευε στα μηνύματα ηλεκτρονικού ταχυδρομείου την εξαπάτηση σχετικά με τον πραγματικό αποστολέα της αλληλογραφίας ή του εμπορικού ενδιαφέροντος εντός του μηνύματος."

5.5 Η νομοθεσία για το Spam στην Ισπανία

Σύμφωνα με την αναφορά **[35],** οι νόμοι που ρυθμίζουν την αποστολή ηλεκτρονικών επικοινωνιών μάρκετινγκ στην Ισπανία είναι ο ***Νόμος 34/2002 και ο Νόμος 32/2003***.

Το ***άρθρο 21.1*** *του νόμου περί υπηρεσιών της κοινωνίας της πληροφορίας ρητά απαγορεύει την αποστολή διαφημιστικών ή την προώθηση των επικοινωνιών μέσω ηλεκτρονικού ταχυδρομείου ή άλλων αντίστοιχων μέσων των ηλεκτρονικών επικοινωνιών για το οποίο δεν έχει προηγουμένως ζητηθεί ή επιτραπεί ρητώς από τους αποδέκτες.*

Η ***οδηγία 2002/58/ΕΚ*** μεταφέρθηκε στον ***Νόμο 32/2003*** όπου τροποποίησε διάφορα άρθρα του ***Νόμου 34/2002***, εισάγοντας την αρχή της "επιλογής" (**opt-in**), *δηλαδή την εκ των προτέρων συγκατάθεση του παραλήπτη για την αποστολή μηνύματος με εμπορικό περιεχόμενο, στο ηλεκτρονικό του ταχυδρομείο.*

Και οι δύο νόμοι χορηγούν αρμοδιότητες στην ισπανική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Ο ***Νόμος 32/2003*** αναθέτει στην Αρχή το καθήκον της διαφύλαξης των δικαιωμάτων και των εγγυήσεων των συνδρομητών και των χρηστών στον τομέα των ηλεκτρονικών επικοινωνιών, η ανάθεση αυτή επιβάλει κυρώσεις για παράβαση στον τομέα της παροχής υπηρεσιών ηλεκτρονικών επικοινωνιών. Από την άλλη πλευρά, ο ***Νόμος 34/2002*** ορίζει ότι συμπίπτει με την Αρχή για την επιβολή κυρώσεων σε περίπτωση παράβασης, λόγω της αποστολής αυτόκλητων διαφημιστικών ανακοινώσεων με ηλεκτρονικό ταχυδρομείο ή ισοδύναμα ηλεκτρονικά μέσα επικοινωνίας.

Το spam μπορεί να σημαίνει και παραβίαση του δικαιώματος στην οικειότητα και την παραβίαση της νομοθεσίας για την προστασία των δεδομένων, δεδομένου ότι πρέπει να ληφθεί υπόψη το γεγονός ότι η διεύθυνση ηλεκτρονικού ταχυδρομείου μπορεί να θεωρηθεί ως δεδομένο προσωπικού χαρακτήρα.

5.6 Η νομοθεσία για το Spam στην Δημοκρατία της Τσεχίας

Σύμφωνα με την αναφορά **[35]**, "ο ***Νόμος 480/2004*** *για ορισμένες υπηρεσίες σε ενημερωτική κοινωνία ρυθμίζει την αποστολή ηλεκτρονικών μηνυμάτων μάρκετινγκ, spam και επιτρέπει να στέλνονται μηνύματα ηλεκτρονικού ταχυδρομείου μόνο μετά την εμπορική συμφωνία των αποδεκτών (ονομαζόμενη αρχή της "επιλογής" (opt-in)).* Η αυτόκλητη εμπορία ηλεκτρονικών επικοινωνιών απαγορεύεται και οι αποστολείς τιμωρούνται με ποινή μέχρι και 10 εκατομμύρια CZK. Η Υπηρεσία Προστασίας Δεδομένων Προσωπικού Χαρακτήρα εκδίδει τα πρόστιμα.

Υπάρχει μια ενημέρωση από τις 20/4/2006, όπου κάνει διάκριση μεταξύ των σημερινών και των δυνητικών **[69]** πελατών. Σύμφωνα με την ενημέρωση οι εταιρείες έχουν τη δυνατότητα να στείλουν μηνύματα ηλεκτρονικού ταχυδρομείου για εμπορικούς σκοπούς, χωρίς τις εκ των προτέρων συμφωνίες των καταναλωτών, αλλά αυτοί οι πελάτες μπορούν να αρνηθούν να λάβουν τα εμπορικά μηνύματα ηλεκτρονικού ταχυδρομείου ανά πάσα στιγμή. Η αποστολή εμπορικών μηνυμάτων ηλεκτρονικού ταχυδρομείου σε δυνητικούς πελάτες, χωρίς προηγούμενη συμφωνία θεωρείται αυτόκλητη εμπορία ηλεκτρονικών επικοινωνιών ή απλώς spam".

6. Νομοθεσία χωρών εκτός Ευρωπαϊκής Ένωσης για την αντιμετώπιση του Spam

Η διεθνής διάσταση του φαινόμενου spam είναι καθοριστικής σημασίας, δεδομένου ότι μεγάλο μέρος των spam φαίνεται ότι προέρχεται από χώρες εκτός Ευρωπαϊκής Ένωσης. Παρακάτω θα αναφερθούν περιληπτικά σε ποιες χώρες εφαρμόζεται νομοθεσία πρόληψης ή / και αντιμετώπισης των spam μηνυμάτων και συνοπτικά ποια μέτρα εφαρμόζονται για τον λόγο αυτό.

6.1 ΗΠΑ (Ηνωμένες Πολιτείες Αμερικής)

Η ΗΠΑ έχουν γίνει πλέον "υπερδύναμη" στην αποστολή ανεπιθύμητων διαφημιστικών μηνυμάτων. Όπως αναμετάδωσε το Γαλλικό Πρακτορείο Ειδήσεων **[70]**, το διάστημα Οκτώβριος- Δεκέμβριος 2007 οι ΗΠΑ παρέμεναν η υπερδύναμη του spam παράγοντας το 21% των μηνυμάτων με εμπορικό περιεχόμενο. Η σημερινή κατάταξη είναι: ΗΠΑ (21%), Ρωσία (8,3%), Κίνα (4,2%), Βραζιλία (4,0%), Νότιος Κορέα (3,9%), Τουρκία (3,8%), Ιταλία (3,5%), Πολωνία (3,4%), Γερμανία (3,2%), Ισπανία (3,1%), Μεξικό (3,1%) και Βρετανία (2,5%). Σε επίπεδο ηπείρων, πρώτη με διαφορά είναι η Ασία (32%), δεύτερη η Ευρώπη (27%) και τρίτη η Βόρειος Αμερική (26,55%).

Στις *16 Δεκεμβρίου 2003* ο τότε πρόεδρος των ΗΠΑ **[71]**, George W. Bush, υπέγραψε τον *νόμο CAN-SPAM Act*. Ο νόμος αυτός ήταν η πρώτη προσπάθεια των ΗΠΑ για μια εθνική ρύθμιση ως προς την αποστολή των εμπορικών ηλεκτρονικών μηνυμάτων. Η Ομοσπονδιακή Επιτροπή Εμπορίου (*Federal Trade Commission – FTC*) είναι αρμόδια για την ρύθμιση και την επιβολή του νόμου.

Σύμφωνα με την αναφορά **[72]**, ***ο νόμος αυτός καθορίζει τις απαιτήσεις που θα πρέπει να πληρούν οι αποστολείς εμπορικών ηλεκτρονικών μηνυμάτων, αναφέρει κυρώσεις ως προς τους spammers αλλά και για τις επιχειρήσεις που διαφημίζουν τα προϊόντα τους μέσω των spam μηνυμάτων και δίνει το δικαίωμα στον παραλήπτη να ζητήσει από τον αποστολέα να σταματήσει να του στέλνει spam μηνύματα.***

Απαγορεύει τις ψευδείς ή παραπλανητικές κεφαλίδες στα μηνύματα. Οι πληροφορίες δρομολόγησης, διεύθυνση αποστολέα και παραλήπτη και το domain name πρέπει να είναι ακριβή και να είναι εύκολο να εντοπιστεί ο αποστολέας του ηλεκτρονικού μηνύματος.

Ο τίτλος του μηνύματος πρέπει να είναι σαφής και αληθής, δίχως να παραπλανά τον παραλήπτη σχετικά με το περιεχόμενο ή το θέμα του μηνύματος. Προϋποθέτει πως το ηλεκτρονικό μήνυμα πρέπει να διαθέτει μέθοδο αποχώρησης (*opt-out*). Θα πρέπει να υπάρχει μια ηλεκτρονική διεύθυνση όπου ο παραλήπτης μπορεί να ζητήσει να μην του στέλνονται ηλεκτρονικά μηνύματα από τον συγκεκριμένο αποστολέα, και θα πρέπει να γίνει σεβαστή η απαίτηση του, ή μπορεί να δημιουργηθεί ένας κατάλογος όπου ο παραλήπτης να μπορεί να επιλέξει ποιες μορφές μηνυμάτων δεν δέχεται να παραλαμβάνει. Το μήνυμα θα πρέπει να έχει μια σαφή και εμφανή προειδοποίηση ότι είναι μήνυμα διαφήμισης.

Εκτιμώ πως ο νόμος διαθέτει αρκετά κενά ως την αντιμετώπιση των spam, πρώτων δεν απαιτεί την εκ των προτέρων άδεια του παραλήπτη αν δέχεται να του στείλουν διαφημιστικά μηνύματα ή όχι. Απαγορεύει σε μεμονωμένες πολιτείες να εφαρμόσουν μια ισχυρότερη και αποτελεσματικότερη αντι-spam νομοθεσία. Επιπλέον οι παραλήπτες που λαμβάνουν spam μηνύματα δεν έχουν το δικαίωμα να ασκήσουν αγωγή κατά του αποστολέα. Επίσης δεν λαμβάνονται μέτρα για τα spam μηνύματα που στέλνονται από χώρες εκτός των ΗΠΑ αλλά παραλαμβάνονται στις ΗΠΑ.

Παρακάτω αναφέρονται πολύ συνοπτικά τα νομοθετικά μέτρα (που προέρχονται / βασίζονται στον νόμο CAN-SPAM Act) όπου έλαβαν μερικές Πολιτείες των ΗΠΑ για την αντιμετώπιση του φαινόμενου των spam μηνυμάτων.

Alaska

Η Αλάσκα θέσπισε τον ***νόμο Alaska Stat. 45.50.479*** "περιορισμός σχετικά με το ηλεκτρονικό ταχυδρομείο" **[73]** όπου απαιτεί ρητά την ετικέτα "ADV:ADLT" στην αρχή κάθε αυτόκλητου σεξουαλικού εμπορικού μηνύματος ηλεκτρονικού ταχυδρομείου, εάν ο αποστολέας γνωρίζει ότι ο παραλήπτης είναι κάτοικος της Αλάσκας.

Arizona

Στην Αριζόνα θεσπίστηκε ***ο νόμος Ariz.Rev.Stat.Ann. 44-1372***, **[74]** όπου απαιτούσε τα αυτόκλητα εμπορικά μηνύματα ηλεκτρονικού ταχυδρομείου να περιέχουν στην αρχή του θέματος τους την ετικέτα “ADV:” και να περιέχουν έναν μηχανισμό αποχώρησης (opt-out) από το μήνυμα. Αυτά τα μηνύματα πρέπει να έχουν έγκυρη διεύθυνση αποστολέα.

Ο νόμος απαγορεύει τους ψευδής ή παραπλανητικούς τίτλους τον εμπορικών μηνυμάτων ηλεκτρονικού ταχυδρομείου, όπως επίσης απαγορεύει την χρήση της ηλεκτρονικής διεύθυνσης τρίτου ή το domain name χωρίς την συγκατάθεση του έτσι ώστε να φαίνεται ότι κάποιος τρίτος έστειλε το μήνυμα.

Ο νόμος ισχύει αν το μήνυμα έχει σταλεί από το εσωτερικό της Αριζόνα, ή εάν ο δικαιούχος του φορέα παροχής υπηρεσιών βρίσκεται ή διαθέτει εξοπλισμό στην Αριζόνα, ή αν ο αποστολέας γνωρίζει ή έχει λόγο να γνωρίζει ότι ο δικαιούχος είναι κάτοικος Αριζόνας.

California

Εγκρίθηκε η ***νομοθεσία Cal.Business & Professions Code 17529-17529.9***, **[75]** στην Καλιφόρνια όπου έκανε την δεύτερη πολιτεία (μετά το Delaware) να υιοθετήσει ένα κανόνα “επιλογής” (opt-in) για τις διαφημίσεις ηλεκτρονικού ταχυδρομείου. Στο πλαίσιο αυτής της νομοθεσίας, είναι παράνομη η αποστολή αυτόκλητων ηλεκτρονικών μηνυμάτων εμπορικού χαρακτήρα από την Καλιφόρνια ή σε ηλεκτρονική διεύθυνση της Καλιφόρνιας.

Ο νόμος ισχύει για τους αποστολείς όσο και για τους διαφημιστές για λογαριασμό των οποίων τα μηνύματα αποστέλλονται.

Colorado

Ο νόμος των διαφημιστικών μαζικής αποστολής του Κολοράντο **[76]** ***Colo.Rev.Stat. 6-1-702-5,*** απαγορεύει την αποστολή των αυτόκλητων ηλεκτρονικών μηνυμάτων εμπορικού χαρακτήρα που χρησιμοποιούν την ηλεκτρονική διεύθυνση τρίτου ή το domain name, χωρίς άδεια, ή να περιλαμβάνει ψευδείς ή ελλιπείς πληροφορίες σχετικά με την διεύθυνση του αποστολέα. Τα αυτόκλητα εμπορικά μηνύματα ηλεκτρονικού ταχυδρομείου πρέπει να περιέχουν μια ετικέτα "ADV:" στην αρχή του τίτλου τους, όπως και οδηγίες “αποχώρησης” (opt-out).

Ο νόμος ισχύει για μηνύματα ηλεκτρονικού ταχυδρομείου που αποστέλλονται σε κατοίκους του Κολοράντο μέσω ενός παρόχου υπηρεσιών που βρίσκεται στο Κολοράντο ή του εξοπλισμού του.

Connecticut

Η νομοθεσία Conn.Gen.Stat. 53-451 του Κονέκτικατ **[77]**, καθιστά παράνομη την αποστολή των μαζικών αυτόκλητων μηνυμάτων ηλεκτρονικού ταχυδρομείου που περιέχουν παραποιημένες πληροφορίες σχετικά με την διεύθυνση του αποστολέα παραβιάζοντας τις πολιτικές των παρόχων, ή για τη διανομή λογισμικού με στόχο να παραποιηθούν πληροφορίες σχετικά με την διεύθυνση του αποστολέα. Ένας ξένος υπήκοος που χρησιμοποιεί ηλεκτρονικό υπολογιστή ή δίκτυο υπολογιστών που βρίσκονται στο Κονέκτικατ εμπίπτει στην δικαιοδοσία των δικαστηρίων.

Ο νόμος 52-570c, **[78]** προβλέπει ότι τα ανεπιθύμητα εμπορικά μηνύματα ηλεκτρονικού ταχυδρομείου πρέπει να περιέχουν μια ετικέτα "ADV" στην αρχή του τίτλου τους, και πρέπει να περιλαμβάνουν τον αποστολέα του μηνύματος ηλεκτρονικού ταχυδρομείου όπως και οδηγίες “αποχώρησης”.

Delaware

Βάσει της νομοθεσίας Del. Code. Tit 11§937-941, **[79]** είναι παράνομη η αποστολή αυτόκλητων μαζικών εμπορικών μηνυμάτων ηλεκτρονικού ταχυδρομείου, ειδικά εάν περιέχουν και παραπλανητικές πληροφορίες δρομολόγησης, ή διανείμουν λογισμικό που έχει σχεδιαστεί για να παραποιηθούν οι πληροφορίες δρομολόγησης. Ο νόμος εφαρμόζεται σε μηνύματα που προέρχονται έξω από την πολιτεία, εάν ο δικαιούχος βρίσκεται στο Delaware και ο αποστολέας έχει επίγνωση του γεγονότος ότι ο αποδέκτης βρίσκεται στο Delaware.

Florida

Ο ***νόμος Fla.Stat. §668.60***, **[80]** απαγορεύει τα ανεπιθύμητα εμπορικά μηνύματα ηλεκτρονικού ταχυδρομείου που χρησιμοποιούν το domain name ενός τρίτου, χωρίς άδεια, ή περιλαμβάνει ψευδείς ή ελλιπείς πληροφορίες σχετικά με την δρομολόγηση. Η απαγόρευση ισχύει και για τα μηνύματα που αποστέλλονται από έναν υπολογιστή στη Φλόριντα, καθώς και για τα μηνύματα που αποστέλλονται στο ηλεκτρονικό ταχυδρομείο κατοίκου της Φλόριντα.

Ο νόμος απαγορεύει επίσης τη διανομή λογισμικού με στόχο την παραποίηση πληροφοριών δρομολόγησης.

Indiana

Η ***νομοθεσία Ind.Code § 24-5-22***, **[81]** της Ιντιάνα απαγορεύει τα εμπορικά μηνύματα ηλεκτρονικού ταχυδρομείου, όπου χρησιμοποιείται το domain name τρίτου, χωρίς άδεια, περιλαμβάνει ψευδή ή παραπλανητικά θέματα, ή παραποιεί το σημείο προέλευσης ή άλλες πληροφορίες σχετικά με τη δρομολόγηση. Τα αυτόκλητα εμπορικά μηνύματα ηλεκτρονικού ταχυδρομείου πρέπει να περιέχουν μια ετικέτα "ADV:" ή "ADV: ADLT" στην αρχή του τίτλου του μηνύματος, μαζί με τις οδηγίες “αποχώρησης”.

Ο νόμος ισχύει και για τα μηνύματα που αποστέλλονται από το εξωτερικό αν ο αποστολέας γνωρίζει ότι ο παραλήπτης είναι κάτοικος της Ιντιάνα.

Louisiana

Ο ποινικός νόμος ***La.Rev.Stat.Ann § 51:2001***, ***51-2002***, **[82]** καθιστά παράνομη την αποστολή μαζικών αυτόκλητων εμπορικών μηνυμάτων ηλεκτρονικού ταχυδρομείου, αν τα μηνύματα ηλεκτρονικού ταχυδρομείου περιέχουν παραποιημένες πληροφορίες σχετικά με την δρομολόγηση ή ο αποστολέας χρησιμοποιεί τις δυνατότητες του παρόχου για τη μετάδοση των μηνυμάτων παραβιάζοντας τις πολιτικές του παρόχου. Ο νόμος απαγορεύει επίσης τη διανομή λογισμικού που έχει ως στόχο την παραποίηση πληροφοριών δρομολόγησης.

Τα μηνύματα πρέπει να φέρουν την ετικέτα "ADV:" στην αρχή του τίτλου τους, και να περιλαμβάνουν μια έγκυρη διεύθυνση απάντησης καθώς και οδηγίες “αποχώρησης”. Ο αποστολέας πρέπει επίσης να διατηρεί σε λειτουργία μια ιστοσελίδα για αιτήσεις “αποχώρησης”.

Τα εμπορικά μηνύματα ηλεκτρονικού ταχυδρομείου με σεξουαλικό περιεχόμενο πρέπει να περιέχουν τους χαρακτήρες "ADV-ADULT" στην αρχή του τίτλου τους. Τα ανεπιθύμητα εμπορικά μηνύματα ηλεκτρονικού ταχυδρομείου με άσεμνο περιεχόμενο πρέπει να περιλαμβάνουν την ετικέτα "ADV: ADLT" στην αρχή του τίτλου τους.

6.2 Καναδάς

Ο Καναδάς ήταν η μόνη χώρα στους G8 που δεν είχε αντι-spam νόμους, μέχρι πρόσφατα, και όλο και περισσότεροι spammers επωφελούνταν από αυτό. Για την

καταπολέμηση των αυτόκλητων ηλεκτρονικών μηνυμάτων, ο Καναδάς ακολούθησε μια πολύπλευρη στρατηγική που περιλάμβανε όλους τους εμπλεκόμενους παράγοντες.

Σύμφωνα με την αναφορά **[83]**, η κυβέρνηση του Καναδά τον Μάιο του 2004 δραστηριοποιήθηκε με ένα αντι-Spam σχέδιο(Bill C-27). Προσδιόρισε τα κύρια εργαλεία που είναι απαραίτητα για να αντιμετωπιστεί το spam:

- *αυστηρή εφαρμογή των υφιστάμενων νόμων που απαγορεύουν τις spamming δραστηριότητες,*
- *καθώς και της νέας νομοθεσίας, όπως απαιτείται για να καλυφθούν τυχόν κενά στην υπάρχουσα νομοθεσία*
- *ισχυρότερη επιβολή κυρώσεων και μηχανισμών για την πιο αποτελεσματική αποτροπή των spammers*
- *δημόσια εκπαίδευση και ευαισθητοποίηση*
- *διεθνής συνεργασία για την αντιμετώπιση του φαινόμενου*

Η προστασία δεδομένων προσωπικού χαρακτήρα του Καναδά και ηλεκτρονικών εγγράφων (PIPEDA) καλύπτει λεπτομερώς την προστασία της ιδιωτικής ζωής και περιλαμβάνει πολλές διατάξεις σχετικά με το μάρκετινγκ μέσω ηλεκτρονικού ταχυδρομείου, όμως ποτέ δεν είχαν έναν νόμο που καθιστά παράνομη την αποστολή spam στον Καναδά. Επιπλέον, ειδική ομάδα της κυβέρνησης συνέστησε ειδική αντι-spam νομοθεσία σε μια έκθεση του 2005 και τον Μάιο του 2008 ένα αντι-spam δίκαιο άρχισε να προχωράει μέσω του καναδικού κοινοβουλίου.

Πρόσφατα θέσπισε τον ***νόμο*** (***Bill C-28***) **[84]**, η καταπολέμηση της Internet και ασύρματο Spam Act (FISA), είναι anti-spam νομοθεσία του Καναδά, που επικυρώθηκε από την ανωτάτη στις 15 Δεκεμβρίου 2010. Το νομοσχέδιο αντικατέστησε τον ***Bill C-27***, το Ηλεκτρονικό Εμπόριο Νόμου περί Προστασίας (ECPA), το οποίο ψηφίστηκε από τη Βουλή των Κοινοτήτων, αλλά πέθανε εξαιτίας της παράτασης της δεύτερης συνόδου της 40ης Καναδικό Κοινοβούλιο στις 30 Δεκεμβρίου 2009. Ο νόμος δεν ισχύει σήμερα?. Οι κανονισμοί που σχετίζονται με αυτό πρέπει να ολοκληρωθεί και θα δημοσιευθεί στην Εφημερίδα της Κυβερνήσεως του Καναδά, το οποίο αναμένεται να παρουσιαστεί στα μέσα του 2012, μετά την οποία ο νόμος θα είναι σε ισχύ,

Σε αυτό πατάσσει το spam μέσω της απαγόρευσης αποστολής εμπορικών μηνυμάτων ηλεκτρονικού ταχυδρομείου σε Καναδούς, χωρίς την συναίνεση τους. Το νομοσχέδιο απαγορεύει μεθόδους, όπως την συγκέντρωση μηνυμάτων ηλεκτρονικού ταχυδρομείου, την απαγόρευση *phishing* επιθέσεων, και απαιτεί από όλα τα εμπορικά μηνύματα ηλεκτρονικού ταχυδρομείου να έχουν έναν σαφή τίτλο θέματος, ακριβή στοιχεία επικοινωνίας, και έναν εύκολο τρόπο "αποχώρησης". Επίσης, δίνει στους παρόχους υπηρεσιών Διαδικτύου (ISP) την δυνατότητα μπλοκαρίσματος, φιλτραρίσματος και άρνησης spam μηνυμάτων - ακόμη και άρνηση υπηρεσίας σε εκείνους που έχουν καταδικαστεί βάσει του νέου νόμου ή νομίζουν ότι τα μηνύματα που θέλουν να αποστείλουν απαγορεύονται βάσει του νέου νόμου . Οι επιχειρήσεις που προωθούν μηνύματα μέσω spam θα είναι επίσης υπεύθυνες εάν δεν αναλάβουν δράση για να σταματήσουν τα μηνύματα ή να ενημερώσουν τις αρχές.

Εξαιρέσεις είναι τα φιλανθρωπικά ιδρύματα, τα πολιτικά κόμματα, εκλογικά γραφεία και επιχειρήσεις που έχουν μια προ υπάρχουσα σχέση με κάποιο μήνυμα ηλεκτρονικού ταχυδρομείου του χρήστη. Εξακολουθεί να υπάρχει η απαίτηση για τις ομάδες αυτές να επιτρέπουν στους χρήστες να επιλέγουν αν θέλουν να "αποχωρήσουν" ή να μην λάβουν περαιτέρω μηνύματα.

Οι κυρώσεις κυμαίνονται σε χρηματικά ποσά από $ 500.000 (ή και δύο χρόνια φυλάκισης) έως $ 1,5 εκατ. (ή πέντε χρόνια φυλάκισης) για επαναλαμβανόμενες παραβάσεις. Επιπλέον πρόστιμα ίσα με τα κέρδη από μια spamming λειτουργία μπορούν να επιβάλλονται.

Αυτοί που ζημιώθηκαν από τα spam έχουν το δικαίωμα να ζητήσουν αποζημίωση από τους δράστες, μέσω της δικαιοσύνης.

6.3 Αυστραλία

Το ***Spam Act 2003*** **[85]** ψηφίστηκε το 2003, ως ομοσπονδιακή νομοθεσία από το Κοινοβούλιο της Κοινοπολιτείας της Αυστραλίας. Τα πρώτα τμήματα της πράξης τέθηκαν σε ισχύ στις 12 Δεκεμβρίου 2003, την ημέρα που η πράξη επικυρώθηκε από την ανωτάτη (Βασίλισσα), με όλα τα υπόλοιπα τμήματα της πράξης τεθεί σε ισχύ στις 10 Απριλίου 2004.

Σκοπός του είναι να δημιουργήσει ένα σύστημα για τη ρύθμιση των εμπορικών e-mail και άλλα είδη των εμπορικών ηλεκτρονικών μηνυμάτων. Περιορίζει το spam, ειδικά e-mail-spam και ορισμένα είδη των spam-τηλέφωνο, καθώς και e-mail διεύθυνση συγκομιδής, ωστόσο υπάρχουν ευρείες εξαιρέσεις.

Ο νομός επιβλήθηκε από την Αυστραλιανή Αρχή Επικοινωνιών και Μέσων (ACMA).

6.4 Νέα Ζηλανδία

Το νομοσχέδιο για τα ανεπιθύμητα ηλεκτρονικά μηνύματα εκπροσωπεί την κυβερνητική προσπάθεια να φέρει την Νέα Ζηλανδία σε συμφωνία με άλλες χώρες όπως την Αυστραλία, το Ηνωμένο Βασίλειο και τις Ηνωμένες Πολιτείες στην καταπολέμηση του αυξανόμενου κόστους του spam.

Το νομοσχέδιο **[86]** αποσκοπεί επίσης στην ανταπόκριση της δέσμευσης που ανέλαβε η κυβέρνηση, στην προσφάτως δημοσιευθείσα Ψηφιακή Στρατηγική, για την εισαγωγή νόμων που θα συμβάλλουν στη διατήρηση των νόμιμων επιχειρηματικών και προωθητικών ενεργειών, ενώ, θα ενθαρρύνουν την υπεύθυνη χρήση των ηλεκτρονικών μηνυμάτων.

Σκοπός του νομοσχεδίου είναι να προωθήσει την υπεύθυνη χρήση των ηλεκτρονικών μηνυμάτων:

- *απαγορεύει την αποστολή εμπορικών ηλεκτρονικών μηνυμάτων όπου έχουν σύνδεση με την Νέα Ζηλανδία, εκτός εάν στο μήνυμα που αποστέλλεται έχει δοθεί προηγουμένως γραπτή συγκατάθεση από τον παραλήπτη για τη λήψη του*
- *απαγορεύει τα διαφημιστικά ηλεκτρονικά μηνύματα που έχουν σύνδεση με τη Νέα Ζηλανδία, όταν ο παραλήπτης έχει δηλώσει ότι δεν επιθυμεί να λαμβάνει αυτά τα μηνύματα πια*
- *απαιτεί όλα τα ηλεκτρονικά μηνύματα που έχουν σύνδεση με τη Νέα Ζηλανδία να εξακριβώνουν την ταυτότητα του προσώπου που εξουσιοδοτείται για την αποστολή του μηνύματος και τον τρόπο με τον οποίο αυτό το άτομο μπορεί να έρθει σε επαφή, και να περιλαμβάνουν ένα λειτουργικό "αποχώρησης" ενσωματωμένο στο ηλεκτρονικό μήνυμα*
- *απαγορεύει τη χρήση λογισμικού για την συγκομιδή ηλεκτρονικών διευθύνσεων και την χρήση των καταλόγων με τις ηλεκτρονικές διευθύνσεις.*

7. Σύγκριση νομοθετικών πλαισίων για την αντιμετώπιση των Spam

Παραπάνω αναφέρθηκαν τα νομικά πλαίσια των χωρών εντός και εκτός της Ευρωπαϊκής Ένωσης ως προς την αντιμετώπιση του φαινόμενου των spam. Για μια καλύτερη προσέγγιση και κατανόηση αυτών, σ ’αυτό το κεφάλαιο θα συγκριθούν αυτά τα νομοθετικά πλαίσια. Στην πρώτη ενότητα θα κατηγοριοποιηθούν συνοπτικά τα νομοθετικά μέτρα αντιμετώπισης του spam των πολιτειών των ΗΠΑ και στην δεύτερη

ενότητα θα υπάρξει μια συγκριτική ανάλυση μεταξύ του κοινοτικού δικαίου και του δικαίου χωρών εκτός Ευρωπαϊκής Ένωσης.

7.1 Επισκόπηση των μέτρων αντιμετώπισης του spam βάση των νομοθεσιών των Πολιτειών των ΗΠΑ

Εκτιμουμε ότι για την αντιμετώπιση του spamming, τα κριτήρια που είναι κοινά στο σύνολο του νομικού πλαισίου των πολιτειών των ΗΠΑ είναι η ποινικοποίηση και οι ανάγκες.

Ποινικοποίηση ή Ανάγκες		Πολιτείες
Ποινικοποίηση	Η μαζική αποστολή ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου που περιέχουν ψευδείς, πλαστογραφημένες ή ελλιπείς πληροφορίες σχετικά με την δρομολόγηση ή συγκαλύπτουν το σημείο προέλευσης ή πληροφορίες σχετικά με την δρομολόγηση	Arizona, Arkansas, Colorado, Connecticut, Delaware, Illinois, Indiana, Iowa, Kansas, Louisiana, Maine, Maryland, Michigan, Minnesota, Nevada, North Carolina, North Dakota, Ohio, Oklahoma, Pennsylvania, Rhode Island, South Dakota, Tennessee, Texas, Utah, Virginia, Washington, West Virginia, and Wyoming
	Η πώληση, διανομή και κατοχή με σκοπό να πουληθεί το λογισμικό που έχει σχεδιαστεί για να παραποιηθούν πληροφορίες δρομολόγησης	Arkansas, Connecticut, Delaware, Illinois, Kansas, Louisiana, Michigan, Nevada, Oklahoma, Pennsylvania, Rhode Island, Tennessee, Virginia, and West Virginia
	Αυτόκλητα ηλεκτρονικά μηνύματα εμπορικού χαρακτήρα με τη χρήση διεύθυνσης Internet τρίτου ή το domain name χωρίς άδεια	Arizona, Arkansas, Colorado, Idaho, Illinois, Indiana, Iowa, Kansas, Maine, Maryland, Minnesota, North Dakota, Oklahoma, Pennsylvania, Rhode Island, Texas, Washington, West Virginia, and Wyoming
Ανάγκες	Απαιτείται τα ανεπιθύμητα εμπορικά μηνύματα ηλεκτρονικού ταχυδρομείου να περιλαμβάνουν το όνομα του αποστολέα και τη διεύθυνση ηλεκτρονικού ταχυδρομείου του, μαζί με οδηγίες αποχώρησης	Arkansas, Colorado, Indiana, Iowa, Kansas, Maine, Minnesota, Missouri, Nevada, new Mexico, Ohio, Oklahoma, Rhode Island, Tennessee, and Utah
	Απαιτείται η ετικέτα “ADV:ADLT” ή “ADV” στην αρχή κάθε αυτόκλητου σεξουαλικού ή μη εμπορικού μηνύματος ηλεκτρονικού ταχυδρομείου.	Alaska, Arizona, Colorado, Connecticut, Indiana, Louisiana

Πίνακα 5: Ποινικοποίηση ή Ανάγκες

Στον πάραπανω πίνακα 5 αναφέρονται τα κριτήρια αυτά, μια συνοπτική διάκριση τους και ποιες πολιτείες των ΗΠΑ διαθέτουν στο νομοθετικό τους πλαίσιο αυτές τις

διακρίσεις των κριτηρίων. Συμπερασματικά διαπιστώνεται πως αρκετές αν όχι όλες οι πολιτείες των ΗΠΑ διαθέτουν το ίδιο νομοθετικό πλαίσιο ως προς την αντιμετώπιση των spam

7.2 Διάκριση μεταξύ κοινοτικού δικαίου και δικαίου χωρών εκτός Ευρωπαϊκής Ένωσης και ΗΠΑ

Ο σκοπός αυτής της ενότητας είναι η γενική επισκόπηση των βασικών απαιτήσεων των μηνυμάτων ηλεκτρονικού ταχυδρομείου στις Ηνωμένες Πολιτείες και την Ευρώπη. Εκτιμώ ότι τα κριτήρια της σύγκρισης των βασικών απαιτήσεων των μηνυμάτων ηλεκτρονικού ταχυδρομείου, όπως προκύπτουν από την *νομοθεσία CAN-SPAM Act*.“***Έλεγχος για επίθεση μη επιδιωκόμενης Πορνογραφίας και Μάρκετινγκ***” των ΗΠΑ και των οδηγιών της Ευρωπαϊκής Ένωσης ως προς την αντιμετώπιση του φαινόμενου spam, είναι: ο τύπος των ηλεκτρονικών μηνυμάτων, απαίτηση / άδεια “*επιλογής*” (***opt-in***), διαγραφή / απαίτηση “*αποχώρησης*” (***opt-out***), η ταυτότητα του αποστολέα, ο τίτλος / αναγνώριση του μηνύματος, επικοινωνία / διεύθυνση του αποστολέα. Παρακάτω συγκρίνω την νομοθεσία των ΗΠΑ και τις οδηγίες της Ευρώπης βάση αυτών των κριτηρίων.

Το νομικό δίκαιο των ΗΠΑ καλύπτει τα εμπορικά μηνύματα ηλεκτρονικού ταχυδρομείου, όπου σκοπός τους είναι η διαφήμιση και εμπορική προώθηση ενός προϊόντος ή υπηρεσίας. Αντιθέτως το κοινοτικό δίκαιο καλύπτει όλα τα άμεσα εμπορικά ηλεκτρονικά μηνύματα αλλά και τα φιλανθρωπικά και πολιτικά μηνύματα που στέλνονται μέσω του ηλεκτρονικού ταχυδρομείου. Διαπιστώνεται πως το κοινοτικό δίκαιο καλύπτει ένα ευρύτερο φάσμα τύπων μηνυμάτων ηλεκτρονικού ταχυδρομείου.

Όσον αφορά την απαίτηση / άδεια “επιλογής” (*opt-in*), η νομοθεσία των ΗΠΑ επιτρέπει την άμεση προώθηση των εμπορικών ηλεκτρονικών μηνυμάτων, δίχως να απαιτείται η εκ των προτέρων άδεια του παραλήπτη και αυτό μπορεί να γίνεται έως ότου ο παραλήπτης ζητήσει ρητά την παύση τους / “αποχώρηση” του (*opt-out*). Αντιθέτως βάση του κοινοτικού δικαίου τα μηνύματα μάρκετινγκ ηλεκτρονικού ταχυδρομείου αποστέλλονται μόνο στους παραλήπτες που έχουν δώσει εκ των προτέρων την άδεια τους (*opt-in*). Η εκ των προτέρων άδεια απαιτείται για την επικοινωνία των επιχειρήσεων προς τους καταναλωτές (*B2C – Business to Customer*) καλύπτοντας όλα τα “φυσικά πρόσωπα”. Εξαιρέσεις του κοινοτικού δικαίου αποτελούν η επιχειρηματική σχέση που έχει ήδη αναπτυχθεί μεταξύ της επιχείρησης και του καταναλωτή. Η επιχείρηση μπορεί να χρησιμοποιήσει τα στοιχεία του καταναλωτή από την προηγούμενη συναλλαγή τους εφόσον ρητά ο καταναλωτής δεν είχε αντιταχθεί από την αρχή σ’αυτό και μέχρι εκείνη την στιγμή δεν έχει ζητήσει την παύση τους / “αποχώρηση” του. Επίσης για επικοινωνία επιχείρησης με επιχείρηση *(B2B – Business to Business)*, ως «νομικά πρόσωπα» τα κράτη μέλη της Ευρωπαϊκής Ένωσης είναι ελεύθερα να κάνουν το *opt-out* ελάχιστη νομοθεσία. Εάν βέβαια σ’αυτό συμφωνεί και η εθνική νομοθεσία των κρατών μελών και δεν απαιτεί opt-in για την B2B επικοινωνία μέσω ηλεκτρονικών μηνυμάτων.

Βάση της νομοθεσίας των ΗΠΑ, κάθε μήνυμα πρέπει να περιέχει οδηγίες διαγραφής / απαίτησης “*opt-out*”. Ο αποστολέας πρέπει να σέβεται, να αποδέχεται και να πραγματοποιεί τις opt-out αιτήσεις των δικαιούχων εντός 10 ημερών. Ο παραλήπτης του ηλεκτρονικού μηνύματος δεν υποχρεούται να καταβάλει ένα χρηματικό ποσό για να καταβάλει τις opt-out απαιτήσεις του ή οποιαδήποτε άλλη πληροφορία του ζητηθεί, εκτός βέβαια αν αποστείλει μήνυμα απάντησης ή επισκεφθεί κάποια Ιστοσελίδα για να δηλώσει τις *opt-out* απαιτήσεις του για την λήψη μελλοντικών μηνυμάτων ηλεκτρονικού ταχυδρομείου από κάποιον αποστολέα. Το ίδιο συμβαίνει και με το κοινοτικό δίκαιο, κάθε μήνυμα πρέπει να περιέχει οδηγίες *opt-out*. Ο παραλήπτης θα πρέπει να έχει την δυνατότητα να στείλει ένα μήνυμα απάντησης στον αποστολέα εάν επιθυμεί να διακόψει την επικοινωνία. Για να συμβεί αυτό απαιτείται να υπάρχει έγκυρη διεύθυνση του αποστολέα. Βεβαίως αυτή η περίπτωση ισχύει εάν ο παραλήπτης δεν είχε εκ προτέρων σαφώς και ευδιάκριτα αντιταχθεί, στην συλλογή και χρήση των ηλεκτρονικών στοιχείων του.

Όσον αφοράν την ταυτότητα του αποστολέα, η νομοθεσία των ΗΠΑ απαγορεύει ψευδείς ή παραπλανητικές κεφαλίδες μηνυμάτων, δημιουργία πολλαπλών διευθύνσεων ηλεκτρονικού ταχυδρομείου για αποστολή, διευθυνσιοδότηση και συγκομιδή επιθέσεων καθώς και άλλα δόλια μέσα για την αποστολή spam. Τα στοιχεία του αποστολέα, του παραλήπτη, οι πληροφορίες δρομολόγησης του ηλεκτρονικού μηνύματος, το domain name θα πρέπει να είναι ακριβή και να μπορεί να εντοπιστεί ο αποστολέας του μηνύματος. Το κοινοτικό δίκαιο απαγορεύει την απόκρυψη ή συγκάλυψη της ταυτότητας του αποστολέα.

Η νομοθεσία των ΗΠΑ απαγορεύει τους ψευδείς ή παραπλανητικούς τίτλους των ηλεκτρονικών μηνυμάτων ως προς το θέμα / περιεχόμενο τους. Απαιτείται η αναγνώριση του μηνύματος για το αν το μήνυμα είναι διαφήμιση ή όχι. Στο κοινοτικό δίκαιο δεν υπάρχει κάποια αναφορά ως προς την αναγνώριση των διαφημιστικών μηνυμάτων ή όχι.

Όσον αφορά την επικοινωνία / διεύθυνση του αποστολέα, η νομοθεσία των ΗΠΑ απαιτεί μια έγκυρη φυσική ταχυδρομική διεύθυνση, για την ικανοποίηση της απαίτησης του νόμου ότι ένα ηλεκτρονικό μήνυμα απεικονίζει μια “φυσική έγκυρη ταχυδρομική διεύθυνση”. Το κοινοτικό δίκαιο αναφέρει πως οι απαιτήσεις ως προς τις πληροφορίες που ισχύουν για τα μηνύματα ηλεκτρονικού ταχυδρομείου των επιχειρήσεων ισχύουν και για την φυσική αλληλογραφία των επιχειρήσεων. Οι εταιρείες που λειτουργούν ή είναι καταχωρημένες στην Ευρωπαϊκή Ένωση πρέπει να δηλώνουν τα εταιρικά τους στοιχεία σε κάθε ηλεκτρονική επιχειρηματική επικοινωνία που αποστέλλεται από την οργάνωση τους. Τα ηλεκτρονικά μηνύματα που αποστέλλονται από μια εταιρεία θα πρέπει να περιλαμβάνουν την πλήρη επωνυμία της επιχείρησης και τη νομική της μορφή, τον τόπο εγγραφής της εταιρείας, τον αριθμό καταχώρησης, την διεύθυνση της έδρας, τον αριθμό ΑΦΜ. Πάντα υπάρχει η προϋπόθεση να υφίσταται μια έγκυρη διεύθυνση επιστροφής.

Το συμπέρασμα αυτής της ενότητας είναι πως η νομοθεσία των ΗΠΑ και του κοινοτικού δικαίου ως προς την αντιμετώπιση του φαινόμενου spam έχουν πολλές ομοιότητες αλλά και αρκετές διαφορές. Η βασική διαφορά τους υπάγεται στον τρόπο αποτροπής των spammer να στείλουν *spam* μηνύματα. Στις ΗΠΑ επιτρέπεται να στείλουν μηνύματα μάρκετινγκ και έπειτα να αντιταχθούν στην αποστολή αυτή δηλαδή λειτουργεί βάση του *opt-out*. Ενώ στα κράτη μέλη της Ευρωπαϊκής Ένωσης επιτρέπεται να σταλθούν μηνύματα μάρκετινγκ μόνο σε όσους έχουν εκ των προτέρων δώσει την συγκατάθεση τους δηλαδή λειτουργεί βάση του *opt-in*.

Παρόλα αυτά στο πλαίσιο των Οδηγιών από την ΕΕ, η έκταση της ευθύνης των φορέων παροχής (ISPs) κινείται σε ασαφή όρια, η δε ασάφεια αυτή δεν είναι προϊόν αβλεψίας του κοινοτικού νομοθέτη, αλλά ενσυνείδητη επιλογή του η θέσπιση ενός νομοθετικού πλαισίου ευνοϊκού προς τους φορείς παροχής της Ευρωπαϊκής Ένωσης συμβάλλει στην ανάπτυξη και την πρόοδο του ηλεκτρονικού εμπορίου, ενισχύοντας παράλληλα την ανταγωνιστικότητα των ISPs της Ευρώπης έναντι των ισχυρών ISPs των ΗΠΑ **[87]**.

Το κοινοτικό δίκαιο και το νομικό δίκαιο των ΗΠΑ είτε έχουν ομοιότητες είτε έχουν διαφορές το μόνο σίγουρο είναι ότι έχουν περιορίσει αρκετά το φαινόμενο του spam. Βέβαια από την παραπάνω συγκριτική ανάλυση διαπιστώνεται πως το κοινοτικό δίκαιο πληρεί καλύτερες προϋποθέσεις για την αντιμετώπιση των spam απ’ ότι το δίκαιο των ΗΠΑ και αυτό φαίνεται και στα στατιστικά που παρατέθηκαν στο (κεφάλαιο 6 στην υποενότητα 6.1)

Δεν παύουν όμως και τα δύο να έχουν αρκετά νομοθετικά κενά και να μπορούν πάντα οι spammers να βρίσκουν παραθυράκια ώστε να ξεφεύγουν των νομικών ευθυνών τους.

8. Τρόποι προστασία από τα Spam μηνύματα

Μια κατηγορία που επηρεάζεται εξίσου αρνητικά από το spamming είναι εκείνη των διαχειριστών δικτύων καθώς και των φορέων παροχής υπηρεσιών διαδικτύου (Internet Service Providers, ISPs). Οι επενδύσεις τους σε εξειδικευμένο τεχνικό εξοπλισμό

(hardware) και λογισμικό κατά του spam (software), καθώς και σε ανθρώπινο δυναμικό ικανό να το χειριστεί αυξάνουν το κόστος διαχείρισης και λειτουργίας των δικτύων. Ανά τακτά μάλιστα διαστήματα προκύπτει η ανάγκη αναβάθμισης του εκάστοτε προστατευτικού λογισμικού, καθώς οι spammers κατορθώνουν να υπερπηδούν τα εμπόδια που τους θέτει η τεχνολογία. Οι ISPs παράλληλα υφίστανται σημαντική μείωση του κύρους, της επαγγελματικής τους φήμης, συχνά δε και της πελατείας τους, καθώς η αδυναμία τους να καταπολεμήσουν το φαινόμενο του spamming ολοκληρωτικά τους καθιστά αναξιόπιστους απέναντι στους δυσαρεστημένους συνδρομητές τους.

Υπάρχουν όμως πολύ και διάφοροι τρόποι όπου μπορούν να εφαρμοστούν προληπτικά ή / και ακόμα να περιορίσουν τα spam μηνύματα που λαμβάνονται. Αναφέρθηκαν παραπάνω διάφορα μέτρα από νομικής πλευράς, στο κεφάλαιο αυτό θα αναφερθούν μέτρα από εμπειρικής πλευράς, για την αντιμετώπιση του φαινόμενου spam.

8.1 Εφαρμογές αντι-phishing τακτικών

Στο δεύτερο κεφάλαιο αναφέρθηκε το phishing ως μορφή spam μηνύματος, παρακάτω θα αναφερθούν τρόποι αποτροπής αυτού. Λαμβάνοντας υπόψη το γεγονός ότι το spam παραμένει ένα μεγάλο πρόβλημα, το να τεθούν σε πλήρη παύση τα εν λόγω δόλια μηνύματα φαίνεται σχεδόν αδύνατο. Σύμφωνα με τις αναφορές **[31]**, πολλές εταιρείες που έχουν την τάση να δίνουν μεγαλύτερη έμφαση στην εκπαίδευση των καταναλωτών σχετικά με το πώς να τηρούν τα προειδοποιητικά σημάδια και να τα εντοπίζουν πριν από το έγκλημα, φαίνεται να αποδίδει καρπούς.

Λόγω της εκτεταμένης εκμετάλλευσης, ορισμένες εταιρείες έχουν δημιουργήσει πολιτικές όπου εξαλείφουν εντελώς την επικοινωνία μέσω ηλεκτρονικών μηνυμάτων, και στηρίζονται στο παραδοσιακό ταχυδρομείο για να επικοινωνούν με τους πελάτες. Άλλες εταιρείες απλώς ενθαρρύνουν τους πελάτες να μην αποκαλύπτουν ευαίσθητες πληροφορίες σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου, όπως αριθμούς τραπεζικών λογαριασμών και κωδικούς πρόσβασης.

Θα πρέπει να ληφθεί υπόψη ότι επιφανειακά, τα περισσότερα από αυτά τα μηνύματα είναι καλά σχεδιασμένα και φαίνεται σαν να στέλνονται από νόμιμες επιχειρήσεις. Φέρουν περιγραφές όπου φαίνονται αυθεντικές όπως λογότυπα έτσι ώστε να πείθουν. Οι φορείς του “phishing”, δημιουργούν ιστοσελίδες που φαίνονται εξίσου καλές, αν όχι και καλύτερες από αυτές που μιμούνται.

Ένας τρόπος περιορισμού του προβλήματος είναι να αναφέρεται το phishing στην εταιρεία από την οποία υποτίθεται ότι στάλθηκε για να αποδείξει την αυθεντικότητα του, και την νομιμότητα της ηλεκτρονικής της διεύθυνσης.

8.2 Εμπειρικοί τρόποι προστασίας από το Spam

Κάποια μηνύματα spam αποστέλλονται από επαγγελματίες spammer, ενώ άλλα μπορεί να στέλνονται από νόμιμες επιχειρήσεις που δεν έχουν όμως συμμορφωθεί με την Ελληνική νομοθεσία για το spam.

Παρακάτω αναφέρονται μερικές δραστικές και αποτελεσματικές ενέργειες, σύμφωνα με τις αναφορές **[88]**, που μπορεί να κάνει κάποιος παραλήπτης από μόνος του εάν λάβει μηνύματα spam στο ηλεκτρονικό του ταχυδρομείο. Με αυτές τις ενέργειες μπορεί να προστατευτεί από τα προβλήματα που πιθανός θα προκαλούσαν τα spam και γιατί όχι και να τα περιορίσει.

10 τρόποι να αποφύγετε το spam:

1. Χρησιμοποιήστε το λιγότερο 2 ηλεκτρονικές διευθύνσεις (e-mail). Την μία θα πρέπει να την χρησιμοποιείτε αποκλειστικά και μόνο για την προσωπική σας αλληλογραφία, ενώ την δεύτερη (κοινόχρηστη) θα μπορείτε να την χρησιμοποιείτε σε δημόσια προσβάσιμες εφαρμογές, όπως για παράδειγμα καταχώρηση στοιχείων

σε ομάδες συζητήσεων (forums), χώρους συζητήσεων (chat rooms), εγγραφές σε λίστες αλληλογραφίας κτλ

2. Μην δημοσιεύετε ποτέ το προσωπικό σας e-mail σε δημόσια προσβάσιμες εφαρμογές.
3. Χρησιμοποιείστε ως προσωπική σας διεύθυνση ένα συνδυασμό από το όνομα και το επίθετο σας αντί για απλά ονόματα που περιέχονται σε λεξικά π.χ. bill, mary. Οι αποστολείς spam χρησιμοποιούν συνδυασμούς ονομάτων, λέξεων και αριθμών για να δημιουργήσουν πιθανές διευθύνσεις.
4. Αν πρέπει οπωσδήποτε να κοινοποιήσετε το προσωπικό σας e-mail ηλεκτρονικά, καμουφλάρετε το, ώστε να δυσκολέψετε το έργο των spammers. Για παράδειγμα το Joe.Smith@yahoo.com, είναι εύκολο να βρεθεί από τις ειδικές μηχανές αναζήτησης (robots), όπως εύκολο είναι και το Joe.Smith at yahoo.com. Δοκιμάστε να το γράψετε Joe-dot-Smith-at-yahoo-dot-com. Επίσης αν πρέπει απαραίτητα να δημοσιεύσετε το προσωπικό σας e-mail σε κάποια ιστοσελίδα (το οποίο δεν συστήνεται), κάντε το ως αρχείο γραφικών ή εικόνα και όχι link.
5. Αντιμετωπίστε το «κοινόχρηστο» e-mail σας, ως προσωρινό. Οι πιθανότητες οι spammers να το βρουν είναι μεγάλες, συνεπώς μην διστάζετε να το αλλάζετε συχνά.
6. Να χρησιμοποιείτε πάντα το «κοινόχρηστο» e-mail για την καταχώρηση στοιχείων σε ομάδες συζητήσεων, χώρους συζητήσεων, για εγγραφή σε λίστες αλληλογραφίας. Επίσης θα μπορούσατε να χρησιμοποιείτε πολλές διαφορετικές «δημόσιες» (κοινόχρηστες) διευθύνσεις, ώστε να εντοπίσετε ποιες υπηρεσίες/ οργανισμοί, πωλούν διευθύνσεις σε spammers.
7. Μην απαντάτε ποτέ σε μηνύματα spam. Οι περισσότεροι spammers επαληθεύουν με τον τρόπο αυτό την λήψη της αλληλογραφίας και άρα την ύπαρξη της συγκεκριμένης διεύθυνσης e-mail. Όσο περισσότερο απαντάτε, τόσο περισσότερη ανεπιθύμητη αλληλογραφία θα λαμβάνετε.
8. Μην επισκέπτεστε συνδέσμους με σκοπό την διαγραφή σας από μία λίστα στην οποία δεν θέλετε να ανήκετε, από ύποπτες/ αμφισβητήσιμες πηγές. Οι spammers στέλνουν τέτοια παραπλανητική αλληλογραφία, σε μία προσπάθεια να συλλέξουν ενεργές διευθύνσεις. Αν η διεύθυνση σας χαρακτηριστεί ως «ενεργή», θα αυξηθεί ο αριθμός των ανεπιθύμητων e-mail που λαμβάνετε.
9. Αν αντιληφθείτε πως το e-mail σας είναι γνωστό σε spammers, αλλάξτε το. Μπορεί να είναι άβολο/δύσκολο, αλλά είναι ένας τρόπος για να αποφύγετε το spam- έστω και για λίγο διάστημα.
10. Σιγουρευτείτε ότι το e-mail σας, φιλτράρεται από κατάλληλο λογισμικό anti-spam. Μπορείτε επίσης να εγκαταστήσετε στον υπολογιστή σας, κάποιο λογισμικό προστασίας από spam.

8.3 Φόρμα καταγγελίας κατά των spammers στο Εξωτερικό / Εσωτερικό

Εξωτερικό

Δραστικότερο μέτρο εναντίον των spammer που στέλνουν αυτόκλητα διαφημιστικά μηνύματα από το εξωτερικό, είναι η καταγγελία. Μπορεί να γίνει καταγγελία του spammer απευθείας στον πάροχο υπηρεσιών που χρησιμοποιεί, π.χ. στο Yahoo, στο Hotmail κ.ά. Εφόσον οι spammers ανοίγουν δωρεάν λογαριασμούς webmail και στέλνουν αυτόκλητα διαφημιστικά μηνύματα μέσω αυτών.

Σχεδόν όλοι οι σοβαροί πάροχοι υπηρεσιών του εξωτερικού απαγορεύουν το spamming **[89]**, αν πληροφορηθούν ότι κάποιος χρησιμοποιεί τους λογαριασμούς τους γι' αυτό το σκοπό, τον διαγράφουν αμέσως. Οι πάροχοι υπηρεσιών διαθέτουν κάποια ηλεκτρονική διεύθυνση για να δέχονται αυτού του είδους τις καταγγελίες, συνήθως το

πρώτο συνθετικό της είναι η λέξη abuse. Για παράδειγμα, αν τα μηνύματα spam που φθάνουν στην ηλεκτρονική διεύθυνση του παραλήπτη προέρχονται από κάποιο λογαριασμό του yahoo, μπορεί να σταλθεί το μήνυμα μαζί με τις κεφαλίδες του στη διεύθυνση: abuse@yahoo.com Αν προέρχονται από λογαριασμό Hotmail, η διεύθυνση στην οποία θα γίνει η καταγγελία είναι abuse@hotmail.com.
Η απάντηση του Yahoo σε καταγγελία που έγινε ήταν :

"Hello. Thank you for writing to Yahoo! Mail. In this particular case, we have taken appropriate action against the Yahoo! account in question, as per our Terms of Service (TOS). For further details about the Yahoo! TOS, you can visit: http://docs.yahoo.com/info/terms/"

Δηλαδή, ο λογαριασμός του spammer έπαψε να υφίσταται.

Αν ακολουθηθούν οι οδηγίες που προαναφέρθηκαν, οι ποσότητες των spam μηνυμάτων που λαμβάνονται θα περιοριστούν σε πολύ μεγάλο βαθμό ή ακόμα και θα εξαλειφθούν. Επειδή το spamming παραμένει ιδιαίτερα αποδοτικό για τους δημιουργούς του, θα εξακολουθήσει να αποτελεί πρόβλημα καθώς νέες τεχνικές θα επινοούνται και οι spammer θα προσπαθούν να "επικοινωνήσουν" με τους καταναλωτές. Πάντα όμως θα ανακαλύπτονται τρόποι για να αντιμετωπιστούν.

Εσωτερικό

Σε περίπτωση που λαμβάνεται κάποιας μορφής μηνύματος μην ζητηθείσας επικοινωνίας (Spamming) από κάποιο spammer μπορείτε να στραφείτε εναντίων του σε πρώτη φάση προειδοποιώντας τον με νομικά μέσα και επιχειρήματα και σε δεύτερη φάση σε περίπτωση μην συμμόρφωσης από την πλευρά του πραγματοποιώντας την προειδοποίηση.

Σύμφωνα με την Ελληνική νομοθεσία, σε κάποιες περιπτώσεις επιτρέπεται η αποστολή μηνυμάτων μέχρι την εναντίωση του παραλήπτη ("**opt-out**"). Ακόμα και σε αυτές τις περιπτώσεις, είναι προτιμότερο η δήλωση εναντίωσης να μη γίνεται ηλεκτρονικά, αλλά π.χ. με τηλεφωνική επικοινωνία ή με γραπτή επιστολή. Για το λόγο αυτό μην απαντάτε ηλεκτρονικά στον αποστολέα και μην ακολουθείτε συνδέσμους (links) που ενδεχομένως αναφέρονται στο μήνυμα, ακόμα και αν πρόκειται για συνδέσμους διαγραφής της διεύθυνσης σας από την λίστα του αποστολέα (unsubscribe links).

Με τις εθνικές εκλογές του 2009 εν όψει, έχει παρατηρηθεί ένα κύμα από spam emails από υποψήφιους βουλευτές. Για αυτό, και για κάθε μελλοντική ανάγκη, παραθέτω εκ νέου μια πρότυπη απάντηση σε spam emails. Η αντιγραφή του παροτρύνεται εντόνως.

- Από μας προς των spammer

Σας ενημερώνω πως με το συννημένο e-mail το οποίο μου αποστείλατε παραβιάζετε τον ***νόμο 3471/2006*** και συγκεκριμένα το ***άρθρο 11 περί μη ζητηθείσας επικοινωνίας***. Για τη δική σας ευκολία σας παραθέτω το άρθρο ακολούθως **[1]*** αλλά μπορείτε να βρείτε και το ΦΕΚ με ολόκληρο τον νόμο στην ηλεκτρονική τοποθεσία της **Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα**. Να σας ενημερώσω ότι έχει προγραμματισθεί κατάθεση μήνυσης εναντίον σας για τις ανωτέρω παραβάσεις των νόμων του Ελληνικού κράτους στην **Δίωξη Ηλεκτρονικού Εγκλήματος** Τόσο η συλλογή των δεδομένων όσο και η χρήση αυτών για σκοπούς άμεσης προώθησης πωλήσεων προϊόντων/υπηρεσιών θα πρέπει να πραγματοποιείται βάσει των διατάξεων της κείμενης νομοθεσίας και λοιπών ειδικότερων διοικητικών αποφάσεων Αρχών. Συγκεκριμένα, η δημιουργία, επεξεργασία ή/και διαβίβαση βάσεως δεδομένων για διαφημιστικούς σκοπούς ή/και σκοπούς προώθησης προϊόντων και υπηρεσιών υπόκειται στις διατάξεις του ***Ν. 2472/1997*** για την προστασία των προσωπικών δεδομένων σε συνδυασμό με τις ειδικότερες προϋποθέσεις νόμιμης συλλογής δεδομένων για σκοπούς απευθείας διαφήμισης και απευθείας προώθησης πωλήσεων προϊόντων ή υπηρεσιών, όπως προσδιορίζονται ειδικότερα στην υπ' ***αριθ. 50/20-1-2000 Απόφαση της ΑΠΔ***.

Περαιτέρω, η χρήση των κατά τα ανωτέρω συλλεχθέντων δεδομένων για σκοπούς απευθείας διαφήμισης και απευθείας προώθησης πωλήσεων προϊόντων ή υπηρεσιών, υπόκειται μεταξύ άλλων στις διατάξεις:

- ***άρθρο 9 παρ. 10, 11 & 12 του Ν. 2251/94***
- ***άρθρο 6 Π.Δ. 131/2003***
- ***άρθρο 11 του Ν. 3471/2006 [μη ζητηθείσα επικοινωνία]***

Όπως προκύπτει από τα όσα αναφέρετε, οι ενέργειές σας συνιστούν μερική εφαρμογή της κείμενης νομοθεσίας περί της μη ζητηθείσας επικοινωνίας (*λ.χ. πλήρη αναγραφή των στοιχείων της εταιρίας σας & δυνατότητα διαγραφής από την λίστα παραληπτών*). Σημειώνουμε ότι σύμφωνα με το ***άρθρο 9 παρ.10 του Ν.2251/94*** η μετάδοση διαφημιστικού μηνύματος απευθείας στον καταναλωτή μέσω τηλεφώνου, τηλεομοιοτυπίας (*φαξ*), ηλεκτρονικού ταχυδρομείου, αυτόματης κλήσης ή άλλου ηλεκτρονικού μέσου επικοινωνίας επιτρέπεται μόνον αν συναινεί **ΡΗΤΑ** ο καταναλωτής.

Η δημοσιοποίηση των στοιχείων από τους παραλήπτες και μόνο δεν νομιμοποιεί την χρήση τους για σκοπούς απευθείας προώθησης προϊόντων/υπηρεσιών. Απαιτείται περαιτέρω η ρητή συγκατάθεση του καταναλωτή / φυσικού / νομικού προσώπου για τη μεταβίβαση και χρήση των στοιχείων αυτών για το σκοπό της άμεσης διαφήμισης. **ΕΞΑΙΡΕΤΙΚΑ**, δεν απαιτείται η ρητή συγκατάθεση, **ΜΟΝΟ** για τα δεδομένα εκείνα που έχουν αποκτηθεί στα πλαίσια προηγούμενων συναλλαγών (*πώλησης προϊόντων/ υπηρεσιών κ.λπ.*) και υπό την προϋπόθεση:

(α) ότι παρέχεται δυνατότητα διαγραφής με κάθε μήνυμα και

(β) ο παραλήπτης δεν είχε αρχικά αντιτεθεί σε τέτοιου είδους χρήση των δεδομένων τους.

Τέλος σε κάθε περίπτωση αποστολής μη ζητηθείσας ηλεκτρονικής επικοινωνίας με σκοπό την απευθείας προώθηση προϊόντων ή/και υπηρεσιών, αυτή θα πρέπει να χαρακτηρίζεται ως τέτοια σαφώς και επακριβώς ευθύς ως περιέλθει στον παραλήπτη της, φέροντας ειδική σήμανση π.χ. "**ADV**" ή "**ΔΙΑΦΗΜΙΣΗ**".

Σας εφιστώ την προσοχή και επιφυλάσσομαι των νόμιμων δικαιωμάτων μου σε περίπτωση που η συγκεκριμένη αλληλογραφία επαναληφθεί είτε προς το πρόσωπο μου είτε προς οιονδήποτε άλλο που δεν έχει συγκαταθέσει ρητώς να λαμβάνει την αλληλογραφία σας και υποπέσει στην προσοχή μου.
[1][*] ***Άρθρο 11*** (***Μη ζητηθείσα επικοινωνία***)

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.

8.4 Πολέμιος των Spammers

Να «καθαρίσει» **[90]** το Ίντερνετ από τα spam, μηνύοντας όσους του στέλνουν ανεπιθύμητη αλληλογραφία, έβαλε σκοπό της ζωής του ένας Αμερικανός δικηγόρος. Ο Ντάνιελ Μπάλσαμ παράτησε πριν από οκτώ χρόνια την καριέρα του ως στέλεχος μάρκετινγκ, αποφάσισε να γίνει δικηγόρος και αφιέρωσε τη ζωή του στην «εξολόθρευση» των spam. Σήμερα, έπειτα από δεκάδες δίκες και αποφάσεις που του επιδικάζουν ένα εκατομμύριο δολάρια ως αποζημίωση, δηλώνει υπερήφανα ότι είναι ένας «*επαγγελματίας*» κυνηγός των spammer.

Ο δικηγόρος πια από το Σαν Φρανσίσκο ήταν ένας από τους αναρίθμητους εξοργισμένους χρήστες υπηρεσιών ηλεκτρονικού ταχυδρομείου που δέχονται κάθε μέρα πλήθος ανεπιθύμητων email. Οι περισσότεροι απλώς τα διαγράφουν. Εκείνος, όμως,

αποφάσισε να μην μείνει με σταυρωμένα χέρια, κινούμενος δικαστικά εναντίον όσων "*παρανόμως*" του έστελναν spam.

Το «χόμπι» που έγινε καριέρα

«*Ξεκίνησε αυθόρμητα, στη συνέχεια μετατράπηκε σε χόμπι και, τελικά, έγινε καριέρα*», δήλωσε στο Associated Press ο Μπάλσαμ, αποκαλύπτοντας ότι ήδη μετρά περισσότερες από 40 θετικές πρωτόδικες αποφάσεις και αρκετές ακόμα σε ανώτερα δικαστήρια. Ο Μπάλσαμ εγκατέλειψε τη δουλειά του, δημιούργησε ένα site με το όνομα Danhatesspam.com («*Ο Ντραν μισεί το spam*»), και γράφτηκε στη Νομική.

Σήμερα ζει από τα έσοδα που του αποφέρουν οι αγωγές που καταθέτει εναντίον των spammer.Μέχρι τώρα έχει επιδικαστεί υπέρ του περίπου ένα εκατ. δολάρια, από υποθέσεις που κέρδισε για παραβίαση της νομοθεσίας περί spamming.

«Νιώθω ότι κάνω καλό»

«*Νιώθω ότι κάνω κάτι καλό, καθαρίζοντας το Διαδίκτυο*», λέει, αναφερόμενος στο πλήθος των ανεπιθύμητων μηνυμάτων που καθημερινά κατακλύζουν το Ίντερνετ. Από διαφημίσεις μαλακών ναρκωτικών και πορνογραφικό περιεχόμενο, μέχρι υποτιθέμενους διαγωνισμούς που χαρίζουν εκατομμύρια και προτάσεις για… μαγευτικές διακοπές. Σύμφωνα με την εταιρεία Cisco Systems, κάθε μέρα αποστέλλονται 200 δισεκατομμύρια μηνύματα spam, αντιπροσωπεύοντας το 90% του συνόλου των διακινούμενων email.

Ο Μπάλσαμ ξεκίνησε τη «*βιομηχανία αγωγών*» το 2002 από τοπικά δικαστήρια, φτάνοντας το 2008 μέχρι τα εφετεία. Τη χρονιά εκείνη πήρε το πτυχίο του δικηγόρου από τη Νομική Σχολή του Hastings College στην Καλιφόρνια. Την τελευταία του νίκη κατήγαγε τον περασμένο Νοέμβριο, αποσπώντας **4.000 δολάρια** από την εταιρεία Various, που ελέγχει το site AdultFriendFinder.com. Η εταιρεία του είχε στείλει τέσσερα email με θέμα « *Γεια σου. Είμαι η Ρεβέκκα και σ' αγαπώ* ! ».

Τι λένε οι αντίδικοι

Οι αντίδικοι του (δηλαδή οι spammer) υποστηρίζουν ότι ο Μπάλσαμ έχει γίνει επαγγελματίας εκμεταλλευτής της νομοθεσίας περί anti-spam. Τον κατηγορούν ότι καταθέτει σωρεία αγωγών εναντίον εταιρειών που ξέρει ότι θα προτιμήσουν τον εξωδικαστικό συμβιβασμό από το να μπουν σε μια μακρά -και πολυέξοδη- δικαστική διαμάχη. «*Φαίνεται καθαρά ότι προσπαθεί να διαστρεβλώσει τα πράγματα για τα λεφτά*», υποστήριξε ο Μπένετ Κέλι, συνήγορος υπεράσπισης πολλών εταιρειών που έχει μηνύσει ο Μπάλσαμ.

Ο Κέλι έφτασε στο σημείο να δημιουργήσει έναν ιστότοπο με το όνομα Danhatespam.com (λείπει μόνο ένα «s» από τη διεύθυνση του site του Μπάλσαμ), το οποίο επέκρινε τον αντίδικό του για τις πρακτικές που ακολουθεί. Σύντομα, όμως, το site «*κλώνος*» τέθηκε εκτός λειτουργίας.

Τον μήνυσαν… για τις μηνύσεις

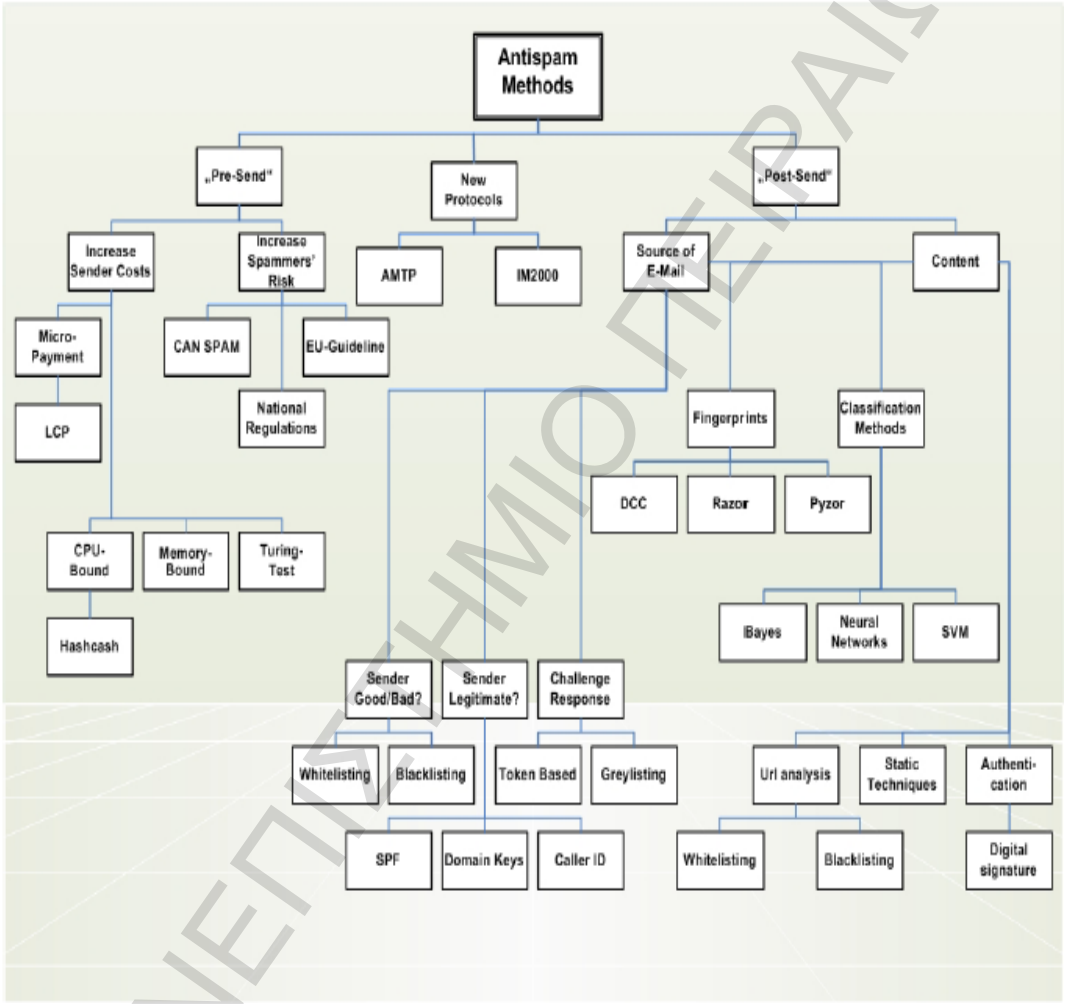
«*Δεν υπάρχει τίποτα κακό με το να πολεμάς το spam. Όμως ο Ντραν κάνει κατάχρηση των προβλεπόμενων διαδικασιών, χρησιμοποιώντας τα δικαστήρια. Πολλοί άνθρωποι συμβιβάζονται μαζί του, προκειμένου να αποφύγουν την ταλαιπωρία*», δήλωσε ο Κέλι, ο οποίος έχει μηνύσει δύο φορές τον Μπάλσαμ, για «*παραβίαση των όρων εμπιστευτικότητας των συμφωνιών συμβιβασμού*».

Το ίδιο έχουν πράξει και άλλες εταιρείες εναντίον των οποίων έχει στραφεί δικαστικά ο Μπάλσαμ. Η Tagged.com, το τρίτο μεγαλύτερο site κοινωνικής δικτύωσης στις Η.Π.Α., κατέθεσε μήνυση εναντίον του, κατηγορώντας τον ότι «*απειλεί να παραβιάσει τους όρους του προγενέστερου συμβιβασμού, σχεδιάζοντας να αναρτήσει το περιεχόμενο της συμφωνίας στο site του*». Παρόμοια μήνυση δέχθηκε και από την ValueClick.

Ο Μπάλσαμ αποκρούει τις κατηγορίες, χαρακτηρίζοντας τις μηνύσεις ως «αντίποινα» στις αγωγές που ο ίδιος πρώτος έκανε. «*Νιώθω καλά που κάνω αυτό που κάνω. Και δεν πρόκειται να κάνω πίσω*», διαμηνύει.

9. Ανάλυση τεχνικών μεθόδων και αρχιτεκτονικών των Spam

Στόχος του κεφαλαίου είναι η ανάλυση των τεχνικών μεθόδων και των αρχιτεκτονικών τους προκειμένου να αντιμετωπιστεί το πρόβλημα της ανεπιθύμητης και αυτόκλητης αλληλογραφίας.



Σχήμα 2 : Σχηματική απεικόνιση των μεθόδων αντιμετώπισης της ανεπιθύμητης αλληλογραφίας

Η εν λόγω ενότητα παρουσιάζει μεθόδους που σχετίζονται με το φιλτράρισμα της αλληλογραφίας και έχουν ως στόχο την εξαρχής αναγνώριση του spam μηνύματος πριν σταλεί ("*Pre-send*"), την αντιμετώπιση του spam μηνύματος αφού σταλεί ("*Post-send*") καθώς και τον έλεγχο του ηλεκτρονικού μηνύματος κατά την διάρκεια της μεταφοράς του μέσω του δικτύου.

9.1 Μέθοδοι αντιμετώπισης ανεπιθύμητης αλληλογραφίας

Τα τελευταία χρόνια ένας μεγάλος αριθμός μεθόδων και τεχνικών για την αντιμετώπιση του προβλήματος των spam μηνυμάτων έχει προταθεί και αναπτυχθεί τόσο στο νομικό χώρο όσο και στον τεχνικό.

Σ 'αυτό το σημείο όμως, προτού γίνει η αναλυτική περιγραφή και αξιολόγηση των μεθόδων, αξίζει να αναφερθεί ότι σχεδόν όλες οι μέθοδοι της κατηγορίας *"Pre-send"* καθώς και όλες οι μέθοδοι της κατηγορίας *"Post-send"* περιλαμβάνουν την διαδικασία κατά την οποία κρίνεται το αν ένα εισερχόμενο ή εξερχόμενο ηλεκτρονικό μήνυμα είναι spam ή όχι. Έτσι μια πρώτη μορφή αξιολόγησης αυτών των μεθόδων είναι η χρησιμοποίηση κάποιων ποιοτικών κριτηρίων που σχετίζονται με τη διαδικασία αυτή (κρίνεται ποιο μήνυμα είναι spam και ποιο όχι).

Αυτά τα κριτήρια περιλαμβάνουν 2 μεταβλητές ***spam*** και ***ham***. Η μεταβλητή spam αναφέρεται στα μηνύματα που χαρακτηρίζονται ως spam ενώ η μεταβλητή ham σ' αυτά που χαρακτηρίζονται ως μη spam. Με αυτή τη βοήθεια λοιπόν των κριτηρίων πραγματοποιείται έλεγχος κατά πόσο οι χαρακτηρισμοί των μηνυμάτων είναι σωστοί ή όχι. Έτσι για παράδειγμα στην περίπτωση που ένα μήνυμα έχει χαρακτηριστεί ως spam αλλά και στην πραγματικότητα αποδεικνύεται ως spam τότε παίρνει τον χαρακτηρισμό ως ***'true positive'***.

Στην αντίθετη περίπτωση, δηλαδή όταν έχει χαρακτηριστεί ως spam αλλά δεν είναι spam, τότε λαμβάνει το χαρακτηρισμό του ***'false positive'***. Με την ίδια λογική, λειτουργεί και η περίπτωση του ham μηνύματος. Δηλαδή όταν κάποιο μήνυμα ταξινομείται ως ham και είναι όντως τότε θεωρείται ως ***'true negative'*** στην περίπτωση όμως που δεν είναι πραγματικά ham τότε καλείται ως ***'false negative'.***

Κατ'αυτόν τον τρόπο προκύπτουν δύο ομάδες (sets) κριτηρίων, οι ***'true positive – false positive' 'true negative – false negative'***

Σχηματική απεικόνιση όσον προαναφέρθηκαν ακολουθεί στον παρακάτω πίνακα 5 :

Message / classified as	*Spam (positives)*	*Ham (negatives)*
Spam	True positive	False negative
Ham	False positive	True negative

Πίνακα 6: Spam και Ham.

Για να είναι επομένως οι μέθοδοι αυτές αποτελεσματικές για τους τελικούς χρήστες θα πρέπει να αναγνωρίζουν με όσο το δυνατόν μεγαλύτερο βαθμό επιτυχίας τα spam μηνύματα έτσι ώστε να μειώνεται το ποσοστό λανθασμένης ταξινόμησης μηνυμάτων. Με άλλα λόγια τα μηνύματα που ταξινομούνται ως spam, να είναι και στην πραγματικότητα κλπ.

Περισσότερο ενδιαφέρον βέβαια έχει η περίπτωση των ***false positive*** (δηλαδή των μηνυμάτων μη spam που χαρακτηρίστηκαν ωστόσο ως spam). Σ'αυτή την περίπτωση, όταν γίνεται δηλαδή λανθασμένη διάγνωση του μηνύματος, προκύπτουν "κοστοβόρες" επιπτώσεις για τους τελικούς χρήστες (απόρριψη χρήσιμων ηλεκτρονικών μηνυμάτων κλπ). Επομένως αυτό που είναι θεμιτό είναι η ύπαρξη μεθόδων οι οποίες αναγνωρίζουν σωστά τα spam μηνύματα, απορρίπτουν την παραλαβή τους από το σύστημα του ηλεκτρονικού ταχυδρομείου και αποτρέπουν την παράδοση τους στον τελικό χρήστη.

9.1.1 Μέθοδος από την πλευρά του αποστολέα (Sender Side (Pre-send) Methods)

Πρόκειται για τις μεθόδους που συναντάμε στο αριστερό μέρος της σχηματικής απεικόνισης (σχήμα 2) και λαμβάνουν χώρα πριν ένα ηλεκτρονικό μήνυμα σταλεί. Η ιδέα που υποβόσκει στις "*Pre-send*" μεθόδους είναι να αποθαρρύνει την αποστολή των spam μηνυμάτων, κατά μία έννοια να αντίκειται στο πρόβλημα πριν αυτό προκύψει. Έτσι οι μέθοδοι αυτές περιλαμβάνουν στρατηγικές που σχετίζονται με την αύξηση του κόστους σχετικά με την αποστολή των μηνυμάτων.

Η κύρια ιδέα αυτών των μεθόδων είναι να καταστήσουν τα επιχειρηματικά μοντέλα των spammers μη κερδοφόρα. Δύο στρατηγικές έχουν αναπτυχθεί προκείμενου να επιτύχουν αυτό τον στόχο – είτε καθυστερώντας την αποστολή κάθε ηλεκτρονικού μηνύματος (Technical solution) είτε εισάγοντας κάποια τιμή πληρωμής για αποστολή του ηλεκτρονικού μηνύματος (money based solution).

Technical Solutions

Οι περισσότερες τεχνικές λύσεις βασίζονται στον υπολογιστικό χρόνο της μνήμης του υπολογιστή: ο αποστολέας θα πρέπει να λάβει υπόψιν του ότι μια λογικά ακριβή συνάρτηση ονόματι *"Pricing Function"* προηγείται της αποστολής του ηλεκτρονικού μηνύματος. Απ'την στιγμή που είναι γνωστό ότι το ηλεκτρονικό μήνυμα δεν είναι ένας τρόπος επικοινωνίας πραγματικού χρόνου αρκετά καλός η καθυστέρηση των μηνυμάτων δεν ενοχλεί ιδιαίτερα τον μέσο χρήστη του ηλεκτρονικού ταχυδρομείου αφού κατά μέσο όρο στέλνει 20 – 50 ηλεκτρονικά μηνύματα την ημέρα και δεν έχει ιδιαίτερες απαιτήσεις στο θέμα του χρόνου. Ωστόσο η καθυστέρηση είναι ιδιαίτερα ενοχλητική για τον spammer αφού έτσι μειώνεται ο αριθμός των πιθανόν πελατών που προσεγγίζονται στην μονάδα του χρόνου.

Το μειονέκτημα της *Pricing Function* είναι ότι διαχωρίζει τους χρόνους παράδοσης των μηνυμάτων ανάλογα με το υλικό (hardware) που διαθέτει ο υπολογιστής από τον οποίο αποστέλλεται το μήνυμα. Έτσι πολλές λύσεις έχουν προταθεί σχετικά με τις *Pricing Functions* όπως για παράδειγμα οι CPU-bound Functions, memory-bound Functions ή Turing tests **[91]**,**[92]**,**[93]**. Ένα αντιπροσωπευτικό παράδειγμα τεχνικής λύσης που βασίζεται στην κατηγορία των CPU-bound Functions αποτελεί η **Hashcash**.

FROM:	someone <test@test.invalid>
TO:	max mustermann <max@mustermann.org>
Subject:	test Hashcash
Date:	xx.xx.200x
X-Hashcash:	0:030626:adam@cypherspace.org:6470e06d773e05a8

Πίνακας 7: Μια τυπική X-Hashcash ετικέτα

Η **Hashcash** είναι ένα λογισμικό που εφαρμόζεται για τους χρήστες ηλεκτρονικών ταχυδρομείων οι οποίοι προσθέτουν ένα Hashcash stamp προκειμένου να στείλουν ένα ηλεκτρονικό μήνυμα. Πιο συγκεκριμένα η προσθήκη ενός Hashcash stamp αφορά στην εισαγωγή μιας γραμμής που θα ξεκινάει με : «X- Hashcash» στο θέμα του μηνύματος όπως αυτό διαφαίνεται σχηματικά παρακάτω:

Προκειμένου να δημιουργηθεί ένα *''Hashcash stamp''* χρειάζεται να καταναλωθεί χρόνος στην CPU. Ένα stamp χρησιμοποιείται για κάθε παραλήπτη ακόμα και όταν το μήνυμα είναι μαζικής αποστολής (BCC) και δείχνει τον βαθμό δυσκολίας μιας εργασίας

που πραγματοποιείται προκειμένου να καταναλωθεί ο χρόνος της CPU. Έχει διαπιστωθεί ότι όσο πιο δύσκολη είναι αυτή η εργασία και άρα όσο πιο πολύς χρόνος καταναλώνεται στην CPU για ένα ηλεκτρονικό μήνυμα τότε οι πιθανότητες αυτό το ηλεκτρονικό μήνυμα να είναι spam είναι ελάχιστες. Τεχνικά αυτές οι εργασίες που χρησιμοποιούνται από την Hashcash βασίζονται στις Hash Functions και πιο ειδικά ονομάζονται *"Partial Hash-collisions".* Μια Hash function είναι μια κρυπτογραφική συνάρτηση για την οποία είναι υποθετικά δύσκολο να βρει κανείς δυο εισόδους που παράγουν την ίδια έξοδο.

Στο σημείο αυτό αξίζει να αναφέρουμε ότι τεχνικά αυτές οι εργασίες που χρησιμοποιούνται από την Hashcash και βασίζονται στις Hash Functions τα πρωτόκολλα ανταλλαγής κλειδιών ικανοποιούν πολλούς στόχους ασφαλείας αναλόγως με το πώς υλοποιούνται και χρησιμοποιούνται. Περιλαμβάνουν ταυτοποίηση και επικύρωση των δύο οντοτήτων, *ασφάλεια* και *προστασία* από αντιπάλους τόσο σε περίπτωση ενεργητικής όσο και παθητικής επίθεσης.

Επειδή απαιτούνται πολύπλοκοι υπολογισμοί τόσο κατά τη δημιουργία των κλειδιών όσο και κατά την κρυπτογράφηση και αποκρυπτογράφηση, όσο μεγαλύτερο είναι το μέγεθος των κλειδιών τόσο βραδύτερος θα είναι ο ρυθμός λειτουργίας του συστήματος.

Money Based Solutions

Η βασική ιδέα πίσω από τις *Money based solutions* (MBS) είναι η πληρωμή κάποιου ποσού για το κάθε Ηλεκτρονικό μήνυμα που αποστέλλεται. Η ιδέα αυτή βασίζεται στο ότι ένα ηλεκτρονικό μήνυμα είναι περισσότερο πιθανό να είναι ham (μη spam) όταν το ποσό που απαιτείται για την παράδοση του είναι υψηλό.

Το ***Lightweight Currency Protocol*** **(LCP)** είναι ένας μηχανισμός που αποτελεί πρόταση για την υλοποίηση της παραπάνω ιδέας. Σύμφωνα με αυτόν τον μηχανισμό λοιπόν επιτρέπεται στους παρόχους της υπηρεσίας του ηλεκτρονικού ταχυδρομείου να εκδίδουν ένα γενικό νόμισμα. Οι πάροχοι αυτοί δημιουργούν ένα ζεύγος κλειδιών το οποίο περιλαμβάνει το ιδιωτικό και το δημόσιο κλειδί για τον κάθε χρήστη. Το LCP είναι ένα πρωτόκολλο αίτησης / απάντησης όπου ο εκδότης του νομίσματος είναι ο server και ο κάτοχος ο client.

Σύμφωνα μ'αυτό το πρωτόκολλο προτείνεται ένας μηχανισμός πληρωμής **[94]** όπου οι servers αιτούνται της πληρωμής αυτής προκειμένου να αποδεχθούν τα εισερχόμενα μηνύματα. Υπεύθυνος για την διαδικασία της πληρωμής καθίσταται ο πάροχος ενώ ο client δεν εμπλέκεται στην διαδικασία αυτή. Η εκτέλεση αυτού του μηχανισμού πληρωμής που βασίζεται στο LCP πρωτόκολλο έχει τα εξής βήματα :

1. ένας χρήστης ξοδεύει ένα συγκεκριμένο ποσό του νομίσματός του στέλνοντας ένα μήνυμα προς τον εκδότη του νομίσματος ως προς την πληρωμή,
2. ο εκδότης με την σειρά του πιστοποιεί το δημόσιο κλειδί του χρήστη, το ποσό καθώς και το αναγνωριστικό κωδικό της συναλλαγής (transaction-id).
3. Αν ο αποστολέας έχει ένα επαρκές υπόλοιπο χρημάτων, ο εκδότης θα χρεώσει τον λογαριασμό του παραλήπτη με το ποσό που ζητήθηκε και θα πιστώσει τον λογαριασμό του αποστολέα.
4. Ο παραλήπτης επαληθεύει την πληρωμή και ο παροχέας απαντάει με μια δήλωση της κατάστασης του λογαριασμού.

Έτσι στην περίπτωση των spammers, αυτοί πρέπει να είναι πολύ επιλεκτικοί σχετικά με τους παραλήπτες των μηνυμάτων τους, αφού θα πρέπει να εστιάζουν σε παραλήπτες για τους οποίους υπάρχει μεγάλη πιθανότητα να ανταποκριθούν στο περιεχόμενο των μηνυμάτων και να επιφέρουν έσοδα έτσι ώστε να μην μειώνεται το περιθώριο κέρδους των spammer.

9.1.2 Μέθοδος από την πλευρά του παραλήπτη (Receiver Side (Pre-send) Methods)

Σ'αυτή την κατηγορία, ομαδοποιούνται όλες οι προσεγγίσεις επίλυσης του προβλήματος από την μεριά του παραλήπτη του ηλεκτρονικού μηνύματος. Πρόκειται για τις μεθόδους που συναντάμε στο δεξί μέρος της σχηματικής απεικόνισης (σχήμα 2) και λαμβάνουν χώρα αφού ένα ηλεκτρονικό μήνυμα σταλεί και έχει παραληφθεί. Σε αντίθεση με τις Pre-send μεθόδους, όπου περιγράφηκαν παραπάνω, οι οποίες λαμβάνουν μέρος πριν σταλεί το ηλεκτρονικό μήνυμα (proactive), οι Post-send λαμβάνουν μέρος αφού σταλεί (reactive). Οι μέθοδοι αυτές μπορούν να κατηγοριοποιηθούν ανάλογα με το περιεχόμενο των ηλεκτρονικών μηνυμάτων, την προέλευση των ηλεκτρονικών μηνυμάτων και τον συνδυασμό των προαναφερθέντων κατηγοριών (προέλευση και περιεχόμενο).

Προσεγγίσεις που βασίζονται στην πηγή των ηλεκτρονικών μηνυμάτων

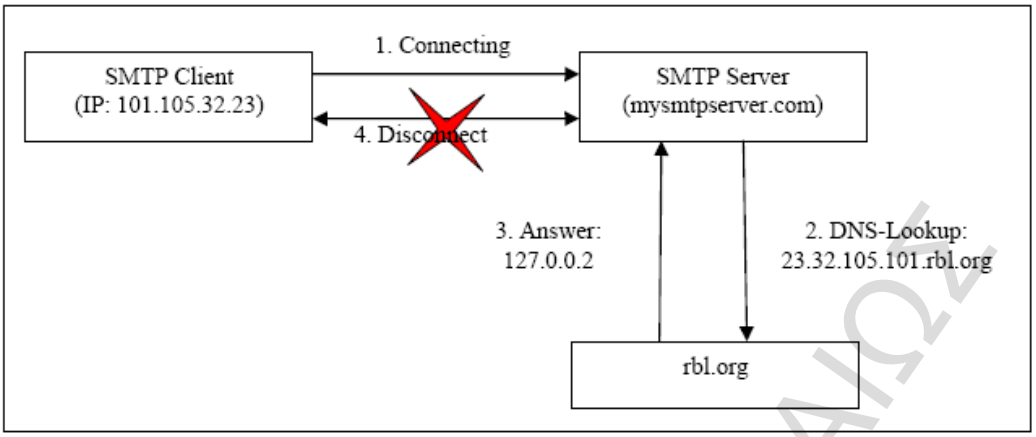
Σ'αυτή την κατηγορία προσεγγίσεων, θα επεξηγηθούν οι πιο σημαντικές μέθοδοι οι οποίες εστιάζουν στην πηγή ενός ηλεκτρονικού μηνύματος. Με την λέξη πηγή εννοούμε στις περισσότερες περιπτώσεις την IP διεύθυνση του client, το domain του αποστολέα ή την πλήρη ταχυδρομική θυρίδα. Τα οποία προέρχονται συνήθως από τον διάλογο μέσω του SMTP ή από το μήνυμα αυτό καθεαυτό. Βάσει αυτών μπορούμε να κατηγοριοποιήσουμε την πηγή με τρεις διαφορετικούς τρόπους. Ο πρώτος τρόπος είναι ο καθορισμός του αποστολέα ως "*καλού*" ή "*κακού*". Μια άλλη πιθανότητα είναι να εξακριβωθεί αν η πηγή έχει κριθεί ως νόμιμη να χρησιμοποιεί την ταυτότητα του. Ο τρίτος τρόπος αφορά στην εξακρίβωση ότι ο αποστολέας είναι πρόθυμος να καταβάλει περισσότερη προσπάθεια προκείμενου να έρθει σε επαφή με τον παραλήπτη.

Πιο συγκεκριμένα αναλύονται τα παρακάτω :

- Blacklist, whitelist (*καλός/κακός αποστολέας*)
- Sender policy Framework, Caller ID, Sender ID, Domain Keys (*νόμιμος / παράνομος αποστολέας*)
- Greylists, ChoiceMail και SFM (*συστήματα challenge-response*)

Blacklist / Whitelist

- Η ***blacklist*** είναι μία βάση δεδομένων η οποία περιέχει τις IP διευθύνσεις ή τα ονόματα των τομέων οι οποίοι είναι ύποπτοι για να στέλνουν spam. Κάθε μήνυμα το οποίο προέρχεται από έναν τομέα ή μια IP διεύθυνση που εμφανίζεται να είναι στην blacklist κάποια λίστα γνωστών πηγών spam στο Internet θα μπλοκάρεται. Υπάρχουν δυο βασικοί τύποι στις *blacklists*- οι *real time blacklists (RBL)* με μία κεντρικοποιημένη και κατανεμημένη βάση δεδομένων και οι *domain levels blacklists* οι οποίες ενημερώνονται κάθε φορά από τους administrators. Ο πιο αποτελεσματικός τρόπος λαμβάνει στοιχεία και από τις δυο παραπάνω μεθόδους και αφορά στην χρήση των RBLs ενημερωμένων όμως από ανεξάρτητους οργανισμούς **[95]** οι οποίοι βασίζονται συνήθως στο DNS (*Domain Name System*). Στον παρακάτω σχήμα απεικονίζεται το βασικό σενάριο που ακολουθείται στις blacklists.



Σχήμα 3 : Τυπικό σενάριο για μία blacklist

Πιο συγκεκριμένα ο SMTP client με την IP διεύθυνση του (IP : 101.105.32.23) συνδέεται με τον SMTP server (*mysmtpserver.com*). Πριν ξεκινήσει ο SMTP διάλογος, ο SMTP server καταγράφει την IP διεύθυνση από την TCP σύνδεση και ενεργεί μια DNS αναζήτηση στον οργανισμό rbl.org. Ο rbl.org επιστρέφει μια απάντηση με τον κωδικό "127.0.0.2" η οποία υποδηλώνει ότι ο SMTP client είναι μια πηγή αυτόκλητων και μαζικών μηνυμάτων (UBE : *Unsolicited Bulk Messages*) οπότε ο SMTP server διακόπτει την σύνδεση με τον client.

- Η ***whitelist*** είναι μία βάση δεδομένων οι οποία περιέχει τις IP διευθύνσεις ή τα ονόματα των τομέων οι οποίοι σίγουρα δεν είναι ύποπτοι για αποστολή spam. Κάθε μήνυμα που λαμβάνεται από μια πηγή η οποία εμφανίζεται να είναι στην whitelist παρακάμπτει την διαδικασία φιλτραρίσματος. Μια whitelist είναι συνήθως ιδιόκτητη, υπάρχουν όμως και άλλες παγκόσμιες whitelists όπου περιέχουν οργανισμούς που έχουν υπογράψει να μην στέλνουν spam μηνύματα. Αυτές οι λίστες είναι συνήθως ελεγχόμενες από ανεξάρτητους οργανισμούς (όπως για παράδειγμα Habeas **[96]**, Bonded Sender Program **[97]**, Brightmail Safe List).

Realtime Blacklists

Λίστες που ενημερώνονται σε πραγματικό χρόνο και περιέχουν διευθύνσεις IP ή Domains (DNSBL) spammers και λίστες με συνδέσμους (URIBL) που περιέχονται στα μηνύματα spam. Οι λίστες αυτές χρησιμοποιούνται πολύ συχνά από τους παροχείς υπηρεσιών e-mails για την απόρριψη των μηνυμάτων που προέρχονται από τις διευθύνσεις αυτές ή περιέχουν συνδέσμους (links) σε αυτές και είναι αρκετά αποτελεσματικές **[98]**.

Είναι ο αποστολέας νόμιμος / παράνομος

Μια σημαντική προσπάθεια είναι η βελτίωση μεθόδων και τεχνικών καθορισμού του πότε ένας αποστολέας ενός ηλεκτρονικού μηνύματος είναι αυθεντικός ή κατά πόσο είναι νόμιμος. Η ελλοχεύουσα ιδέα είναι αφενός ότι οι spammers δεν θέλουν να αυθεντικοποιούνται προκειμένου να αποφεύγεται η εγκληματική δίωξή τους και αφετέρου – για τον ίδιο λόγο – οι spammers φροντίζουν ώστε να διαστρεβλώνουν την πληροφορία στην κεφαλίδα του ηλεκτρονικού μηνύματος τους, το οποίο μπορεί να οδηγήσει σε αντιφατικές πληροφορίες (για παράδειγμα, ο υποτιθέμενος αποστολέας δεν είναι νόμιμος για τον υποτιθέμενο server ηλεκτρονικού ταχυδρομείου).

Παρακάτω, θα αναφερθούμε συνοπτικά στις σημαντικότερες τεχνικές αυτού του τομέα. Οι τεχνικές αυτές αρχικά κατατέθηκαν ως προτάσεις στο IETF (*Internet Engineering Task Force*).

Προτάσεις για αντι-spam πρότυπα, οι οποίες έχουν κατατεθεί στο IEFT το 2004 για τη αντιμετώπιση του spam.

- *Caller ID* : προτάθηκε από τις Microsoft, Sendmail, Amazon.com και Brightmail
- *DomainKeys* : προτάθηκε από την Yahoo
- *Sender Policy Frameworks* (SPF) : υποστηρίχθηκε από τις AOL, GMX

Τα SFP, *Sender-ID* και *DomainKeys* είναι έννοιες οι οποίες ελαχιστοποιούν την πιθανότητα πλαστών domain. Τα πρωτόκολλα προσπαθούν να αφήσουν την κοινή διαδικασία αποστολής ανεπηρέαστη και επικοινωνούν με το SMTP έτσι ώστε να υποστηριχθεί η κατανομή και η αποδοχή του πρωτοκόλλου. Όλα τα πρωτόκολλα που προαναφέραμε έχουν ως κοινό σημείο την χρήση DNS για επαλήθευση των ηλεκτρονικών μηνυμάτων. Οπότε αυξάνεται η κίνηση στο δίκτυο που χρησιμοποιείται, λόγω του ότι κάθε ηλεκτρονικό μήνυμα που παραλαμβάνεται πρέπει να ελέγχεται ως προς την περιοχή (domain) που καθορίζεται από την διεύθυνση του ηλεκτρονικού μηνύματος.

Το ***Sender Policy Framework (SPF)*** **[99]**, αναπτύχθηκε από τους *Meng Wong* και *Mark Lentczner* και χρησιμοποιεί την "MAIL FROM :" ταυτότητα από τον SMTP διάλογο για να επιβεβαιώσει την περιοχή (domain) του αποστολέα. Αυτό επιτρέπει την απόρριψη ενός ηλεκτρονικού μηνύματος κατά τον SMTP διάλογο. Μια SPF καταγραφή υποδεικνύει τους εξερχόμενους SMTP servers της περιοχής του αποστολέα. Όταν ένας SMTP client συνδέεται με έναν ανταλλάκτη ηλεκτρονικών μηνυμάτων, ο server ψάχνει για μια SPF καταγραφή στο DNS δέντρο, από την απαιτούμενη περιοχή του αποστολέα. Αν το αποτέλεσμα που θα παραληφθεί από το DNS ερώτημα περιέχει την IP διεύθυνση του client, τότε ο αποστολέας είναι εξουσιοδοτημένος να χρησιμοποιήσει στο "MAIL FROM :" την περιοχή (domain). Αν όχι τότε η περιοχή (domain) ήταν πλαστή.

Η έννοια του ***Caller-Id***, αναπτύχθηκε από την Microsoft, πραγματοποιεί την επονομαζόμενη έννοια, αλλά χρησιμοποιεί την αποκαλούμενη "εσκεμμένη αρμόδια διεύθυνση" (*purposed responsible address*, "PRA") για την επαλήθευση. Η εσκεμμένη αρμόδια διεύθυνση αναφέρεται στην ταχυδρομική θυρίδα η οποία άμεσα άρχισε την διαδικασία αποστολής και είναι καθορισμένη στην κεφαλίδα του μηνύματος. Για παράδειγμα, εάν μια κεφαλίδα περιέχει ένα πεδίο "FROM:" και το πεδίο "SENDER:", τότε το PRA λαμβάνεται από το πεδίο "SENDER:" **[100]**.

Η ***Sender-Id*** **[101]** υποδομή είναι αποτέλεσμα της συγχώνευσης του Caller-Id και του SPF.

Το ***DomainKeys*** **[102]** χρησιμοποιεί επίσης το DNS αλλά η διαδικασία επιβεβαίωσης γίνεται μέσω της ψηφιακής υπογραφής αντί της IP διεύθυνσης. Από την πλευρά του αποστολέα, αυτή η παραλλαγή αποτελείται από δύο βήματα :

- **Ρύθμιση** : Στο πρώτο βήμα, ο κάτοχος του domain παράγει ένα δημόσιο / ιδιωτικό ζευγάρι κλειδιών. Αυτό το ζευγάρι κλειδιών χρησιμοποιείται για να υπογράφονται όλα τα εξερχόμενα μηνύματα. Το δημόσιο κλειδί παραμένει στο DNS, και το ιδιωτικό κλειδί στο ηλεκτρονικό ταχυδρομείο εξερχόμενων μηνυμάτων.

- **Υπογραφή** : Όταν ο τελικός χρήστης στέλνει ένα ηλεκτρονικό μήνυμα, μια ψηφιακή υπογραφή με το ιδιωτικό του κλειδί παράγεται από το DomainKey όπου διευκολύνει το σύστημα του ταχυδρομείου.

Για να επιβεβαιωθεί ένα ηλεκτρονικό μήνυμα από την πλευρά του παραλήπτη, τρία βήματα είναι απαραίτητα :

1) **Προετοιμασία** : Το domainkey από την πλευρά του παραλήπτη εξάγει την υπογραφή και την απαιτούμενη περιοχή για το "*FROM* :" από την κεφαλίδα του ηλεκτρονικού μηνύματος και προσκομίζει το δημόσιο κλειδί από τον DNS για την απαιτούμενη περιοχή του "*FROM* :".

2) **Επιβεβαίωση** : Με το δημόσιο κλειδί που παραλαμβάνεται από το DNS, το σύστημα παραλαβής των ηλεκτρονικών μηνυμάτων επιβεβαιώνει εάν η υπογραφή του μηνύματος παράχθηκε από το ιδιωτικό κλειδί (όπου ανήκει στο ίδιο ζεύγος κλειδιών με το δημόσιο).

3) **Παράδοση** : Εάν το ηλεκτρονικό μήνυμα επιβεβαιωθεί επιτυχώς, τότε το μήνυμα παραδίδεται στην εισερχόμενη αλληλογραφία του παραλήπτη

Challenge - Response

Τα Challenge-Response συστήματα **[103]** αρχικά μπλοκάρουν ή συγκρατούν τα ηλεκτρονικά μηνύματα που στάλθηκαν από άγνωστους αποστολείς. Οι αποστολείς ειδοποιούνται για το μπλοκάρισμα, κατόπιν απαιτείται να αποδείξουν ότι είναι άνθρωποι και όχι κάποια αυτοματοποιημένη διαδικασία απαντώντας σε μια απλή για τον ανθρώπινο εγκέφαλο δοκιμασία η οποία παράλληλα είναι πολύ δύσκολη έως αδύνατη για μια μηχανή. Εάν αυτό αποδειχθεί τότε το ηλεκτρονικό μήνυμα παραδίδεται.

Τα Challenge-Response συστήματα διατηρούν μια λίστα όλων των επιτρεπόμενων αποστολέων. Ένα ηλεκτρονικό μήνυμα ενός νέου αποστολέα κρατείται προσωρινά χωρίς να παραδοθεί ενώ ο αποστολέας παραλαμβάνει πίσω ένα ηλεκτρονικό μήνυμα πρόκληση (challenge). Αυτή η πρόκληση μπορεί να είναι ένα «διπλό κλίκ» πάνω σε ένα URL ή απάντηση σ'αυτό το ηλεκτρονικό μήνυμα. Εάν οι spammers χρησιμοποιούν πλαστές διευθύνσεις για την αποστολή μηνυμάτων, δεν θα λάβουν ποτέ την πρόκληση (challenge), ακόμα όμως και στην περίπτωση που χρησιμοποιούν πραγματικές διευθύνσεις για την αποστολή μηνυμάτων δεν θα είναι ποτέ εφικτό να απαντήσουν σε όλες τις προκλήσεις (challenges) για ένα συγκεκριμένο χρονικό διάστημα.

Δυστυχώς όμως υπάρχουν ορισμένοι περιορισμοί σ'αυτή την προσέγγιση. Εάν και οι δυο συμμετέχοντες στην επικοινωνία χρησιμοποιούν Challenge-Response σύστημα, τότε δεν θα έχουν την δυνατότητα να επικοινωνήσουν μεταξύ τους. Άλλο ένα μειονέκτημα είναι ότι τα αυτοματοποιημένα συστήματα ή οι κατάλογοι διευθύνσεων δεν μπορούν να ανταποκριθούν σε μια πρόκληση. Το τρίτο πρόβλημα είναι η αναγνώριση χαρακτήρων ή το ταίριασμα προτύπων. Αυτά τα χαρακτηριστικά γνωρίσματα πρόκλησης ασφάλειας είναι εύκολο να παρακαμφθούν και τελικά ένας spammer μπορεί να πλαστογραφήσει τη διεύθυνση ηλεκτρονικού ταχυδρομείου ενός νόμιμου χρήστη.

Υπάρχουν αρκετές εφαρμογές των Challenge-Response συστημάτων – παρακάτω θα αναλυθούν τρεις διαφορετικοί τύποι: η Greylisting, ένα ανθρώπινο σύστημα αλληλεπίδρασης καλούμενο ως ChoiceMail και μια συνδρομή στον mail server καλούμενη ως SFM (Spam Free Mail).

Η ***Greylisting*** **[104]** είναι μια δραστική μέθοδος μπλοκαρίσματος των spam. Βασίζεται στο γεγονός ότι αν τα spam μηνύματα δεν παραδοθούν με την πρώτη απόπειρα αποστολής τους τότε δεν θα υπάρξει δεύτερη και αυτό γιατί οι spammers συνήθως δεν γνωρίζουν αν η ηλεκτρονική διεύθυνση ενός παραλήπτη υπάρχει πραγματικά ή όχι, οπότε και δεν μπορούν να ξέρουν αν ένα μήνυμα παραλήφθηκε ή όχι, ενώ αν ένας απλός mail server προσπαθήσει να παραδώσει ένα μήνυμα και η παραλαβή του μηνύματος δεν γίνει αποδεκτή θα προσπαθήσει ξανά μετά από ένα καθορισμένο χρονικό διάστημα.

Όταν ένας client συνδεθεί με έναν server ο οποίος χρησιμοποιεί Greylisting, ο server καταγράφει τις ακόλουθες πληροφορίες :

1. Την διεύθυνση IP αυτού που παρέχει hosting και προσπαθεί να κάνει την παράδοση
2. Την διεύθυνση του αποστολέα
3. Την διεύθυνση του παραλήπτη

Ο server έπειτα συγκρίνει τα στοιχεία αυτά με μια τοπική βάση δεδομένων. Αν τα στοιχεία αυτά δεν ταιριάξουν με καμία εγγραφή της βάσης δεδομένων, το μήνυμα θα

απορριφθεί με μια προσωρινή αποτυχία απόκρισης και τα στοιχεία θα αποθηκευθούν. Αν το μήνυμα σταλεί για δεύτερη φορά μέσα σε ένα συγκεκριμένο χρονικό διάστημα τότε θα παραληφθεί από τον τελικό του παραλήπτη.

Σχήμα 3: Καταχώρηση αποστολέα σε ChoiceMail

Το ***ChoiceMail*** **[105]** (βλ. Σχήμα 3) μπορεί να λειτουργήσει με διάφορους τρόπους. Ελεύθερο για οικιακή χρήση, Server έκδοση, Enterprice έκδοση, και χρησιμοποιεί σύστημα *Challenge-Response*. Εάν το ChoiceMail δεν μπορεί να αναγνωρίσει το μήνυμα, αφού το έχει ελέγξει βάσει της whitelist, blacklist και όποιων άλλων μεθόδων και κανόνων χρησιμοποιούνται, τότε στέλνει ένα μήνυμα καταχώρησης αίτησης στον αποστολέα.

Αυτό το σύντομο ηλεκτρονικό μήνυμα κατευθύνει τον αποστολέα σε μια Web σελίδα όπου καλείται να συμπληρώσει το όνομα του/της, την ηλεκτρονική διεύθυνση και τον λόγο που θέλει να επικοινωνήσει. Ο αποστολέας επίσης καλείται να συμπληρώσει έναν κωδικό, ο οποίος εμφανίζεται στην οθόνη σε γραφική απεικόνιση, κάτι που ένας άνθρωπος μπορεί να κάνει πολύ εύκολα ενώ είναι πολύ δύσκολο να γίνει από αυτοματοποιημένα συστήματα. Αυτή η απλή διαδικασία ελαχιστοποιεί σχεδόν όλα τα άχρηστα ηλεκτρονικά μηνύματα για δυο λόγους. Πρώτον, γιατί οι spammers συνήθως χρησιμοποιούν ψεύτικες διευθύνσεις απόκρισης οπότε και δεν λαμβάνουν ποτέ τα μηνύματα καταχώρησης αίτησης. Δεύτερον, οι spammers εξαρτώνται από τον αυτοματισμό, και η καταχώρηση απόκρισης δεν μπορεί να αυτοματοποιηθεί.

Το ***SFM*** **[106]** είναι μια συνδρομή στον e-mail server του οποίου η υπηρεσία μπορεί να χαρακτηριστεί ως επέκταση της παραδοσιακής e-mail υπηρεσίας. Επιτρέπει την δημιουργία (κυρίως αυτοματοποιημένα) πολλαπλών διευθύνσεων / ψευδώνυμων για κάθε παραλήπτη αυστηρά και μόνο νόμιμων αποστολέων.

Σχήμα 4 : SFM πρόκληση

Οι αρχικές λειτουργίες είναι πολύ εύκολες. Υπάρχουν δυο τύποι δυναμικών διευθύνσεων: η δημοσιευμένη (*master*) και η ιδιωτική (*ψευδώνυμο).* Ένα ψευδώνυμο είναι σκόπιμα περιορισμένο σε μια επαφή ή σε μια ομάδα. Εάν κάποιος προσπαθήσει να επικοινωνήσει μαζί μας για πρώτη φορά, στέλνει ένα ηλεκτρονικό μήνυμα στην δημοσιευμένη διεύθυνση. Αυτό το μήνυμα ποτέ δεν φτάνει στο προορισμό του, αντίθετα ο αποστολέας λαμβάνει μια πρόκληση όπως το πιο πάνω σχήμα 4:

Ένα νέο ψευδώνυμο παραμένει ακάλυπτο (ανοιχτό) για ένα προκαθορισμένο χρονικό διάστημα και κατά τη διάρκεια αυτής της περιόδου μπορεί οποιοσδήποτε να το χρησιμοποιήσει για να στείλει σ'αυτό μηνύματα. Όποτε συμβαίνει αυτό, η διεύθυνση του αποστολέα προστίθεται στην λίστα επαφών του ψευδώνυμου. Αφού το ψευδώνυμο καλυφθεί (κλείσει), τότε θα δέχεται ηλεκτρονικά μηνύματα από αποστολείς που βρίσκονται στην λίστα επαφών του.

Όταν ένα μήνυμα στέλνεται μέσω του server, εντοπίζει το κατάλληλο ψευδώνυμο του παραλήπτη, εάν δεν υπάρχει αυτό το ψευδώνυμο, παράγει ένα νέο ψευδώνυμο για τον παραλήπτη και διαβιβάζει το μήνυμα στον παραλήπτη όπου αντικαθιστά το ψευδώνυμο αυτό στη διεύθυνση αποστολέων.

Προσεγγίσεις βασισμένες στο περιεχόμενο

Σ' αυτή την κατηγορία καλύπτονται τεχνικές οι οποίες χρησιμοποιούνται για την ανάλυση ενός ηλεκτρονικού μηνύματος σύμφωνα με το περιεχόμενό του. Το θέμα δεν είναι να γίνει πλήρης κατανόηση του περιεχομένου του μηνύματος αλλά περισσότερο να βρεθούν σημαντικά χαρακτηριστικά , όπως η συχνότητα των λέξεων κ.λ.π. Απλές προσεγγίσεις όπως το ταίριασμα των λέξεων κλειδιών (keywords) έχουν εισαχθεί, όπως επίσης και πιο εξελιγμένες προσεγγίσεις οι οποίες συνδυάζουν απλές μεθόδους χρησιμοποιούμενες συνήθως στο γνωστικό πεδίο της ανάκτησης πληροφορίας από κείμενο.

Στατικές τεχνικές

Οι προσεγγίσεις που βασίζονται στις λέξεις- κλειδιά εμπεριέχουν απλές αναζητήσεις τόσο στη γραμμή του θέματος όσο και στην ολότητα του μηνύματος για συγκεκριμένες λέξεις-κλειδιά όπως '*Games*', '*Newsletters*' ή '*get this for free'* . Αν οι λέξεις ή οι φράσεις αυτές εμφανίζονται στην αναζήτησή, αυτός ο τρόπος χρησιμοποιείται ως δείκτης για spam μηνύματα. Αυτοί οι τρεις κύριοι τύποι ταύτισης που βασίζονται στις λέξεις κλειδιά περιγράφονται παρακάτω:

- ***Keyword Based:*** Κατ' αυτόν τον τρόπο γίνεται αναζήτηση για λέξεις ή φράσεις που ταυτίζονται ακριβώς. Για παράδειγμα, η λέξη 'Games' ταιριάζει μόνο με τη λέξη 'Games'.

- ***Pattern matching:*** Καλύπτει απλές παραλλαγές αναμειγνύοντας το σταθερό κείμενο με ευέλικτα χαρακτηριστικά, όπως ειδικούς χαρακτήρες (αστερίσκος ή ερωτηματικό) που μπορούν να αναπαραστήσουν έναν ή περισσότερους χαρακτήρες, χωρίς τη διάκριση πεζών- κεφαλαίων, καθώς και επανάληψη συμβάντων. Έτσι για παράδειγμα η λέξη 'Games' ταυτίζεται με τις λέξεις 'G.a.m.e.s' ή 'GGaammmmeeesss',…

- ***Rule Based:*** Οι κανόνες είναι πιο σύνθετες δομές με τις οποίες ένα μήνυμα μπορεί να εξεταστεί. Για παράδειγμα ο κανόνας 'SUB_Games' ανιχνεύει αν η λέξη 'Games' είναι το κύριο θέμα (είτε ως φράση στην κεφαλίδα του μηνύματος, είτε ως περιεχόμενο σ'αυτό) σ' ένα δοθέν μήνυμα. Αποτελεί μια κοινή πρακτική ο ορισμός μιας συγκεκριμένης τιμής σε κάθε κανόνα και η πρόσθεση όλων αυτών των τιμών προκειμένου να υπολογιστεί ένας συνολικός δείκτης για το spam. Σε τακτά χρονικά διαστήματα οι κανόνες ανανεώνονται προκειμένου να είναι σε θέση να αναγνωρίσουν και να βαθμολογήσουν μηνύματα στα οποία οι spammers εφαρμόζουν νέες τακτικές. Επιπλέον, ο διαχειριστής της υπηρεσίας ηλεκτρονικού ταχυδρομείου ή ο τελικός χρήστης έχει τη δυνατότητα να προσαρμόσει τη βαθμολογία του κάθε κανόνα ώστε να ικανοποιεί τις ανάγκες του ή ακόμα να δημιουργήσει τους δικούς του κανόνες.

Ανάλυση του URL

Η πιο απλή μορφή ανάλυσης του URL είναι εκείνη που περιλαμβάνει το κριτήριο των white και blacklists ενός URL. Ωστόσο, έχουν αναπτυχθεί προσεγγίσεις που είναι πιο εξελιγμένες όπως αυτή που περιγράφεται παρακάτω και περιλαμβάνει το συνδυασμό πολλών τεχνικών.

- ***Filtering spam using Search Engines:*** Πρόκειται για μια προσέγγιση που 'φιλτράρει' τα spam μηνύματα με τη χρήση μηχανών αναζήτησης όπως το Google και το Yahoo. Η κεντρική ιδέα σ' αυτή την περίπτωση είναι το φιλτράρισμα των spam μηνυμάτων με βάση τα URL που εμπεριέχονται μέσα σ' ένα ηλεκτρονικό μήνυμα. Αυτό πραγματοποιείται κατηγοριοποιώντας τα URL μέσω των μηχανών αναζήτησης. Η εν λόγω προσέγγιση ξεχωρίζει τα κατηγοριοποιημένα URLs τα οποία έχουν ήδη ταξινομηθεί ανά κατηγορία από την μηχανή αναζήτησης με τα μη- κατηγοριοποιημένα URLs, τα οποία δεν έχουν ακόμη καταχωρηθεί σε κάποιο κατάλογο του Διαδικτύου.

Αυθεντικοποίηση

Το πρόβλημα που προκύπτει στο θέμα των spam μηνυμάτων είναι η δυσκολία αναγνώρισής τους. Η απάντηση στο συγκεκριμένο πρόβλημα είναι η ύπαρξη ενός τρόπου ώστε να αναγνωρίζονται τα μηνύματα που δεν είναι spam. Η επιλογή της λύσης των whitelists ήταν για αρκετό διάστημα μια πραγματικότητα, αλλά δεν μπορούν να λύσουν ένα σημαντικό πρόβλημα: Το e-mail πρωτόκολλο που χρησιμοποιείται δεν παρέχει χαρακτηριστικά ασφάλειας, αφού ο κάθε αποστολέας μπορεί να καταχωρήσει ότι θέλει ως δική του διεύθυνση.

Digital signature, Encryptions of E-Mail

Μια υποδομή δημοσίου κλειδιού θα μπορούσε να αποτελέσει λύση του παραπάνω προβλήματος. Αν κάθε μήνυμα είχε υπογραφεί μ' ένα ιδιωτικό κλειδί, τότε δεν θα υπήρχε πρόβλημα αυθεντικοποίησης όλων των αποστολέων. Δυστυχώς, και σ' αυτή τη λύση αντιμετωπίζετε ένα μεγάλο πρόβλημα: μόνο ένα μικρό ποσοστό των χρηστών ηλεκτρονικών μηνυμάτων έχει έγκυρη πιστοποίηση. Η δημιουργία μίας υποδομής η οποία επιτρέπει σε κάθε χρήστη mail να χρησιμοποιεί ψηφιακή υπογραφή, θα μπορούσε να αποτελεί μια καλή πρόκληση. Έτσι, έχουν δημιουργηθεί φίλτρα τα οποία βασίζονται στην υπογραφή που προκύπτει μετά από κατάλληλη επεξεργασία για το κάθε μήνυμα. Για να δημιουργηθεί η υπογραφή του κάθε μηνύματος λαμβάνονται υπόψη πέρα από το περιεχόμενο του μηνύματος και διάφορες πληροφορίες που βρίσκονται στην κεφαλίδα του, όπως η ηλεκτρονική διεύθυνση του αποστολέα, η IP διεύθυνση από την οποία ξεκίνησε το μήνυμα καθώς και οι IP διευθύνσεις από τις οποίες πέρασε το μήνυμα προκειμένου να παραδοθεί. Οι υπογραφές των spam μηνυμάτων συγκεντρώνονται σε κατανεμημένες βάσεις και ανανεώνονται σε τακτά χρονικά διαστήματα.

Κάθε φορά που παραλαμβάνεται ένα ηλεκτρονικό μήνυμα υπολογίζεται η υπογραφή του και συγκρίνεται με τις υπογραφές που είναι ήδη γνωστές για μηνύματα που έχουν χαρακτηριστεί ως spam. Αν βρεθεί ότι η υπογραφή αυτού του μηνύματος υπάρχει στη βάση με τις χαρακτηρισμένες ως spam υπογραφές, το μήνυμα χαρακτηρίζεται ως spam ή λαμβάνει μια βαθμολογία. Το τι από τα δύο θα γίνει εξαρτάται από την υλοποίηση που έχει επιλεχθεί.

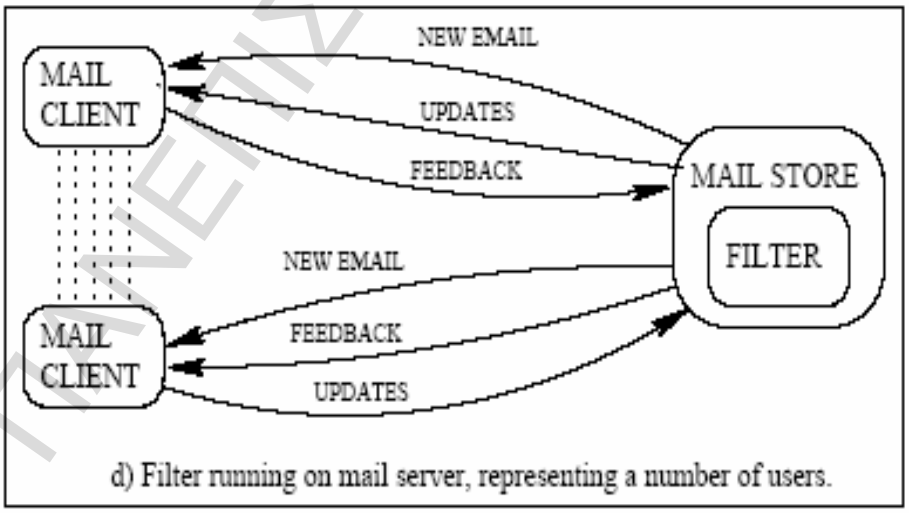
Χαρακτηριστικό παράδειγμα τέτοιου φίλτρου είναι το Vipul's Razor **[107]**. Πρόκειται για ένα κατανεμημένο, συνεργαζόμενο και συνεχώς ανανεώσιμο δίκτυο ανίχνευσης και φιλτραρίσματος ανεπιθύμητης αλληλογραφίας (spam). Με την συμβολή των χρηστών, αλλά και με διευθύνσεις «παγίδες» για τους spammers, συντηρείται μια κατανεμημένη βάση από υπογραφές spam μηνυμάτων. Η αναγνώριση μηνυμάτων με τη χρήση του συγκεκριμένου φίλτρου γίνεται με στατιστικές και τυχαίες υπογραφές οι οποίες αποτελεσματικά εντοπίζουν ακόμα και αλλοιωμένο spam περιεχόμενο.

CASSANDRA

Είναι μία αρχιτεκτονική που βασίζεται στη μέθοδο *Signature Based Filtering*, και επιτρέπει τη δημιουργία εξατομικευμένων συνεργατικών φίλτρων χαρακτηρισμού για spam μηνύματα. Το ονομα του προερχεται απο τα αρχικα (Collaborative Anti-Spam System Allowing Node-Decentralized Research Algorithms) **[108].**

Ο λόγος που οι χρήστες παραλαμβάνουν spam μηνύματα είναι γιατί η διεύθυνσή τους εμπεριέχεται σε λίστες για αποστολή spam. Ως εκ τούτου, ένα καλό εξατομικευμένο συνεργατικό φίλτρο είναι αυτό που παραδίδει σε κάθε έναν χρήστη τις πιο σχετικές πληροφορίες για το αν ένα μήνυμα είναι spam, βασισμένο στην όλη πληροφορία που οι υπόλοιποι χρήστες ενός δικτύου έχουν παράσχει σχετικά με το τι έχουν χαρακτηρίσει ως spam. Επιπλέον, ατομικά για κάθε χρήστη, ο χαρακτηρισμός ενός ηλεκτρονικού μηνύματος ως spam θα πρέπει να γίνεται μόνο για τα μηνύματα που ο ίδιος ο χρήστης θεωρεί ως τέτοια. Έτσι, κάθε φορά που ένα ηλεκτρονικό μήνυμα κατηγοριοποιείται ως spam, η υπογραφή του πρέπει να υπολογίζεται και να διανέμεται στους χρήστες που είναι πιθανό να παραλάβουν το ίδιο μήνυμα. Αυτό το σύνολο χρηστών που αποτελούν μια ομάδα συμμετεχόντων αποτελούν έναν κόμβο (*peer*).

Οι κόμβοι που παραλαμβάνουν μηνύματα μπορούν να συνεργάζονται μεταξύ τους, ανταλλάσσοντας υπογραφές και αποφασίζοντας με ποιους άλλους θα συνεργάζονται και θα ανταλλάσσουν πληροφορίες. Σε αυτή την περίπτωση, οι υπογραφές παίζουν το ρόλο των ταξινομητών (classifiers) των μηνυμάτων. Νέοι ταξινομητές δημιουργούνται ως αποτέλεσμα της ανατροφοδότησης από τους χρήστες για σήμανση ενός μηνύματος ως false positive ή false negative, και προστίθενται στη σχετική βάση ενός κόμβου. Οπότε, με την ανταλλαγή πληροφορίας μεταξύ των κόμβων κάθε νέος ταξινομητής μεταδίδεται και στους γειτονικούς του. Ο μόνος περιορισμός είναι ότι αυτοί οι ταξινομητές πρέπει να είναι εκφρασμένοι σε γλώσσα XML . Σε περίπτωση που ένας κόμβος δεν γνωρίζει τον αλγόριθμο με τον οποίο δημιουργήθηκε ένας ταξινομητής, υπάρχει η υπηρεσία διαχείρισης αλγορίθμων (Algorithm Management Service) η οποία και αναλαμβάνει να βρει και να προσθέσει στον κόμβο την γνώση για τον αντίστοιχο αλγόριθμο. Επίσης, η ίδια υπηρεσία έχει ως ρόλο να διαχειρίζεται το σύνολο των αλγορίθμων που ένας κόμβος χρησιμοποιεί, είναι υπεύθυνη για τη δημιουργία των νέων ταξινομητών και επιπλέον ελέγχει ότι κάθε υπογραφή συγκρίνεται μόνο με τις υπόλοιπες υπογραφές που έχουν υπολογιστεί με τον ίδιο αλγόριθμο.



Σχήμα 5 : Αρχιτεκτονική Cassandra

Η επικοινωνία μεταξύ των κόμβων γίνεται με XML μηνύματα μέσω του πρωτοκόλλου SMTP. Οι κόμβοι (*peers*) επικοινωνούν μεταξύ τους σε τρεις περιπτώσεις:

α) για να γίνουν μέλος ενός δικτύου όπου βρίσκονται ήδη κι άλλοι,

β) για να μοιραστούν πληροφορία αναφορικά με νέους κόμβους (*peers*) και νέους ταξινομητές και

γ) για να ανακαλέσουν έναν ταξινομητή (συνήθως γιατί ο χρήστης το σήμανε ως *false positive*)

Ένας τρόπος υλοποίησης της συγκεκριμένης αρχιτεκτονικής παρουσιαζεται πιο πανω στον σχημα 5.

Bayesian Filtering

Μια τεχνική ιδιαίτερα πρωτοποριακή όπου με την χρήση στατιστικής ανάλυσης και φίλτρα που προσαρμόζονται σε κάθε χρήστη ξεχωριστά γίνεται προσπάθεια προσωποποιημένου φιλτραρίσματος των e-mails βάσει του περιεχομένου τους. Το όνομά τους προέρχεται από τον μαθηματικό Thomas Bayes (1702-1761) και στηρίζονται στον προσδιορισμό της πιθανότητας ένα μήνυμα να είναι spam βάσει των λέξεων/φράσεων που περιέχει και κατά πόσο αυτές εμφανίζονται στα μηνύματα που έχει ήδη λάβει ο συγκεκριμένος χρήστης **[109]**.

9.2 Συνδυασμός μεθόδων – Ολοκληρωμένες λύσεις

Προκειμένου να υλοποιηθούν αποτελεσματικά αντίμετρα στην καταπολέμηση του φαινομένου της ανεπιθύμητης αλληλογραφίας έχουν συνδυαστεί πολλές από τις παραπάνω μεθόδους. Όλες οι εφαρμογές χρησιμοποιούν συνδυασμούς από τις μεθόδους που αναφέρθηκαν προηγουμένως με διαφορετικές παραμετροποιήσεις προκειμένου να αυξήσουν την αποτελεσματικότητας τους.

Στη συνέχεια παρουσιάζεται ο τρόπος λειτουργίας μερικών ολοκληρωμένων μη εμπορικών λύσεων.

9.2.1 SpamGuru

Το πρόγραμμα Spam Guru **[110]** είναι ένα πρόγραμμα αναγνώρισης – διαχείρισης Spam μηνυμάτων το οποίο δίνει δυνατότητα για παραμετροποίηση τόσο από την πλευρά του διαχειριστή όσο και από την πλευρά του τελικού χρήστη.

Κάθε ένα εισερχόμενο μήνυμα που παραλαμβάνεται από τον mail server αναλύεται και του αποδίδεται μια βαθμολογία από 0 έως 1000, όπου το '1000' υποδηλώνει την βεβαιότητα ότι είναι spam.

Αφού αξιολογηθεί το μήνυμα και σε περίπτωση που υπάρχει ένδειξη ότι είναι spam, μπορούν να ακολουθήσουν οι εξής ενέργειες:

α) να διαγραφεί το μήνυμα

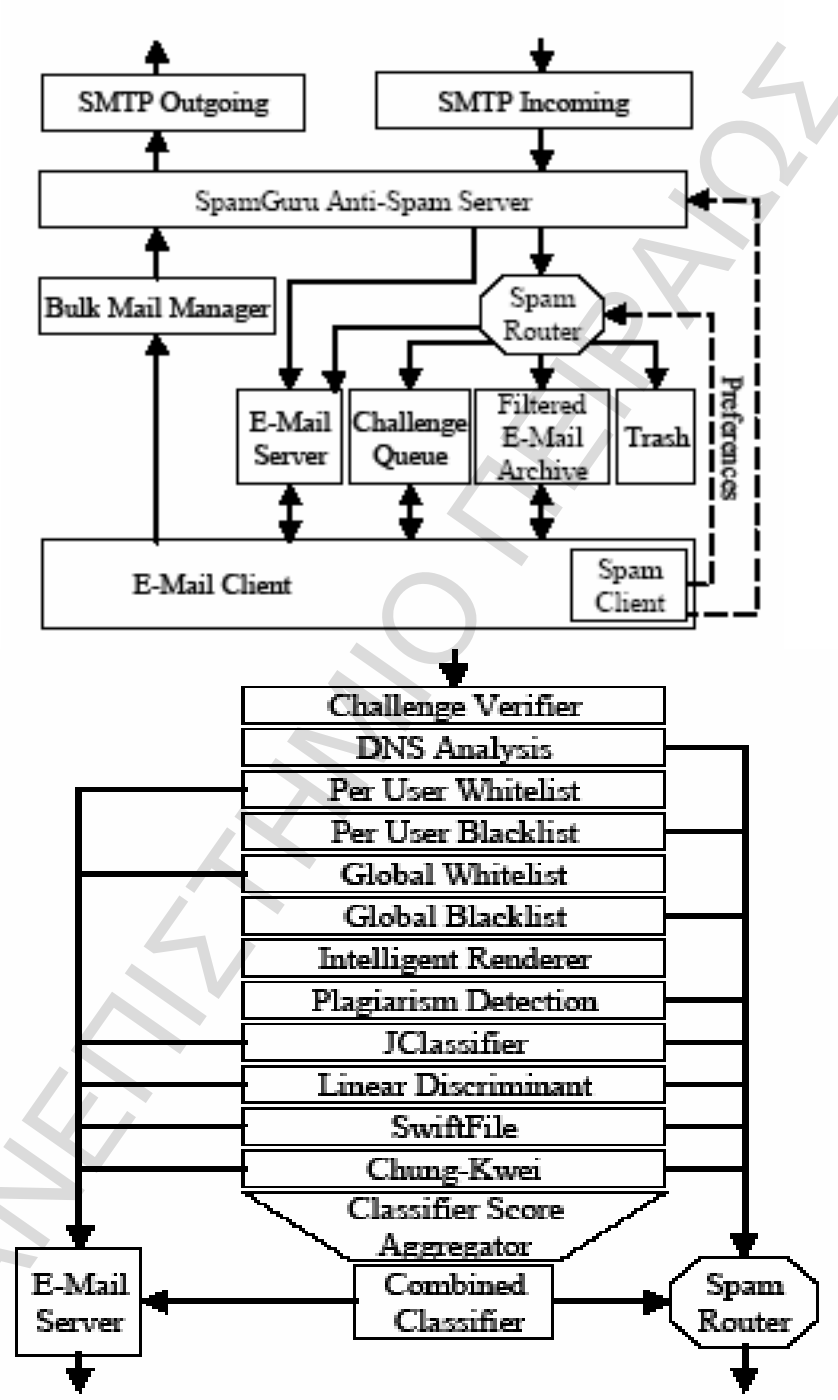
β) να μπει σε ένα αρχείο (archive) με τα πιο πρόσφατα μηνύματα που κρατήθηκαν και δεν προωθήθηκαν στον τελικό αποδέκτη

γ) να μπει σε μια διαδικασία challenge / response, όπου πρώτα θα απαιτηθεί πιστοποίηση της ταυτότητας του αποστολέα πριν προωθηθεί στον τελικό αποδέκτη

δ) να χαρακτηριστεί με μια ένδειξη στον τίτλο ως πιθανό spam και να προωθηθεί στον τελικό παραλήπτη ο οποίος θα πρέπει να αποφασίσει τι θα κάνει με το συγκεκριμένο μήνυμα.

Το συγκεκριμένο πρόγραμμα βελτιστοποιεί τις μεθόδους που έχει για να χαρακτηρίζει τα μηνύματα ως spam ή όχι με τη βοήθεια των χρηστών της υπηρεσίας e-mail, δίνοντάς τους τη δυνατότητα να χαρακτηρίζουν ένα ηλεκτρονικό μήνυμα που παρέλαβαν ως spam ή όχι. Οι απαντήσεις τους δίνονται ως είσοδος στους αλγορίθμους του προγράμματος, με αποτέλεσμα, αν κάποιο συγκεκριμένο μήνυμα το παραλάβουν

π.χ. 4 χρήστες και ο ένας από αυτούς το χαρακτηρίσει spam ενώ οι άλλοι όχι, αυτός ο ένας θα σταματήσει να δέχεται μηνύματα από τον συγκεκριμένο αποστολέα, ενώ οι άλλοι θα συνεχίσουν να τα παραλαμβάνουν. Ένα μήνυμα το οποίο αποδίδεται τελικά στους χρήστες, χρειάζεται να το χαρακτηρίσουν αρκετοί χρήστες ως spam για να σταματήσουν να το λαμβάνουν καθολικά, εισάγοντάς το ουσιαστικά σε μια black list.



Σχήμα 6 : Αρχιτεκτονική Spamguru

Με το που παραλαμβάνεται ένα ηλεκτρονικό μήνυμα από το πρόγραμμα, περνάει διαδοχικά από διαφορετικά φίλτρα. Αρχικά τα φίλτρα – ταξινομητές (classifiers) χρησιμοποιούν δύο δείκτες, έναν για να ορίσουν ότι ένα ηλεκτρονικό μήνυμα είναι spam και ένα για να χαρακτηρίσουν ένα ηλεκτρονικό μήνυμα ως «καλό». Στη δεύτερη

περίπτωση, το μήνυμα μπορεί να παραδοθεί άμεσα στον τελικό παραλήπτη. Στην πρώτη, αν η βαθμολογία είναι αρκετά υψηλή ώστε να μην αφήνει αμφιβολία για τον χαρακτηρισμό του μηνύματος ως spam, δεν γίνεται περαιτέρω επεξεργασία και ακολουθείται όποια πολιτική έχει αποφασιστεί για την διαχείριση των spam. Για τα μηνύματα που έχουν λάβει ενδιάμεση βαθμολογία από τα φίλτρα, συνδυάζονται οι βαθμολογίες όλων των φίλτρων μαζί ώστε να σημανθεί το μήνυμα με έναν χαρακτηρισμό και να αποφασιστεί αν θα δρομολογηθεί στον τελικό χρήστη ή όχι. Σε ιεράρχηση, προηγούνται τα φίλτρα που ελέγχουν τις κεφαλίδες των μηνυμάτων και αυτά που έχουν χαμηλή βαθμολογία στα false positives. Ακολούθως, ελέγχεται αν υπάρχει πιθανότητα το μήνυμα να έχει προέλθει από διεύθυνση που δεν θεωρείται έμπιστη ή που παρουσιάζεται διαφορετική από την πραγματική.

Τέλος το μήνυμα περνάει μέσα από τις white και black lists που έχουν διαμορφωθεί με την βοήθεια του χρήστη.

Επίσης, το Spam Guru μελετάει και την κίνηση της εξερχόμενης αλληλογραφίας με σκοπό να ενημερώνει και να διαμορφώνει τις whitelists του.

Μια τέτοια μελέτη φαίνεται αναλυτικά στο πιο πάνω σχήμα 6.

9.2.2 Filtron

Το Filtron **[111]** είναι ένα learning-based antiSpam φίλτρο.

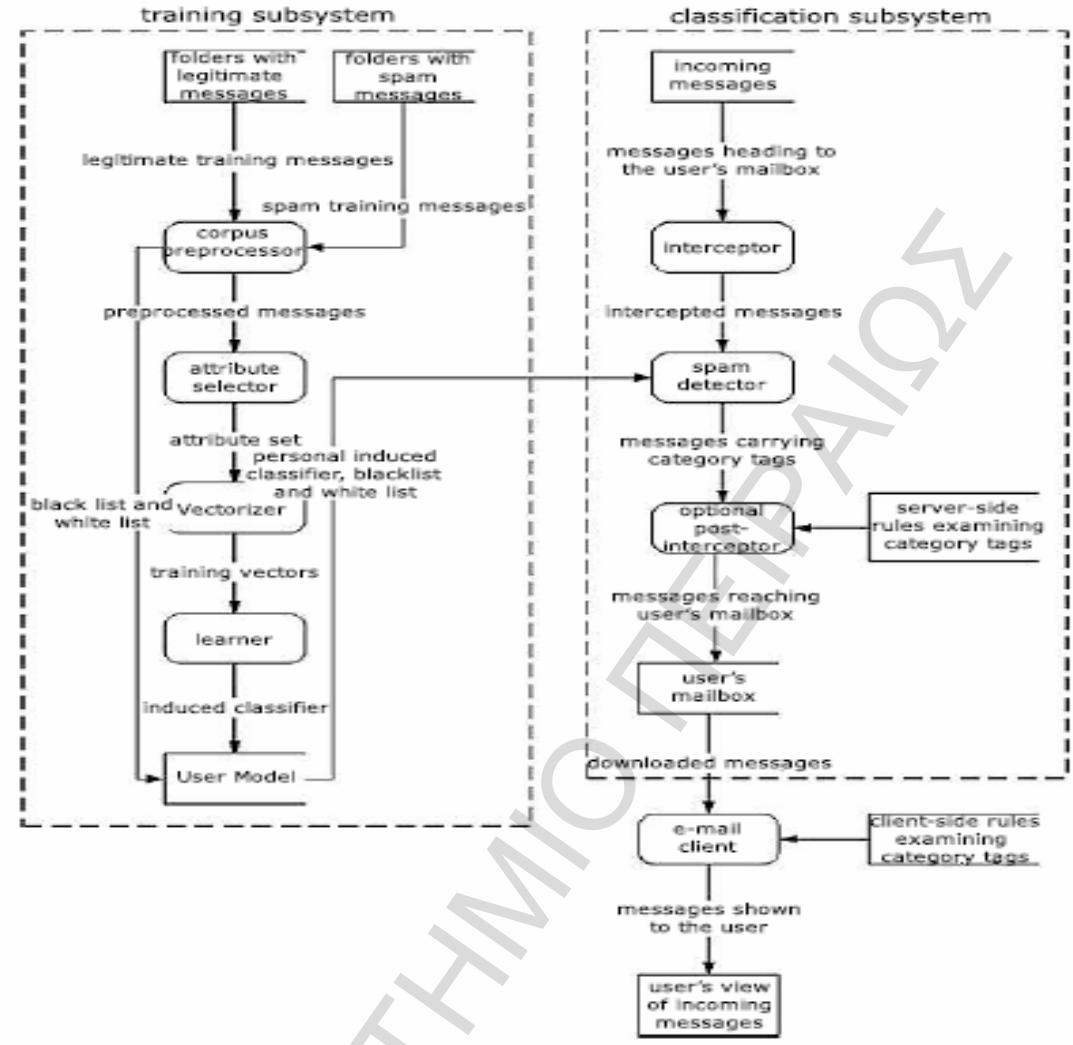
Το Filtron «*μαθαίνει*» να αναγνωρίζει τα μηνύματα του χρήστη δημιουργώντας αντίστοιχα white & black lists είτε χρησιμοποιώντας πραγματικά μηνύματα που αποστάλθηκαν στον χρήστη και αυτός τα χαρακτήρισε ως spam ή όχι, είτε χρησιμοποιώντας ένα δικό του σώμα μηνυμάτων. Κάθε φορά που καταφτάνει ένα μήνυμα για τον χρήστη, γίνεται κατηγοριοποίηση του μηνύματος.

Επίσης, δίνεται η δυνατότητα, οι καταχωρημένες διευθύνσεις από τον χρήστη στο βιβλίο διευθύνσεών του να μπορούν να θεωρηθούν καθαρά ότι ανήκουν στην white list και καμία επεξεργασία να μην γίνεται στα μηνύματα που προέρχονται από αυτές τις διευθύνσεις. Ο χρήστης έχει πρόσβαση να αλλάξει και τις δύο λίστες. Η υλοποίηση του συγκεκριμένου φίλτρου έχει γίνει σε java οπότε και μπορεί να εκτελεστεί στις περισσότερες πλατφόρμες.

Το τμήμα του φίλτρου που κάνει την κατηγοριοποίηση των μηνυμάτων εγκαθίσταται στον mail server και είναι συμβατό με smtp mail servers που συνεργάζονται με Linux.

Ουσιαστικά, η μόνη επέμβαση που γίνεται στο μήνυμα είναι να παραδοθεί με την προσθήκη μιας επισήμανσης π.χ. [*Spam*] στον τίτλο του μηνύματος για όσα μηνύματα θεωρεί ότι είναι spam. Από εκεί και πέρα ο χρήστης μπορεί να φτιάξει κανόνες ώστε να μετακινεί τα μηνύματα που έχουν αυτή τη σήμανση σε άλλους φακέλους.

Για το συγκεκριμένο φίλτρο, η συχνή επανεκπαίδευσή του κρίνεται απαραίτητη, και επίσης είναι ανάγκη να συμπεριληφθεί περισσότερη τεχνική επεξεργασία στα μηνύματα.



Σχήμα 7 : Αρχιτεκτονική Filtron

9.2.3 MailScanner χρησιμοποιώντας SpamAssassin

Πρόκειται για ένα λογισμικό ανοιχτού κώδικα το οποίο παρέχει τη δυνατότητα φιλτραρίσματος μηνυμάτων ηλεκτρονικού ταχυδρομείου **[112]**. Το φιλτράρισμα για το spam βασίζεται στο spamassassin **[113]** και χρησιμοποιείται ήδη από αρκετούς φορείς και οργανισμούς. Υλοποιείται στον mail server αλλά δίνει τη δυνατότητα της διαφορετικής παραμετροποίησης από τον κάθε χρήστη του συστήματος όσον αφορά στη βαθμολογία που δίνει το κάθε φίλτρο που θα χρησιμοποιηθεί.

Όσον αφορά στο spam filtering και ανάλογα με την παραμετροποίηση του συστήματος μπορούν να χρησιμοποιηθούν τα ακόλουθα φίλτρα:

- Rule-Based Filters
- Sender Policy Framework
- Black & White Lists (*τοπικές ή απομακρυσμένες*)
- Signature-Based Filters

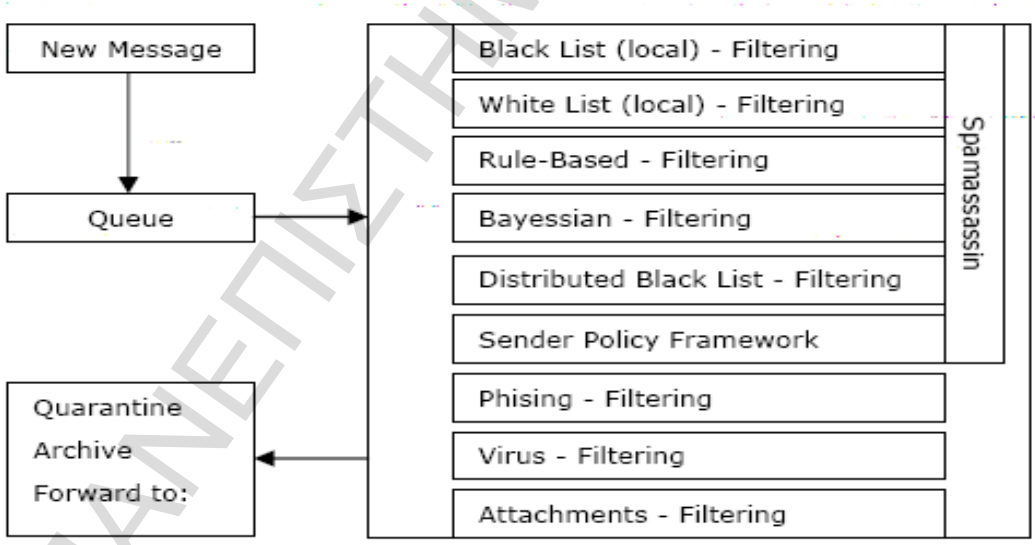
Όταν λαμβάνεται ένα μήνυμα από το σύστημα τότε αυτό τοποθετείται σε μια ουρά προκειμένου να ελεγχθεί. Κατά τον έλεγχο του κάθε μηνύματος εφαρμόζονται όλα τα φίλτρα που έχει ορίσει ο διαχειριστής του συστήματος ή ο τελικός χρήστης. Το κάθε

φίλτρο προσθέτει μια θετική βαθμολογία στο βαθμό που θεωρεί το μήνυμα σαν spam ή μια αρνητική βαθμολογία στο βαθμό που θεωρεί το μήνυμα κανονικό. Στο τέλος όλων των ελέγχων το μήνυμα έχει χαρακτηριστεί από μια καθολική βαθμολογία. Υπάρχουν δύο βαθμολογίες που ορίζονται από τον διαχειριστή του συστήματος. Η πρώτη και μικρότερη από τις δύο είναι η «βάση» που πρέπει να πιάσει ένα μήνυμα για να χαρακτηριστεί σαν spam και η δεύτερη και μεγαλύτερη είναι ένα όριο, όπου τα μηνύματα με μεγαλύτερη βαθμολογία από αυτό είναι σχεδόν βέβαιο ότι είναι spam. Αν το μήνυμα έχει βαθμολογία μικρότερη της βάσης τότε παραδίδεται στους χρήστες χωρίς καμιά επιπλέον επεξεργασία ή αλλαγή. Αν το μήνυμα έχει βαθμολογία μεταξύ πρώτης και δεύτερης τότε υπάρχει η δυνατότητα να προστεθεί στο θέμα του μηνύματος μια διακριτική λέξη ή φράση ώστε να ενημερώνεται ο χρήστης για την κατηγοριοποίηση του μηνύματος. Επιπλέον υπάρχει η δυνατότητα της μη παράδοσης μηνυμάτων με τέτοια βαθμολογία. Αν το μήνυμα έχει βαθμολογία μεγαλύτερη από τη δεύτερη υπάρχει πάλι η δυνατότητα να προστεθεί διακριτική λέξη ή φράση στο θέμα του μηνύματος διαφορετική από την προηγούμενη. Και σε αυτή τη περίπτωση υπάρχει η δυνατότητα της μη παράδοσης του μηνύματος με τέτοια βαθμολογία.

Πέρα από το χαρακτηρισμό του κάθε μηνύματος σαν spam ή όχι, το συγκεκριμένο λογισμικό δίνει τη δυνατότητα της ανίχνευσης Phising μηνυμάτων ελέγχοντας αν οι εμφανιζόμενες υπερσυνδέσεις στο κείμενο του μηνύματος αντιστοιχούν με τους πραγματικούς προορισμούς τους. Και σε αυτή τη περίπτωση διαμορφώνεται το θέμα του μηνύματος κατάλληλα, προκειμένου να δοθεί η δυνατότητα στον τελικό χρήστη να διευθετήσει τέτοιου είδους μηνύματα.

Επιπλέον το MailScanner υποστηρίζει μια πληθώρα εμπορικών ή μη, antivirus μηχανισμών οι οποίοι μπορούν να λειτουργήσουν ταυτόχρονα με τους υπόλοιπους ελέγχους. Επίσης δίνει τη δυνατότητα του φιλτραρίσματος «επικίνδυνων» συνημμένων τα οποία τις περισσότερες φορές είναι ιοί, όπως για παράδειγμα αρχεία με καταλήξεις exe, com, pif, scr, vbs κτλ.

Στο παρακάτω σχήμα αποτυπώνεται η λειτουργία του MailScanner:



Σχήμα 8 : Αρχιτεκτονική MailScanner χρησιμοποιώντας SpamAssassin

9.2.4 Φιλτράροντας εικόνα και κείμενο με το SPAMfighter

Η τελευταία έκδοση του SPAMfighter **[114]** προσφέρει στον χρήστη του καλύτερη ανίχνευση spam εναντίον των τελευταίων μορφών μηνυμάτων spam που μαστίζουν τα email των χρηστών σήμερα.

Ο SPAMfighter συνέχισε να βελτιώνει το μοναδικό του φίλτρο spam με νέες μεθόδους ανίχνευσης των τελευταίων μορφών μηνυμάτων spam εικόνας, καθώς επίσης και άλλα τεχνάσματα που χρησιμοποιούν οι spammers. Αυτό σημαίνει συνολικά καλύτερο φιλτράρισμα για τους χρήστες του SPAMfighter.

«*Αφού εργαστήκαμε πολύ σκληρά για να προλαβαίνουμε τα νέα τεχνάσματα των spammers, βελτιώσαμε σημαντικά το φίλτρο του SPAMfighter, φιλτράροντας τις τελευταίες μορφές μηνυμάτων of spam. Θα συνεχίσουμε την επιμονή μας εναντίον των spammers, προσφέροντας όσο το δυνατόν καλύτερο φιλτράρισμα*»

δηλώνει ο συνιδιοκτήτης και συνιδρυτής Martin Thorborg.

Τα περισσότερα φίλτρα spam που προσφέρονται στο ίντερνετ σήμερα είναι Bayesian φίλτρα. Αυτά τώρα λειτουργούν βάσει κειμένου, αποκλείοντας την δυνατότητα φιλτραρίσματος μηνυμάτων spam εικόνας που είναι η τελευταία μεγαλύτερη απειλή των spammers. Ο SPAMfighter πάντα χρησιμοποιεί ένα μοναδικό βάσει υπογραφής φίλτρο, το οποίο ανιχνεύει και τα μηνύματα spam βάσει κειμένου, καθώς επίσης και αυτά που περιέχουν εικόνες.

Η τελευταία ενημέρωση του SPAMfighter περιέχει σημαντική αναβάθμιση της μηχανής ανίχνευσης spam. Η μηχανή εκτελεί έναν αριθμό τοπικών δοκιμών για να πιάσει ύποπτα email. Αυτό θα αυξήσει τον αριθμό των μηνυμάτων spam που ανιχνεύθηκαν και φιλτραρίστηκαν από τον SPAMfighter.

Ο SPAMfighter βελτίωσε την ανίχνευση των νέων μορφών spam. Ένα παράδειγμα είναι μηνύματα spam που επιχειρούν να αποκρύψουν εικόνες κειμένων, περιστρέφοντας, ή διαιρώντας τις εικόνες σε μορφή παζλ κάνοντάς το δύσκολο για τα φίλτρα spam να το ανιχνεύσουν. Μια άλλη μορφή μηνυμάτων spam περιέχει κείμενο μέσα από τα προσαρτημένα τμήματα εικόνων. Ο SPAMfighter μπορεί τώρα να ανιχνεύσει το κείμενο μέσα σε αυτές τις εικόνες και να τις φιλτράρει όπως χρειάζεται.

Ακόμα ένα παράδειγμα του νέου μηνύματος spam που ο SPAMfighter μπορεί να φιλτράρει είναι εκείνα που επιχειρούν να μιμηθούν την κεφαλίδα του email. Αυτό σημαίνει, ότι πλαστογραφούν την διεύθυνση IP του αποστολέα, ισχυριζόμενοι ότι την στέλνουν από μία εφαρμογή email ενώ την στέλνουν από μια άλλη. Ο πυρήνας της μηχανής του SPAMfighter σχεδιάστηκε για να χρησιμοποιεί την διεύθυνση IP να ενεργοποιεί μια ταξινόμηση spam σε ύποπτα email.

Ο SPAMfighter είναι ένα φίλτρο κοινότητας, που δίνει στους χρήστες την δύναμη να αναφέρουν τα μηνύματα spam. Όταν ένα μήνυμα spam αναφέρεται αρκετές φορές, φιλτράρεται αυτόματα για όλους τους υπόλοιπους χρήστες του SPAMfighter. Επιπρόσθετα, ο SPAMfighter ανιχνεύει μηνύματα spam με την μηχανή πυρήνα κάνοντας χρήση έναν αλγόριθμο spam, προσδιορίζοντας εάν ένα e-mail είναι spam. Με την τελευταία ενημέρωση του SPAMfighter, οι χρήστες προστατεύονται εναντίον των τελευταίων μορφών των μηνυμάτων spam.

Ο SPAMfighter είναι ο προπορευόμενος κατασκευαστής φίλτρων spam στην Ευρώπη Η Δανική εταιρεία ανήκει στους ιδρυτές της εταιρείας Jubii.dk, Henrik Sørensen και Martin Thorborg, μαζί με δύο προγραμματιστές, τους Daniel Hjortholt και Martin Dyring. Η εταιρεία SPAMfighter εδρεύει στην Κοπεγχάγη. Κάθε μέρα, ο SPAMfighter αφαιρεί περίπου 15 εκατομμύρια μηνύματα spam από 20 εκατομμύρια δοκιμασμένα ληφθέντα email από 3.3 εκατομμύρια χρήστες σε 215 χώρες/περιοχές.

Η κινητήρια δύναμη του SPAMfighter είναι το γεγονός ότι πάνω από 3.3 εκατομμύρια χρήστες αναφέρουν spam στην ώρα της λήψης με ένα μόνο κλικ. Όταν αρκετοί χρήστες έχουν αναφέρει το ίδιο μήνυμα spam, φιλτράρεται αυτομάτως από όλους τους υπόλοιπους χρήστες. Το αποτέλεσμα είναι ότι 90 τοις εκατό συνολικό φιλτράρισμα του spam πριν ακόμα φθάσει σε κάποιον άλλο χρήστη.

9.3 Συγκριτική μελέτη των χαρακτηριστικών κάθε μεθόδου

9.3.1 Money based solution

Γενικά, οι μέθοδοι σχετικά με τη χρηματική επιβάρυνση των αποστολέων και βλάβης του επιχειρησιακού πρότυπου των spammers είναι μια πολύ ενδιαφέρουσα και ελπιδοφόρα προσέγγιση για να εξεταστεί το πρόβλημα των spam. Σε αντίθεση με πολλές άλλες προσεγγίσεις που τείνουν να εστιάσουν μόνο στα "συμπτώματα", αυτές προσπαθούν να καταπολεμήσουν το πρόβλημα από "τη ρίζα του". Επιπλέον, τεχνικά είναι πολύ προσιτές σε ISPs και e-mail providers και κατά συνέπεια ταιριάζουν πολύ φυσικά στην φιλοσοφία του ISP. Εντούτοις, υπάρχουν ακόμα μερικές σημαντικές αδυναμίες, που μας οδηγούν να θεωρούμε ότι αυτές οι μέθοδοι μόνο δεν θα αρκέσουν, αλλά μάλλον θα πρέπει να ενσωματωθούν και να συνδυαστούν με άλλες προσεγγίσεις.

Στον τομέα των ***τεχνικών λύσεων***, μια από τις κύριες ερωτήσεις είναι πώς γίνεται η προσαρμογή των λειτουργιών τιμολόγησης σε διαφορετικό hardware. Εκτιμώντας ότι οι *CPU-bound* λειτουργίες τιμολόγησης (όπως *Hashcash*) πάσχουν από μια αδυναμία λόγω των διαφορών στις ταχύτητες επεξεργασίας μεταξύ των διαφορετικών τύπων ηλεκτρονικών υπολογιστικών συστημάτων, μερικοί εμπειρογνώμονες αναμένουν τις *memory-bound* λειτουργίες τιμολόγησης **[92]** οι οποίες θα είναι λιγότερο ευαίσθητες σε αυτό το πρόβλημα.

Για την αξιολόγηση των τεχνικών λύσεων ως προς την αύξηση των δαπανών των αποστολέων, είναι απαραίτητο να αναλυθεί προσεκτικά η οικονομική βάση μιας επιχείρησης των spammers. Εάν μια μείωση από 10 εκατομμύρια μηνύματα ηλεκτρονικού ταχυδρομείου που στέλνονται ανά ημέρα (παραδείγματος χάριν) σε 100.000 μηνύματα ηλεκτρονικού ταχυδρομείου καταστρέφει το επιχειρησιακό πρότυπο ενός spammer, τότε οι μέθοδοι που είναι βασισμένες στις αυξανόμενες δαπάνες αποστολέων θα μπορούσαν να είναι η "*τέλεια*" anti-spam μέθοδος.

Τα κύρια προβλήματα των *money-based solutions* είναι η σχετικά υψηλού κόστους διοίκηση και το γεγονός ότι οι πολύ δημοφιλείς ελεύθεροι e-mail λογαριασμοί δεν αρμόζουν σε αυτήν την στρατηγική.

Το τελευταίο σημείο οδηγεί σε μια πιθανή γενική αδυναμία όλων των προσεγγίσεων όσον αφορά στο αυξανόμενο κόστος του αποστολέα. Η επιτυχία τους θα απαιτούσε κάποιο βαθμό συντονισμού μεταξύ των παροχέων των e-mail υπηρεσιών και την διάπραξη ενός σημαντικού μέρους των provider παγκοσμίως. Εάν μόνο μια μειονότητα των e-mail υπηρεσιών υιοθετήσει πολιτικές αύξησης δαπανών των αποστολέων παγκοσμίως , οι spammers θα αποφύγουν απλά το εμπόδιο και θα επιλέξουν τους προμηθευτές που δεν εφαρμόζουν τέτοιες πολιτικές.

Παρόμοια με την προσεκτική ανάλυση των λειτουργιών τιμολόγησης που απαιτούνται ακόμα και στις τεχνικές λύσεις σχετικά με τις αυξανόμενες δαπάνες αποστολέων, η βέλτιστη δομή αμοιβών στις money-based solutions πρέπει να ερευνηθεί προσεκτικά.

9.3.2 Προσέγγιση βασιζόμενη στην πηγή του ηλεκτρονικού μηνύματος

Οι χαμηλές απαιτήσεις των πόρων και η ευκολία συντήρησής τους είναι τα δύο κύρια οφέλη των blacklists. Οποιοδήποτε μήνυμα spam μπορεί να απορριφθεί, προτού μεταδοθεί. Ένα άλλο μεγάλο πλεονέκτημα είναι ότι οι ηλεκτρονικές διευθύνσεις των spammers διαγράφονται αυτόματα, εάν ένα ηλεκτρονικό μήνυμα απορριφθεί.

Επίσης, ένα μεγάλο μειονέκτημα είναι ότι είτε όλα τα ηλεκτρονικά μηνύματα ενός host γίνονται αποδεκτά, είτε όλα απορρίπτονται. Μερικοί spammers προσπαθούν να κρυφτούν πίσω από μεγάλα ISP's και γι'αυτό χρησιμοποιούν για spamming τα Hotmail ή AOL . Ένα μεγάλο πρόβλημα των blacklists είναι η πιθανή άρνηση τους από το νόμιμο ταχυδρομείο επειδή οι blacklists είναι συχνά ανεπαρκώς συντηρούμενες και μη ενημερωμένες.

Οι περιορισμοί των *whitelists* είναι παρόμοιοι με των *blacklists*. Εάν ένας spammer πλαστογραφήσει μια διεύθυνση, θα μπορέσει να περάσει μέσω ενός whitelist. Πρέπει να αναβαθμίζονται τακτικά κάτι που είναι σχετικά χρονοβόρο, ωστόσο οι black / whitelists σταματούν χαρακτηριστικά περίπου το 10% των spam. **[115]**

Όσον αφορά στα *challenge-response συστήματα*, ένα μεγάλο μειονέκτημα είναι η αυξανόμενη κυκλοφορία του ταχυδρομείου.

9.3.3 Προσέγγιση βασιζόμενη στο περιεχόμενο του μηνύματος

Οι στατικές τεχνικές είναι χρήσιμες ως ένα βαθμό στον ιδιώτη ή ακόμα και σε εταιρικό επίπεδο. Εντούτοις, η λέξη 'Games' μπορεί να ενδιαφέρει ένα παιδί ή ένα γονέα που θέλει να ψωνίσει κάποιο δώρο στο παιδί του, αφού το φιλτράρισμα που βασίζεται σε λέξεις κλειδιά δεν μπορεί να αποτελέσει μία γενικώς αποδεκτή λύση. Η απόδοση θα μπορούσε να αποτελέσει το μόνο πλεονέκτημα σε τέτοιου είδους προσεγγίσεις , παρολ' αυτά ένα επιπλέον μειονέκτημα θα μπορούσε να αποτελεί η ανάγκη ενημέρωσης των λέξεων- κλειδιών.

Όσον αφορά στην προσέγγιση της ανάλυσης του URL, αυτή φαίνεται να είναι πολλά υποσχόμενη. Ωστόσο, εξετάζοντάς την πιο προσεκτικά, και σ' αυτή την μέθοδο συναντάμε πολλά μειονεκτήματα. Πραγματοποιώντας πολλαπλά ερωτήματα σε μια μηχανή αναζήτησης, μπορεί να απαιτηθεί πολύς χρόνος. Αυτό μπορεί να οδηγήσει σ' ένα σημείο όπου οι επιθέσεις άρνησης παροχής υπηρεσίας (denial of service) να σχετίζονται με μηνύματα που περιέχουν μεγάλες ποσότητες URLs οι οποίες με τη σειρά τους αποσυντονίζουν μια ολοκληρωμένη υπηρεσία e-mail.

Η έλλειψη της αυθεντικοποίησης είναι μία από τις μεγαλύτερες αδυναμίες της τωρινής υποδομής e-mail , αλλά η αυθεντικοποίηση από μόνη της δεν θα μπορούσε να αποτελέσει πανάκεια για το πρόβλημα του spam και η αποστολή μαζικών απρόσκλητων μηνυμάτων θα ήταν πιθανή. Η ίδρυση μιας κεντρικής αρχής αυθεντικοποίησης θα μπορούσε να είναι η λύση για ένα ασφαλές περιβάλλον αλλά αυτή η κίνηση δε μοιάζει να είναι ρεαλιστική.

10. Γιατί το Spamming αποτελεί πρόβλημα

Για τους οικιακούς χρήστες η ανεξέλεγκτη ροή απρόσκλητων διαφημιστικών εμπορικών μηνυμάτων, πέρα από ενόχληση συνιστά και απειλή. Το περιεχόμενο των μηνυμάτων αυτών συχνά είναι ακατάλληλο, ενώ δεν είναι καθόλου σπάνιες οι καλά οργανωμένες απάτες. Οι ανήλικοι και οι αφελείς ενήλικοι κινδυνεύουν περισσότερο, χωρίς αυτό να σημαίνει ότι και… πανέξυπνοι διαδικτυακοί περιηγητές δεν πιάστηκαν κορόιδα σε κάποια φάση της ξέγνοιαστης διαδικτυακής τους ζωής.

Το βέβαιο είναι ότι θα πρέπει να υπάρξουν διεθνείς συμφωνίες και συνεργασίες και μια σωστά δομημένη, σε παγκόσμιο επίπεδο, αντί-spam πολιτική, διότι αν αφεθούμε σε λογικές αυτορρύθμισης, τότε, αργά ή γρήγορα η σχέση μας με το ίντερνετ και συγκεκριμένα με το πιο δημοφιλές κομμάτι του, το ηλεκτρονικό ταχυδρομείο, θα απορρυθμιστεί πλήρως.

Ο Steve Linford, διευθυντής της Spamhaus **[116]**, της μεγαλύτερης αντί-spam μη κυβερνητικής οργάνωσης στη Βρετανία, υποστηρίζει ότι ακόμα κι αν ένα μικρό ποσοστό των Αμερικανικών επιχειρήσεων αποφάσιζε να ακολουθήσει τακτικές spamming (δηλαδή την αδιάκριτη και ανεξέλεγκτη αποστολή διαφημιστικών μηνυμάτων, χωρίς καμία ειδική ταξινόμηση ή πληθυσμιακή στόχευση), τότε σε κάθε Ευρωπαίο χρήστη του ίντερνετ θα αναλογούσαν 230.000 spam ηλεκτρονικά μηνύματα την εβδομάδα!

Στις επιχειρήσεις υπάρχει μεγάλη απώλεια χρόνου για το ξεκαθάρισμα της αλληλογραφίας τους, κάτι που προκαλεί σημαντική επιβάρυνση στους δείκτες παραγωγικότητας των εργαζομένων. Οι εργαζόμενοι θα πρέπει, πολλές φορές την ημέρα, να ελέγχουν το mailbox τους, θα πρέπει δηλαδή να ανοίγουν τα μηνύματα που αφορούν την επιχείρησή τους και να διαγράφουν τα μηνύματα spam (που αρκετές φορές αποτελούν την πλειοψηφία…).

Οι περισσότεροι κάνουν πλήρη και χρονοβόρο έλεγχο σε ολόκληρη την αλληλογραφία τους (ανοίγουν και εξετάζουν με προσοχή όλα τα μηνύματά τους), ενίοτε από… περιέργεια, συνήθως όμως για να σιγουρευτούν ότι δεν θα διαγράψουν από λάθος κάτι σημαντικό για την εταιρία τους. Επίσης, χρησιμοποιώντας ειδικά φίλτρα για το spam, ώστε να περιορίσουν κάπως τις συνολικές ποσότητες spam ηλεκτρονικών μηνυμάτων που λαμβάνουν, κάποια από τα μηνύματα που θα ήθελαν να διαβάσουν παίρνουν το δρόμο χωρίς γυρισμό…

Και ενώ οι οικιακοί χρήστες έχουν τη δυνατότητα συχνών αλλαγών των ηλεκτρονικών διευθύνσεών τους (μέσω webmail), αυτό δεν είναι εφικτό για τις επιχειρήσεις, οι οποίες για λόγους κύρους δεν μπορούν να χρησιμοποιήσουν webmail λογαριασμούς, ενώ παράλληλα η ηλεκτρονική διεύθυνση τους αποτελεί ένα ακόμα στοιχείο της επιχειρησιακής τους ταυτότητας. Μια αλλαγή της ηλεκτρονικής τους διεύθυνσης μπορεί να οδηγήσει σε αρκετά λειτουργικά προβλήματα.

Οι συνολικές απώλειες εργατοωρών και το παρεπόμενο κόστος στο σύνολο της οικονομίας φθάνουν σε δυσθεώρητα ύψη. Σύμφωνα με τον αρμόδιο Επίτροπο της Ευρωπαϊκής Ένωσης Erkki Liikanen **[117]**, η απώλεια που προκλήθηκε, λόγω του spam, στην παραγωγικότητα της Ε.Ε. το 2002 ανήλθε στα 2,5 δισεκατομμύρια Ευρώ, ενώ τα συγκεντρωτικά αποτελέσματα για το έτος 2003, ήταν αισθητά υψηλότερα.

Προβλήματα δημιουργεί επίσης και στους *Παρόχους Υπηρεσιών Διαδικτύου (ΠΥΔ)*, καθώς μπορεί να μειώσει την ποιότητα των παρεχόμενων υπηρεσιών και τον χρόνο απόκρισης του δικτύου τους, πλήττοντας έτσι τη διαθεσιμότητα και αξιοπιστία τους.

Επιπλέον, τα μηνύματα spam, εκτός από ενοχλητικά, μπορεί να είναι προσβλητικά, απατηλά ή ακόμα και επικίνδυνου περιεχομένου. Για παράδειγμα αρκετά μηνύματα spam σήμερα διαφημίζουν πλαστά προϊόντα (π.χ. φαρμακευτικά προϊόντα ή προϊόντα λογισμικού) ως προϊόντα γνωστών εταιρειών, διαδίδουν παραπλανητικές ειδήσεις (όπως π.χ. σχετικά με τη "*δύναμη*" συγκεκριμένων μετοχών), ή / και προωθούν προϊόντα και υπηρεσίες σεξουαλικού ή / και πορνογραφικού χαρακτήρα. Επίσης, τα μηνύματα spam χρησιμοποιούνται συχνά και ως μέσα μετάδοσης ιών ή άλλων επιβλαβών ή / και κατασκοπευτικών λογισμικών που σκοπεύουν στην "κατάληψη" του υπολογιστή του χρήστη (ή την μετατροπή του σε *zombie computer*) και την μετέπειτα χρήση του ως μέσο αποστολής νέων μηνυμάτων spam.

Μεγάλη έκταση επίσης έχει πάρει το spam τύπου *phishing* που στοχεύει στην παραπλάνηση των χρηστών και στην εκμαίευση προσωπικών τους δεδομένων, συχνά με απώτερο σκοπό την απάτη και την απόσπαση χρηματικών ποσών μέσω τραπεζικών λογαριασμών.

10.1 Αποφάσεις εναντίον του Spamming

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ Αθήνα, 23-12-2008
Αριθ. Πρωτ.: Γ/ΕΞ/7132/23-12-2008

ΑΠΟΦΑΣΗ 69/2008

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, συνήλθε μετά από πρόσκληση του Προέδρου της σε τακτική συνεδρίαση την 03.07.2008 στο κατάστημά της, αποτελούμενη από τους Χ. Γεραρή, Πρόεδρο, Λ. Κοτσαλή, Α. Πομπόρτση, Α. Παπανεοφύτου, Α. Πράσσο, Α.Ι. Μεταξά, Α. Ρουπακιώτη, τακτικά μέλη. Στη συνεδρίαση, χωρίς δικαίωμα ψήφου, κατά τη συζήτηση του θέματος παρέστησαν ο εισηγητής Γ. Ρουσόπουλος, υπάλληλος του τμήματος Ελεγκτών και η Μ. Γιαννάκη ως γραμματέας, υπάλληλος του Διοικητικού-Οικονομικού Τμήματος, μετά από εντολή του Προέδρου.

Η Αρχή έλαβε υπόψη τα παρακάτω:

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 τηλεηχοπληροφόρησης. 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 προηγείτο 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/ΕΚ 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 "OPOI: 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.

Ο Πρόεδρος Η Γραμματέας

Χρίστος Γεραρής Μ. Γιαννάκη

ΑΠΟΦΑΣΗ 83/2009

Η Αρχή πραγματοποίησε το 2008 επιτόπιο έλεγχο στα γραφεία της εταιρείας "CALINO" Α.Ε. αναφορικά με τη διαδικασία επεξεργασίας προσωπικών δεδομένων που διενεργείται από την εταιρεία. Η Αρχή διαπίστωσε ότι η εταιρεία συνέλεγε διευθύνσεις ηλεκτρονικού ταχυδρομείου από ιστοσελίδες, μια πρακτική που είναι γνωστή ως harvesting. Ειδικότερα, διαπιστώθηκε ότι η εταιρεία πραγματοποιούσε συλλογή διευθύνσεων ηλεκτρονικού ταχυδρομείου από ιστοσελίδες ελληνικών ονομάτων χώρου (domain names) με τη χρήση αυτόματου λογισμικού-αράχνης (web-crawler).

«**Τα στοιχεία αυτά αναρτώνται στις ιστοσελίδες από τους κατόχους τους προς το σκοπό της επαγγελματικής ή προσωπικής επικοινωνίας μαζί τους, όχι για την προώθηση προϊόντων ή υπηρεσιών»**.

Τα στοιχεία αυτά η εταιρεία τα συμπεριέλαβε σε ηλεκτρονικό προϊόν καταλόγου διευθύνσεων, το οποίο πωλούσε σε τρίτους, με σκοπό την πραγματοποίηση στοχευόμενης διαφήμισης εκ μέρους τους. Επίσης, τα στοιχεία αυτά τα χρησιμοποιούσε η ίδια η εταιρεία για την αποστολή διαφημιστικών μηνυμάτων, με τα οποία διαφήμιζε το ως άνω προϊόν της.

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

1. Όσον αφορά τη συλλογή διευθύνσεων ηλεκτρονικού ταχυδρομείου που ανήκουν σε φυσικά πρόσωπα και τη συμπερίληψή τους στο ηλεκτρονικό προϊόν της εταιρείας, επιβλήθηκε πρόστιμο **25.000 ευρώ** και η κύρωση της καταστροφής του αρχείου με τις συλλεχθείσες διευθύνσεις.

2. Επίσης, η εταιρεία υποχρεώθηκε να ενημερώσει όλους τους αγοραστές του προϊόντος ότι περιέχει δεδομένα που δεν είναι νόμιμα και πρέπει να διαγραφούν.

3. Αναφορικά με την αποστολή των μηνυμάτων από την εταιρεία σε όλη τη λίστα διευθύνσεων ηλεκτρονικού ταχυδρομείου και αριθμών τηλεομοιοτυπίας που είχε συλλέξει από το διαδίκτυο και όχι μόνο σε όσους είχαν κάποια προηγούμενη συναλλαγή μαζί της, οπότε και θα αρκούσε σύμφωνα με την παρ. 3 του άρθρου 11 του ν. 3471/2006 η παροχή δυνατότητας αντίρρησης (εναντίωσης) στην περαιτέρω αποστολή τέτοιων μηνυμάτων, επιβλήθηκε επίσης στην εταιρεία πρόστιμο **25.000 ευρώ** .

ΑΠΟΦΑΣΗ 59/2011

Σε άλλη της απόφαση (59/2011) η Αρχή εξέτασε:

1. τη νομιμότητα της συλλογής διευθύνσεων ηλεκτρονικού ταχυδρομείου χωρίς τη συγκατάθεση των υποκειμένων των δεδομένων προς το σκοπό της αποστολής αζήτητης ηλεκτρονικής επικοινωνίας από διάφορες πηγές (συνέδρια και κλαδικές εκθέσεις, στα οποία συμμετείχε ο καταγγελλόμενος υπεύθυνος επεξεργασίας, συλλογή διευθύνσεων ηλεκτρονικού ταχυδρομείου από ιστοσελίδες -πρακτική γνωστή και ως harvesting- συλλογή διευθύνσεων ηλεκτρονικού ταχυδρομείου από αιτήσεις που δέχεται ο υπεύθυνος επεξεργασίας),

2. την ικανοποίηση του δικαιώματος αντίρρησης παραληπτών του ενημερωτικού φυλλαδίου του υπευθύνου επεξεργασίας,

3. την ικανοποίηση των υποχρεώσεων του υπευθύνου επεξεργασίας αναφορικά με συγκεκριμένες διατάξεις του ***ν. 2472/1997*** (***άρθρα 6 και 10***) και

4. την αποστολή μηνυμάτων αζήτητης ηλεκτρονικής επικοινωνίας. Με την εν λόγω απόφαση η Αρχή έκρινε ότι η συλλογή διευθύνσεων ηλεκτρονικού ταχυδρομείου από ιστοσελίδες και οδηγούς κλαδικών εκθέσεων με σκοπό την αποστολή αζήτητης ηλεκτρονικής επικοινωνίας είναι παράνομη.

Για το λόγο αυτό, επέβαλε πρόστιμο ύψους **2.000 ευρώ** στον υπεύθυνο επεξεργασίας για την παράνομη συλλογή διευθύνσεων ηλεκτρονικού ταχυδρομείου,

καθώς και πρόστιμο **2.000 Ευρώ** για την αποστολή αζήτητης επικοινωνίας χωρίς την προηγούμενη συγκατάθεση των συνδρομητών.

ΤΟ ΔΙΚΑΣΤΗΡΙΟ ΤΟΥ ΑΡΕΙΟΥ ΠΑΓΟΥ

Απόφαση **1700 / 2010** (ΣΤ, ΠΟΙΝΙΚΕΣ)
***Θέμα**: Έκδοση.*

Περίληψη:
Έφεση κατ' αποφάσεως του Συμβουλίου Εφετών που διέταξε εκτέλεση Ευρωπαϊκού εντάλματος συλλήψεως της Εισαγγελίας της Βόννης του εκζητουμένου Ουκρανού υπηκόου. Απορρίπτει έφεση.

Συγκροτήθηκε από τους Δικαστές: Αιμιλία Λίτινα, Προεδρεύουσα Αρεοπαγίτη, που ορίσθηκε με τη με αριθμό 101/21.7.2010 Πράξη του Προέδρου του Αρείου Πάγου, ως αρχαιότερο μέλος της συνθέσεως, Ανδρέα Τσόλια, Νικόλαο Κωνσταντόπουλο, Παναγιώτη Ρουμπή και Ανδρέα Ξένο, που ορίσθηκε με τη με αριθμό 104/21.7.2010 Πράξη του Προέδρου του Αρείου Πάγου - Εισηγητή, Αρεοπαγίτες.

Συνήλθε σε δημόσια συνεδρίαση στο Κατάστημά του στις 19 και 26 Οκτωβρίου 2010, με την παρουσία του Αντεισαγγελέως του Αρείου Πάγου Ιωάννη Τζαγκουρνή (γιατί κωλύεται ο Εισαγγελέας του Αρείου Πάγου) και της Γραμματέως Πελαγίας Λόζιου, για να δικάσει την έφεση του εκκαλούντος-εκζητουμένου Χ, Ισραηλινού υπηκόου, κατοίκου ... και προσωρινά κρατουμένου στη Δικαστική Φυλακή ..., ο οποίος παραστάθηκε στο ακροατήριο με τον πληρεξούσιο δικηγόρο του Εμμανουήλ Κουτσούκο, κατά της με **αριθμό 98/2010** απόφασης του Β' Τμήματος Διακοπών του Συμβουλίου Εφετών Δωδεκανήσου. Το Συμβούλιο Εφετών Δωδεκανήσου με την ως άνω απόφασή του αποφάσισε την εκτέλεση του από 9 Ιουλίου 2008 Ευρωπαϊκού Εντάλματος Σύλληψης, που εκδόθηκε από την Εισαγγελία της Βόννης, σε βάρος του ανωτέρω εκζητουμένου. Κατά της αποφάσεως αυτής ο εκζητούμενος και τώρα εκκαλών, άσκησε τη με **αριθμό "69/01.9.2010"** έφεση, για τους λόγους που αναφέρονται σ' αυτήν, η οποία συντάχθηκε ενώπιον της Γραμματέως του Εφετείου Δωδεκανήσου Σταματίας Ζανετούλη και καταχωρίστηκε στο οικείο πινάκιο με τον **αριθμό 1166/2010**. Προκειμένης συζητήσεως Αφού άκουσε τον πληρεξούσιο δικηγόρο του εκκαλούντος-εκζητουμένου, που ζήτησε να γίνει δεκτή η έφεσή του και να μην εκδοθεί και τον Αντεισαγγελέα του Αρείου Πάγου, ο οποίος πρότεινε απορριφθεί η προκειμένη έφεση και να εκτελεστεί το προαναφερόμενο Ευρωπαϊκό Ένταλμα Σύλληψης.

ΣΚΕΦΘΗΚΕ ΣΥΜΦΩΝΑ ΜΕ ΤΟ ΝΟΜΟ

Κατά το ***άρθρο 22 §1 ν.3251/2004*** "Ευρωπαϊκό Ένταλμα Σύλληψης κλπ" σε περίπτωση μη συγκαταθέσεως του εκζητουμένου επιτρέπεται η άσκηση εφέσεως στον Άρειο Πάγο από τον εκζητούμενο ή τον Εισαγγελέα κατά της οριστικής αποφάσεως του Συμβουλίου Εφετών, εντός είκοσι τεσσάρων ωρών από τη δημοσίευση της αποφάσεως, σύμφωνα με τα οριζόμενα του ***άρθρου 451 Κ.Ποιν.Δ***. Για την έφεση συντάσσεται έκθεση ενώπιον του γραμματέα Εφετών στην οποία πρέπει να διατυπώνονται και οι λόγοι για τους οποίους πρέπει να διατυπώνονται ότι ασκείται. Επομένως, η υπό κρίση υπ' **αριθμό 69/1-9-2010**, νομίμως και εμπροθέσμως ενώπιον της αρμοδίας γραμματέως του Εφετείου Δωδεκανήσου ασκηθείσα από τον εκζητούμενο δια του πληρεξουσίου δικηγόρου του έφεση κατά της υπ' **αριθμό 98/31-8-2010** αποφάσεως του Συμβουλίου Εφετών Δωδεκανήσου, με την οποία τούτο αποφάσισε την εκτέλεση του από **9-7-2008** Ευρωπαϊκού εντάλματος συλλήψεως της Εισαγγελίας της Βόννης κατά του ήδη εκκαλούντος εκζητουμένου Χ, πρέπει να γίνει τυπικά δεκτή και να εξετασθεί περαιτέρω κατ' ουσίαν.

Ι. Κατά το ***άρθρο 1 §1 του άνω ν.3251/2004***, το Ευρωπαϊκό ένταλμα συλλήψεως είναι

απόφαση ή διάταξη δικαστικής αρχής κράτους μέλους της Ευρωπαϊκής Ενώσεως που εκδίδεται με σκοπό τη σύλληψη και την προσαγωγή προσώπου, το οποίο ευρίσκεται στο έδαφος άλλου κράτους μέλους της Ευρωπαϊκής Ενώσεως, εφόσον το πρόσωπο αυτό ζητείται από τις αρμόδιες αρχές του κράτους εκδόσεως του εντάλματος στο πλαίσιο ποινικής διαδικασίας:

α) προκειμένου σε πρόσωπο στο οποίο έχει ήδη αποδοθεί η αξιόποινη πράξη να ασκηθεί ποινική δίωξη ή

β) να εκτελεστεί ποινή ή μέτρο ασφαλείας, τα οποία στερούν την ελευθερία. Στο ***άρθρο 2*** του ιδίου νόμου ορίζεται το περιεχόμενο και ο τύπος του Ευρωπαϊκού Εντάλματος

Συλλήψεως, που περιέχει ειδικότερα τα ακόλουθα στοιχεία:

α) την υπηκοότητα και ιθαγένεια του εκζητουμένου,

β) το όνομα διεύθυνση, αριθμό τηλεφωνικής και τηλεομοιοτυπικής συνδέσεως και ηλεκτρονικής διευθύνσεως της δικαστικής αρχής εκδόσεως του εντάλματος,

γ) μνεία της εκτελεστής δικαστικής αποφάσεως, του εντάλματος συλλήψεως ή της συναφούς διατάξεως δικαστικής αρχής,

δ) φύση και νομικό χαρακτηρισμό του εγκλήματος,

ε) περιγραφή των περιστάσεων τελέσεως του εγκλήματος στις οποίες περιλαμβάνονται ο χρόνος και τόπος τελέσεως καθώς και η μορφή συμμετοχής του εκζητουμένου στην αξιόποινη πράξη,

στ) την επιβληθείσα ποινή, αν πρόκειται για αμετάκλητη απόφαση ή το πλαίσιο της ποινής που προβλέπεται για την αξιόποινη πράξη από τη νομοθεσία του κράτους μέλους εκδόσεως του εντάλματος και

ζ) στο μέτρο του δυνατού, κάθε άλλη πληροφορία σχετικά με την αξιόποινη πράξη και τις συνέπειές της.

Εξάλλου, ***κατά το άρθρο 5*** του ιδίου νόμου, το Ευρωπαϊκό ένταλμα σύλληψης, εκδίδεται για πράξεις οι οποίες τιμωρούνται κατά τους Ελληνικού ποινικούς νόμους με στερητική της ελευθερίας ποινή ή με στερητικό της ελευθερίας μέτρο ασφαλείας, το ανώτατο όριο των οποίων είναι τουλάχιστον δώδεκα μηνών ή σε περίπτωση που έχει ήδη επιβληθεί ποινή ή μέτρο ασφαλείας, τα οποία στερούν την ελευθερία για απαγγελθείσες καταδίκες διαρκείας τουλάχιστον τεσσάρων μηνών. Κατά το άρθρο ***10 §1 στοιχ. α'*** του ιδίου νόμου, υπό την επιφύλαξη των όσων ορίζονται στα ***άρθρα 11 έως 13*** αυτού, το Ευρωπαϊκό ένταλμα συλλήψεως εκτελείται εφόσον η αξιόποινη πράξη, για την οποία έχει εκδοθεί τούτο, συνιστά έγκλημα σύμφωνα και με τους Ελληνικούς ποινικούς νόμους, ανεξαρτήτως του νομικού του χαρακτηρισμού, το οποίο τιμωρείται σύμφωνα με το δίκαιο του κράτους εκδόσεως του εντάλματος με στερητική της ελευθερίας ποινή ή με στερητικό της ελευθερίας μέτρο ασφαλείας, το ανώτατο όριο των οποίων είναι τουλάχιστον δώδεκα μηνών. Κατά τα οριζόμενα στην ***παράγραφο 2 του άρθρου 10*** του άνω νόμου, η εκτέλεση του Ευρωπαϊκού εντάλματος συλλήψεως επιτρέπεται χωρίς έλεγχο του διττού αξιοποίνου, για τις αναφερόμενες στην παράγραφο αυτήν αξιόποινες πράξεις, όπως αυτές ορίζονται από το δίκαιο του Κράτους εκδόσεως του εντάλματος, εφόσον τιμωρούνται στο κράτος αυτό, με στερητική της ελευθερίας ποινή ή στερητικό της ελευθερίας μέτρο ασφαλείας, το ανώτατο όριο των οποίων είναι τουλάχιστον τριών ετών, ειδικότερα δε, μεταξύ των άλλων, και για τις αναφερόμενες στην εν λόγω διάταξη υπό στοιχεία

α' εγκληματική οργάνωση,

β' εγκλήματα σχετικά με ηλεκτρονικούς υπολογιστές και απάτη.

Στην προκειμένη περίπτωση, από όλα τα έγγραφα που υπάρχουν στη δικογραφία μεταξύ των οποίων περιλαμβάνονται και τα πρακτικά της πρωτοβάθμιας δίκης στα οποία περιέχονται και οι καταθέσεις των ενόρκως εξετασθέντων μαρτύρων, σε συνδυασμό με όσα εξέθεσε και στο ακροατήριο του Συμβουλίου Εφετών και το παρόν Δικαστήριο ο εκζητούμενος και από όσα ανέφερε ο παραστάς συνήγορός του προφορικώς στο ακροατήριο και με το υποβληθέν από **19-10-2010** υπόμνημά του, προέκυψαν τα ακόλουθα: Το **από 9-7-2008** Ευρωπαϊκό ένταλμα συλλήψεως, που υπογράφεται από τον αναφερόμενο εκπρόσωπο της ανωτέρω Εισαγγελικής Αρχής, εκδόθηκε με βάση το

μνημονευόμενο σ' αυτό από **8-7-2008** υπ' αριθμό φακέλου ***υποθέσεως 20G5 928/08*** ένταλμα συλλήψεως που εκδόθηκε από το Ειρηνοδικείο της Βόννης σε βάρος του ήδη εκκαλούντος. Με αυτό, ο εκζητούμενος διώκεται για δημιουργία και συμμετοχή σε εγκληματική οργάνωση για κατ' επάγγελμα και για κερδοσκοπικούς σκοπούς συμμετοχή σε ηλεκτρονική απάτη, καθώς και για συμμετοχή σε τροποποίηση δεδομένων/στοιχείων, με αναφερόμενη μορφή συμμετοχής αυτή του συνεργού.

Οι ως άνω πράξεις είναι αξιόποινες κατά το Γερμανικό Ποινικό Νόμο ως προβλεπόμενες και τιμωρούμενες από τις διατάξεις των *παραγράφων **129 εδάφιο 1, 263α εδάφιο 1 και εδάφιο 2, 263 εδάφιο 2 και εδάφια 3 αρ. 1 και 5, 303α εδάφιο 1, 22, 23, 25 εδάφιο 2, 52 53 Γερμανικού Ποινικού Κώδικα***.

Οι πράξεις αυτές είναι αξιόποινες και προβλέπονται και τιμωρούνται από τους Ελληνικού ποινικούς νόμους και ειδικότερα ως κακούργημα σύμφωνα με τις διατάξεις των άρθρων:

α) ***187 §1 ΠΚ*** (όπως τροποποιήθηκε με ***το νόμο 2928/2001***, στην συνέχεια με το ***νόμο 3064/2002*** και τελικά με ***το άρθρο 11 του ν.3658/2008*** με κάθειρξη μέχρι 10 ετών η πράξη της συγκρότησης και συμμετοχής σε εγκληματική οργάνωση, με κάθειρξη έως 10 ετών σύμφωνα με τις διατάξεις των ***άρθρων 13 εδάφ. στ', 386 §§ 1, 3, 386 Α του ΠΚ***, η πράξη της απάτης κατ' επάγγελμα και με σκοπό πορισμού περιουσιακού οφέλους άνω των 73.000 ευρώ με επηρεασμό στοιχείων υπολογιστή.

Επίσης, ως πλημμέλημα σύμφωνα με το ***άρθρο 370 Β του ΠΚ***, τιμωρείται με φυλάκιση τουλάχιστον 3 μηνών η παραβίαση στοιχείων ή προγραμμάτων υπολογιστών, ενώ σύμφωνα με τα ***άρθρα 1, 2, 3, 8, 10, 22 §§ 1, 3, 5, 6 ν.2472/1997*** η επεξεργασία, η παραβίαση αυτοματοποιημένων δεδομένων προσωπικού χαρακτήρα τιμωρούνται και πλημμέλημα με φυλάκιση τουλάχιστον ενός έτους αλλά και ως κακούργημα με κάθειρξη στην περίπτωση που ο υπαίτιος είχε σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος ή να βλάψει τρίτον. Από το ένδικο Ευρωπαϊκό ένταλμα συλλήψεως το οποίο προσκομίζεται σε πρωτότυπο και σε μετάφραση στην Ελληνική γλώσσα, επικυρωμένη για την ακρίβειά της από ορκωτή μεταφράστρια, προκύπτει ότι οι πράξεις για τις οποίες διώκεται ο εκζητούμενος προς άσκηση κατ' αυτού ποινικής διώξεως, φέρονται τελεσθείσες κατά το χρονικό διάστημα από **20-9-2006** μέχρι την ημερομηνία εκδόσεως του εντάλματος και συνίστανται, σύμφωνα με όσα αναφέρονται σ' αυτό στο ότι ο εκζητούμενος και οι συγκατηγορούμενοί του Φ με το ψευδώνυμο TNTJ, ... με το ψευδώνυμο ... μαζί με τα παρακάτω άτομα, εμφανιζόμενα με τα ψευδώνυμα ..., δημιούργησαν μαζί μια εγκληματική οργάνωση έχοντας σαν σκοπό τους να νοικιάζουν παγκοσμίως SERVER, να συντάσσουν σελίδες PHISING σε SERVER PHISING, να λειτουργούν BOTNETS για τις παράνομες δραστηριότητές τους, να ιδρύουν εταιρείες με σκοπό την απόκρυψη της χρηματοδοτικής ροής, να έχουν δικούς τους υπαλλήλους για χρηματοπιστωτικές υπηρεσίες εικονικού χρήματος, να διακινούν παγκοσμίως έσοδα μέσω εικονικών τραπεζικών λογαριασμών. Μεταξύ των κατηγορουμένων και των συνεργών τους διαμορφώθηκαν με τον καιρό σταθερές δημιουργημένες δομές στις οποίες ο Φ και ο ήδη εκκαλών εκζητούμενος, θεωρούνται ως ηγετικές μορφές της συμμορίας αυτής. Αυτοί καταλαμβάνουν τη θέση του συντονισμού στα πλαίσια των πράξεών τους. Οι άλλοι κατηγορούμενοι τους υποστηρίζουν εδώ σε σημαντικό βαθμό. Οι κατηγορούμενοι και οι συνεργοί τους ενεργούσαν με βάση ένα κοινό σχέδιο δράσεως. Οι "κεφαλές" της εγκληματικής οργανώσεως είναι σύμφωνα με τα αποτελέσματα των διεξαχθεισών ερευνών οι κατηγορούμενοι Φ και Χ (εκζητούμενος) ενώ οι υπόλοιποι είχαν αναλάβει κατά τη διανομή των καθηκόντων διαφόρους τομείς μεταξύ των οποίων τη διαχείριση και φροντίδα των ιστοσελίδων και των SERVER, τον προγραμματισμό των Τραπεζικών δεδομένων και τη διακίνηση του χρήματος. Οι κατηγορούμενοι ίδρυσαν από κοινού με περαιτέρω συνεργούς των, τα στοιχεία των οποίων δεν έχουν ακόμη εξακριβωθεί, με βάση ένα κοινό σχέδιο δράσεως, μία οργάνωση της οποίας ο σκοπός απέβλεπε στο να εξακριβώσει τους Τραπεζικούς λογαριασμούς και τα στοιχεία προσβάσεως σε τραπεζικούς λογαριασμούς για το ON LINE BANKING πελατών τραπεζών και μάλιστα τον αριθμό λογαριασμού τους, τον κωδικό PIN καθώς και τον αριθμό TAN, έτσι ώστε να μπορούν να χρησιμοποιούν αυτά τα στοιχεία προς όφελός τους για διακινήσεις χρήματος από τους λογαριασμούς των πελατών των τραπεζών. Οι τραπεζικοί λογαριασμοί των πελατών της τράπεζας, ανακαλύπτονταν από τους

κατηγορουμένους με την βοήθεια ενός επιβλαβούς για τον υπολογιστή προγράμματος, κατά το οποίο χρησιμοποιούσαν ένα λεγόμενο "BACKDOOR TROJANER". Αυτό το πρόγραμμα απενεργοποιεί τα προγράμματα προστασίας από ιούς στο κομπιούτερ, αλλάζει στοιχεία και δεδομένα στον υπολογιστή, συλλέγει δεδομένα και στοιχεία και εγκαθίσταται στην εγγραφή. Αυτός ο ιός που λέγεται τρογιάνερ, επεκτείνεται αυτόνομα και "κρυφακούει" στο παρασκήνιο κατά την τυπική διαδικασία μεταφοράς χρήματος/τραπεζικού εμβάσματος ON LINE, όπου "ψαρεύει" αμέσως πριν τη μεταβίβαση των στοιχείων στον υπολογιστή της τράπεζας τον αριθμό του λογαριασμού όπως και τους αριθμούς PIN και TAN του πελάτη, χωρίς ο τελευταίος να παρατηρεί τίποτα από την όλη διαδικασία. Τα στοιχεία που διαπιστώνονταν με τον τρόπο αυτό, χρησιμοποιούνταν αργότερα για τραπεζικά εμβάσματα, τα προγράμματα δε αυτά επεκτείνονταν σε συνημμένο αρχείο που στέλνονταν μέσω e-mail, στα πλαίσια των ΄΄SPAM - e-mails΄΄, όπου αντίστοιχα e-mails στέλνονταν σε έναν αόριστο αριθμό παραληπτών. Οι παραλήπτες παρακινούνταν σε αυτά τα e-mails να ανοίξουν το συνημμένο αρχείο με απατηλές οδηγίες. Με το άνοιγμα του συνημμένου αρχείου από τον παραλήπτη κολλούσε το σύστημά του με τον ιό του προγράμματος αυτού χωρίς να το καταλάβει ο παραλήπτης και τα στοιχεία τραπεζικής πρόσβασης και συνδιαλλαγής κατά το ON LINE BANKING γινόταν γνωστά μέσω του προγράμματος, καταγράφονταν και στη συνέχεια χρησιμοποιούνταν στα συστήματα υπολογιστών και στις τράπεζες δεδομένων των κατηγορουμένων και των συνεργών τους, με σκοπό τη διεξαγωγή αδικαιολογήτων εμβασμάτων τραπέζης από τους λογαριασμούς των θυμάτων. Οι κατηγορούμενοι και οι συνεργοί τους, χρησιμοποιούσαν τα στοιχεία αυτά και διενεργούσαν εμβάσματα στα πλαίσια του ON LINE BANKING, χρησιμοποιώντας τον αριθμό τραπεζικού λογαριασμού καθώς και τους αριθμούς προσβάσεως PIN και TAN από τους λογαριασμούς των θυμάτων, μεταφέροντας τα χρήματα σε λογαριασμούς κάποιων "χρηματοδοτικών πρακτόρων", τους οποίους είχαν πριν προσλάβει και στρατολογούσαν οι κατηγορούμενοι σε τακτά χρονικά διαστήματα. Οι κατηγορούμενοι εμφανίζονταν στο διαδίκτυο ως επιχείρηση με παγκόσμιες δραστηριότητες, ισχυριζόμενοι ότι ζητούν συνεργάτες για υπηρεσίες εμβασμάτων παγκοσμίως. Οι χρηματοδοτικοί πράκτορες είχαν ως καθήκον να μεταβιβάζουν χρήματα που παρελάμβαναν, από τα οποία έπαιρναν κάποια προμήθεια και το μόνο που έπρεπε να κάνουν ήταν να θέτουν τον αριθμό του τραπεζικού τους λογαριασμού στη διάθεση των εργοδοτών τους. Για την πρόσληψη των πρακτόρων αυτών γινόταν χρήση των σελιδων SCHNELL-POST, COM, SCHWEITZER - GELDTANSFER-DIENST.COM, FAST-CASH-UNION.COM και INTERNETDOLLAR.NET με τις διευθύνσεις e-mail: domains@modestus.org ή TDZ@ modestus.org, οι οποίες είχαν συσταθεί και χρησιμοποιούνταν από τους ίδιους. Οι κατηγορούμενοι μεταβίβαζαν στους χρηματοδοτικούς πράκτορες χρηματικά ποσά, τα οποία έπαιρναν από τους τραπεζικούς λογαριασμούς των θυμάτων και τους έδιναν την εντολή, να κάνουν έμβασμα των χρημάτων που πήγαιναν στον λογαριασμό τους, μετά την αφαίρεση της προμήθειάς τους, μέσω της χρηματοδοτικής υπηρεσίας "WESTERN UNION" σε συγκεκριμένα άτομα στη ... ή στην .... Ένα μεγάλο μέρος των χρημάτων αυτών μεταφερόταν στη συνέχεια μέσω εμβάσματος σε λογαριασμούς στο εξωτερικό ή σε εικονικούς λογαριασμούς τρίτων ατόμων. Από εκεί ακολουθούσαν πληρωμές στους λογαριασμούς των κατηγορουμένων οι οποίοι είχαν πλέον τα χρήματα στη διάθεσή τους. Στα πλαίσια των διεξαχθεισών ερευνών προέκυψε ότι λόγω των ιστοσελίδων ζήτησης πρακτόρων προσλήφθηκαν άτομα, τα οποία δραστηριοποιήθηκαν στον τομέα αυτόν από τις **20.9.2006** (INTERNETDOLLAR.NET) έως τις **10.11.2007** (SCHEWEITZER-GELDTRANFER-DEINST.DE) και σε 21 περιπτώσεις μετέφεραν επιτυχώς τα χρήματα, τα οποία είχαν "ψαρέψει" στο εξωτερικό. Σε 26 περιπτώσεις κατέστη δυνατό τα χρήματα αυτά να επιστραφούν από τον τραπεζικό λογαριασμό του πράκτορα στους ιδιοκτήτες τους. Συνολικά "ψαρεύτηκε" το ποσό των **287.783 ευρώ**. Το συνολικό ύψος των χρηματικών ποσών τα οποία μεταφέρθηκαν στο εξωτερικό μέσω της "WESTERN UNION" και δεν είναι δυνατόν να επιστραφούν ανέρχεται σε **110.182 ευρώ**. Ο εκζητούμενος, συνεπώς, σύμφωνα με όσα πραγματικά περιστατικά αναφέρονται στο άνω ευρωπαϊκό ένταλμα συλλήψεως είχε συμμετοχή στις πιο πάνω αξιόποινες πράξεις, οι οποίες φέρονται ότι τελέσθηκαν στην ... και σε άλλα μέρη, ως συναυτουργός. Για αυτές τις πράξεις (όπως χαρακτηρίζονται από το Γερμανικό Ποινικό Νόμο) δηλαδή της δημιουργίας εγκληματικής και συμμετοχής σε αυτήν, της κατ' επάγγελμα και για κερδοσκοπικούς σκοπούς

ηλεκτρονικής απάτης και της τροποποιήσεως δεδομένων/στοιχείων η μέγιστη διάρκεια της στερητικής της ελευθερίας ποινή που μπορεί να επιβληθεί κατά του υπαιτίου σύμφωνα με τον Γερμανικό Ποινικό Κώδικα, είναι δεκαπέντε ετών. Κατά τους Ελληνικούς ποινικούς νόμους, ανεξαρτήτως νομικού χαρακτηρισμού τους αυτές οι αξιόποινες πράξεις τιμωρούνται με στερητικές της ελευθερίας ποινές το ανώτατο όριο των οποίων υπερβαίνει για όλες τους δώδεκα μήνες.

Το άνω Ευρωπαϊκό ένταλμα συλλήψεως φέρει στο πρωτότυπό του ημεροχρονολογία εκδόσεως, όνομα και υπογραφή του Εισαγγελέα που το υπέγραψε ως εκπρόσωπος της Εισαγγελικής Αρχής και περιέχει (στο πρωτότυπο και τη μετάφρασή του) όλα τα στοιχεία που προβλέπονται από το ***άρθρο 2 ν.3251/2004*** (ταυτότητα και ιθαγένεια του εκζητουμένου, όνομα και διεύθυνση και λοιπά στοιχεία της δικαστικής αρχής του Κράτους εκδόσεως του εντάλματος, μνεία του από 8.7.2008 με αριθμό **φακέλου 50 Gs 928/08** εντάλματος του Ειρηνοδικείου Βόννης, στο οποίο βασίσθηκε η έκδοση του ελεγχόμενου εντάλματος, φύση και νομικό χαρακτηρισμό των αξιοποίνων πράξεων που αποδίδονται στον εκζητούμενο, περιγραφή των περιστάσεων τελέσεων των εγκλημάτων στις οποίες περιλαμβάνονται ο χρόνος και ο τόπος τελέσεως, το πλαίσιο της ποινής που προβλέπεται για τις πράξεις αυτές από το Κράτος εκδόσεως του εντάλματος και άλλες σχετικές πληροφορίες σχετικά με τη φύση και τις συνέπειές τους και συνεπώς πληρούσε τις προϋποθέσεις του ***άρθρου 6 παρ. 1 του Συντάγματος*** και της τυπικής νομιμότητάς του κατά ***το ν.3251/2004***.

Οι πράξεις για τις οποίες ζητείται η παράδοση του ήδη εκκαλούντος - εκζητουμένου στις αρμόδιες δικαστικές αρχές της Γερμανίας στη Βόννη προκειμένου να ασκηθεί ποινική δίωξη σε βάρος του ανήκουν σε εκείνες τις αξιόποινες πράξεις για τις οποίες κατά το ***άρθρο 10 παρ. 2 περ. α', ια', κ' του ν.3251/2004*** επιτρέπεται η εκτέλεση του Ευρωπαϊκού εντάλματος συλλήψεως χωρίς έλεγχο του διττού αξιοποίνου αφού συντρέχει εν προκειμένω η προϋπόθεση να τιμωρούνται στο κράτος εκδόσεως του εντάλματος με στερητική της ελευθερίας ποινή ή αντίστοιχο μέτρο ασφαλείας τουλάχιστον τριών ετών. Επί πλέον οι εν λόγω πράξεις περιλαμβάνονται και σε εκείνες για τις οποίες κατά το ***άρθρο 10 παρ. 1α*** σε συνδυασμό με το ***άρθρο 5*** του ίδιου άνω ***ν.3251/2004*** επιτρέπεται η έκδοση και η εκτέλεση του Ευρωπαϊκού εντάλματος συλλήψεως για τη σύλληψη και παράδοση ενός προσώπου από ένα κράτος μέλος της Ευρωπαϊκής Ενώσεως σε άλλο κράτος μέλος αυτής προκειμένου να ασκηθεί ποινική δίωξη για την πράξη που του έχει αποδοθεί εφόσον τιμωρούνται κατά τους ελληνικούς ποινικούς νόμους αλλά και σύμφωνα με το δίκαιο του Κράτους εκδόσεως του εντάλματος με στερητική της ελευθερίας ποινή το ανώτατο όριο των οποίων είναι τουλάχιστον δώδεκα μηνών, δεν συντρέχει δε στην κρινόμενη υπόθεση ουδεμία των περιπτώσεων υποχρεωτικής ή δυνητικής μη εκτελέσεως του Ευρωπαϊκού εντάλματος συλλήψεως που προβλέπονται ***στα άρθρα 11 και 12 του ν.3251/2004***.

Κατά συνέπεια συντρέχουν στην προκειμένη περίπτωση οι νόμιμες προϋποθέσεις για την εκτέλεση του ανωτέρω Ευρωπαϊκού εντάλματος συλλήψεως όπως και το Συμβούλιο Εφετών Δωδεκανήσου ορθώς κρίνοντας δέχθηκε. Δεν επηρεάζεται η πληρότητα και η εγκυρότητα του ενδίκου Ευρωπαϊκού εντάλματος συλλήψεως, το οποίο περιέχει όλα τα από το ***άρθρο 2 του ν.3251/2004*** απαιτούμενα στοιχεία από το ότι δεν είναι ενάριθμο, αλλά προσδιορίζεται με βάση την ημερομηνία εκδόσεώς του (**9.8.2008**). Για την εκτέλεση του ως άνω Ευρωπαϊκού Εντάλματος Συλλήψεως ελήφθη υπόψη από το Συμβούλιο Εφετών το ευρισκόμενο στη δικογραφία πρωτότυπο του εντάλματος αυτούς και η νόμιμη μετάφρασή του στην Ελληνική που περιλαμβάνεται στα αναγνωσθέντα κατά τη διαδικασία στο ακροατήριο έγγραφα και είναι απορριπτέα ως αβάσιμα όσα αντίθετα υποστηρίζονται από τον ήδη εκκαλούντα με το σχετικό λόγο εφέσεως. Επομένως πρέπει να απορριφθεί κατ' ουσίαν η κρινόμενη έφεση και να καταδικασθεί ο εκκαλών στα δικαστικά έξοδα (583 παρ. 1 Κ.Ποιν.Δ.).

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Δέχεται τυπικά και Απορρίπτει κατ' ουσίαν την **από 1.9.2010 έφεση** του Χ, που γεννήθηκε **στις 11.6.1973** στο DONEC Ουκρανίας, κατά της **98/2010** αποφάσεως του Συμβουλίου Εφετών Δωδεκανήσου με την οποία αποφασίστηκε η εκτέλεση κατ'αυτού του

από **9.7.2008** Ευρωπαϊκού Εντάλματος Συλλήψεως που εκδόθηκε από την Εισαγγελία της Βόννης Γερμανίας.

Καταδικάζει τον εκκαλούντα στα δικαστικά έξοδα που ανέρχονται σε διακόσια είκοσι (220) ευρώ.
Κρίθηκε και αποφασίσθηκε στην Αθήνα στις 26 Οκτωβρίου 2010.
Δημοσιεύθηκε στην Αθήνα, σε δημόσια συνεδρίαση, στο ακροατήριό του στις 26 Οκτωβρίου 2010.

Η ΠΡΟΕΔΡΕΥΟΥΣΑ Η ΓΡΑΜΜΑΤΕΑΣ

Εξαρθρώθηκε διεθνές κύκλωμα spam [118]

Στην καταβολή προστίμου 15 εκατομμυρίων δολαρίων καταδικάστηκε από δικαστήριο στις ΗΠΑ ο «εγκέφαλος» ενός διεθνούς δικτύου spam. Πρόκειται για τον Lance Atkinson από τη Νέα Ζηλανδία, ο οποίος μαζί με τον Αμερικανό συνεργό του, Jody Smith, έστειλαν δισεκατομμύρια παράνομα e-mail διαφημίζοντας φάρμακα και χάπια αδυνατίσματος, τα οποία, όπως ισχυρίζονταν, ήταν αντίγραφα σκευασμάτων που κυκλοφορούν στις ΗΠΑ. Η απόφαση είναι αποτέλεσμα έρευνας της Ομοσπονδιακής Επιτροπής Εμπορίου, η οποία αποκάλυψε το διεθνές δίκτυο με το οποίο λειτουργούσε η συγκεκριμένη σπείρα με το όνομα «HerbalKing».

Η σπείρα δρούσε από το 2005 και στην κορυφή της δράσης τους εκτιμάται ότι έστελναν το ένα τρίτο των spam e-mails που στέλνονται παγκοσμίως.

Όχι στο φιλτράρισμα για πειρατικό υλικό από τα κοινωνικά δίκτυα λέει το Ευρωπαϊκό Δικαστήριο

Τα κοινωνικά δίκτυα δεν είναι υποχρεωμένα να εγκαθιστούν συστήματα για τον εντοπισμό και το φιλτράρισμα του πειρατικού περιεχομένου που δημοσιεύουν οι χρήστες τους, αποφάνθηκε το Ευρωπαϊκό Δικαστήριο στο Λουξεμβούργο. Ο λόγος, σύμφωνα με την απόφαση, βρίσκεται στο ότι η εγκατάσταση τέτοιων φίλτρων παραβιάζει την ιδιωτική ζωή των χρηστών και είναι αντίθετη στην αρχή της ελεύθερης διακίνησης της πληροφορίας. Επιπλέον, δεν είναι και οικονομικά βιώσιμη λύση, αφού η εγκατάσταση και συντήρηση ενός τέτοιου συστήματος επιβαρύνει τις υπηρεσίες κοινωνικής δικτύωσης με υπέρογκα κόστη.

Η απόφαση **[119]** προήλθε μετά από την εκδίκαση υπόθεσης κατά την οποία η βελγική **SABAM**, που ασχολείται με την προστασία των πνευματικών δικαιωμάτων καλλιτεχνών, απαίτησε από το κοινωνικό δίκτυο **Netlog** να σταματήσει τους χρήστες της από το να διακινούν παράνομο υλικό. Η βελγική Δικαιοσύνη παρέπεμψε την υπόθεση στο Ευρωπαϊκό Δικαστήριο, το οποίο τελικά δικαίωσε το Netlog και τους 95 εκατομμύρια συνδρομητές του.

Πρόκειται για μια ενδιαφέρουσα απόφαση, που έρχεται σε κρίσιμο χρονικό σημείο, αφού τόσο τα νομοσχέδια SOPA / PIPA, όσο και η συνθήκη ACTA έχουν φέρει σε πρώτο πλάνο παγκοσμίως το ζήτημα της ελευθερίας της έκφρασης στο διαδίκτυο.

11. Συμπεράσματα

Το φαινόμενο της ανεπιθύμητης αλληλογραφίας ή αλλιώς spam αποτελεί μια μεγάλη πληγή στην ηλεκτρονική αλληλογραφία και προκαλεί '*πονοκέφαλο*' τόσο στην επιστημονική κοινότητα όσο και στους τελικούς χρήστες του ηλεκτρονικού ταχυδρομείου. Μέσα σε μια προσπάθεια αντιμετώπισης της αδυναμίας αυτής, έχουν προταθεί κατά καιρούς διάφορες νομικές διατάξεις και μέθοδοι αντιμετώπισής του. Οι διατάξεις και οι μέθοδοι αυτές περιλαμβάνουν τόσο την αναγνώριση των spam μηνυμάτων όσο και την παρεμπόδιση αποστολής τους στο ηλεκτρονικό γραμματοκιβώτιο των τελικών χρηστών.

Στην διπλωματική αυτή, ο στόχος ήταν να τονιστεί πόσο οι νομοθετικές προσεγγίσεις μπορούν να βοηθήσουν στην καταπολέμηση των αυτόκλητων ηλεκτρονικών μηνυμάτων, και να συγκριθούν οι νομοθετικές προσεγγίσεις σε ΗΠΑ και Ευρωπαϊκή Ένωση.

Όπως αναφέρθηκε παραπάνω, η αντι-spam νομοθεσία αντιμετωπίζει ορισμένα προβλήματα, όπως η εισβολή στην ιδιωτική ζωή των συνδρομητών από τα ανεπιθύμητα αυτόκλητα μηνύματα για άμεσους εμπορικούς σκοπούς, όπως επίσης παρέχει σαφείς οδηγίες για ψευδείς ταυτότητες ή επιστροφές ψευδών διευθύνσεων. Ωστόσο, αρκετή δουλειά χρειάζεται ακόμα να γίνει προκειμένου να αντιμετωπιστεί το πρόβλημα.

Όσον αφορά τις τεχνικές μεθόδους αντιμετώπισης των spam. Η κάθε μέθοδος ξεχωριστά αντιμετωπίζει (αναγνωρίζει ή περιορίζει) ως ένα βαθμό το spam ωστόσο καμία δεν αντιμετωπίζει το πρόβλημα από τη γένεση του.

Έτσι, τα αντίμετρα που χρησιμοποιούνται τόσο από τους διαχειριστές των ηλεκτρονικών ταχυδρομείων όσο και από τους τελικούς χρήστες, αν και περιλαμβάνουν συνδυασμό των μεθόδων που περιγράφηκαν στην παρούσα διπλωματική, δεν εξαλείφουν το πρόβλημα. Κύρια αιτία για αυτή την κατάσταση αποτελεί το γεγονός ότι οι spammers συνεχίζουν να βρίσκουν συνεχώς εναλλακτικούς τρόπους προσέγγισης του θέματος, όντας πάντα ένα βήμα μπροστά στο ζήτημα της ανεπιθύμητης αλληλογραφίας και αιφνιδιάζοντας δυσάρεστα την απέναντι πλευρά.

Όσον αφορά στα οφέλη που έχουν οι spammers λόγω των μηνυμάτων ανεπιθύμητης αλληλογραφίας, αυτά είναι πολλά και ιδιαίτερα δελεαστικά αφού ως κύριο γνώμονά τους έχουν το χρηματικό κέρδος με ελάχιστο έως μηδαμινό κόστος. Απ΄την πλευρά όμως των τελικών χρηστών και των διαχειριστών του ηλεκτρονικού ταχυδρομείου το spam κοστίζει τόσο χρηματικά όσο και ηθικά. Πιο συγκεκριμένα, χάνονται ανθρωποώρες, πολύτιμοι πόροι στα υπολογιστικά συστήματα αλλά επιπλέον διαστρεβλώνεται και η φήμη του ηλεκτρονικού ταχυδρομείου, μιας υπηρεσίας που έχει γράψει τη δική της ιστορία στο χώρο του Internet. Επιπλέον, η ‘εφεύρεση - spam’ επιφέρει κοστολογικά έξοδα ακόμα και στην περίπτωση που κάποιοι προβούν στην αντιμετώπισή της.

Έτσι, τα αντίμετρα πέραν του ότι κοστίζουν χρηματικά για την εφαρμογή τους, δημιουργούν κι ένα επιπλέον κόστος, του οποίου το αποτέλεσμα είναι υπολογιστικά δύσκολο να εξαχθεί. Πρόκειται για το κόστος σχετικά με την λάθος απόρριψη ενός κανονικού μηνύματος ή με την αποδοχή ενός spam λόγω λανθασμένου χαρακτηρισμού. Το κόστος αυτό, δεν μπορεί να υπολογιστεί ωστόσο μπορεί να είναι από πολύ μικρό έως πολύ μεγάλο και εξαρτάται κάθε φορά από την περίπτωση.

Συνοψίζοντας, συμπεραίνεται πως χρειάζεται αρκετή δουλεία ακόμα για την αντιμετώπιση του φαινόμενου των spam μηνυμάτων. Η μεμονωμένη νομοθεσία δεν είναι σε θέση να εξαλείψει το φαινόμενο αυτό. Αυτό που απαιτείται είναι μια ενιαία προσέγγιση, ενσωματώνοντας τους αποτελεσματικότερους μηχανισμούς, διασυνοριακή συνεργασία, εκπαίδευση των καταναλωτών, των επιχειρήσεων και της βιομηχανίας, συνδυασμένη με την αποτελεσματική εφαρμογή προηγμένων τεχνικών λύσεων. Με την συνεργασία μεταξύ των αντι-spam ομάδων, των νομοθετικών οργάνων, των γνωμοδοτικών συμβούλων, και των ISPs (φορέα παροχής υπηρεσιών) για μια κοινή συντονισμένη δράση, μπορεί να επιτευχθεί ο αποτελεσματικότερος τρόπος καταπολέμησης και εξάλειψης του φαινόμενου των spam μηνυμάτων.

12. Πηγές & Πληροφορίες

[1] Spam (electronics) – Wikipedia, the free encyclopedia
http://en.wikipedia.org/wiki/spam_(electronic)#History

[2] Πρόγονος του σημερινού Internet.

[3] Εκτιμάται ότι το 80 με 85% των μηνυμάτων ηλεκτρονικής αλληλογραφίας σε παγκόσμιο επίπεδο αποτελεί spam. (πηγή: Wikipedia, http://en.Wikipedia.org/wiki/Spam_(electronic)).

[4] 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», άρθρο 2 αριθμ. 8 ν. 3471/2006.

[5] Το κείμενο αποτέλεσε εισήγηση της κ. *Αριστέας Σινανιωτη – Μωρούδη* στο 1ο Επιστημονικό Συνέδριο του Πανεπιστήμιου Πελοποννήσου σε συνεργασία με την Ελληνική Εταιρία Επιχειρήσεων Ερευνων,Τριπολη 31-10-2002.(βλέπε βιβλίο Ηλεκτρονική Τραπεζική από σελ 75-84.)

[6] ‘’Ηλεκτρονικό Επιχειρειν΄΄ (e-business) είναι κάθε είδους επιχειρηματική δραστηριότητα που μπορεί να ολοκληρωθεί ηλεκτρονικά, μέσω εναλλακτικών ηλεκτρονικών καναλιών επικοινωνίας και ανταλλαγής πληροφοριών. .(βλέπε βιβλίο Ηλεκτρονική Τραπεζική από σελ 75-84..)

[7] Βλ. *Αλεξανδριδου*, Το δίκιο του ηλεκτρονικού εμπορίου, ελληνικό και κοινοτικο,2004, Παντού, *Πιτσιρίκο,* Σύγχρονα μέσα επικοινωνίας(τηλεομοιοτυπο,τηλετυπημα,ηλεκτρονικο έγγραφο)για την κατάρτιση τυπικών δικαιοπραξιών ως ζήτημα της σχέσης έγγραφου τύπου και δκαιοπραξιας,2002,σελ,1επ.

[8] *Βλ. Καράκωστα*, Δίκαιο και Ίντερνετ. Νομικά ζητήματα του Διαδικτιου ,β΄εκδωση, 2003,σελ.167

[9] *Βλ. Σαμαρά*. Η Οδηγία της Ευρωπαϊκής Κοινότητας σχετικά με τα ηλεκτρονικό εμπόριο (e-commerce) στη εσωτερική αγορά. Μια εισαγωγή, ΔΕΕ 2000, 1200, *Χριστοδούλου*, Ηλεκτρονικά έγγραφα και ηλεκτρονική δικαιοπραξία 2001, σελ.1, *Μέτρου*,Το δίκαιο στη κοινωνία της πληροφορίας 2002,σελ.17επ.,*Σιδηροπουλου*,Το δίκαιο του διαδικτιου,2003, σελ 2.

[10] Βλ. *Καράκωστα*. οπ., σελ.165-166.

[11] Βλ. *Δουκιδη* / *Θεμιστοκλέους* / *Δράκο* / *Παπαζαφειροπουλου*, Ηλεκτρονικό Εμπόριο, 1998, σελ. 20, *Γ. Γεωργιάδη*, Η σύναψη συμβάσεως μέσω του διαδικτύου, 2003,σελ. 26-28, *Ιγγλεζακη*, Το νομικό πλαίσιο του ηλεκτρονικό εμπορίου, 2003, passim, ίδιος Εισαγωγή, σελ.19-23.

[12] Βλ. *Λαζαρακο*, Ηλεκτρονικό εμπόριο, Δυνατότητες αξιοποίησης και νομικά προβλήματα, Συνήγορος 2000, 44-45.

[13] *Δ. Πολίτης*, Μια τεχνικοοικονομική θεώρηση του “spam” στην ηλεκτρονική βιομηχανία πληροφόρησης, σε: Διαφήμιση & Παρενόχληση Spam και Τηλεόραση, Πρακτικά Ημερίδας 4 Φεβρουαρίου 2005, *Φ. Κοζύρης* / *Κ. Θεοδωρίδης*, 2006.

[14] n-Επιχειρείν: Συχνές ερωταποκρίσεις για την διαφήμιση
http://www.go-online.gr/ebusiness/specials/article.html?article_id=448

[15] Αξιοποίηση του web-marketing για την προώθηση των πωλήσεων http://www.go-online.gr/training/pdfs/E3/E3_kef3_math2.pdf

[16] Ορισμός του Spam: http://www.sch.gr/schportlets/static/manual/aboutSpam/index.php?_list=whatis

[17] *Χ. Μουζάκης*, Ανεπιθύμητη εμπορική ηλεκτρονική αλληλογραφία - η αντιμετώπισή του φαινομένου στην ελληνική και διεθνή έννομη τάξη, ΔiΜΕΕ 3/2008, σελ. 323.

[18] *Κ. Δελούκα- Ιγγλέση*, Η προστασία του καταναλωτή από την άμεση διαφήμιση στο διαδίκτυο, ΔiΜΕΕ 4/2004, σελ. 487 υποσημ. αριθμ. 19: «σε μια χαρακτηριστική περίπτωση όπου στάλθηκαν 3,5 εκατομμύρια ηλεκτρονικά μηνύματα, μόλις 18 πωλήσεις πραγματοποιήθηκαν την πρώτη εβδομάδα, ποσοστό δηλαδή περίπου 0,0023%. Ωστόσο, όπως απεδείχθη, το ποσοστό αυτό ήταν αρκετό να επιφέρει καθαρά κέρδη της τάξεως των 25.000$ στην επιχείρηση. Βλ. Wall Street Journal, 13 Νοεμβρίου 2002».

[19] Spam statistics 2006 – TopTenREVIEWS http://spam-filter-review.toptenreviews.com/spam-statistics.html

[20] Anti-spam and Virus SoftwareVendor Sophos, Dirty Dozen, the 12 most spamming countries. http://www.sophos.com

[21] http://epirus-tv-news.blogspot.gr/2012/10/spam.html#more http://techit.gr/2012/10/proth-chora-h-india-sthn-apostoli-spam/ http://www.skai.gr/news/technology/article/201075/protia-ston-arithmo-ton-spam-katagrafei-i-india/

[22] Πρόκειται για υπολογιστές απλών χρηστών που έχουν προσβληθεί από ιό ("zombie computers") οργανωμένους σε ομάδες ("botnets"), *L. Edwards / C. Waelde, Law and the Internet, 2009.*

[23] Κύριος σκοπός της ημερίδας είναι η παρουσίαση και συζήτηση προτάσεων για μια Εθνική Στρατηγική για το Απόρρητο και την Ασφάλεια Δικτύων και Πληροφοριών, και αποσκοπεί στη συγκρότηση διαρκούς forum, με την ευρύτερη δυνατή συμμετοχή, για τη συνεχή αντιμετώπιση των σχετικών προκλήσεων αλλά και δυνατοτήτων στο διεθνές περιβάλλον. http://www.adae.gr

[24] «Υπολογιστής που χρησιμοποιείται για την υποστήριξη τοπικών δικτύων υπολογιστών (π.χ. σε μία επιχείρηση) με μεγάλη υπολογιστική ισχύ και αποθηκευτική χωρητικότητα, ώστε να λειτουργεί και ως βάση δεδομένων για τους υπόλοιπους συνδεδεμένους υπολογιστές του δικτύου που ονομάζονται πελάτες (clients)», *Γ. Γιαννόπουλος*, Ροή πληροφοριών στο διαδίκτυο - τεχνολογία και νομικές ρυθμίσεις, 2002, σελ. 33, υποσημ. αριθμ. 18.

[25] "Email harvesting is the process of obtaining lists of email addresses using various methods for use in bulk email or other purposes usually grouped as spam", πηγή: http://en.wikipedia.org/wiki/E-mail_address_harvesting

[26] Για παράδειγμα, η διαφημιστική εταιρία "Double Click" που δραστηριοποιείται στο Internet, αγόρασε τη βάση δεδομένων της εταιρίας "Abacus Direct", η οποία περιείχε εκατομμύρια προσωπικών δεδομένων αμερικανών καταναλωτών. Υπό την απειλή των καταναλωτών να προσφύγουν στην Ομοσπονδιακή Επιτροπή Εμπορίου (Federal Trade Commission, FTC), η "Double Click" δεσμεύτηκε ότι θα ενημερώνει τους αποδέκτες των διαφημιστικών της μηνυμάτων για τους σκοπούς του άμεσου μάρκετινγκ και θα τους παρέχει το δικαίωμα να δηλώνουν ότι δεν επιθυμούν να λαμβάνουν τέτοια ηλεκτρονικά μηνύματα. Η. Καστανάς, Ίντερνετ και προστασία των προσωπικών δεδομένων, ΔτΑ 11/2001, σελ. 717.

[27] “Data mining, a branch of computer science and artificial intelligence, is the process of extracting patterns from data. Data mining is an increasingly important tool by modern business to transform data into business intelligence giving an informational advantage. It is currently used in a wide range of profiling practices such as marketing (…)”, πηγή: http://en.wikipedia.org/wiki/Data_mining .

[28] http://www.phorum.gr/viewtopic.php?f=15&t=157407
http://www.freestuff.gr/forums/viewtopic.php?p=416440#416440

[29] http://www.dpa.gr/portal/page?_pageid=33,20920&_dad=portal&_schema=PORTAL#7
http://www.noc.ntua.gr/index.php?module=ContentExpress&func=display&ceid=104

[30] https://www.google.gr/#q=picture+about+spam+messages

[31] Phishing: http://en.wikipedia.org/wiki/phishing & Spam Laws – Phishing, http://www.spamlaws.com/phishing.

[32] http://dide.ilei.sch.gr/keplinet/tech/spam.php

[33] *J. Rosenberg et al*, "Session Initiation Protocol (SIP): Locating SIP Servers", RFC 3263, June 2002.

[34] *Y.Rebahi, D.Sisalem*, “SIP Service Providers and The Spam Problem”, Germany.

[35] Y*. Rebahi, S. Ehlert, M. Theoharidou, J. Mallios, S. Dritsas, G. F. Marias, D. Gritzalis, Benjamin Pannier, Oriol Capsada, Jiri Markl,* “SPam over Internet telephony Detection sERvice”, January 2007.

[36] http://www.dpa.gr.

[37] http://www.adae.gr.

[38] http://computerscrimes.blogspot.gr/2012/01/blog-post_9609.html

[39] *Ε. Αλεξανδροπούλου-Αιγυπτιάδου*, Ζητήματα από το δίκαιο της πληροφορικής, 2002, σελ. 48.

[40] Οδηγία 97/7/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 20ής Μαΐου 1997 για την προστασία των καταναλωτών κατά τις εξ αποστάσεως συμβάσεις
http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0007:EL:HTML

[41] Οδηγία 95/46/ΕΚ του Ευρωπαϊκού 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 αυτών.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EL:HTML

[42] Νόμος 2251/1994, http://www.acci.gr/ecomm/legal/pdf/2251final.pdf

[43] Επεξεργασία δεδομένων: http://el.wikipedia.org/wiki/

[44] Αιτιολογική σκέψη 4 Οδ. 2002/58: «Η οδηγία 97/66/ΕΚ πρέπει να προσαρμοσθεί 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. Η εν λόγω οδηγία θα πρέπει, ως εκ τούτου, να καταργηθεί και να αντικατασταθεί από την παρούσα οδηγία».

[45] Council of Europe, Recommendation No R(85) 20 of the Committee of Ministers to Member States on the protection of personal data used for the purposes of direct marketing.

[46] ΜΠρΑθ (Μονομελές Πρωτοδικείο Αθηνών) 1327/2001, ΔΕΕ 4/2001, σελ. 377.

[47] *Κ. Κόμνιος*, ό.π., σελ. 1013· *Κ. Δελούκα-Ιγγλέση*, Η προστασία του καταναλωτή από την άμεση διαφήμιση στο διαδίκτυο, ό.π., σελ. 494.

[48] Directive 2002/58/EC of the European Parliament and of the Council, official Journal L201
http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PF

[49] *J.Kabel*, "Spam : A terminal Threat to ISPs", Computer und Recht International 2003 – 1.

[50] *N. Lugaresi,* "European Union vs Spam: A legal Response" (2005).

[51] OECD-Directorate for Science, Technology and Industry – Spam Task Force, Anti-spam regulation, DSTI/CP/ICCP/SPAM (2005) 10/FINAL.

[52] Commission of the European Communities, Unsolicited commercial communication and data protection – Summary of Study findings (2001).

[53] Data protection Working Party(DPWP), Privacy on the Internet-Glossary (2000).

[54] DPWP, Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC (WP 90 – February 2004)http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp90_en.pdf.

[55] J.Hladjk, "Effective EU and US approaches to spam? Moves towards a coordinated technical and legal response" – Part 1, Communications Law, Vol.10, No3, 2005, p.p 71.

[56] This code has been approved by the DPWP (wp 77 – 2003)
http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2003/wp77annex_en.pdf

[57] Παλαιό άρθρο 28 ΣυνθΕΚ, πριν από τη Συνθήκη της Λισσαβόνας.

[58] *Μ. Μαρίνος,* Αθέμιτος ανταγωνισμός, 2009, σελ. 205, παράγραφος 454.

[59] Commission of the European Communities, Communication on unsolicited commercial communication or spam, COM (2004) 28 final, January 2004.

[60] Οδηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8ης Ιουνίου 2000, οδηγία για το ηλεκτρονικό εμπόριο.
http://www.acci.gr/ecomm/legal/pdf/dir.2000_31.pdf

[61] Νόμος 2472/1997, http://www.acci.gr/ecomm/legal/pdf/2472.pdf.

[62] Νόμος 3471/2006 Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997
http://www.dsanet.gr/Epikairothta/Nomothesia/n3471_06.html

[63] Κ. Χριστοδούλου, Προστασία της προσωπικότητας και της συμβατικής ελευθερίας στα κοινωφελή δίκτυα, ό.π., σελ. 125.

[64] Anti-spam laws in the UK, http://www.email-marketing-reports.com/canspam/uk/.

[65] Data Protection Act 1998, http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_6

[66] ELECTRONIC COMMUNICATIONS, The Privacy and Electronic Communications (EC Directive) Regulations 2003, http://www.opsi.gov.uk/si/si2003/20032426.html'

[67] Fighting European spam, Italy, http://www.euro.cauce.org/en/countries/c_it.html

[68] *Απ. Γέροντας,* Πληροφορική και Δίκαιο, 1990, σελ. 243.

[69] Δυνητικό (potential) λέγεται ένα Φυσικό Μέγεθος όταν εκφράζει την δυνατότητα ενός σώματος, ενός Υλικού Μέσου ή ενός Πεδίου να ασκήσει ενδεχομένως επίδραση σε άλλο σώμα. π.χ. η ενέργεια (E) και το Ηλεκτρικό Δυναμικό (V) εκφράζουν δυνατότητα να ασκηθεί επίδραση σε ένα σώμα (και όχι ικανότητα) και επομένως είναι δυνητικά μεγέθη.

[70] http://www.afp.com/afpcom/en/

[71] Bush Signs CAN-SPAM, http://emailuniverse.com/list-news/?id=963

[72] ''Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003'', or the ''CANSPAM Act of 2003'', http://www.spamlaws.com/f/pdf/pl108-187.pdf.

[73] http://www.legis.state.ak.us/cgi

[74] http://www.azleg.state.az.us/FormatDocument.asp?inDoc=/ars/44/01372-01.htm&Title=44&DocType=ARS.

[75] http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=17001-18000&file=17529-17529.9

[76] www.michie.com/colorado/lpext.dll?f=templates&fn=main-h.htm&cp=

[77] Computer Crimes, http://www.cga.ct.gov/2005/pub/Chap949g.html

[78] http://www.cga.ct.gov/2007/pub/Chap925.htm#Sec52-570c.html

[79] http://delcode.delaware.gov/title11/c005/sc03/index.shtml#P1847_142921

[80]http://www.flsenate.gov/Statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=Ch0668/PART03.HTM

[81] http://www.in.gov/legislative/ic/code/title24/ar5/ch22.html.

[82] http://www.legis.state.la.us/lss/lss.asp?doc=104222 και http://www.legis.state.la.us/lss/lss.asp?doc=411230

[83] Lori Assheton-Smith Michael Binder (Chair),Tom Copeland Bernard Courtois, Michael Geist Amanda Maltby, Suzanne Morin Geneviève Reed, Neil Schwartzman Roger Tassé, "Stopping Spam", May 2005, http://www.ic.gc.ca/eic/site/ecicceac.nsf/vwapj/stopping_spam_May2005.pdf/$file/stopping_spam_May2005.pdf

[84] http://en.wikipedia.org/wiki/Fighting_Internet_and_Wireless_Spam_Act

[85] http://en.wikipedia.org/wiki/Spam_Act_2003.

[86] Legislative Issues / Legislative against spam http://www.med.govt.nz/templates/MultipageDocumentPage____686.aspx

[87] *Κ. Χριστοδούλου*, ΔiΜΕΕ (Δίκαιο Μέσων Ενημέρωσης και Επικοινωνίας (περιοδικό)) 3/2004, ό.π., σελ. 356.

[88] http://www.noc.ntua.gr/index.php?module=ContentExpress&func=display&ceid=104 & 10 Τρόποι για να αντιμετωπιστεί η ανεπιθύμητη αλληλογραφία http://www.tm.teiher.gr/Portal/DesktopDefault.aspx?tabid=322.

[89] All about Greek spam problem: http://spam_info.eu/09.html

[90] http://www.xrisimos-odigos.com/eidiseis/texnologia/458-xoris-spam. Πηγή : Τα Νέα.

[91] A.Birrel,et al : "The Penny Black Project": http://research.microsoft.com/research/sv/Penny Black/

[92] C.Dwork, A.Goldberg, and M.Naor "on memory-bound functions fot fighting spam", proceedings of the 23rd Annual International Cryptografy Conference (CRYPTO 2003), August 2003

[93] M.Abidi, M.Burrows, M.Manasse, and T.Wobber: "Moderately Hard, Memory-bound functions", proccedings of the 10th Annual Network and Distributed system security symposium, February 2003

[94] D.Turner, D.Havey: "Controlling spam through Lightweight currency", November 4,2003 http://ftp.csci.csusb.edu/tuner/papers/tuner-spam.pdf

[95] Spamhaus, The spamhaus project: http://www.spamhaus.org

[96] Habeas, Sender warranted e-mail, 2004 http://www.habeas.com

[97] Bonded sender program, Ironport http://www.bondedsender.com

[98] http://www.noc.ntua.gr/index.php?module=ContentExpress&func=display&ceid=104

[99] Sender Policy Framework, www.spf.pobox.com

[100] J.Lyon: Purposed Responsible Address in e-mail messages specification", October 2004. http://www.microsoft.com/downloads/detail.aspx?familyid=f8e9cb40-cc7c-46d6-8cd1- 3a86a46546d5&displaylang=en.

[101] Microsoft Corporation: "Sender ID" http://www.microsoft.com/senderid

[102] Yahoo! INC : "DomainKeys" http://antispam.yahoo.com/domainkeys

[103] T.Loder, M.V Alstyne, R.Wash : "An economic answer to unsolicited communication", ACM 2004.

[104] E.Harris: "The next step in the spam control war: Greylisting", August 28, 2003 http://projects.puremagic.com/greylisting/whitepaper.html

[105] Digiportal software Inc : "ChoiceMail, A spam blocker- not just a spam filter" http://www.digiportal.com

[106] P.Gburzynski: "Spam-free email service" http://sfm.cs.ualberta.ca/

[107] http://razor.sourceforge.net/

[108] Alan Gray and Mads Haahr, “Personalised, Collaborative Spam Filtering”

[109] http://www.no-spam.gr/tools.htm

[110] Richard Segal, Jason Crawford, Jeff Kephart, Barry Leiba, “SpamGuru: An Enterprise Anti-Spam Filtering System”

[111] Eirinaios Michelakis, Ion Androutsopoulos, Georgios Paliouras, George Sakkis, and Panagiotis Stamatopoulos, “Filtron: A Learning-Based Anti-Spam Filter”

[112] http://www.mailscanner.info/

[113] http://spamassassin.apache.org/

[114] http:// SPAMfighter.com

[115] MXLogic-Spam Classification Techniques.: http://www.mxlogic.com

[116] http://en.wikipedia.org/wiki/The_Spamhaus_Project

[117] http://en.wikipedia.org/wiki/Erkki_Liikanen

[118] Τελευταία ενημέρωση: Τρίτη, 1 Δεκεμβρίου 2009, 19:35
Πηγη: http://www.zougla.gr/page.ashx?pid=2&aid=83319&cid=5

[119] http://www.freeweird.com/2012/02/social-networks-filtering-users-content.html (17/02/2012, 9:24)