ΕΠΙΘΕΩΡΗΣΗ ΤΡΑΠΕΖΙΚΟΥ-ΑΞΙΟΓΡΑΦΙΚΟΥ ΧΡΗΜΑΤΙΣΤΗΡΙΑΚΟΥ ΔΙΚΑΙΟΥ

ΤΕΥΧΟΣ 3ο -Σεπτεμβριος-Δεκεμβριος 2009

Τεχνικά και νομικά ζητήματα ηλεκτρονικού ταχυδρομείου με αφορμή την απόφαση 1327/2001 του μονομελούς πρωτοδικείου Αθηνών[1]

Μουρατίδη Στράτου

1. Εισαγωγή

Η εισβολή των ηλεκτρονικών υπολογιστών στην ζωή μας και η αλματώδης εξέλιξη του διαδικτύου που ακολούθησε, προκάλεσε μια επανάσταση που δεν εισήγαγε απλά στην καθημερινότητά μας νέα μέσα, όπως συνέβη με την βιομηχανική επανάσταση του προηγούμενου αιώνα, αλλά μετασχημάτισε ριζικά τον τρόπο ζωής του σύγχρονου ανθρώπου, επεμβαίνοντας στις ανθρώπινες ενέργειες και σχέσεις[2]. Η αλλαγή αυτή του τρόπου ζωής απαιτεί την ανάλογη προσαρμογή του δικαίου, ως ρυθμιστή των ανθρώπινων σχέσεων, έτσι ώστε, να ανταποκρίνεται στο έργο του. Η προσαρμογή αυτή απαιτεί σειρά επεμβάσεων για τη ρύθμιση όλων των πτυχών της νέας "ηλεκτρονικής" διαδικτυακής συμπεριφοράς.

Η πρώτη χρονικά πρόκληση που κλήθηκε να αντιμετωπίσει το δίκαιο, ήταν το "προϊόν" της χρήσης των υπολογιστών, το "άυλο[3]" ηλεκτρονικό αρχείο στην πιο "συμβατική"[4] του μορφή, αυτή του ηλεκτρονικού εγγράφου. Ταχύτατα και πριν η νομική επιστήμη αντιμετωπίσει τα θέματα που εισήγαγε η νέα μορφή εγγράφου, παρουσιάστηκε και η τεχνική δυνατότητα διακίνησής του μέσω του διαδικτύου, είτε αυτοτελώς ως έχει, είτε ως επισυναπτόμενο σε μια νέα μορφή, στην ηλεκτρονική αλληλογραφία (email), καθιστώντας με αυτό τον τρόπο ακόμα πιο δυσχερές το έργο της.

[1] Δίκη 32 σελ. 457, ΔΕΕ 2001 σελ. 377, ΕΤρΑξΧρΔ 2002, σελ. 558.

[2] **Λίλιαν Μήτρου**, Το δίκαιο στην κοινωνία της πληροφορίας, σελ. 16.

[3] Σε αντίθεση με τα συνηθισμένα έγγραφα που απαιτούν ακοτύπωση σε χαρτί τα ηλεκτρονικά αποτυπώνονται σε μαγνητικά μέσα που δεν είναι άμεσα ορατά χωρίς να χρησιμοποιηθεί τεχνικός εξοπλισμός.

[4] Συμβατική από την άποψη ότι ένα ηλεκτρονικό έγγραφο μετά την απεικόνιση του από τον ηλεκτρονικό υπολογιστή ή μετά την εκτύπωσή του, παρουσιάζει μορφή συνηθισμένου εγγράφου, σε αντίθεση με άλλα είδη αρχείων δεδομένων όπως τα αρχεία εφαρμογών.

2. Αντικείμενο της εργασίας

Η αναφερθείσα ιδιαίτερη "ηλεκτρονική" φύση του ηλεκτρονικού εγγράφου και η δυνατότητα διακίνησής του μέσω του ηλεκτρονικού ταχυδρομείου, προκαλεί ποικίλα ζητήματα, τόσο ουσιαστικού όσο και δικονομικού δικαίου, η ορθή αντιμετώπιση των οποίων απαιτεί πλήρη γνώση των ιδιοτήτων, των δυνατοτήτων αλλά και του τρόπου λειτουργίας των νέων τεχνολογιών. Ελλιπής γνώση μπορεί να οδηγήσει σε συμπεράσματα ικανά να προκαλέσουν σύγχυση, που είναι δυνατό να μεταφερθεί από τη θεωρία στη νομολογία των δικαστηρίων, ή και αντίστροφα, δημιουργώντας, πέρα από άδικες αποφάσεις, εσφαλμένο προηγούμενο, η ανατροπή του οποίου μπορεί να καταστεί εξαιρετικά χρονοβόρα και δυσχερής. Ενισχυτικό ρόλο παίζουν σε αυτό το σημείο τα μαζικά μέσα ενημέρωσης, τα οποία, δρώντας με προχειρότητα μπορούν νι παραπλανήσουν το κοινό, σχηματίζοντάς του εσφαλμένες εντυπώσεις[5].

Στόχος της εργασίας αυτής είναι να παρουσιάσει με τρόπο απλό και παραστατικό, χωρίς εμμονή σε ειδικές τεχνικές λεπτομέρειες[6], τη λειτουργία του ηλεκτρονικού ταχυδρομείου, καταδεικνύοντας τα σημεία στα οποία τα συμπεράσματα της θεωρίας και της νομολογίας παρουσιάζουν "αναντιστοιχία" με τις πραγματικές καταστάσεις ή περιστατικά που εμφανίζονται, ή δύναται να εμφανιστούν στο χώρο του διαδικτύου.

3. Τεχνικά Θέματα

3.1 Γενικά

Το ηλεκτρονικό ταχυδρομείο αποτέλεσε το πρώτο μέσο διαπροσωπικής ηλεκτρονικής επικοινωνίας στο διαδίκτυο. Προηγήθηκαν εφαρμογές που εί-

[5] Χαρακτηριστικό παράδειγμα το δημοσίευμα της εφημερίδας Έθνος, **Μ. Μπενέ-α**, Ισοδύναμο με υπογραφή το email, Δευτέρα 6/12/2004, σελ. 56.

[6] Αλλά ταυτόχρονα με πληρότητα και τεχνική αρτιότητα, παραπέμποντας όπου απαιτείται σε τεχνικές πηγές για περισσότερες πληροφορίες.

χαν ως στόχο τη διακίνηση πληροφοριών μεταξύ συστημάτων[7]. Η δυνατότητα προσωπικής επικοινωνίας μεταξύ των χρηστών αυτών των συστημάτων προέκυψε ως φυσικό επακόλουθο· ως διάδοχος της συμβατικής αποστολής μηνυμάτων μέσω κλασικού ταχυδρομείου. Αρχικά η επικοινωνία περιλάμβανε αποστολή απλού κειμένου και στη συνέχεια επεκτάθηκε στην ανταλλαγή ηλεκτρονικών αρχείων[8].

Οι πρώτες υλοποιήσεις ηλεκτρονικού ταχυδρομείου αφορούσαν χρήστες ενός μόνο υπολογιστικού συστήματος ή μικρά τοπικά δίκτυα. Το μικρό μέγεθος και ο πειραματικός χαρακτήρας των δικτύων οδήγησε στον σχεδιασμό πρωτοκόλλων, με κύριο εκπρόσωπο το SMTP-Simple Mail Transfer Protocol, που είχαν ως στόχο την εύκολη υλοποίηση και λειτουργία, αγνοώντας θέματα ασφαλείας, αυθεντικότητας, διασφάλισης ακεραιότητας, μυστικότητας κ.α. Τα θέματα αυτά απασχόλησαν την τεχνική κοινότητα σχετικά πρόσφατα, μετά την εξάπλωση του διαδικτύου και την υιοθέτησή του για εμπορικούς σκοπούς, οπότε και εμφανίστηκαν θέματα κακόβουλης χρήσης του ηλεκτρονικού ταχυδρομείου με τη μορφή του spamming[9], phishing[10] κ.α. Η εξέλιξη αυτή οδήγησε στην εκ των υστέρων πυροσβεστική επέμβαση με την υιοθέτηση νέων τεχνικών και πρωτοκόλλων. Αναμενόμενο αποτέλεσμα των παραπάνω ενεργειών είναι η μερική αντιμετώπιση των ζητημάτων που δημιουργήθηκαν και αφορούν ένα σύστημα που δεν σχεδιάστηκε με γνώμονα την ασφάλεια και την αξιοπιστία.

3.2 Ιστορική αναδρομή

Το ηλεκτρονικό ταχυδρομείο αποτέλεσε μία από τις πρώτες εφαρμογές που ακολούθησαν τη δημιουργία του διαδικτύου. Στα πρώιμα στάδια της εξέλιξης του διαδικτύου αποτέλεσε την πιο σημαντική και πολυχρησιμοποι-

[7] Προηγούμενες μέθοδοι αποστολής εγγράφων περιλάμβαναν τη μεταφορά αρχείων με χρήση ειδικών πρωτοκόλλων, όπως το FTP -File Transfer Protocol, μεταξύ τοποθεσιών στο δίκτυο.

[8] Αυτό έγινε δυνατό με την προσθήκη επεκτάσεων στο αρχικό πρωτόκολλο, βλ. πιο αναλυτικά ενότητα 3.3 και υποσημείωση 15.

[9] Βλ. αναλυτικά παρακάτω, υποσημείωση 33.

[10] Οι νέες αυτές μορφές απειλών έχουν παρουσιαστεί και στον ημερήσιο τύπο βλ. Εφημερίδα Τα Νέα, Κανελλόπουλος, Υποκλέπτουν κάρτες, καταθέσεις, με «δόλωμα» emails που φαίνεται να έχουν σταλεί από τράπεζες, ένθετο Οικονομία, 5/10/2005, σελ. 46.

ημένη εφαρμογή προσφέροντας νέες δυνατότητες στην επικοινωνία και τη συνεργασία[11]. Το πρώτο email στάλθηκε το 1971 από τον Ray Tomlinson στον εαυτό του και περιείχε το μήνυμα "Testing 1-2-3". Ο ίδιος υιοθέτησε το σύμβολο @ στη διεύθυνση ηλεκτρονικού ταχυδρομείου[12].

3.3 Χαρακτηριστικά ηλεκτρονικού ταχυδρομείου

Τα βασικά χαρακτηριστικά του ηλεκτρονικού ταχυδρομείου είναι τα παρακάτω:

Α) Αποτελεί ένα μέσο **ασύγχρονης** επικοινωνίας. Αυτό σημαίνει ότι σε αντίθεση με τις **σύγχρονες** μεθόδους επικοινωνίας, όπως το τηλέφωνο· το ηλεκτρονικό ταχυδρομείο δεν απαιτεί την ταυτόχρονη διαθεσιμότητα των προσώπων που επιθυμούν να επικοινωνήσουν. Το χαρακτηριστικό αυτό είναι ιδιαίτερα επιθυμητό στο διαδίκτυο που περιλαμβάνει επικοινωνία μεταξύ ατόμων που βρίσκονται σε διαφορετικές γεωγραφικές και χρονικές ζώνες.

Β) Χρησιμοποιεί ως "όχημα" το διαδίκτυο εξασφαλίζοντας παγκόσμια παρουσία.

Γ) Είναι εύκολο, ταχύτατο και ταυτόχρονα εξαιρετικά οικονομικό.

Δ) Έχει το χαρακτήρα επικοινωνίας one-to-many αφού χρησιμοποιώντας τις λίστες ηλεκτρονικού ταχυδρομείου μπορεί ένα μήνυμα να αποσταλεί σε πολλούς αποδέκτες.

Ε) Χρησιμοποιεί το απλό πρωτόκολλο SMTP[13]. Το πρωτόκολλο αυτό είναι πρωτόκολλο προώθησης (Push protocol) σε αντίθεση με τα περισσότερα

[11] **James F. Kurose/Keith W. Ross**, Computer Networking, A top-down approach featuring the internet, 2nd edition, σελ.106.

[12] Βλ. ιστοσελίδα http://openmap.bbn.com/~tomlinso/ray/firstemailframe.html.

[13] Το πρωτόκολλο SMTP-Simple Mail Transfer Protocol περιγράφεται στο RFC 821. Τα RFC- Request For Comments είναι μια σειρά τεχνικών εγγράφων που δημιουργούνται από ειδικούς που περιγράφουν ή προτείνουν μεθόδους ή διαδικασίες για εφαρμογή στο διαδίκτυο (Για περισσότερες πληροφορίες βλ. **Σ. Γκρίζαλη / Κ. Κάτσικα / Δ. Γκρίζαλη**, Ασφάλεια Δικτύων Υπολογιστών, σελ. 49). Σε αυτά τα έγγραφα αποδίδονται μοναδικοί αριθμοί αναγνώρισης, δημοσιεύονται και διατίθενται ελεύθερα, ενώ κατά τη διάρκεια της ζωής τους περιέρχονται σε διάφορες καταστάσεις (informational, experimental, proposed standard, standard κ.α). Σε περίπτωση που κάποιο από αυτά υιοθετηθεί για χρήση σε ολόκληρο το διαδίκτυο από το Internet Engineering Task Force τότε χαρακτηρίζεται ως Internet Standard. Το πρωτόκολλο SMTP αποτελεί το standard

πρωτόκολλα του διαδικτύου που είναι πρωτόκολλα ανάκτησης (Pull protocols)[14].

Ζ) Η ανταλλασσόμενη πληροφορία αρχικά περιλάμβανε μόνο κείμενο ενώ με τη χρήση των MIME Extensions[15] επεκτάθηκαν οι δυνατότητές του σε μεταφορά εικόνας, ήχου, ή βίντεο ή οποιουδήποτε ψηφιακού αρχείου.

3.4 Τεχνικά στοιχεία

Η επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου διεξάγεται μεταξύ ενός αποστολέα και ενός παραλήπτη και για την επίτευξή της απαιτείται το κατάλληλο υλικό και λογισμικό υλοποίησης των οδηγιών που περιέχονται στα προβλεπόμενα πρωτόκολλα. Το υλικό περιλαμβάνει ειδικούς διαδικτυομένους εξυπηρετητές διαδικτύου[16] που λειτουργούν με βάση ειδικό λογισμικό[17], και στους οποίους οι χρήστες διαθέτουν λογαριασμό ηλεκτρονικού ταχυδρομείου[18].

Οι mail servers διακρίνονται με βάση το είδος της χρήσης για την οποία προορίζονται (για εξυπηρέτηση σκοπών εμπορικών, επαγγελματικών, ακαδημαϊκών ή προσωπικής επικοινωνίας). Ανάλογα με τη χρήση προκύπτουν και οι αντίστοιχες απαιτήσεις από πλευράς υπολογιστικής ισχύος και διαχειριστικού ελέγχου και υποστήριξης. Συνήθως συντηρούνται από μεγάλους τηλεπικοινωνιακούς οργανισμούς[19] οι οποίοι παρέχουν την υπηρεσία ηλε-

No11 (STD11). Πιο αναλυτικά για το SMTP βλ. **Rotriguez / Gatrell / Karas / Peschke**, TCP/IP Tutorial and Technical Overview, 7th edition, σελ. 387-389.

14 Η διαφορά τους έγκειται στην πρωτοβουλία για την έναρξη της επικοινωνίας βλ. **James F. Kurose / Keith W. Ross**, ο.π., σελ. 111. Το χαρακτηριστικό αυτό στο σχεδιασμό του πρωτοκόλλου SMTP προκαλεί και τη βασική αδυναμία του συστήματος αποστολής email για τα αποτελέσματα του οποίου βλ. παρακάτω παραγράφους 3.5.2, 3.6, 3.7.

15 Multipurpose Internet Mail Extensions. Αναλυτικά ο τρόπος λειτουργίας τους παρουσιάζεται στα RFC 2045 έως RFC2049.

16 Η mail servers όπως έχει επικρατήσει να ονομάζονται. Την ονομασία αυτή θα χρησιμοποιήσουμε και εμείς στο παρακάτω κείμενο.

17 Γνωστότερο είναι το sendmail για mail servers που χρησιμοποιούν το λειτουργικό σύστημα unix (βλ. www.sendmail.org).

18 Βλ. αναλυτικά παρακάτω στην ίδια ενότητα.

19 Internet Service Providers-ISPs, χωρίς να αποκλείεται η δυνατότητα δημιουργίας, διασύνδεσης και λειτουργίας mail server ακόμα και από ένα και μόνο έμπειρο χρήστη.

κτρονικού ταχυδρομείου σε συνδυασμό με την πρόσβαση στο διαδίκτυο[20]. Η υπηρεσία αυτή διαβαθμίζεται από την εξυπηρέτηση ενός απλού χρήστη μέχρι πολυπληθούς ομάδας χρηστών σε συνδυασμό, τις περισσότερες φορές, με τη δέσμευση ονόματος χώρου (domain name) και χρησιμοποιώντας ειδικό mail server (dedicated server).

Η διάθεση λογαριασμού ηλεκτρονικού ταχυδρομείου περιλαμβάνει:

Α) Την αποκλειστική χρήση κάποιων χαρακτήρων ως username του χρήστη, που σε συνδυασμό με το domain name (όνομα χώρου) του server, διαχωρισμένα από το σύμβολο @, συνιστούν την πλήρη διεύθυνση ηλεκτρονικού ταχυδρομείου του χρήστη π.χ mouratidis@otenet.gr ή stratosm@hotmail.com

Κάθε χρήστης επιλέγει ελεύθερα το username του (εφόσον αυτό δεν έχει ήδη διατεθεί σε κάποιον άλλον) χωρίς να είναι απαραίτητο να συνδέεται λογικά με το όνομα ή το επίθετο του (μπορεί να χρησιμοποιεί ψευδώνυμο).

Ο χρήστης είναι δυνατόν να έχει αποκτήσει το δικό του domain name, οπότε σε αυτήν την περίπτωση έχει την ευχέρεια να διαχειριστεί κατά βούληση όλα τα usernames που μπορούν να σχηματιστούν. Έτσι ο κάτοχος του domain mouratidis.gr μπορεί να χρησιμοποιεί την ηλεκτρονική διεύθυνση stratos@mouratidis.gr ή sales@mouratidis.gr

Β) Τη δημιουργία στο server ειδικού προσωπικού φακέλου για κάθε χρήστη, πεπερασμένου μεγέθους[21], που διακρίνεται από τους άλλους με βά-

20 Σχετικά πρόσφατα (το 1995) εμφανίστηκαν εταιρίες (με πρώτη την Hotmail) που παρείχαν πρόσβαση σε δικούς τους mail servers χωρίς οικονομικό αντάλλαγμα με μόνο στόχο τη διαφημιστική τους προβολή. Βλ. παρακάτω στην ίδια ενότητα καθώς και υποσημείωση 29.

21 Υπέρβαση του χώρου αυτού μπορεί να οδηγήσει σε απόρριψη εισερχόμενων email ή διαγραφή των παλαιών ανάλογα με την πολιτική που θα επιλέξει να εφαρμόσει ο διαχειριστής του server. Στην τεχνική ορολογία το όριο αυτό ονομάζεται quota. Προβληματισμό μπορεί να προκαλέσει η απόρριψη ενός μηνύματος για τον παραπάνω λόγο, σε συνδυασμό με την υιοθέτηση από το ελληνικό δίκαιο της θεωρίας της λήψεως που ακολουθεί ο Αστικός Κώδικας (167 ΑΚ) (βλ. **Καράκωστα**, Δίκαιο και Ίντερνετ, Β' έκδοση, σελ. 184). Το πρόβλημα έγκειται στο κατά πόσο η απευθυντέα δήλωση βούλησης που περιέχει το email πρέπει, σε αυτή την περίπτωση, να θεωρηθεί ενεργός ή όχι. Η αρνητική απάντηση φαίνεται να υπερέχει εξαιτίας της ενημέρωσης του αποστολέα σχετικά με την μη παράδοση του email. Εντούτοις υπάρχει περίπτωση η ενημέρωση αυτή να μην γίνει άμεσα, αλλά να καθυστερήσει για μεταβλητό χρονικό διάστημα (που ο server του αποστολέα ξαναπροσπαθεί να αποστείλει το μήνυμα- βλ. ενότητα 3.5.1), προκαλώντας αβεβαιότητα για την ενέργεια της δήλωσης βούλησης στο μεσοδιάστημα

ση το username και είναι μοναδικός. Στο χώρο αυτό φυλάσσεται η ηλεκτρονική αλληλογραφία του χρήστη (εισερχόμενα, εξερχόμενα ή πρόχειρα email κ.α) και πρόσβαση σε αυτόν έχουν μόνο ο ίδιος ο χρήστης μέσω ειδικού κωδικού (password[22]) και ο διαχειριστής του συστήματος για λόγους ασφαλείας, συντήρησης κ.α[23].

Ένα email διακρίνεται σε δύο τμήματα: στις κεφαλίδες (headers) και στο περιεχόμενο του email (κυρίως σώμα-body) που διαχωρίζονται μεταξύ τους από μια κενή γραμμή. Περισσότερες πληροφορίες για τη δομή του email δίνονται με παραστατικό τρόπο στο παράδειγμα της παρακάτω ενότητας.

3.5 Τρόπος λειτουργίας ηλεκτρονικού ταχυδρομείου

Οι τρόποι αποστολής ηλεκτρονικού μηνύματος διακρίνονται σε δυο κατηγορίες: **στους ορθόδοξους** και στους **ανορθόδοξους**.

3.5.1 Ορθόδοξοι τρόποι αποστολής

Πρόκειται για τις περιπτώσεις 1, 2 και 3 του παρακάτω σχήματος. Η σειρά που παρουσιάζονται ταυτίζεται με τη χρονική σειρά που εμφανίστηκαν στο διαδίκτυο. Βασικό χαρακτηριστικό των περιπτώσεων αυτών είναι ότι ο αποστολέας του ηλεκτρονικού μηνύματος ***χρησιμοποιεί*** **το server στον οποίο έχει λογαριασμό[24] ηλεκτρονικού ταχυδρομείου για να αποστείλει email.**

αυτό. Αντίθετη άποψη έχει ο **Ιγγλεζάκης** βλ. Το νομικό πλαίσιο του ηλεκτρονικού εμπορίου, κεφ. 5.1.7, σελ. 137. Επίσης πρβλ. υποσημείωση 30.

22 Ο κωδικός αυτός έχει δημιουργήσει σύγχυση στην νομολογία όπως στην απόφαση 1327/2001 του μονομελούς πρωτοδικείου Αθηνών (βλ. Δίκη 32, σελ. 458). Στην απόφαση αυτή ο κωδικός πρόσβασης στο χώρο του χρήστη (password) αναφέρεται **λανθασμένα** ως η ηλεκτρονική διεύθυνση του χρήστη. Πιο αναλυτικά βλ. ενότητα 4.5.

23 Η δυνατότητα αυτή του διαχειριστή του mail server να έχει πρόσβαση στο ηλεκτρονικό ταχυδρομείο των χρηστών εγείρει ερωτήματα σχετικά με το απόρρητο της ηλεκτρονικής αλληλογραφίας και την ευθύνη των Internet Service Providers. Σημειώνεται ότι ο διαχειριστής του συστήματος δεν γνωρίζει το password του κάθε χρήστη αλλά αποκτά την δυνατότητα πρόσβασης μέσω των δικαιωμάτων υπερχρήστη-administrator που διαθέτει.

24 Για τον λογαριασμό ηλεκτρονικού ταχυδρομείου και τι αυτός περιλαμβάνει βλ. ενότητα 3.4.

- **Περίπτωση 1:** Ο αποστολέας συνδέεται online στο mail server του και μέσω ειδικού λογισμικού που είναι εγκατεστημένο σε αυτόν (mail server) διαχειρίζεται το ηλεκτρονικό του ταχυδρομείο[25]. Η περίπτωση αυτή χρησιμοποιούταν παλαιότερα ενώ σήμερα έχει σχεδόν ολοκληρωτικά αντικατασταθεί από άλλους τρόπους αποστολής, που διακρίνονται για την ευχρηστία τους και τις αυξημένες δυνατότητες που παρέχουν. Βασικό πλεονέκτημα της περίπτωσης αυτής είναι ότι παρέχεται πρόσβαση από οποιοδήποτε υπολογιστή χωρίς να απαιτείται ειδικό λογισμικό στην πλευρά του χρήστη.
- **Περίπτωση 2:** Ο αποστολέας συνδέεται στον mail server μέσω προγράμματος εγκατεστημένου στον υπολογιστή του (αποστολέα). Το πρόγραμμα αυτό (π.χ Microsoft Outlook Express) αναλαμβάνει την επικοινωνία με το mail server του αποστολέα. Στα μειονεκτήματα αυτής της μεθόδου καταλογίζεται η απαίτηση για χρήση ειδικού software, ενώ στα πλεονεκτήματα η εύκολη διαχείριση των email (δυνατότητα ταξινόμησης, αναζήτησης, δημιουργίας ευρετηρίου κ.α). Ο χρήστης μπορεί να επιλέξει από δυο πρωτόκολλα[26] για την πρόσβαση στο λογαριασμό του στο mail server.
- **Περίπτωση 3:** Σύνδεση μέσω εφαρμογής webmail[27]. Η περίπτωση αυτή συγκεντρώνει τα πλεονεκτήματα των δυο παραπάνω μεθόδων χωρίς τα μειονεκτήματά τους. Αποτελεί την πιο σύγχρονη προσέγγιση και σημειώνει τη μεγαλύτερη προτίμηση των χρηστών του διαδικτύου. Δεν απαιτεί ειδικό λογισμικό στον υπολογιστή του χρήστη ενώ πρόσβαση παρέχεται από οποιοδήποτε υπολογιστή μέσω ενός κοινού browser[28]. Οι ευκολίες διαχείρισης που παρέχονται είναι παρόμοιες με την προηγούμενη περίπτωση 2. Ιστορικά η εμφάνιση των εφαρμογών webmail συνοδεύτηκε από την παροχή δωρεάν λογαριασμών ηλεκτρονικού ταχυδρομείου από εταιρίες όπως η Hotmail[29] ή η Google (με το gmail) ή ακόμα και από ελληνικές εταιρίες (ό-

25 Κλασικό παράδειγμα αποτελεί η εφαρμογή pine του πανεπιστημίου της Ουάσινγκτον που συνόδευε στο παρελθόν κάθε mail server που χρησιμοποιείτο στο διαδίκτυο. Πιο αναλυτικά βλ. ιστοσελίδα http://www.washington.edu/pine/

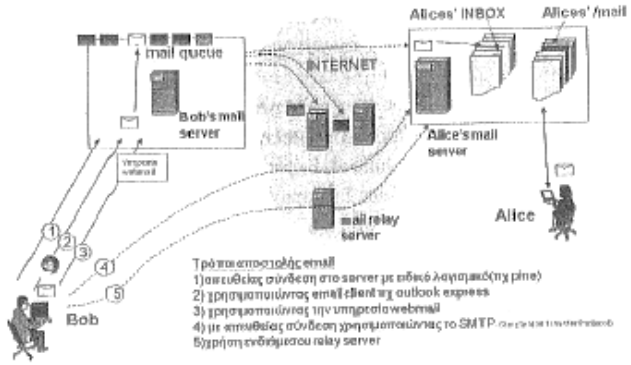
26 POP3-Post Office Protocol 3 ή IMAP4-Internet Mail Access Protocol 4.

27 Έχουν αναπτυχθεί διάφορες εφαρμογές webmail με δημοφιλέστερες την horde (βλ. ιστοσελίδα www.horde.org), roundcube (βλ. www.roundcube.net) και squirrelmail (βλ. http://squirrelmail.org)

28 Όπως ο Internet Explorer ή ο Mozilla Firefox.

29 Η Hotmail υπήρξε η πρωτοπόρος στην παροχή δωρεάν email. Υπήρξε εξαιρετικά κερδοφόρος αφού περιλάμβανε διαφημίσεις. Αργότερα αποκτήθηκε από την

πως π.χ in.gr) με αντάλλαγμα την παροχή διαφημίσεων. Η παροχή δωρεάν λογαριασμών ηλεκτρονικού ταχυδρομείου αυτής της μορφής οδήγησε στην επιφυλακτική αντιμετώπιση, όσον αφορά την φερεγγυότητά τους, καθώς και στον χαρακτηρισμό τους ως εργαλείων παροχής ανωνυμίας για την αποστολή email.



Χρησιμοποιώντας μια από τις παραπάνω μεθόδους, το email εισάγεται στην ουρά αναμονής του server του αποστολέα και αποστέλλεται το συντομότερο δυνατό στον mail server του παραλήπτη, ο οποίος με την σειρά του το αποθηκεύει στον φάκελο του παραλήπτη. Τυχόν αδυναμία σύνδεσης αντιμετωπίζεται με επανάληψη της προσπάθειας αποστολής ανά τακτά χρονικά διαστήματα μέχρι ενός καθορισμένου από τον διαχειριστή του mail server χρονικού ορίου, που συνήθως δεν υπερβαίνει τις δυο ημέρες. Ο παραλήπτης όποια χρονική στιγμή το επιθυμεί μπορεί να συνδεθεί και να παραλάβει τα email του[30].

Microsoft. Για περισσότερες λεπτομέρειες βλ. **James F. Kurose / Keith W. Ross**, ο.π., σελ. 108.

[30] Για αυτό το λόγο η επικοινωνία ονομάζεται ασύγχρονη. βλ. ενότητα 3.3. Κατά την παραλαβή ενός email μπορεί, εφόσον το έχει επιλέξει ο αποστολέας, να ζητηθεί από τον παραλήπτη επιβεβαίωση παραλαβής του email. Η επιβεβαίωση αυτή ανήκει στη διακριτική ευχέρεια του παραλήπτη οπότε δεν μπορεί να χρησιμοποιηθεί από τον αποστολέα ως μέσο εγγύησης παραλαβής του email.

3.5.2 Ανορθόδοξοι τρόποι αποστολής

Πρόκειται για τις περιπτώσεις 4 και 5 όπως σημειώνονται στο παραπάνω σχήμα. Βασικό χαρακτηριστικό των περιπτώσεων αυτών είναι ότι ο αποστολέας δεν συνδέεται στο δικό του server για να αποστείλει το email, αλλά **συνδέεται απευθείας στον server του παραλήπτη** για την παράδοση του email. Η λειτουργία αυτού του τρόπου αποστολής βασίζεται σε μια ιδιαιτερότητα του πρωτοκόλλου SMTP. Η ιδιαιτερότητα αυτή εντοπίζεται στο γεγονός ότι το πρωτόκολλο αυτό **δεν προβλέπει έλεγχο της διεύθυνσης του αποστολέα**. Εντούτοις απαιτείται μια διεύθυνση αποστολέα που μπορεί όμως να είναι ψευδής.

Η διαφοροποίηση της περίπτωσης 5 από την 4 συνίσταται στο ότι χρησιμοποιείται ενδιάμεσος mail server με αποτέλεσμα την εμφάνιση ως πηγή της αποστολής τον ενδιάμεσο server[31]. Η δυνατότητα αυτή (που ονομάζεται mail relay[32]) οδήγησε στην εμφάνιση του τόσο ενοχλητικού spam email[33]. Το spam χρησιμοποιείται για την αποστολή ανεπιθύμητης, εμπορικής συνήθως, αλληλογραφίας με ελάχιστο κόστος. Στους στόχους του συγκαταλέγονται η αποφυγή των παραπόνων από τον παραλήπτη[34] και η εκμετάλλευση του εύρους ζώνης (bandwidth) του relay server. Σήμερα οι περισσότεροι mail servers έχουν διαμορφωθεί έτσι ώστε, να μην επιτρέπουν το mail relaying.

[31] Στην περίπτωση αυτή η διεύθυνση του παραλήπτη που θα χρησιμοποιήσει ο αποστολέας θα έχει τη μορφή:@mail.forthnet.gr,@mx.otenet.gr:stmour@uom.gr Έτσι το email αποστέλλεται αρχικά στο server της forthnet με οδηγία να αποσταλεί στο server της otenet, ο οποίος και θα το στείλει στον τελικό παραλήπτη stmour@uom.gr

[32] Περισσότερες πληροφορίες για το mail relay βλ. **Rotriguez / Gatrell / Karas / Peschke**, ο.π., σελ. 394.

[33] SPAM σημαίνει Spiced Pork And Meat και αφορά κονσέρβα κρέατος χαμηλού κόστους που λανσαρίστηκε το 1937 από την Hormel Foods. Ήταν από τις λίγες μορφές κρέατος που διατίθετο στην Αγγλία χωρίς δελτίο κατά τη διάρκεια του Β΄Παγκοσμίου πολέμου. Πρωτοχρησιμοποιήθηκε σε ένα σκετς των Monty Pythons στο οποίο οι πελάτες ενός εστιατορίου σερβίρονταν μόνο spam ανεξαρτήτως του τι είχαν παραγγείλει. Καθιερώθηκε στο διαδίκτυο ως χαρακτηρισμός της ανεπιθύμητης αλληλογραφίας. Για περισσότερα στοιχεία βλ. την ιστοσελίδα http://www.cs.berkeley.edu/~ddgarcia/spam.html#MontyPython.

[34] Συνήθως σε συνδυασμό με παραποίηση διαδικτυακών διευθύνσεων –Spoofed IP Addresses.

Η διαδικασία απευθείας αποστολής email στο server του παραλήπτη δεν είναι ιδιαίτερα δύσκολη και μπορεί να γίνει από τη γραμμή εντολής[35] των windows. Στο παράδειγμα που ακολουθεί παρουσιάζεται ο τρόπος υλοποίησης (με έντονα γράμματα δηλώνονται τα δεδομένα που εισάγει ο αποστολέας ενώ με ειδική γραμματοσειρά η απάντηση του server). Ο στόχος του παραδείγματος είναι διπλός: να καταδειχθεί η ευκολία με την οποία μπορεί να γίνει η αποστολή ενός email και ταυτόχρονα να παρουσιαστεί στην πράξη **η δυνατότητα χρησιμοποίησης ως έγκυρης, οποιασδήποτε διεύθυνσης αποστολέα!**[36]

ΠΑΡΑΔΕΙΓΜΑ[37]

Υποθέτουμε ότι θέλουμε να αποστείλουμε ένα email στον χρήστη stmour@uom.gr

Ανοίγουμε μια γραμμή εντολών windows. Αρχικά απαιτείται να βρούμε τον mail server του παραλήπτη όπως προκύπτει από το όνομα χώρου (domain name) της ηλεκτρονικής του διεύθυνσης (δηλ. στην περίπτωσή μας το uom.gr). Αυτό το κάνουμε μέσω της παρακάτω εντολής.

Εντολή 1	**nslookup -q=mx uom.gr**
Απάντηση 1	Non-authoritative answer: uom.gr MX preference = 10, mail exchanger = thessaloniki.uom.gr. uom.gr MX preference = 100, mail exchanger = macedonia.uom.gr

Η απάντηση που προκύπτει έχει την παραπάνω μορφή και μας γνωστοποιεί ότι υπάρχουν δυο server διαθέσιμοι, με προτεραιότητα σύνδεσης σε αυτόν που έχει μικρότερη τιμή στο πεδίο preference, δηλ. ο προτεινόμενος mail server για σύνδεση είναι ο thessaloniki.uom.gr.

Συνδεόμαστε στο server αυτόν στην πόρτα 25 που λειτουργεί το πρωτόκολλο SMTP.

[35] Για την εκκίνηση της Γραμμής Εντολών/Command Prompt των windows εκτελούμε την παρακάτω ακολουθία επιλογών: Έναρξη > προγράμματα > Βοηθήματα > Γραμμή εντολής ή Start > Programs > Accessories > Command Prompt

[36] Μια πιο εποπτική παρουσίαση της διαδικασίας (υπό την μορφή video) περιέχεται στη διαδικτυακή διεύθυνση http://users.auth.gr/~stmour

[37] Ο αναγνώστης μπορεί να ακολουθήσει τις οδηγίες αποστολής του παραδείγματος. Ενδεχόμενο μήνυμα λάθους κατά την πληκτρολόγηση της εντολής 3 θα οφείλεται στην ύπαρξη block list από τον Internet Service Provider του αναγνώστη, βλ. υποσημειώσεις 49, 50 και 51.

Εντολή 2	**telnet thessaloniki.uom.gr 25**
Απάντηση 2	220 thessaloniki.uom.gr ESMTP Postfix (Debian/GNU)

Η παραπάνω απάντηση είναι το καλωσόρισμα από το mail server του παραλήπτη το οποίο ανταποδίδουμε με την παρακάτω εντολή προσποιούμενοι ότι είμαστε ο server mail.whitehouse.com (ψευδώς προφανώς).

Εντολή 3	**Helo mail.whitehouse.com**
Απάντηση 3	250 thessaloniki.uom.gr Hello ppp-94-68-105-74.home.otenet.gr [94.68.105.74], pleased to meet you

Στην απάντηση που λαμβάνουμε ο server αναγνωρίζει την πραγματική IP διεύθυνση από την οποία συνδεόμαστε[38]. Ακολούθως εκδηλώνουμε την πρόθεσή μας να παραδώσουμε ένα email ως obamab@whitehouse.com για να λάβουμε την απάντηση ότι η διεύθυνση του αποστολέα έγινε δεκτή!

Εντολή 4	**MAIL FROM : <obamab@whitehouse.com>**
Απάντηση 4	250 2.1.0 obamab@whitehouse.com... Sender ok

Ακολουθεί η εισαγωγή της διεύθυνσης του παραλήπτη η οποία απαιτείται να είναι πραγματική αλλιώς το email θα απορριφθεί.

Εντολή 5	**RCPT TO : <stmour@uom.gr>**
Απάντηση 5	250 2.1.5 stmour@uom.gr... Recipient ok.

Μετά τη αποδοχή της διεύθυνσης του παραλήπτη γίνεται η εισαγωγή των δεδομένων.

Εντολή 6	**DATA** **From: <obamab@whitehouse.com>** **To: <stmour@uom.gr>** **Subject: I want to ask you smth** **What about turkey? What should i do?** .	[39]
Απάντηση 6	250 2.0.0 n6T1joel3032551 Message accepted for delivery	

Το μήνυμα έχει παραληφθεί και θα παραδοθεί στον παραλήπτη όποτε και αποσυνδεόμαστε από το server του παραλήπτη.

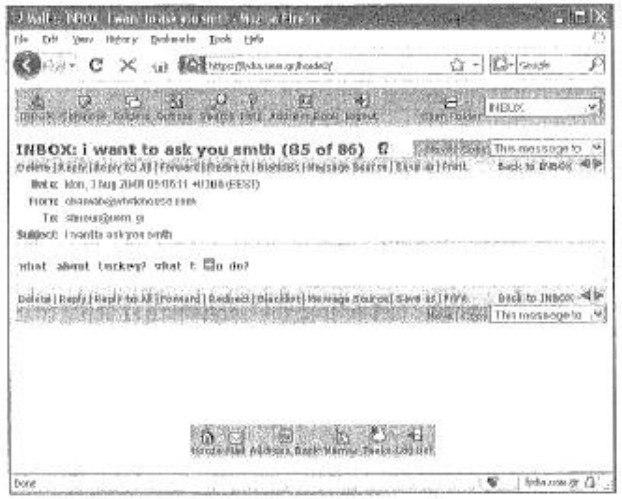
Εντολή 7	**QUIT**
Απάντηση 7	221 2.0.0 thessaloniki.uom.gr closing connection

[38] Η IP (Internet Protocol) διεύθυνση αποτελεί το μέσο με το οποίο γίνεται η επικοινωνία στο διαδίκτυο. Σε κάθε συνδεδεμένο στο διαδίκτυο υπολογιστή αποδίδεται μια μοναδική IP διεύθυνση.

[39] Μετά το Subject απαιτείται να πατηθεί 2 φορές το Enter. Για να δηλώσουμε το τέλος του κειμένου τοποθετούμε μια τελεία σε μια κενή γραμμή.

	Connection to host lost.

Ο παραλήπτης κατά την παραλαβή του μηνύματος θα δει την παρακάτω εικόνα από την εφαρμογή webmail που χρησιμοποιεί.



Με μια πρόχειρη ματιά το email φαίνεται γνήσιο ως προς τον αποστολέα του μηνύματος! Η γνησιότητά του δεν είναι εύκολο να διαπιστωθεί ενώ όπως καθίσταται προφανές **η διεύθυνση αποστολέα δεν μπορεί να είναι κριτήριο της ταυτότητας του αποστολέα.** Ο μόνος τρόπος για τη διαπίστωση της ταυτότητας του αποστολέα είναι η ηλεκτρονική υπογραφή του μηνύματος με χρήση αναγνωρισμένου πιστοποιητικού[40]. Πάντως στο συγκεκριμένο email μπορούν να ανιχνευτούν κάποιες ενδείξεις που μπορούν να δημιουργήσουν υποψίες σχετικά με την ταυτότητα του αποστολέα[41]. Οι ενδείξεις αυτές παρουσιάζονται στην παρακάτω ενότητα.

3.5.3 Ανάλυση ενός email

[40] Στις ηλεκτρονικές υπογραφές αναφέρεται η ενότητα 3.7.

[41] Εκτός από το προφανές του ονόματος του αποστολέα στο παραπάνω παράδειγμα!

Όπως αναφέρθηκε παραπάνω[42] ένα email διακρίνεται σε δύο τμήματα: στις κεφαλίδες (headers[43]) και στο περιεχόμενο του email (κυρίως σώμα-body) που διαχωρίζονται μεταξύ τους από μια κενή γραμμή[44]. Το πλήρες κείμενο ενός email (message source) μας δίνει πληροφορίες για τη διαδρομή που αυτό ακολουθεί[45], τη διεύθυνση IP από την οποία αποστάλθηκε, καθώς και τους mail servers που μεσολάβησαν για την παράδοσή του.

Έτσι, στο email του προηγούμενου παραδείγματος μπορούμε εύκολα να διαπιστώσουμε την πραγματική IP διεύθυνση του αποστολέα! (βλ. παρακάτω πίνακα). Γνωρίζουμε συνεπώς, πότε και από πού έγινε η αποστολή email, δηλαδή, από την IP διεύθυνση 94.68.88.241 της OTENET[46].

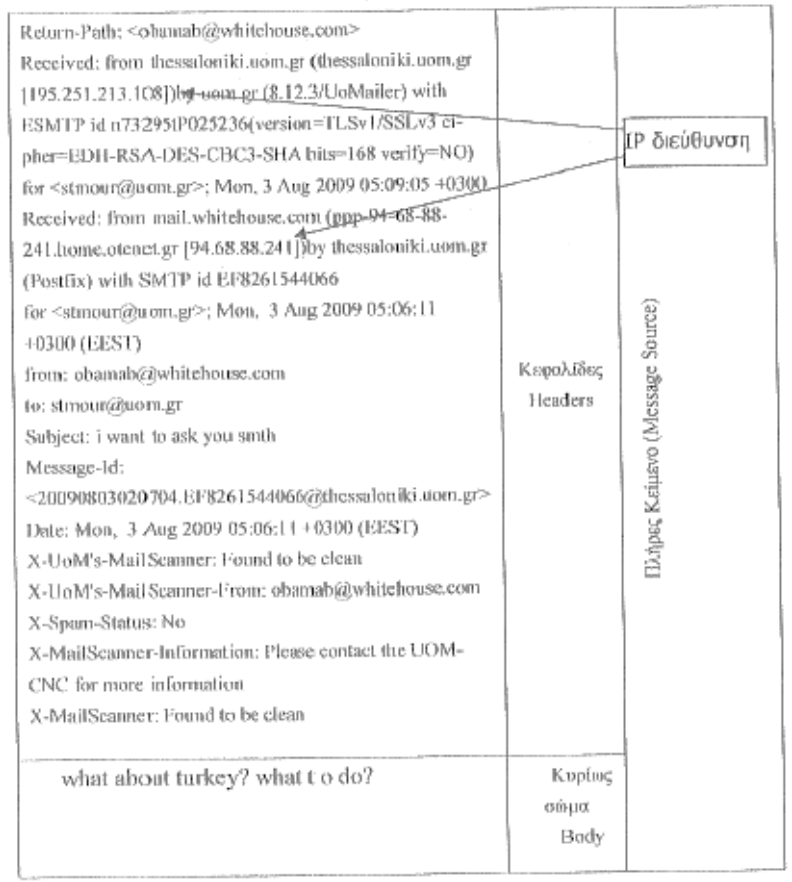
[42] Ενότητα 3.4.

[43] Λεπτομέρειες σχετικά με τις κεφαλίδες των email περιέχονται στο RFC822.

[44] Το πλήρες κείμενο (message source) ενός email μπορεί να ανακτηθεί επιλέγοντας message source (ή άλλη παρόμοια έκφραση) από οποιαδήποτε εφαρμογή webmail ή αν χρησιμοποιείτε το outlook express επιλέγοντας το email του οποίου θέλουμε να δούμε το source code, μετά δεξί κλικ, Properties (ιδιότητες), επιλογή καρτέλας Details (λεπτομέρειες) και μετά επιλογή Message source.

[45] Οι πληροφορίες αυτές προστίθενται από τους servers που μεσολαβούν και οι οποίοι εισάγουν πληροφορίες μέσω πρόσθετων headers στο email περιγράφοντας τις ενέργειές τους.

[46] Βεβαίως ο αποστολέας έχει τη δυνατότητα να αποκρύψει την θέση του έμμεσα, χρησιμοποιώντας υπολογιστή ενός Internet Cafe καθιστώντας αυτόν «πηγή» της αποστολής.



3.5.4 Αντιμετώπιση ενός email απεσταλμένου από ψεύτικο αποστολέα-spam email

Όπως είδαμε παραπάνω, ο σχεδιασμός του πρωτοκόλλου SMTP που χρησιμοποιείται για την αποστολή email δεν απαιτεί τον έλεγχο γνησιότητας της ηλεκτρονικής διεύθυνσης του αποστολέα, επιτρέποντας την ανίχνευση μόνο της IP διεύθυνσης από την οποία έγινε η αποστολή. Η αδυναμία αυτή αντιμετωπίζεται εν μέρει με δυο βασικές κατηγορίες τεχνικών μεθόδων, που

ακολουθούν διαφορετική φιλοσοφία, προσεγγίζοντας το πρόβλημα σε διαφορετικό χρονικό στάδιο. Η πρώτη μέθοδος εστιάζεται στο σημείο εισόδου των email στον server του παραλήπτη απαγορεύοντας τη σύνδεση, ενώ η δεύτερη ενεργεί μετά την παράδοση των email.

3.5.4.1 Πρώτη Κατηγορία

Η αντιμετώπιση περιλαμβάνει:

Α) Έλεγχο και ταυτοποίηση του mail server κατά τη χρονική στιγμή που αυτός συνδέεται με το mail server του παραλήπτη για την παράδοση του email. Ο έλεγχος υλοποιείται μέσω της διαπίστωσης ότι η IP διεύθυνση από την οποία γίνεται η σύνδεση αντιστοιχεί στο domain name που δηλώνει ο συνδεόμενος[47].

Β) Εισαγωγή τυχαίας μεταβλητής χρονικής καθυστέρησης κατά τη σύνδεση για να αποτραπούν αυτόματοι μηχανισμοί αποστολής μαζικών email. Η αντιμετώπιση αυτή είναι προσανατολισμένη στην αντιμετώπιση της μαζικότητας του spam email και αδυνατεί να αντιμετωπίσει επιτυχώς τα μη αυτόματα παραποιημένα email (forged email)[48].

Γ) Χρησιμοποίηση block lists[49]. Οι λίστες αυτές είναι δυναμικές[50] και περιλαμβάνουν τις IP διευθύνσεις που θεωρούνται ως "πηγές" αποστολής spam email. Κατά την προσπάθεια σύνδεσης σε έναν mail server που χρησιμοποιεί αυτήν τη μέθοδο ακολουθεί αυτόματος έλεγχος εάν η IP διεύθυνση του συνδεόμενου περιλαμβάνεται στη "μαύρη λίστα". Εάν η απάντηση είναι θετική ο server αρνείται τη σύνδεση. Η μέθοδος αυτή είναι μερικώς αποτελεσματική αφού είναι δυνατόν να παρακαμφθεί[51].

---

47 Πρόκειται για την τεχνική που αποσκοπεί στον έλεγχο ορθότητας domain name, και ονομάζεται reverse nslookup.

48 Παράδειγμα τέτοιας εφαρμογής που χρησιμοποιείται από αρκετούς ISPs είναι η εφαρμογή Greetpause βλ. ιστοσελίδα http://www.deer-run.com/~hal/sysadmin/greet_pause.html

49 Πολύ γνωστή λίστα είναι αυτή που έχει δημιουργήσει η ομάδα Spamhaus. Τη λίστα αυτή (και άλλες παρόμοιες) χρησιμοποιούν οι περισσότεροι Internet Service Providers βλ. ιστοσελίδα www.spamhaus.org

50 Ανανεώνονται συνεχώς μέσω αναφορών των ISPs, διαχειριστών mail servers ή και απλών παραληπτών spam email.

51 Η μεθοδολογία εστιάζεται στην αφαίρεση της IP διεύθυνσης του αποστολέα από τη μαύρη λίστα, ακολουθώντας την ειδική διαδικασία που προβλέπεται σε αυτές τις περιπτώσεις και περιλαμβάνει αίτηση αφαίρεσης και επιβεβαίωση του αι-

3.5.4.2 Δεύτερη Κατηγορία

Περιλαμβάνει εργαλεία εγκατεστημένα στους mail servers που αποσκοπούν στην αναγνώριση των spam emails και την αφαίρεσή τους από τα εισερχόμενα μηνύματα των παραληπτών. Η αναγνώρισή των spam email έχει φτάσει σε πολύ ικανοποιητικό βαθμό, παραμένει όμως αδύνατη η 100% αναγνώρισή τους, ενώ πάντα θα ελλοχεύει ο κίνδυνος της απώλειας ενός μηνύματος λόγω λανθασμένου χαρακτηρισμού του ως spam. Χαρακτηριστικό παράδειγμα τέτοιας εφαρμογής είναι το SpamAssassin[52].

3.6 Ασφάλεια περιεχομένου ηλεκτρονικού ταχυδρομείου

Είναι γενικά παραδεκτό ότι για το ηλεκτρονικό ταχυδρομείο, ως μορφή αλληλογραφίας, ισχύουν οι προβλεπόμενοι της συμβατικής αλληλογραφίας κανόνες που αφορούν τη διατήρηση του απορρήτου[53]. Η ανάγκη για προστασία της ηλεκτρονικής αλληλογραφίας είναι μεγαλύτερη από τη συμβατική εξαιτίας της διαρκώς αυξανόμενης χρήσης της, ενώ βαρύνουσα σημασία προσδίδει το γεγονός ότι η πρόσβαση σε αυτή δεν απαιτεί τη φυσική παρουσία (όπως στην κλασική αλληλογραφία). Επιπρόσθετα, πολλές από τις πληροφορίες που διακινούνται μέσω ηλεκτρονικού ταχυδρομείου διακρίνονται για την πολυτιμότητά τους, καθιστώντας την ηλεκτρονική αλληλογραφία στόχο υποκλοπής[54]. Παρόμοια περιστατικά δεν είναι άγνωστα και στην

τήματος. Ακολουθεί η αφαίρεση της εγγραφής από τη λίστα και επανάληψη της διαδικασίας της παραγράφου 3.5.2.

[52] Για περισσότερες πληροφορίες βλ. ιστοσελίδα http://spamassassin.apache.org/

[53] Η ελεύθερη ανταπόκριση και επικοινωνία προστατεύεται συνταγματικά από το άρθρο 19 (8 της Ευρωπαϊκής Σύμβασης των Δικαιωμάτων του Ανθρώπου και 17 του Διεθνούς Συμφώνου για τα ατομικά και πολιτικά δικαιώματα). Επίσης η παραβίαση του προσωπικού χώρου χρήστη στον οποίο φυλάσσονται οι ηλεκτρονικές επιστολές (βλ. ενότητα 3.4) αποτελεί παραβίαση του απορρήτου των επιστολών και εμπίπτει στις διατάξεις του άρθρου 370 του Ποινικού Κώδικα.

[54] Αίσθηση προκάλεσε η υπόθεση υποκλοπής από το Ισραήλ των email της συζύγου του προέδρου της Συρίας που διέρρευσε στον ημερήσιο τύπο, βλ. Οι ισραηλινοί κατασκόπευαν τα email της κυρίας Άσαντ με Ιό, εφημερίδα Το Βήμα, ενότητα διεθνή, 7/6/2005, σελ. Α23(63).

Ελλάδα αφού έχουν απασχολήσει και την ελληνική δικαιοσύνη[55]. Εντούτοις παρά την αυξημένη σημασία που δίδεται παγκοσμίως στη διαφύλαξη του απορρήτου, οι τρομοκρατικές ενέργειες στο Λονδίνο το 2005 οδήγησαν το Ευρωπαϊκό Συμβούλιο στην έκδοση την 15η Μαρτίου 2006 της οδηγίας 2006/24/ΕΚ[56] σχετικά με διατήρηση τηλεπικοινωνιακών δεδομένων και την τροποποίηση της οδηγίας 2002/58/ΕΚ. Συγκεκριμένα η οδηγία ορίζει στο άρθρο 6, ότι τα κράτη μέλη πρέπει να διασφαλίζουν ότι ορισμένες κατηγορίες δεδομένων (συμπεριλαμβανομένων και των δεδομένων κίνησης των email-όχι όμως και του περιεχομένου τους) πρέπει να διατηρούνται για χρονικό διάστημα από 6 μήνες μέχρι 2 έτη.

Παρά την αυξημένη σπουδαιότητα που έχει η ασφάλεια του περιεχομένου του ηλεκτρονικού ταχυδρομείου για τους κοινωνούς του διαδικτύου, στο σχεδιασμό του πρωτοκόλλου SMTP, δεν λήφθηκε υπόψη η μυστικότητα των μηνυμάτων[57]. Η ηλεκτρονική αλληλογραφία διατηρείται σε απλή, μη κρυπτογραφημένη μορφή στους servers του αποστολέα και του παραλήπτη και είναι τεχνικά προσβάσιμη για λόγους διαχείρισης στους διαχειριστές τους[58]. Στους οργανισμούς που διαχειρίζονται και συντηρούν τους servers ανατίθεται η υποχρέωση για διαβαθμισμένη πρόσβαση στα δεδομένα μόνο από ειδικά εξουσιοδοτημένο προσωπικό. Εκτός όμως από τη διατήρηση των μηνυμάτων και των συνημμένων σε αυτά αρχείων στους servers, αντίστοιχος είναι και ο τρόπος μεταφοράς τους μέσω του διαδικτύου. Τα μηνύματα και τα συνημμένα σε αυτά αρχεία διακινούνται ως απλό κείμενο[59] μεταξύ των mail server. Αυτό το γεγονός τα καθιστά ευάλωτα σε όλους τους

[55] Υπόθεση Μαργαρίτας Παπανδρέου κατά περιοδικού Νέμεσις για τη δημοσίευση υποκλεμμένων email της πρώτης, Βλ. ιστοσελίδες http://news.kathimerini.gr/4dcgi/_w_articles_politics_1_18/01/01_I7065073%3DI7065073%3D|01%2601-0101!cod180101$39517.html
http://archive.enet.gr/online/online_text/c=112,dt=29.11.2005,id=71453720

[56] Το πλήρες κείμενο της οδηγίας διατίθεται ηλεκτρονικά στη διεύθυνση http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EL:PDF

[57] Βλ. παραπάνω ενότητα 3.1 όπου αναφέρονται οι σχεδιαστικές αδυναμίες του SMTP.

[58] Βλ. υποσημείωση 23.

[59] Σε απλό κείμενο 7-bit ASCII μετασχηματίζονται όλα τα συνημμένα δεδομένα για να εξασφαλιστεί η μεταφορά τους χωρίς σφάλματα βλ. **Rotriguez / Catrell / Karas / Peschke**, ο.π., σελ.400.

κόμβους από τους οποίους διέρχονται τα δεδομένα[60]. Τέλος, συνήθως παραβλέπεται, όμως είναι ιδιαίτερα σημαντική η χρήση ισχυρού κωδικού πρόσβασης στο λογαριασμό ηλεκτρονικού ταχυδρομείου κάθε χρήστη, διότι μπορεί να αποτρέψει την απευθείας πρόσβαση τρίτου, καθιστώντας ανούσιο κόπο τις προσπάθειες πρόβλεψής του.

Περιγράφοντας τις παραπάνω αδυναμίες του συστήματος προκύπτει ότι η μόνη ασφαλής λύση για την εξασφάλιση του περιεχομένου της ηλεκτρονικής αλληλογραφίας είναι η κρυπτογράφησή της χρησιμοποιώντας προσωπικό ηλεκτρονικό πιστοποιητικό (βλ. παρακάτω ενότητα). Η χρήση του πιστοποιητικού εξασφαλίζει την εξ αρχής κρυπτογράφηση του περιεχομένου της επικοινωνίας. Έτσι οι αδυναμίες στην επικοινωνία ως συνέπεια του πρωτοκόλλου SMTP καλύπτονται εμμέσως.

3.7 Ηλεκτρονικά πιστοποιητικά και email. Ηλεκτρονική υπογραφή και κρυπτογράφηση

Τα ηλεκτρονικά πιστοποιητικά αποτελούν το μέσο για την παροχή "εμπιστοσύνης" μεταξύ των οντοτήτων που επικοινωνούν μέσω διαδικτύου. Η "εμπιστοσύνη" περιλαμβάνει την ταυτότητα των οντοτήτων, την ακεραιότητα και αυθεντικότητα των δεδομένων και τον αποκλεισμό δυνατότητας άρνησης της επικοινωνίας, ενώ επιτυγχάνεται χρησιμοποιώντας ηλεκτρονικές υπογραφές παραγόμενες από ηλεκτρονικά πιστοποιητικά στα πλαίσια μιας κατάλληλης υποδομής δημοσίου κλειδιού ([61]PKI-Public Key Infrastructure).

[60] Η μεταφορά των email μεταξύ των servers δεν γίνεται όπως θα νόμιζε κάποιος απευθείας μεταξύ τους. Η πληροφορία που περιέχουν αφού τεμαχίζεται σε μικρότερα πακέτα δεδομένων διέρχεται από διάφορα δίκτυα μέχρι να καταλήξει στον προορισμό της. Ένας κατάλληλος ωτακουστής (network sniffer) θα μπορούσε να συλλέξει αυτή την πληροφορία συνθέτοντας τα "διερχόμενα" πακέτα.

[61] Η υποδομή Δημοσίου κλειδιού είναι ένας συνδυασμός λογισμικού, τεχνολογιών κρυπτογραφίας και υπηρεσιών που επιβεβαιώνουν και πιστοποιούν την εγκυρότητα της κάθε οντότητας που επικοινωνεί στο διαδίκτυο. Η Υποδομή Δημοσίου Κλειδιού ενσωματώνει ψηφιακά πιστοποιητικά, κρυπτογραφία δημοσίου κλειδιού και αρχές πιστοποίησης σε ένα ασφαλές αρχιτεκτονικό σχήμα. Μια τυπική υλοποίηση της Υποδομής Δημοσίου Κλειδιού περιλαμβάνει την παροχή ψηφιακών πιστοποιητικών σε χρήστες και servers, καθώς επίσης και εργαλείων για τη διαχείριση, ανανέωση και ανάκληση των πιστοποιητικών αυτών. Για περισσότερες πληροφορίες βλ. **Carlisle Adams / Steve Lloyd**, Understanding PKI, 2nd Edition, σελ.58.

Στην περίπτωση του ηλεκτρονικού ταχυδρομείου χρησιμοποιούνται τα προσωπικά ηλεκτρονικά πιστοποιητικά[62].

Ένα προσωπικό ηλεκτρονικό πιστοποιητικό αποτελεί σύμφωνα με το ορισμό του άρθρου 2 του ΠΔ150/2001 την: "*ηλεκτρονική βεβαίωση, η οποία συνδέει δεδομένα επαλήθευσης υπογραφής με ένα άτομο και επιβεβαιώνει την ταυτότητά του*[63]". Ο πρωτεύον στόχος του προσωπικού ηλεκτρονικού πιστοποιητικού είναι παρόμοιος με αυτόν της ιδιόχειρης υπογραφής στα συμβατικά έγγραφα, δηλαδή η σύνδεση ενός εγγράφου με ένα πρόσωπο. Η διαφορά εντοπίζεται στην άϋλη φύση του εγγράφου που στην περίπτωση αυτή έχει ψηφιακή μορφή ενώ η πιστοποίηση της ταυτότητας δεν προκύπτει από την οπτική σύγκριση αλλά διαπιστώνεται με απόλυτα αξιόπιστο τρόπο (μέσω της υποδομής δημοσίου κλειδιού) εφαρμόζοντας κρυπτογραφικούς αλγορίθμους. Ταυτόχρονα εξασφαλίζεται η ακεραιότητα και αυθεντικότητα ενός μηνύματος ενώ αποτρέπεται η άρνηση της αποστολής[64]. Επίσης βεβαιώνεται η χρονική στιγμή που τέθηκε η υπογραφή. Λευτερεύον στόχος που είναι δυνατόν να επιτευχθεί παράλληλα με την ηλεκτρονική υπογραφή αποτελεί και η κρυπτογράφηση του περιεχομένου του μηνύματος.

Είναι προφανές ότι η χρήση ηλεκτρονικής υπογραφής σε ένα email καλύπτει πολλές από τις αδυναμίες που έχει το ηλεκτρονικό ταχυδρομείου ως συνέπεια του πρωτοκόλλου SMTP, με βασικότερη την πιστοποίηση του αποστολέα. Ανάλογα με το είδος των πιστοποιητικών που θα χρησιμοποιη-

[62] Υπάρχουν διάφορες κατηγορίες πιστοποιητικών ανάλογα με τη χρήση για την οποία προορίζονται. Εκτός των προσωπικών πιστοποιητικών υπάρχουν τα πιστοποιητικά server(server certificate), πιστοποιητικά αρχών πιστοποίησης (Certificate Authority) καθώς και τα πιστοποιητικά υπογραφής κώδικα-λογισμικού (code signing certificate) βλ. **Πάγκαλος / Μαυρίδης**, Ασφάλεια πληροφοριακών συστημάτων και δικτύων, σελ.221.

[63] Ο νομικός αυτό ορισμός είναι τεχνικά ακριβής και προέρχεται από την οδηγία 99/93/ΕΚ. Δεδομένο επαλήθευσης υπογραφής αποτελεί το δημόσιο κλειδί του κατόχου του πιστοποιητικού. Το δημόσιο αυτό κλειδί κρυπτογραφείται με το ιδιωτικό κλειδί μιας αρμόδιας αρχής πιστοποίησης. Έτσι προκύπτει το ηλεκτρονικό πιστοποιητικό το οποίο περιέχει και άλλες πληροφορίες σχετικά με τον κάτοχό του. Για περισσότερες πληροφορίες σχετικά με τον τρόπο λειτουργίας των πιστοποιητικών βλ. την ιστοσελίδα της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) στη διεύθυνση http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/IntroEsign.html

[64] Βλ. **Rotriguez/Gatrell/Karas/Peschke**, ο.π., σελ.662.

θούν στην αποστολή (προηγμένα ή μη ανάλογα με το αν χρησιμοποιείται αναγνωρισμένο ή όχι πιστοποιητικό), προκύπτει και διαφορετική νομική αντιμετώπιση (όπως αυτή προβλέπεται στο ΠΔ150/2001 για τις ηλεκτρονικές υπογραφές).

3.8 Επισυναπτόμενα έγγραφα σε email

Η επισύναψη ενός εγγράφου, που παράγεται από εφαρμογή επεξεργασίας κειμένου, σε ένα email γίνεται με βάση τα MIME extensions, όπως προαναφέρθηκε (ενότητα 3.3). Σε περίπτωση επισύναψης τέτοιου εγγράφου δεν προκύπτει ταυτοποίηση του αποστολέα από το επισυναπτόμενο έγγραφο. Αυτό διότι όπως είναι γνωστό τα έγγραφα που παράγονται από εφαρμογές επεξεργασίας κειμένου ενώ περιέχουν πληροφορίες σχετικά με το συντάκτη τους (στα metadata[65] του εγγράφου), εντούτοις αυτές μπορούν εύκολα να τροποποιηθούν. Τέτοια απλά έγγραφα χωρίς υπογραφή κάποιας μορφής εξομοιώνονται με τα ανυπόγραφα ιδιωτικά έγγραφα και διατηρούν την αποδεικτική δύναμη δικαστικού τεκμηρίου[66].

[65] Πρόκειται για δεδομένα που όπως λέγεται «περιγράφουν» τα δεδομένα. Προσθέτονται από το λειτουργικό σύστημα και η πρόσβαση σε αυτά στο λειτουργικό σύστημα windows γίνεται αφού επιλέξουμε το αρχείο, μετά δεξί κλικ και ιδιότητες(Properties) και στη συνέχεια ανάγνωση των καρτελών general, custom και summary.

[66] Η αξία της αποδεικτική δυνατότητας σε αυτήν την περίπτωση δεν πρέπει να υποβαθμίζεται. Απλά ηλεκτρονικά έγγραφα αποτέλεσαν την αιτία για την ανακάλυψη εγκλημάτιών που απασχολούσαν τη δικαιοσύνη για μεγάλο χρονικό διάστημα. Κλασικό παράδειγμα αποτελεί η σύλληψη και καταδίκη του Dennis Rader, του γνωστού και ως BTK serial killer στην περιοχή Wichita του Kansas. Πρόκειται για κατά συρροή δολοφόνο που διέπραξε 10 δολοφονίες στην περίοδο 1974-1991 στην περιοχή Wichita του Kansas. Μετά από κάθε δολοφονία απέστειλε επιστολή στις αρχές γνωστοποιώντας λεπτομέρειες για κάθε έγκλημα. Μότο του αποτελούσε η έκφραση Bind, Torture, Kill από την οποία προέκυψε και ο χαρακτηρισμός του ως "The BTK Killer". Ήταν ιδιαίτερα προσεκτικός στις κινήσεις του και για αυτό και παρέμενε ασύλληπτος για 30 χρόνια μέχρι το 2005. Το Φεβρουάριο του 2005 έστειλε την τελευταία του επιστολή γραμμένη σε Microsoft Word σε ένα floppy disk 1.44MB. Από τα metadata του εγγράφου προέκυψε ότι ο συγγραφέας του ήταν ο "Dennis" και η εταιρία η "Christ Lutheran Church". Απλή αναζήτηση στο Google είχε ως αποτέλεσμα τον άμεσο εντοπισμό του. Ο Dennis Rader συνελήφθη στις 25 Φεβρουαρίου 2005 και κατα-

Ειδική αντιμετώπιση όμως χρήζουν έγγραφα που παράγονται από εφαρμογές επεξεργασίας κειμένου που φέρουν ηλεκτρονική υπογραφή[67]. Τα έγγραφα αυτά έχουν αποδεικτική δύναμη που διαβαθμίζεται όπως παρακάτω:

Α) έγγραφα που φέρουν προηγμένη ηλεκτρονική υπογραφή δηλαδή υπογραφή που έχει παραχθεί από αναγνωρισμένα πιστοποιητικά σύμφωνα με το ΠΔ150/2001, εξομοιώνονται με τα ιδιωτικά έγγραφα και έχουν πλήρη αποδεικτική δύναμη[68]. Η αποδεικτική δύναμη όμως δεν επεκτείνεται και στον αποστολέα του email στο οποίο είναι συνημμένο το υπογραφέν έγγραφο. Ο αποστολέας του email και αυτός που έθεσε την υπογραφή στο συνημμένο έγγραφο μπορεί να είναι δυο διαφορετικά πρόσωπα

Β) έγγραφα που φέρουν ηλεκτρονική υπογραφή που έχει παραχθεί από μη αναγνωρισμένα πιστοποιητικά εξομοιώνονται με τις απεικονίσεις του άρθρου 444 παρ. 3 του ΚΠολΔ και παράγουν πλήρη απόδειξη μόνο για τα πράγματα ή γεγονότα που αναγράφουν, ενώ τη γνησιότητά τους πρέπει να την αποδείξει αυτός που τα επικαλείται. Όπως και παραπάνω η αποδεικτική δύναμη δεν επεκτείνεται και στον αποστολέα του email στο οποίο είναι συνημμένο το υπογραφέν έγγραφο

Πρακτικά μια τέτοια περίπτωση μπορεί να προκύψει από την αποστολή μέσω email ενός ψηφιακά υπογεγραμμένου φύλλου της εφημερίδας της κυβερνήσεως[69]. Είναι προφανές ότι ένα τέτοιο έγγραφο διατηρεί πλήρη αποδεικτική δύναμη χωρίς να ταυτοποιείται ο αποστολέας του email που το συμπεριλαμβάνει στο μήνυμα.

3.9 Συμπεράσματα

Συνοψίζοντας, μετά την παράθεση των τεχνικών ζητημάτων που αφορούν το email, καθίσταται προφανής η ομοιότητα της λειτουργίας του ηλε-

δικάστηκε σε 175 χρόνια φυλάκιση αφού βρέθηκε ένοχος για 10 δολοφονίες.
Περισσότερες πληροφορίες στις διευθύνσεις:
http://www.crimelibrary.com/news/ap/0305/03_06_btk_case.html και
http://www.garykessler.net/library/role_of_computer_forensics.html

[67] Η ηλεκτρονική υπογραφή αυτής της μορφής έχει τεθεί χρησιμοποιώντας πιστοποιητικό υπογραφής λογισμικού (code signing certificate) βλ. υποσημείωση 62.

[68] Σύμφωνα με άρθρο 3 παρ. 1 ΠΔ 150/2001. Βλ. **Σιδηρόπουλος**, Το δίκαιο του Διαδικτύου, σελ.78.

[69] Ήδη το εθνικό τυπογραφείο υπογράφει ψηφιακά την ηλεκτρονική μορφή των Φύλλων Εφημερίδος της Κυβερνήσεως αυτόματα με την παραγωγή τους.
Βλ. http://www.et.gr/products-services/products/Digital%20Sign

κτρονικού ταχυδρομείου με αυτή του συμβατικού ταχυδρομείου, ως απόρροια του πρωτοκόλλου SMTP. Ο αποστολέας ενός email δηλώνει προσωπικά την ηλεκτρονική του διεύθυνση, που μπορεί να είναι ψευδής, όπως ακριβώς ο αποστολέας μιας συμβατικής ταχυδρομικής επιστολής αναγράφει το όνομά του, μπορεί όχι το αληθινό, στο φάκελο πριν την παράδοση στο ταχυδρομείο. Αντίστοιχα, κατά την παραλαβή ενός email ο παραλήπτης γνωρίζει αξιόπιστα μόνο την IP διεύθυνση από την οποία στάλθηκε το email, όπως ο παραλήπτης μιας συμβατικής ταχυδρομικής επιστολής αναγνωρίζει την περιοχή προέλευσης της επιστολής από τη σφραγίδα του τοπικού ταχυδρομείου.

4. ΝΟΜΙΚΑ ΘΕΜΑΤΑ

4.1 Γενικά

Το δίκαιό μας ορίζει ως ηλεκτρονικό ταχυδρομείο "*κάθε μήνυμα με κείμενο, φωνή, ήχο ή εικόνα που αποστέλλεται μέσω δημοσίου δικτύου επικοινωνιών, το οποίο μπορεί να αποθηκεύεται στο δίκτυο ή στον τερματικό εξοπλισμό του παραλήπτη, έως ότου ληφθεί από τον παραλήπτη*"[70].

Ο γενικός αυτός ορισμός δεν περιλαμβάνει ως αντικείμενο αποστολής το αρχείο εφαρμογών, σε αντίθεση με την καθιερωμένη πρακτική να αποστέλλονται όλα τα είδη ηλεκτρονικών αρχείων, περιλαμβανομένων και αρχείων εφαρμογών, με ηλεκτρονικό ταχυδρομείο. Εντούτοις δεν πρέπει η παράλειψη αυτή, να χρησιμοποιείται σε συνδυασμό με την άποψη μερίδας της επιστήμης[71], ότι το αρχείο εφαρμογών δεν αποτελεί έγγραφο (διότι έχει διαφορετική λειτουργία), για να περιορίσει το περιεχόμενο του μηνύματος ηλεκτρονικού ταχυδρομείου, στη "συμβατική μορφή" του ηλεκτρονικού εγγράφου[72]. Εξάλλου υπέρ της περίπτωσης να πρόκειται για παράλειψη, εκ μέρους του νομοθέτη, να προβλέψει αυτή τη δυνατότητα, συνηγορεί το γεγονός ότι περιλαμβάνονται στον ορισμό η φωνή και ο ήχος, που δεν μπορούν να θεωρηθούν ηλεκτρονικά έγγραφα. Απαιτείται λοιπόν η διασταλτική

[70] Άρθρο 2 περ. 8 ν. 3471/2006. Ο ορισμός αυτός (προέρχεται από την οδηγία 2002/58/ΕΚ άρθρο 2 περ. η) ταυτίζεται με την τεχνική περιγραφή που δόθηκε στην ενότητα 3.3 σχετικά με τα χαρακτηριστικά του email.

[71] **Καράκωστας**, ο.π. σελ. 207, **Βελέντζας**, Δίκαιο τεχνολογίας και καινοτομίας, σελ. 111.

[72] Βλ. υποσημείωση 4.

ερμηνεία του ορισμού αυτού ώστε να περιλαμβάνει και τα αρχεία εφαρμογών ως αντικείμενο αποστολής ηλεκτρονικού ταχυδρομείου.

4.2 Το email ως έγγραφο

Ο χαρακτηρισμός του ηλεκτρονικού ταχυδρομείου ως εγγράφου διχάζει την επιστήμη. Στηριζόμενοι στον ποινικό κώδικα, μπορούμε να θεωρήσουμε ότι το email πληροί τις προϋποθέσεις του άρθρου 13εδ.γ και εμφανίζει τα χαρακτηριστικά λειτουργίας του παραδοσιακού εγγράφου, με την ιδιαιτερότητα ότι απαιτεί τη μεσολάβηση υπολογιστών και δικτύων για την παρουσίαση του περιεχομένου του, σε κατανοητή από τον άνθρωπο μορφή. Όμως είναι αμφισβητήσιμο εάν το ίδιο συμβαίνει και με τις ιδιότητες που απαιτείται, κατά γενική ομολογία, να έχει ένα έγγραφο, δηλαδή τη διάρκεια, την εγγύηση και την απόδειξη[73]. Κυριότερο πρόβλημα αποτελεί η εγγυητική λειτουργία διότι απαιτείται από τη σταθερή ενσωμάτωση να προκύπτει η πηγή προέλευσης, δηλαδή ο αποστολέας του email[74]. Στα email η πηγή προέλευσης υπάρχει, αφού είναι υποχρεωτικό να δηλώνεται η διεύθυνση του αποστολέα, χωρίς, όμως, να σημαίνει αυτό ότι πρέπει να είναι υποχρεωτικά αληθινή[75].

Το ηλεκτρονικό ταχυδρομείο υποστηρίζεται ότι μπορεί να εξομοιωθεί με έγγραφο ως μηχανική απεικόνιση του άρθρου 444 παρ. 3 του ΚΠολΔ. Στην άποψη αυτή αντιτίθεται μέρος της επιστήμης[76], υποστηρίζοντας ότι το ηλεκτρονικό έγγραφο δεν συνιστά μηχανική απεικόνιση. Τούτο διότι, δεν απεικονίζει το αποδεικτέο γεγονός, δηλαδή τη δικαιοπραξία, αλλά διαλαμβάνει απλώς σύμβολα-λέξεις που παριστάνουν το αφηρημένο νοηματικό περιεχόμενό της[77]. Πάντως, η μέχρι σήμερα νομολογία[78] θεωρεί ότι το email εμπί-

[73] Βλ. **Καράκωστας**, ο.π, σελ.207-208 και **Βελέντζας**, ο.π., σελ. 111.

[74] Ως προς τη διάρκεια, αυτή γίνεται αποδεκτό ότι είναι εφικτή αφού τα email αποθηκεύονται στους servers (δηλ σε σκληρό δίσκο-υλικό φορέα) αποστολέα και παραλήπτη. Επίσης παρέχεται απόδειξη αφού το περιεχόμενο του email προφρίζεται ή είναι απλά πρόσφορο να αποδείξει γεγονότα σημαντικά για το δίκαιο. βλ. **Καράκωστα** ο.π σελ.207-208.

[75] Πρβλ. ενότητα 3.5.2

[76] Βλ. **Χριστοδούλου** στο σχολιασμό της απόφασης 1327/2001 του μονομελούς πρωτοδικείου Αθηνών (Βλ. Δίκη 32, ενότητα 3.1, σελ.463).

[77] Το αντίθετο υποστηρίζει ο **Μπέης** Βλ. παρατηρήσεις στην ίδια απόφαση (Δίκη 32, σελ.467-468).

πτει στην έννοια του ιδιωτικού εγγράφου ως μηχανική απεικόνιση του άρθ.444 παρ. 3 του ΚΠολΔ.

4.3 Το email ως μέσο εξωτερίκευσης της βούλησης

Ένα email είναι δυνατό να χρησιμοποιηθεί για τη σύναψη ηλεκτρονικών συμβάσεων ως φορέας της δήλωσης βουλήσεως. Μια τέτοια "ηλεκτρονική" δήλωση βούλησης, εφόσον είναι μη αυτοματοποιημένη, αποτελεί κατά την κρατούσα στην επιστήμη άποψη, γνήσια δήλωση βούλησης[79], η οποία μπορεί να εξωτερικευτεί με την αποστολή email[80]. Προβληματισμό εντούτοις δημιουργούν θέματα καθορισμού του χρόνου περιέλευσης της δήλωσης βούλησης[81] με την θεωρία να διακρίνει ανάλογα με την ιδιότητα του παραλήπτη (έμπορος, ή ιδιώτης, ή χρήστης αυτόματων συστημάτων)[82].

4.4 Το email ως συστατικός ή αποδεικτικός τύπος

Το ηλεκτρονικό ταχυδρομείο μπορεί να λειτουργήσει ως συστατικός ή αποδεικτικός τύπος.

4.4.1 Ως συστατικός τύπος

Με βάση το άρθρο 160 του ΑΚ σε συνδυασμό με το 443 ΚΠολΔ και το άρθρο 8 παρ. 1 ΠΔ 131/2001, προκύπτει ότι όταν προβλέπεται έγγραφος τύπος, αυτός μπορεί να αναπληρωθεί από ηλεκτρονικό έγγραφο, εφόσον αυτό φέρει προηγμένη ηλεκτρονική υπογραφή[83]. Εξαιρέσεις προκύπτουν από το άρθρο 8 παρ. 2 ΠΔ 131/2001 όπου προβλέπεται ρητά ότι εξαιρούνται οι εμπράγματες συμβάσεις επί ακινήτων, οι συμβάσεις που καταρτίζονται ενώπιον δικαστηρίου δημόσιων αρχών ή δημόσιων λειτουργών, καθώς κι οι συμβάσεις του οικογενειακού και κληρονομικού δικαίου.

[78] Μονομελές Πρωτοδικείο Αθηνών αποφάσεις 1327/2001 (Δίκη 32 σελ.457) και 6302/2004 (Αρμενόπουλος 2007 61^Α σελ.239).
[79] Βλ. **Ιγγλεζάκης**, ο.π., σελ.129.
[80] Βλ. **Ιγγλεζάκης**, ο.π., σελ.131.
[81] Πρβλ. υποσημείωση 21.
[82] Βλ. **Ιγγλεζάκης**, ο.π., σελ.136.
[83] Βλ. **Ιγγλεζάκης**, ο.π., σελ.141.

4.4.2 Ως αποδεικτικός τύπος[84]

Ένα email μπορεί να λειτουργήσει ως αποδεικτικός τύπος. Ειδικότερα, μπορεί να θεωρηθεί ιδιωτικό έγγραφο με αποδεικτική δύναμη, σύμφωνα με το άρθρο 444 παρ. 3 ΚΠολΔ ως μηχανική απεικόνιση[85].

Στις άτυπες δικαιοπραξίες η χρήση ηλεκτρονικού εγγράφου επιτρέπεται σε κάθε περίπτωση, εφόσον τα μέρη συμφώνησαν να υπαγάγουν τη σύμβαση σε ηλεκτρονικό τύπο (159 παρ. 2 εδ α ΑΚ)[86]. Όμως, η κατάρτιση δικαιοπραξιών περιορίζεται σε μικρής οικονομικής αξίας συμβάσεις λόγω του άρθρου 393 παρ. 1 του ΚΠολΔ που περιορίζει χρηματικά την απόδειξη με μάρτυρες σε συμβάσεις μέχρι 5.869 ευρώ.

Η αποδεικτική δύναμη του ηλεκτρονικού ταχυδρομείου διαβαθμίζεται όπως παρακάτω:

Α) email που φέρει προηγμένη ηλεκτρονική υπογραφή, δηλαδή υπογραφή που έχει παραχθεί από αναγνωρισμένο πιστοποιητικό σύμφωνα με το ΠΔ 150/2001, εξομοιώνεται με ιδιωτικό έγγραφο και έχει πλήρη αποδεικτική δύναμη[87].

Β) email που φέρει ηλεκτρονική υπογραφή που έχει παραχθεί από μη αναγνωρισμένο πιστοποιητικό, εξομοιώνεται με τις απεικονίσεις του άρθρου 444 παρ. 3 του ΚΠολΔ και παράγει πλήρη απόδειξη μόνο για τα πράγματα ή γεγονότα που αναγράφει, ενώ τη γνησιότητά του πρέπει να την αποδείξει αυτός που το επικαλείται.

Γ) απλό email χωρίς υπογραφή κάποιας μορφής εξομοιώνεται με ανυπόγραφο ιδιωτικό έγγραφο και διατηρεί την αποδεικτική δύναμη δικαστικού τεκμηρίου.

Επιπρόσθετα, email μπορεί να αναπτύξει πλήρη αποδεικτική δύναμη ακόμα και εάν παρουσιάζει ελάττωμα (πχ. λήξη του πιστοποιητικού που χρησιμοποιήθηκε για την υπογραφή), το οποίο όμως έχει προβληθεί καταχρηστικά (ΚΠολΔ 116 ή και 281 ΑΚ) ή εκπρόθεσμα (πχ. ΚΠολΔ 899, αρθρ. 4 παρ. 9 Ν 2251/1994)[88].

[84] Σχετικά με την αποδεικτική δύναμη των επισυναπτόμενων σε email εγγράφων βλ. ενότητα 3.8.
[85] Βλ. **Ιγγλεζάκης** ο.π, σελ. 143.
[86] Βλ. **Σιδηρόπουλος**, ο.π., σελ. 77.
[87] Βλ. **Σιδηρόπουλος**, ο.π, σελ.78.
[88] Βλ. **Χριστοδούλου**, Επιτομή ηλεκτρονικού αστικού δικαίου, σελ. 58.

4.5 Νομολογιακή περιπτωσιολογία

Τα ελληνικά δικαστήρια σε δύο περιπτώσεις κλήθηκαν να αντιμετωπίσουν υποθέσεις που περιείχαν θέματα ηλεκτρονικού ταχυδρομείου[89]. Κυριότερη απόφαση ήταν η υπ' αριθμ. 1327/2001 του μονομελούς πρωτοδικείου Αθηνών.

Τα σφάλματα στο σκεπτικό της απόφασης είναι τα ακόλουθα:

Α) Σύγχυση εμφανίζεται στο σκεπτικό της απόφασης σχετικά με τον κωδικό με τον οποίο αναγνωρίζεται ο χρήστης στο σύστημα ηλεκτρονικού ταχυδρομείου. Ο κωδικός αυτός (password) είναι μυστικός, τον γνωρίζει μόνο ο χρήστης, χρησιμοποιείται από το χρήστη για την πρόσβαση στο χώρο που του έχει αποδοθεί και στον οποίο φυλάσσονται τα email του[90]. Δεν αποτελεί, όπως εσφαλμένα αναφέρεται, την ηλεκτρονική διεύθυνση του χρήστη. Είναι το μέσο πρόσβασης στο λογαριασμό ηλεκτρονικού ταχυδρομείου.

Β) Το σκεπτικό της απόφασης συνοπτικά είναι το ακόλουθο: το email είναι ιδιωτικό έγγραφο (ως μηχανική απεικόνιση του άρθρου 444 παρ. 3 ΚΠολΔ) και έχει αποδεικτική δύναμη με βάση το άρθρο 443 ΚΠολΔ, όπου όμως η ταυτοποίηση του εκδότη και η σύνδεσή του με το έγγραφο δεν προκύπτει με τον παραδοσιακό τρόπο της ιδιόχειρης υπογραφής, αλλά από την ηλεκτρονική διεύθυνση του αποστολέα. Η λογική στην οποία εδράζεται η αντικατάσταση αυτή (και η υποκρύπτουσα αναλογία), προκύπτει ως συνέπεια της τεχνικής της αποστολής, η οποία αντιμετωπίζόμενη ως ενιαίο σύνολο, **υποτίθεται** ότι συνδέει άρρηκτα την ηλεκτρονική διεύθυνση του αποστολέα (ταυτοποιώντας τον αφού την έχει ορίσει ο ίδιος) με το περιεχόμενο

[89] Πρόκειται για τις υποθέσεις υπ'αριθμ. 1327/2001 και 6302/2004 του μονομελούς πρωτοδικείου Αθηνών (βλ. Δίκη 32 σελ. 457 και Αρμενόπουλος 2007, σελ. 239 αντίστοιχα) Η υπ' αριθμ. 6302/2004 απόφαση ακολούθησε το σκεπτικό της απόφασης 1327/2001.

[90] Η τυχόν γνώση του κωδικού πρόσβασης (password) παρέχει στον οποιοδήποτε τρίτο τη δυνατότητα πρόσβασης στο συγκεκριμένο λογαριασμό (με επακόλουθο την ανάγνωση, διαγραφή και αποστολή email) και για αυτό διατηρείται μυστικός, ενώ προτείνεται να έχει τουλάχιστον 6 χαρακτήρες (συνδυασμό γραμμάτων και ψηφίων) που δεν είναι δυνατό να προβλεφθούν εύκολα. Το κωδικό αυτό δεν το γνωρίζει ούτε ο διαχειριστής του server (μπορεί να τον διαγράψει ή να τον αλλάξει αλλά όχι να τον διαβάσει). Σχετικά βλ. διεύθυνση http://help.meccahosting.com/email_help/SAMS_1.2_Users_Guide.pdf όπου παρουσιάζεται ο τρόπος λειτουργίας του λογισμικού διαχείρισης ηλεκτρονικού ταχυδρομείου (σελ.44)

του μηνύματος (το οποίο περιλαμβάνει και τη δήλωση βούλησής του)[91]. Έτσι η απόφαση θεωρεί ότι η ηλεκτρονική διεύθυνση εξομοιώνεται με την ιδιόχειρη υπογραφή.

Όπως είναι προφανές με βάση τα αναφερόμενα στην ενότητα 3.5.2 και με βάση το παράδειγμα που παρουσιάστηκε, η δήλωση της ηλεκτρονικής διεύθυνσης σε ένα αποστελλόμενο μήνυμα αποτελεί **ένδειξη ταυτότητας** του εκδότη. Η αποστολή μπορεί να **πιθανολογηθεί** ότι έγινε από τον νόμιμο κάτοχο της συγκεκριμένης ηλεκτρονικής διεύθυνση εφόσον αυτός ενήργησε με βάση τις περιπτώσεις 1,2 και 3 της ενότητας 3.5.1. Η ύπαρξη των περιπτώσεων 4 και 5 (ανορθόδοξη αποστολή) καθιστούν απόλυτα λανθασμένη τη βεβαιότητα απόδειξης της ταυτότητας του αποστολέα με βάση την ηλεκτρονική διεύθυνση που σημειώνεται πάνω στο απεσταλμένο μήνυμα.

Γ) Η παραπάνω ιδιότητα του ηλεκτρονικού ταχυδρομείου επηρεάζει και τα αντίγραφα των ηλεκτρονικών μηνυμάτων και τη δυνατότητα επικύρωσής τους. Έτσι, το επικυρωμένο κατά τον νόμο αντίγραφο ενός ηλεκτρονικού μηνύματος, το οποίο περιέχεται στο σκληρό δίσκο του παραλήπτη, **δεν μπορεί** να αποτελεί πλήρη απόδειξη ότι η περιλαμβανόμενη σε αυτό δήλωση, προέρχεται **με βεβαιότητα** από τον φαινόμενο αποστολέα-κάτοχο της ηλεκτρονικής διεύθυνσης αποστολέα.

Δ) Στην απόφαση αναγνωρίζεται ο κίνδυνος αποστολής του μηνύματος από άλλο πρόσωπο από αυτό στο οποίο ανήκει η συγκεκριμένη ηλεκτρονική διεύθυνση, κάνοντας χρήση αυτής (με οποιοδήποτε τρόπο) χωρίς την έγκρισή του. Όμως, ο κίνδυνος αυτός συνδέεται με την επέμβαση τρίτου, υπονοώντας επέμβαση στον κωδικό πρόσβασης του αποστολέα[92], θεωρώντας ότι "*η λειτουργία του συστήματος του ηλεκτρονικού ταχυδρομείου παρέχει εγγυήσεις για την πιστότητά της, και η οποιαδήποτε παθολογία εμφανίζεται δεν προέρχεται από ελάττωμα του συστήματος*". Αυτή η υπόθεση όμως δεν είναι ακριβής, εξαιτίας της **αδυναμίας** του συστήματος που επισημάνθηκε αναλυτικά στο τεχνικό τμήμα της ανάλυσης αυτής. **Πρέπει συνεπώς να γίνει α-**

[91] Σωστά ο **Χριστοδούλου** επισημαίνει ότι δεν είναι άρρηκτη η σύνδεση περιεχομένου με την ηλεκτρονική διεύθυνση αποστολής βλ. σχολιασμό της απόφασης. Δίκη 32 ενότητα 1.2 και 2.2, σελ.462-463.

[92] Το σκεπτικό αυτό παραβίασης επικρατεί στη θεωρία παραπέμποντας στις διατάξεις του άρθ. 370Γ ΠΚ, βλ. **Χριστοδούλου** στις παρατηρήσεις της απόφασης 1327/2001 του μονομελούς πρωτοδικείου Αθηνών (Δίκη 32 ενότητα 1.4, σελ. 462) όπου αναφέρεται σε κινδύνους υποκλοπής. Ομοίως **Βελέντζας**, ο.π., σελ. 106, υποσημείωση 25 αλλά και **Καράκωστας**, ο.π, σελ. 208, υποσημείωση 491.

ντιληπτό ότι ο κίνδυνος οικειοποίησης της διεύθυνσης του αποστολέα είναι εγγενής στο ηλεκτρονικό ταχυδρομείο εξαιτίας σχεδιασμού του πρωτοκόλλου.

Ε) Σχετικά με τον περιορισμό ουσιαστικά της ενέργειας της παραγράφου 4 του άρθρου 457 ΚΠολΔ[93] μόνο για τον αποστολέα και όχι για τον παραλήπτη, αφού αυτός μπορεί να στηρίζεται στην πιστότητα του συστήματος ηλεκτρονικού ταχυδρομείου, είναι προφανές με βάση τα παραπάνω ότι κάτι τέτοιο δεν ισχύει. Η γνησιότητα ενός μηνύματος δεν μπορεί να αποδειχθεί παρά μόνο εάν αυτό είναι ψηφιακά υπογεγραμμένο με ηλεκτρονικό πιστοποιητικό ακόμα και μη αναγνωρισμένο.

Για την ενίσχυση του τεκμηρίου της γνησιότητας ενός απλού email στην αποδεικτική διαδικασία μπορούν συμπληρωματικά να επιωθούν τα ακόλουθα: Από την ανάλυση του email με πλήρης κεφαλίδες (full headers) μπορεί να σημειωθεί η IP διεύθυνση από την οποία αυτό αποστάλθηκε. Στην συνέχεια να ζητηθούν τα αρχεία καταγραφής από τον ISP στον οποίο είναι καταχωρημένη η συγκεκριμένη IP διεύθυνση. Από αυτά προκύπτει ο χρήστης στον οποίο είχε αποδοθεί η IP διεύθυνση τη συγκεκριμένη χρονική περίοδο (Περίπτωση Dynamic IP). Με τη διαδικασία αυτή ενισχύεται η γνησιότητα του email (το τεκμήριο που καθιερώνεται δεν είναι αμάχητο αλλά εξαιρετικά ισχυρό-ανταπόδειξη μπορεί να βασιστεί μόνο σε επίκληση κοινόχρηστης IP, ή παροχή στοιχείων που αποδεικνύει ότι χρησιμοποιήθηκαν τεχνικές απόκρυψης όπως spoofed IP).

5 Συμπεράσματα

Το σύστημα ηλεκτρονικού ταχυδρομείου που χρησιμοποιείται σήμερα στο διαδίκτυο περιέχει, λόγω προχειρότητας σχεδιασμού, σημαντικές αδυναμίες. Κυριότερη είναι η **εγγενής αδυναμία της έλλειψης ελέγχου της ταυτότητας** του αποστολέα. Μεγάλο τμήμα των αδυναμιών αυτών έχει καλυφθεί κυρίως με την υιοθέτηση των ηλεκτρονικών πιστοποιητικών. Η υιοθέτηση, όμως, αυτή, δεν είναι και μάλλον δεν θα γίνει ποτέ, καθολική, αλλά αφορά μικρό τμήμα των απεσταλμένων μηνυμάτων ηλεκτρονικού ταχυδρομείου. Λόγοι εμφάνισης αυτού του φαινομένου είναι αφενός πρακτικοί, όπως η πολυπλοκότητα διαχείρισης των πιστοποιητικών και λιγότερο η δυ-

[93] Που απαιτεί στις μηχανικές απεικονίσεις η υποχρέωση απόδειξης να βαρύνει αυτόν που τις επικαλείται και τις προσάγει.

σκολία χειρισμού τους, αλλά και ψυχολογικοί λόγοι ανασφάλειας για τη φύλαξή τους.

Συνοπτικά, καταλήγουμε στο συμπέρασμα ότι, **η διεύθυνση του αποστολέα ενός μηνύματος ηλεκτρονικού ταχυδρομείου, δεν αποτελεί απόλυτα ασφαλές και αξιόπιστο κριτήριο της ταυτότητάς του, που να μπορεί να τον συνδέσει με το περιεχόμενο του μηνύματος, αλλά μόνο ένδειξη αυτής.** Επίσης, γίνεται εμφανής η γενικότερη ανάγκη (παρά την ορθότητα της κρίσης του δικαστηρίου στη συγκεκριμένη απόφαση 1327/2001, όπου, έτσι και αλλιώς δεν υπήρξε αμφισβήτηση περί της ταυτότητας του αποστολέα ηλεκτρονικού μηνύματος), αφενός για προσφυγή σε πραγματογνωμοσύνη σε περιπτώσεις σύγχρονων θεμάτων ηλεκτρονικού δικαίου, και αφετέρου για ενημέρωση του νομικού κόσμου σε θέματα νέων τεχνολογιών, όπως το ηλεκτρονικό ταχυδρομείο, ώστε στο μέλλον να συμβαδίζει η νομική σκέψη με την τεχνική πραγματικότητα.