ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΛΟΓΙΣΤΙΚΗΣ

ΑΝΑΣΤΑΣΙΑ-ΔΙΟΝΥΣΙΑ
ΣΤΑΜΑΤΗ
ΚΡΙΝΑ ΦΙΛΗ

# ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ - ΔΙΑΣΦΑΛΙΣΗ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

ΕΠΟΠΤΗΣ
ΒΑΣΙΛΕΙΟΣ ΓΟΥΓΑΣ

# ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

# 1

# ΕΠΙΧΕΙΡΗΜΑΤΙΚΑ ΜΟΝΤΕΛΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΑΓΟΡΩΝ

## ΕΙΣΑΓΩΓΗ

Το ηλεκτρονικό εμπόριο περιλαμβάνει την ηλεκτρονική ανταλλαγή φυσικών προϊόντων όπως βιβλία, CDs (Οπτικούς Δίσκους), ηλεκτρονικούς υπολογιστές, λογισμικό, εισιτήρια, κλπ., καθώς και άλλες μορφές αγαθών όπως πληροφορίες, υπηρεσίες, (π.χ. νομικές συμβουλές) κλπ. Ουσιαστικά, περικλείει όλα τα βήματα των εμπορευματικών διαδικασιών όπως είναι το on-line μάρκετινγκ, οι παραγγελίες, οι πληρωμές, η τεχνική υποστήριξη, και η διανομή των προϊόντων. [European Commission, 1997], [Mougayar, 1997].

Μορφές ηλεκτρονικού εμπορίου, όπως είναι η Ηλεκτρονική Ανταλλαγή Δεδομένων (EDI – Electronic Data Interchange), εφαρμόζονται πάνω από 20 χρόνια σε τομείς όπως είναι οι λιανικές πωλήσεις. Τα τελευταία χρόνια όμως παρατηρείται μια ραγδαία ανάπτυξη στο χώρο του ηλεκτρονικού εμπορίου. Σε αυτό συντέλεσαν το Διαδίκτυο και ο Παγκόσμιος Ιστός που διευκόλυναν την πρόσβαση των χρηστών στα ηλεκτρονικά καταστήματα και προσέφεραν εύχρηστες και χαμηλού κόστους υπηρεσίες [Πομπόρτσης, Τσούλφας, 2002].

Το ηλεκτρονικό εμπόριο με βάση το Διαδίκτυο αποτελεί ένα πολύτιμο εργαλείο για τη διεξαγωγή επιχειρηματικών συναλλαγών ενώ υπολογίζεται ότι το B2B (Business To Business - Επιχείρηση προς Επιχείρηση) θα αποτελέσει το μεγαλύτερο κομμάτι του. Με τη βοήθεια του νέου μέσου, του Διαδικτύου, διευκολύνεται η ανάπτυξη νέων μεθόδων διεξαγωγής επιχειρηματικών συναλλαγών προσανατολιζόμενες κυρίως στον πελάτη όπως για παράδειγμα η Amazon (http://www.amazon.com) και η Tesco (http://www.tesco.com). Νέοι τύποι ηλεκτρονικού εμπορίου λειτουργούν πιλοτικά σε διάφορους τομείς της βιομηχανίας, για συνεργασίες επιχείρηση-προς-επιχείρηση, επιχείρηση-προς-καταναλωτή και επιχείρηση-προς-δημόσια διοίκηση. Από τη μεριά της και η Ευρωπαϊκή Κοινότητα (http://europa.eu.int/information_society/topics/ebusiness/index_en.htm) υποστηρίζει μέσω ερευνητικών και αναπτυξιακών προγραμμάτων (IST, ESPRIT, ACTS, Innovation, κλπ.) πιλοτικά έργα για νέα επιχειρηματικά μοντέλα, τα οποία εντάσσονται σε ένα ευρύτερο πλαίσιο πολιτικών - αποφάσεων και προγραμμάτων παγκοσμίου ηλεκτρονικού εμπορίου.

Η ευχρηστία όμως των ηλεκτρονικών συναλλαγών, δεν είναι ικανό κίνητρο από μόνη της για να προσελκύσει το κοινό. Είναι αναγκαίο ο συναλλασσόμενος να μπορεί να διαφυλάξει την ακεραιότητα οποιασδήποτε ενέργειάς του μέσα στο διαδίκτυο, ειδικά όταν είναι οικονομικής φύσεως και να βεβαιωθεί ότι δεν πρόκειται να γίνει αντικείμενο εκμετάλλευσης από τρίτους. Στη σύγχρονη τεχνολογία πληροφοριών, η λεγόμενη πιστοποίηση ταυτότητας ενσωματώνεται μέσα σε άλλους μηχανισμούς ασφάλειας, όπως η κρυπτογράφηση και ο λογιστικός έλεγχος ασφάλειας, για να παρέχει την τεχνική προστασία.

Η σημαντικότερη χρήση της πιστοποίησης ταυτότητας στην τεχνολογία πληροφοριών (ΤΠ) είναι να παρασχεθεί η διαβεβαίωση ότι ο αναγραφόμενος χρήστης είναι ο έγκυρος κάτοχος του κώδικα προσδιορισμού που παρουσιάζεται. Μια άλλη χρήση της πιστοποίησης ταυτότητας στο περιβάλλον ΤΠ είναι να παρασχεθεί η διαβεβαίωση για την προέλευση και την αυθεντικότητα ενός μηνύματος κατά τρόπο ανάλογο με τη χρήση μιας υπογραφής σε μια επιστολή. Αυτή η τεχνική καλείται συχνά ψηφιακός μηχανισμός υπογραφών. Τα μέτρα πιστοποίησης ταυτότητας χρησιμοποιούνται επίσης

για να επιβεβαιώσουν ότι η άδεια εισόδου και η πρόσβαση πραγματοποιούνται στο σωστό σύστημα.

Ένας κώδικας πιστοποίησης ταυτότητας είναι τόσο αξιόπιστος όσο οι ενισχυτικοί μηχανισμοί του. Τότε υπάρχει κίνδυνος για ένα τεχνικά ειδικευμένο χάκερ, ενδεχομένως ένα μέλος προσωπικού, που μπορεί να έχει πρόσβαση στη βάση δεδομένων πιστοποίησης ταυτότητας. Μόλις μια τέτοια πρόσβαση διαρρηχθεί, ένας χάκερ μπορεί είτε να τροποποιήσει τη βάση δεδομένων άμεσα είτε να την αντιγράψει για να πραγματοποιήσει μια επίθεση στους κώδικες πιστοποίησης ταυτότητας. Η πιστοποίηση ταυτότητας μπορεί να επιτευχθεί με διάφορους τρόπους.

Οι μηχανισμοί που θα μελετηθούν είναι:

- κωδικοί πρόσβασης,
- κρυπτογραφική πιστοποίηση ταυτότητας,
- κώδικες πιστοποίησης ταυτότητας μηνυμάτων,
- trusted third part,
- σημεία ασφάλειας, και
- βιομετρική.

## 1.1 ΚΩΔΙΚΟΙ ΠΡΟΣΒΑΣΗΣ

Όπου οι πολιτικές ασφάλειας απαιτούν οι χρήστες να είναι υπεύθυνοι για τη χρήση συστημάτων, ή όπου οι κανόνες ελέγχου πρόσβασης είναι σε θέση να περιορίσουν την πρόσβαση στα συγκεκριμένα αρχεία, οι χρήστες πρέπει να προσδιοριστούν μεμονωμένα. Αυτό μπορεί να επιτευχθεί με τη χρησιμοποίηση μιας προσδιοριστικής τοποθέτησης που μπορεί να είναι το όνομα του χρήστη, ή κάποια μορφή του δομημένου κωδικού πρόσβασης και ένας κωδικός πρόσβασης για την πιστοποίηση ταυτότητας.

Ένας κωδικός πρόσβασης (password) είναι η συνηθέστερη χρησιμοποιούμενη πιστοποίηση ταυτότητας. Δεδομένου ότι ο κωδικός είναι φτηνός για να εφαρμοστεί και απλός στην διαχείριση. Η πιστοποίηση ταυτότητας βεβαιώνεται εφ' όσον είναι γνωστός ο κωδικός πρόσβασης που συνδέεται με κάθε προσδιοριστικό χρηστών μόνο στον εξουσιοδοτημένο χρήστη. Δυστυχώς, οι κωδικοί πρόσβασης είναι τρωτοί στην κακή χρήση και την επίθεση με διάφορους τρόπους. Επίσης μπορούν να καταγραφτούν και έτσι ένας πιθανός χάκερ μπορεί να τους βρει. Οι κωδικοί πρόσβασης μπορούν να

παρατηρηθούν στο σημείο της εισόδου. Μια ψευδής **sign-on** οθόνη μπορεί να παρουσιαστεί για να συλλάβει το προσδιοριστικό και τον κωδικό πρόσβασης χρηστών. Ένας χάκερ μπορεί να είναι σε θέση να προσδιορίσει τους κωδικούς πρόσβασης μέσω της παρεμπόδισης του συμβιβασμού των εκπορεύσεων από την παρεμπόδιση εξοπλισμού ή των δικτύων υπολογιστών άδειας εισόδου. Τα υποσυστήματα πιστοποίησης ταυτότητας μπορούν να υπονομευθούν και το αρχείο κωδικού πρόσβασης μπορεί να εξαχθεί ή να επιτεθεί άμεσα χρησιμοποιώντας μια λεκτική επίθεση.

Υπάρχουν διάφοροι τρόποι με τους οποίους τα σχέδια κωδικών πρόσβασης μπορούν να ενισχυθούν ενάντια στις ανωτέρω επιθέσεις. Ένας από τους αποτελεσματικότερους τρόπους ενίσχυσης σε ένα σχέδιο πιστοποίησης ταυτότητας κωδικού πρόσβασης, είναι να εξασφαλιστεί ότι μόνο οι ισχυρά δομημένοι κωδικοί πρόσβασης χρησιμοποιούνται στο σύστημα. Ακόμα κι αν υπάρχει μόνο ένας αδύνατος κωδικός πρόσβασης στο σύστημα, ολόκληρο το σύστημα μπορεί να εκτεθεί στην επίθεση.

### 1.1.1 ΠΡΟΣΤΑΣΙΑ ΚΩΔΙΚΟΥ ΠΡΟΣΒΑΣΗΣ

Η αποτελεσματικότητα ενός σχεδίου κωδικού πρόσβασης εξαρτάται από το πόσο καλά οι χρήστες προστατεύουν τους κωδικούς πρόσβασής τους, και αυτό θα εξαρτηθεί στη συνέχεια από το επίπεδο συνειδητοποίησης της ασφάλειας υπολογιστών των χρηστών. Επιπλέον, εάν στο προσωπικό ζητηθεί να υπογράψει μια δήλωση προστασίας κωδικού πρόσβασης, όταν αρχικά προμηθεύονται έναν κώδικα χρήστη (user code) και έναν κωδικό πρόσβασης χρηστών (password), τότε είναι πιθανότερο να αντιμετωπίσουν σοβαρά την απαίτηση να προστατευθεί ο κωδικός πρόσβασής τους.

### 1.1.2 ΔΟΜΗ ΚΩΔΙΚΟΥ ΠΡΟΣΒΑΣΗΣ

Η σύνθεση ενός κωδικού πρόσβασης μπορεί να είναι κρίσιμη για την επιτυχία οποιουδήποτε κωδικού πρόσβασης - βασισμένου στο σχέδιο πιστοποίησης ταυτότητας. Το μήκος και η δομή του κωδικού πρόσβασης πρέπει να παρέχουν έναν αρκετά μεγάλο αριθμό πιθανών συνδυασμών για να εξασφαλίσουν ότι οποιαδήποτε προσπάθεια σπασίματος του κωδικού πρόσβασης μέσω της δοκιμής και του σφάλματος ανιχνεύεται

προτού να σπάσουν τον κωδικό πρόσβασης. Όπου το σύστημα ελέγχου πρόσβασης επιτρέπει μόνο έναν περιορισμένο αριθμό δοκιμών πριν παράγει έναν συναγερμό ασφάλειας και αποσυνδέει τον ενδεχόμενο χρήστη, ένας μικρός κωδικός πρόσβασης μπορεί να είναι επαρκής. Όταν κανένας περιορισμός στις προσπάθειες άδειας εισόδου δεν παρέχεται ένας πολύ ισχυρότερος κωδικός πρόσβασης πρέπει να χρησιμοποιηθεί για να προστατεύσει έναν συνδεδεμένο υπολογιστή που παράγει συνεχώς τις προσπάθειες άδειας εισόδου (login) σε υψηλή ταχύτητα.

Οι κωδικοί πρόσβασης μπορούν να χρησιμοποιήσουν κανονικά είτε τον πλήρη ASCII εκτυπώσιμο κώδικα χαρακτήρων είτε μπορούν να είναι αριθμητικοί μόνο - όπως στην περίπτωση των αριθμών PIN. Το ελάχιστο μήκος οποιουδήποτε κωδικού πρόσβασης και στις δύο περιπτώσεις πρέπει να επιλεχτεί λαμβάνοντας υπόψη τον αναμενόμενο χρόνο διάρκειας του κωδικού πρόσβασης, του μέσου χρόνου που λαμβάνεται για να προσπαθήσουν μια άδεια εισόδου χωρίς την ανίχνευση ή αποσύνδεση, και του αριθμού προσπαθειών (ενδεχομένως) στους οποίους ένας χάκερ περιορίζεται από το σύστημα ελέγχου πρόσβασης. Η απλούστερη μορφή του κωδικού πρόσβασης είναι ο κοινός προσωπικός αριθμός αναγνώρισης (PIN) που χρησιμοποιείται από κοινού με τις τραπεζικές κάρτες. Το PIN είναι κανονικά ένας αριθμός τεσσάρων ψηφίων, και τα τερματικά καρτών επιτρέπουν συνήθως ένα μέγιστο τριών ανεπιτυχών προσπαθειών σύνδεσης προτού να συγκρατηθεί η κάρτα.

Οι χρήστες θα θυμηθούν έναν κωδικό πρόσβασης που έχουν επιλέξει ευκολότερα από ότι έναν που έχει παραχθεί από ένα σύστημα. Εντούτοις, πρέπει να ληφθεί προσοχή, ώστε να εξασφαλιστεί ότι η επιλογή των κωδικών πρόσβασης των χρηστών γίνεται ώστε να ελαχιστοποιηθεί η πιθανότητα μιας επιτυχούς εικασίας ή λέξης.

Οι κωδικοί πρόσβασης που αποφεύγονται περιλαμβάνουν: δομημένους κωδικούς πρόσβασης, όπως οι συνδυασμοί αρχικών και ημερομηνιών, παρωνύμια, ονόματα κατοικίδιων ζώων, όνομα του συζύγου και άλλα προφανή.

Ο καλύτερος τρόπος εγγύησης των χρηστών ώστε να μην υιοθετούν εγγενώς ανασφαλείς κωδικούς πρόσβασης είναι να χρησιμοποιούν το λογισμικό ελέγχου πρόσβασης που αναθεωρεί τον κωδικό πρόσβασης πριν την αποδοχή για να αποβάλει τις γνωστές λέξεις, να ανιχνεύσει και να αποτρέψει την επαναχρησιμοποίηση ή την κυκλική χρήση των κωδικών πρόσβασης, και να επιβάλει τέτοιους άλλους κανόνες όπως

απαιτείται από την πολιτική ασφάλειας του συστήματος. Η χρησιμοποίηση των αρχικών γραμμάτων των λέξεων που αποτελούν μια φράση θα παράσχει έναν εύκολα αναφερόμενο κωδικό πρόσβασης που δεν θα εμφανιστεί σε ένα λεξικό.

Η παραγωγή των κωδικών πρόσβασης από τον υπολογιστή επιτρέπει τη δημιουργία των ισχυρών κωδικών πρόσβασης που δεν κινούν εύκολα υποψίες, αλλά αυτοί οι κωδικοί μπορούν να είναι χωρίς νόημα και επομένως έχουν κάποιο βαθμό δυσκολίας στην απομνημόνευση. Ο υψηλός κίνδυνος είναι ότι ένας δύσκολος κωδικός πρόσβασης θα καταγραφτεί κάπου και θα ανακαλυφθεί στη συνέχεια από έναν επιτιθέμενο χάκερ. Μερικά συστήματα εξετάζουν αυτό το πρόβλημα μέσω της παραγωγής των κωδικών πρόσβασης χωρίς νόημα, αλλά να μοιάζουν με αγγλικές λέξεις, γι' αυτό συνέθεσαν μια ή περισσότερες συλλαβές ανούσιων λέξεων.

Εάν οι κωδικοί πρόσβασης παράγονται από τον υπολογιστή, η χρησιμοποιούμενη μέθοδος δεν πρέπει να είναι προβλέψιμη. Επομένως, τα συστήματα παραγωγής κωδικού πρόσβασης, απαιτούν μια τυχαία ή ψευδοτυχαία πηγή καλής ποιότητας. Οι τυχαίες γεννήτριες αριθμού που παρέχονται συνήθως στα συγκροτήματα ηλεκτρονικών υπολογιστών είναι κανονικά κατάλληλες για λόγους παραγωγής κωδικού πρόσβασης.

### 1.1.3 ΕΠΙΘΕΣΕΙΣ ΚΑΙ ΑΝΤΙΜΕΤΡΑ–ΑΝΑΚΑΛΥΨΗ ΚΩΔΙΚΟΥ ΠΡΟΣΒΑΣΗΣ

Η πιο βασική μορφή της επίθεσης σε ένα σχέδιο πιστοποίησης ταυτότητας κωδικού πρόσβασης είναι η αναρμόδια χρήση ενός γνωστού κωδικού πρόσβασης. Όλοι οι χρήστες πρέπει να γνωρίζουν την ανάγκη να κρατηθούν οι κωδικοί πρόσβασής τους ασφαλείς με την μη καταγραφή τους, την αποφυγή της επισκόπησης κατά τη διάρκεια της εισόδου, και την μη διανομή τους. Επιπλέον, οι απλοί κωδικοί πρόσβασης όπως τα επώνυμα, οι αριθμοί οδών, και οι εγγραφές αυτοκινήτων πρέπει να αποφευχθούν.

### 1.1.4 ΠΡΟΚΑΘΟΡΙΣΜΕΝΟΙ ΚΩΔΙΚΟΙ ΠΡΟΣΒΑΣΗΣ

Μια ευπάθεια σε πολλά συγκροτήματα ηλεκτρονικών υπολογιστών είναι η παρουσία προσδιοριστικών και κωδικών πρόσβασης χρηστών που οργανώθηκαν ενώπιον

ή κατά τη διάρκεια της εγκατάστασης συστημάτων. Οι συνδυασμοί **a/a,** και πολλά άλλα χρησιμοποιούνται συνήθως από τους προμηθευτές για να εκτελέσουν την εγκατάσταση συστημάτων, αλλά ξεχνιούνται να αφαιρεθούν μόλις το σύστημα καταστεί λειτουργικό. Οι χάκερ χρησιμοποιούν τους καταλόγους τέτοιων "πρότυπων" κωδικών πρόσβασης κατά την προσπάθεια ανύποπτων προσβάσεων στα συστήματα. Οι CPO των συστημάτων μπορούν να αντιμετωπίσουν αυτόν τον τύπο επίθεσης με την προσεκτική αναθεώρηση του αρχείου κωδικού πρόσβασης μόλις το σύστημα καθίσταται λειτουργικό, και σε τακτά χρονικά διαστήματα έκτοτε.

### 1.1.5 ΔΟΚΙΜΗ ΚΑΙ ΣΦΑΛΜΑ

Ένας χάκερ θα μπορούσε να δοκιμάσει μια σειρά από πιθανούς κωδικούς πρόσβασης, και εάν το τερματικό του είναι ένας μικροϋπολογιστής, μπορεί ακόμη και να υποστηριχθεί από ένα πρόγραμμα που προσπαθεί **logons** αυτόματα έως ότου βρίσκεται ο επιτυχής κωδικός πρόσβασης. Αυτό το σχέδιο μπορεί να αναχαιτιστεί με τον περιορισμό του αριθμού προσπαθειών σύνδεσης, χαρακτηριστικά σε τρεις προσπάθειες, και την έκδοση κάποιας μορφής συναγερμού εάν ο μέγιστος αριθμός αποτυχημένων προσπαθειών εξαντληθεί. Αυτή η μορφή της υπεράσπισης θα κλειδώσει συχνά το τερματικό τουλάχιστον έως ότου το επαναρυθμίσει χειροκίνητα ο χειριστής.

### 1.1.6 ΕΠΙΘΕΣΗ ΛΕΞΙΚΩΝ (Dictionary Attack)

Ακόμα και ένα αρχείο κωδικού πρόσβασης μπορεί να κρυπτογραφηθεί, και αυτό είναι τρωτό στην επίθεση. Ένας χάκερ που αποκτά πρόσβαση στο σύστημα μπορεί να είναι σε θέση να επιτεθεί στο αρχείο επί τόπου ή να το αντιγράψει σε ένα ανεξέλεγκτο περιβάλλον. Μια επίθεση λεξικών χρησιμοποιεί μια αυτοματοποιημένη βάση δεδομένων των πιθανών κωδικών πρόσβασης για να προσπαθήσει μια αντιστοιχία στο αρχείο κωδικού πρόσβασης. Τέτοιες βάσεις δεδομένων μπορούν να δημιουργηθούν απλά με την κρυπτογράφηση των λέξεων spell-check που βρίσκονται συνήθως στους επεξεργαστές λέξεων. Αυτή η επίθεση μπορεί να αντιμετωπιστεί με διάφορους τρόπους:

- **UUCP/FTP Περιορισμοί:** Ο απλούστερος τρόπος για να αντιμετωπιστεί μια επίθεση λέξεων είναι να σταματήσει κάποιος τον επιτιθέμενο στο αρχείο κωδικού πρόσβασης. Όταν ο επιτιθέμενος είναι εκτός περιβάλλοντος, οι περιορισμοί στη χρήση της εξαγωγής αρχείων δίνουν εντολές σε τέτοια χαρακτηριστικά γνωρίσματα όπως το FTP και UUCP ώστε να αποφευχθεί εξαγωγή του αρχείου κωδικού πρόσβασης (password).
- **Shadow File:** Η χρήση ενός **Shadow** αρχείου κωδικού πρόσβασης στο Unix και παρόμοια περιβάλλοντα θα δημιουργήσει περιορισμούς πρόσβασης.
- **Non-Dictionary Passwords:** Οι επιθέσεις λειτουργούν επειδή οι επιλεγμένοι κωδικοί πρόσβασης του προσωπικού μπορούν να βρεθούν σε ένα λεξικό. Η προφανής αντίδραση προς αυτήν την επίθεση είναι να εξασφαλίσει ότι οι κωδικοί πρόσβασης δεν είναι πραγματικές λέξεις που βρίσκονται στα λεξικά.

### 1.1.7 ΚΡΥΠΤΑΝΑΛΥΤΕΣ ΚΩΔΙΚΟΥ ΠΡΟΣΒΑΣΗΣ (Password Crackers)

Όλα τά κρυπτογραφημένα αρχεία κωδικού πρόσβασης είναι τρωτά στις **κρυπτοανελυμένες** επιθέσεις εάν μπορούν να προσεγγιστούν άμεσα ή να αντιγραφούν σε ένα μη ελεγμένο περιβάλλον. Το επίπεδο ευπάθειας θα εξαρτηθεί από τη γνώση του επιτιθεμένου του μηχανισμού κρυπτογράφησης και τη δύναμη του κρυπτογραφικού σχεδίου που χρησιμοποιείται. Το **GCSB** μπορεί να παρέχει κατόπιν αιτήσεως τις συμβουλές με βάση τα συγκεκριμένα συστήματα.

### 1.1.8 ΠΑΡΕΜΠΟΔΙΣΗ ΔΙΚΤΥΩΝ (Network Interception)

Ένα σημαντικό πρόβλημα με τα σύγχρονα συγκροτήματα ηλεκτρονικών υπολογιστών είναι η ευπάθεια των κωδικών πρόσβασης στην παρεμπόδιση κατά τη διάρκεια μιας απομακρυσμένης ακολουθίας σύνδεσης. Ο κεντρικός υπολογιστής θα εκδώσει χαρακτηριστικά ένα αίτημα για τον προσδιορισμό χρηστών και την πιστοποίηση ταυτότητας κωδικού πρόσβασης, και η ταυτότητα χρήστη και ο προσωπικός κωδικός θα πληκτρολογηθούν στο τερματικό και θα διαβιβαστούν στο σαφές κείμενο πίσω στον υπολογιστή. Καθένας που ελέγχει τέτοια κυκλοφορία γραμμών μπορεί να λάβει έναν

έγκυρο συνδυασμό ταυτότητας χρήστη/κωδικού πρόσβασης. Αυτό είναι ένα σημαντικό πρόβλημα στα δίκτυα τοπικής περιοχής, όπου οποιοδήποτε συνδεδεμένο τερματικό μπορεί να διαμορφωθεί για να ελέγξει όλη την κυκλοφορία δικτύων. Με την κρυπτογράφηση του κωδικού πρόσβασης πριν από τη μετάδοση θα αποφευχθεί αυτό το πρόβλημα. Αυτή η στρατηγική χρησιμοποιείται από τις αυτόματες μηχανές ταμείων και μερικά δίκτυα τοπικής περιοχής. Ένα άλλο αντίμετρο είναι να χρησιμοποιηθούν οι **one-time** κωδικοί πρόσβασης από κοινού με χειροκίνητες συσκευές πιστοποίησης ταυτότητας. Αυτό το σχέδιο συζητείται λεπτομερώς σε επόμενα κείμενα.

### 1.1.9 ΑΛΛΑ ΖΗΤΗΜΑΤΑ

Σε περίπτωση που ένας συνδυασμός ταυτότητας χρήστη/κωδικού πρόσβασης κινδυνεύει, τα τμήματα πρέπει να εξασφαλίσουν ότι η περίοδος της μη πιστοποιημένης πρόσβασης ελαχιστοποιείται. Εάν η θέση ανιχνεύεται, ο σχετικός κωδικός πρόσβασης πρέπει να ανακληθεί αμέσως. Εντούτοις, δεδομένου ότι η θέση του κωδικού πρόσβασης δεν μπορεί να ανιχνευθεί, τα συστήματα πρέπει να υφίστανται αλλαγή κωδικού πρόσβασης, ανά τακτά χρονικά διαστήματα.

Η πιθανότητα μιας μη πιστοποιημένης πρόσβασης μπορεί να μειωθεί αν οι χρήστες συμβουλεύονται την ημερομηνία και τον χρόνο της τελευταίας επιτυχούς άδειας εισόδου για κάθε χρήστη.

## 1.2 ΟΡΙΣΜΟΣ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΥ ΜΟΝΤΕΛΟΥ

Στη βιβλιογραφία σχετικά με το ηλεκτρονικό εμπόριο δεν αναφέρεται συγκεκριμένος και σαφής ορισμός του όρου **επιχειρηματικά μοντέλα (business models)** [Rappa, 2001], [Spiller, Lohse, 1997], [Timmers, 1998], γι'αυτό και στη συνέχεια της ενότητας θα προσπαθήσουμε να δώσουμε εμείς ένα. Ένα επιχειρηματικό μοντέλο είναι:

- μια αρχιτεκτονική για τα προϊόντα, τη ροή πληροφορίας και τις υπηρεσίες, ενώ περιλαμβάνει επίσης και μια περιγραφή των διαφόρων επιχειρηματικών παιχτών καθώς και των ρόλων τους,

- μια περιγραφή των πιθανών πλεονεκτημάτων και ωφελειών για τους διάφορους επιχειρηματικούς παίχτες,
- μια περιγραφή των πηγών εσόδων.

Ένα επιχειρηματικό μοντέλο από μόνο του δεν αποσαφηνίζει τον τρόπο με τον οποίο συνεισφέρει στην κατανόηση του επιχειρηματικού στόχου καμιάς από τις επιχειρήσεις που συμμετέχουν σε αυτό. Είναι απαραίτητο να γνωρίζει κανείς τη στρατηγική του μάρκετινγκ της επιχείρησης ώστε να εκτιμηθεί η εμπορική βιωσιμότητα και να μπορούν να απαντηθούν ερωτήσεις όπως:

- πώς χτίζονται ανταγωνιστικά πλεονεκτήματα;
- ποιός είναι ο καθορισμός των θέσεων;
- ποια στρατηγική πωλήσεων προϊόντων θα ακολουθηθεί;

Επομένως πρέπει να δώσουμε ορισμό και για τα μοντέλα μάρκετινγκ (marketing model). Ένα μοντέλο μάρκετινγκ είναι:

- ένα επιχειρηματικό μοντέλο,
- και η στρατηγική μάρκετινγκ της επιχείρησης που βρίσκεται υπό θεώρηση.

### 1.2.1 ΑΛΥΣΙΔΕΣ ΑΞΙΩΝ ΚΑΙ ΕΠΙΧΕΙΡΗΜΑΤΙΚΑ ΜΟΝΤΕΛΑ

Οι αρχιτεκτονικές των επιχειρηματικών μοντέλων, βασίζονται στη μελέτη της αλυσίδας αξιών (value chains), δηλαδή στο συνδυασμό των επιμέρους στοιχείων της καθώς και των τρόπων ενοποίησης των διαφόρων πληροφοριών. Επίσης λαμβάνεται υπόψη η δημιουργία ηλεκτρονικών αγορών. Οι αγορές είναι είτε πλήρως ανοιχτές δηλαδή με ακαθόριστο αριθμό πωλητών και αγοραστών, είτε μερικώς ανοικτές με έναν αγοραστή και πολλαπλούς πωλητές και το αντίθετο. Το σχέδιο που ακολουθείται αποτελείται από:

- Τη **μελέτη της αλυσίδας αξιών**, η οποία περιλαμβάνει τον καθορισμό των στοιχείων της. Συγκεκριμένα, οι Porter και Millar διέκριναν εννιά διαφορετικά στοιχεία που αποτελούν την αλυσίδα αξιών: εισερχόμενα λογιστικά, λειτουργίες,

εξερχόμενα λογιστικά, πωλήσεις και μάρκετινγκ, υπηρεσίες, υποστήριξη δραστηριοτήτων ανάπτυξης τεχνολογιών, προμήθειες, διαχείριση ανθρώπινων πόρων και εταιρική υποδομή.

- Τα **πρότυπα αλληλεπίδρασης**, τα οποία μπορεί να είναι «1-προς-1», «1-προς-πολλά», «πολλά-προς-1» και «πολλά-προς-πολλά». Το «1-προς-1» αναφέρεται στον αριθμό των εμπλεκόμενων φορέων, ενώ το «πολλά» σημαίνει συνδυασμό πληροφοριών από διαφορετικούς συμμετέχοντες.
- Τον **επαναπροσδιορισμό της αλυσίδας αξιών**, που σημαίνει την ενοποίηση της διαδικασίας πληροφόρησης κατά μήκος της. Σε μια τέτοια διαδικασία, οι συνδυασμοί γίνονται μεταξύ των στοιχείων που σχετίζονται με την αλυσίδα αξιών. Έτσι σχηματίζονται αρχιτεκτονικές επιχειρηματικών μοντέλων κατά περίπτωση, όπως για παράδειγμα, ένα **ηλεκτρονικό κατάστημα (e-shop)** είναι «1-προς-1» μάρκετινγκ και πωλήσεις. Μια **ηλεκτρονική αγορά (e-mall)** που έχει μια διαδεδομένη επωνυμία προσφέρει «πολλά-προς-1» μάρκετινγκ και πωλήσεις. Μια **ηλεκτρονική δημοπρασία (e-auction)** όπου πολλοί αγοραστές κάνουν προσφορές τιμής για προϊόντα ή υπηρεσίες ενός προμηθευτή, συνδυάζει πωλήσεις από έναν προμηθευτή σε πολλούς αγοραστές, ενώ παράλληλα συνδυάζει τις πληροφορίες προσφορών όλων των αγοραστών. Η εμπορική βιωσιμότητα κάθε επιχειρηματικού μοντέλου είναι ένα διαφορετικό θέμα που ανήκει στην ανάλυση του μοντέλου μάρκετινγκ. Τα συμπεράσματα που έχουν προκύψει από την παρατήρηση επιχειρήσεων στο διαδίκτυο είναι τα εξής:
- Οι τεχνολογίες πληροφοριών και επικοινωνιών ευνοούν την ανάπτυξη μεγάλου αριθμού επιχειρηματικών μοντέλων.
- Οι δυνατότητες των τεχνολογιών αποτελούν απλώς ένα κριτήριο κατά τη διαδικασία επιλογής του επιχειρηματικού μοντέλου.
- Η τεχνολογία από μόνη της δεν παρέχει κατευθυντήριες οδηγίες για την επιλογή του επιχειρηματικού μοντέλου.
- Η επιτυχημένη υιοθέτηση ενός νέου επιχειρηματικού μοντέλου είναι ικανή να κατευθύνει την ανάπτυξη της τεχνολογίας.
- Πολλά επιχειρηματικά μοντέλα δεν έχουν ακόμα δοκιμαστεί εμπορικά.

## 1.3 ΠΑΡΟΥΣΙΑΣΗ ΕΠΙΧΕΙΡΗΜΑΤΙΚΩΝ ΜΟΝΤΕΛΩΝ

Παρόλα αυτά ένας μικρός αριθμός από τα επιχειρηματικά μοντέλα υλοποιούνται, άλλα πειραματικά και άλλα σε πλήρη λειτουργία. Σε αυτό το σημείο περιγράφονται οι 10 γενικευμένες περιπτώσεις συνηθέστερων επιχειρηματικών μοντέλων που συναντούμε στο διαδίκτυο

### 1.3.1 ΗΛΕΚΤΡΟΝΙΚΟ ΚΑΤΑΣΤΗΜΑ (E-shop)

Πρόκειται για το ηλεκτρονικό μάρκετινγκ μιας εταιρίας ή ενός καταστήματος, αρχικά ως μέσο προώθησης των προϊόντων και υπηρεσιών της, ενώ στην πορεία προσθέτονται νέες δυνατότητες (π.χ. παραγγελία και αγορά προϊόντων ή υπηρεσιών). Στα άμεσα οφέλη της επιχείρησης περιλαμβάνονται η αυξημένη ζήτηση, η παγκόσμια παρουσία με χαμηλό κόστος και η μείωση εξόδων για διαφήμιση και πωλήσεις. Για τους καταναλωτές, τα οφέλη είναι οι χαμηλότερες τιμές, περισσότερες επιλογές, 24ωρη διαθεσιμότητα και ευκολία στην επιλογή, αγορά και παραλαβή. Στην περίπτωση επαναλαμβανόμενων επισκέψεων σε ένα ηλεκτρονικό κατάστημα, «το 1-προς-1» μάρκετινγκ βελτιώνει και εξελίσσει τη σχέση μεταξύ πελάτη και πωλητή. Τα περισσότερα εμπορικά web-sites είναι επιχείρηση-προς-καταναλωτή (B2C) και ηλεκτρονικά καταστήματα όπως για παράδειγμα ανθοπωλεία, βιβλιοπωλεία, πωλήσεις εισιτηρίων, κλπ. Ακολουθεί μια ενδεικτική λίστα e-shops ανθοπωλείων και βιβλιοπωλείων της ελληνικής αγοράς.

Ανθοπωλεία

- http://www.antonello.gr
- http://www.valentine.gr
- http://www.louloudia.gr
- http://www.vintzileos.gr
- http://www.flowers.gr
- http://www.zerbera-flowers.com

Βιβλιοπωλεία

- http://www.greekbooks.gr
- http://www.paratiritis.gr
- http://www.books-in-greek.gr
- http://www.bookstore.gr
- http://www.greekbooksonline.gr
- http://www.ianos.gr
- http://www.helassbooks.gr
- http://www.mgiurdas.gr/store.htm
- http://www.leaderbooks.gr

- . http://www.stamoulis.gr/vivliognosia
- . http://www.vivliopolis.gr
- . http://www.diavlos.gr/zach/book.htm
- . http://greekbook.vitualave.net
- . http://www.papasotiriou.gr
- . http://www.forthnet.gr/ellgr
- . http://www.katoptro.gr
- . http://www.malliaris.gr
- . http://www.protoporia.gr

### 1.3.2 ΗΛΕΚΤΡΟΝΙΚΗ ΠΡΟΜΗΘΕΙΑ (E-procurement)

Είναι η διαδικασία ηλεκτρονικής προσφοράς και προμήθειας αγαθών και υπηρεσιών. Μεγάλες εταιρίες και δημόσιες υπηρεσίες έχουν υλοποιήσει τέτοιες εφαρμογές στο Διαδίκτυο π.χ. PublicBuy.Net, (http://home.publicbuy.net/solutions/index.html), Ariba (http://www.ariba.net/solutions/procurement_overview.cfm), κλπ. Στα οφέλη περιλαμβάνονται η δυνατότητα μεγαλύτερης επιλογής από προμηθευτές που μπορεί με τη σειρά της να οδηγήσει σε χαμηλότερα έξοδα, καλύτερη ποιότητα, βελτιωμένη διανομή σε παγκόσμια κλίμακα και μειωμένα έξοδα προμηθειών (π.χ. φυλλάδια προσφορών μπορούν να «κατεβάζονται» δικτυακά από τους προμηθευτές αντί να στέλνονται μέσω του συμβατικού ταχυδρομείου). Επιπλέον, οι ηλεκτρονικές διαπραγματεύσεις και εφαρμογές μπορεί να οδηγήσουν σε ακόμη μικρότερους χρόνους, έξοδα και ευχρηστία.

Οι βασικές λειτουργίες αυτού του επιχειρηματικού μοντέλου είναι οι ακόλουθες:

- Παρουσίαση καταλόγων προϊόντων.
- Διαχείριση παραγγελιών.
- Διαχείριση πληρωμών.
- Μηχανισμός αξιολόγησης προσφορών.

### 1.3.3 ΗΛΕΚΤΡΟΝΙΚΗ ΔΗΜΟΠΡΑΣΙΑ (E- auction)

Αποτελούν την ηλεκτρονική μορφή των παραδοσιακών δημοπρασιών μέσα στις οποίες ενσωματώνονται εκτός από την παρουσίαση, οι διαδικασίες πωλήσεων,

πληρωμών και παράδοσης. Οι πηγές εσόδων για τον παροχέα της δημοπρασίας σχετίζονται με την πώληση της πλατφόρμας τεχνολογιών, τις αμοιβές των συναλλαγών και τη διαφήμιση. Τα οφέλη για τους προμηθευτές και τους αγοραστές αφορούν την αυξημένη αποδοτικότητα και την εξοικονόμηση χρόνου, τη μεγάλη ποικιλία ενώ δεν είναι απαραίτητη η φυσική μεταφορά των συναλλασσόμενων παρά μόνο όταν η επιτευχθεί η συμφωνία μεταξύ τους. Οι προμηθευτές επωφελούνται από τη μείωση των εξόδων πώλησης και διαθέτουν το στοκ τους σε χαμηλές τιμές, ενώ οι αγοραστές από τη μείωση των τιμών των προσφερόμενων αγαθών και υπηρεσιών.

Παραδείγματα ηλεκτρονικών δημοπρασιών είναι το πρόγραμμα ESPRIT Infomar (περισσότερες πληροφορίες για τα προγράμματα ESPRIT και ACTS στη διεύθυνση http://www.ispo.cec.be/ecommerce/ecomproj.htm) και το FastParts (www.fastparts.com). Άλλες γνωστές διευθύνσεις ηλεκτρονικών δημοπρασιών είναι οι ακόλουθες:

- http://www.ebay.com,
- http://auctions.yahoo.com,
- http://www.3nsold.com.

### 1.3.4 ΗΛΕΚΤΡΟΝΙΚΗ ΑΓΟΡΑ (E- mall)

Πρόκειται για συλλογή από ηλεκτρονικά καταστήματα, συνήθως συγκεντρωμένα κάτω από ένα γνωστό εμπορικό σήμα. Ένα παράδειγμα είναι η ηλεκτρονική αγορά Bodensee (http://www.emb.ch), που παρέχει πρόσβαση σε πολλά ανεξάρτητα ηλεκτρονικά καταστήματα. Όταν τέτοιες ηλεκτρονικές αγορές ειδικεύονται σε κάποιο συγκεκριμένο τομέα της αγοράς, μετατρέπονται σε βιομηχανικές αγορές, όπως η Industry.Net (http://www.industry.net), προσφέροντας επιπλέον υπηρεσίες (FAQ, φόρουμ συζητήσεων, κλειστές ομάδες χρηστών, κλπ.).

Ο διαχειριστής της ηλεκτρονικής αγοράς είναι πιθανό να μην ενδιαφέρεται για μια ανεξάρτητη επιχείρηση που φιλοξενείται στην αγορά. Αντίθετα μπορεί να αναζητήσει οφέλη μέσα από τις βελτιωμένες πωλήσεις των τεχνολογιών υποστήριξης (π.χ. η IBM – World Avenue). Εναλλακτικά οφέλη προκύπτουν μέσα από τις υπηρεσίες, από τη διαφήμιση και τη χρήση του εμπορικού σήματος. Τα οφέλη για τους πελάτες είναι η

άνεση και ευκολία στην πρόσβαση πολλών καταστημάτων ταυτόχρονα και την ευχρηστία ενός κοινού περιβάλλοντος. Αν η ηλεκτρονική αγορά βρίσκεται κάτω από ένα διαδεδομένο εμπορικό σήμα τότε επιτυγχάνεται μεγαλύτερη εμπιστοσύνη (e-trust) και επομένως αυξημένη πιθανότητα αγορών. Τα οφέλη για τα καταστήματα - μέλη είναι η μείωση των εξόδων δικτυακής παρουσίας, με σύνθετες υπηρεσίες όπως είναι οι ηλεκτρονικές πληρωμές.

Επίσης σημαντική είναι πρόσθετη κίνηση που δημιουργείται τόσο από τα γειτονικά καταστήματα στην ηλεκτρονική αγορά όσο και από την εμπορική επωνυμία κάτω από την οποία φιλοξενούνται. Έσοδα προκύπτουν από τις αμοιβές συμμετοχής (που μπορεί να συμπεριλάβουν μια συνεισφορά σε υλικό/λογισμικό καθώς και έξοδα εγκατάστασης και ελέγχου-service), από διαφημίσεις και από αμοιβές κατά τις συναλλαγές (αν η ηλεκτρονική αγορά υποστηρίζει ηλεκτρονικές πληρωμές).Η βιωσιμότητα του μοντέλου ηλεκτρονικών αγορών βρίσκεται υπό αμφισβήτηση και παραμένει υπό παρακολούθηση. Η IBM για παράδειγμα με το World Avenue, έχει αποτύχει. Ένας από τους πιθανούς λόγους μπορεί να είναι το γεγονός ότι η έννοια της «γειτονιάς» δεν μεταφράζεται σε φυσική απόσταση στον κυβερνοχώρο, όπου κάθε τοποθεσία βρίσκεται σε απόσταση ενός μόνο «κλικ». Επιπλέον, ο έμπειρος χρήστης είναι ικανός να διαχειριστεί τα διάφορα περιβάλλοντα αλληλεπίδρασης μεταξύ αγοραστών - χρηστών και επομένως δεν έλκεται περισσότερο από ένα σταθερό και ομοιόμορφο περιβάλλον αλληλεπίδρασης.

### 1.3.5 ΑΓΟΡΕΣ ΤΡΙΤΟΥ ΦΟΡΕΑ (Third Party Marketplace)

Είναι ανερχόμενο μοντέλο, χρήσιμο στις εταιρίες που επιθυμούν να παραχωρήσουν το δικτυακό τους μάρκετινγκ σε ένα τρίτο φορέα, με αποτέλεσμα να προσφέρουν τουλάχιστον ένα κοινό περιβάλλον αλληλεπίδρασης στους καταλόγους προϊόντων των προμηθευτών τους. Πολλά επιπρόσθετα χαρακτηριστικά όπως εμπορικό σήμα, πληρωμές, λογιστικά και παραγγελίες προστίθενται στις Third Party αγορές. Ένα παράδειγμα στο χώρο του επιχείρηση-προς-καταναλωτή ηλεκτρονικού εμπορίου είναι η παροχή κοινής πρακτικής μάρκετινγκ σχετικά με ένα ιδιαίτερο γεγονός, όπως το πρόσφατο πείραμα e-Christmas. Οι παροχείς δικτυακών υπηρεσιών μπορεί να χρησιμοποιήσουν το μοντέλο αυτό για επιχείρηση-προς-επιχείρηση ηλεκτρονικό εμπόριο

χρησιμοποιώντας την τεχνογνωσία τους στο διαδίκτυο. Επίσης, μπορεί να κεντρίσει το ενδιαφέρον τραπεζών και άλλων φορέων. Έσοδα δημιουργούνται από τις αμοιβές συμμετοχής, αμοιβές υπηρεσιών, συναλλαγών ή από ποσοστό επί της αξίας συναλλαγών. Τέτοια παραδείγματα είναι το TradeZone (http://tradezone.onyx.net) και το FedEx VirtualOrder (http://www.fedex.com).

### 1.3.6 ΕΙΚΟΝΙΚΕΣ ΚΟΙΝΟΤΙΚΕΣ (Virtual Communities)

Η μεγαλύτερη αξία των εικονικών κοινοτήτων προέρχεται από τα μέλη τους (πελάτες και συνεργάτες), οι οποίοι προσθέτουν τις πληροφορίες τους σε ένα βασικό περιβάλλον το οποίο παρέχεται από την εικονική κοινότητα. Οι αμοιβές συμμετοχής καθώς και οι διαφημίσεις δημιουργούν έσοδα.

Επίσης οι εικονικές κοινότητες μπορούν να αποτελέσουν ένα επιπρόσθετο εργαλείο στις υπάρχουσες πρακτικές τους μάρκετινγκ έτσι ώστε να χτίσουν μια σχέση εμπιστοσύνης με τους πελάτες τους και να πάρουν πληροφορίες ανατροφοδότησης από αυτούς. Εικονικές κοινότητες βρίσκονται σε αφθονία σε εξειδικευμένους τομείς αγοράς όπως για παράδειγμα:

Amazon.com (http://www.amazon.com),

Apparel/garment (http://apparelex.com/bbs/index.htm),

Steelindustry (http://www.indconnect.com/steelweb),

Nanotechnology (http://www.nanothinc.com) και πολλές άλλες.

Η Firefly παρέχει μια ενδιαφέρουσα περίπτωση δημιουργίας εικονικής κοινότητας, με καινοτομία τη δημιουργία προφίλ για τους πελάτες (http://www.firefly.net).

### 1.3.7 ΠΑΡΟΧΟΣ ΥΠΗΡΕΣΙΩΝ ΑΛΥΣΙΔΑΣ ΑΞΙΩΝ (Value Chain Service Provider)

Το μοντέλο αυτό ειδικεύεται σε μια συγκεκριμένη λειτουργία, όπως είναι οι ηλεκτρονικές πληρωμές ή τα λογιστικά, με πρόθεση να την καταστήσουν ξεχωριστό και ανταγωνιστικό τους πλεονέκτημα, όπως συμβαίνει με την περίπτωση των τραπεζών, όπου η εξειδικευμένη τεχνογνωσία προσφέρεται από νέους ενδιάμεσους.

### 1.3.8 ΕΝΟΠΟΙΗΣΗ ΑΛΥΣΙΔΑΣ ΑΞΙΩΝ (Value Chain Integrators)

Το συγκεκριμένο μοντέλο βασίζεται στην ενοποίηση πολλαπλών βημάτων στην αλυσίδα αξιών εκμεταλλευόμενο τη ροή πληροφορίας αυξάνοντας την αξία μεταξύ των βημάτων αυτών. Κέρδη θα προκύψουν από αμοιβές συμβουλών και πιθανών συναλλαγών. Παράδειγμα ενός Value chain integrator είναι το πρόγραμμα ESPRIT TRANS2000 στην περιοχή πολλαπλών μεταφορών. Ο διαχειριστής προσφέρει στους πελάτες προστιθέμενη αξία από την ανταλλαγή πληροφοριών, όπως αυτή παρέχεται από ενδοδικτυακές λύσεις όπως είναι τα PartnerNet και MarshallNet. Ένα μέρος από τους παροχείς Third Party αγορών έχουν αρχίσει να μετακινούνται προς αυτή την κατεύθυνση.

### 1.3.9 ΠΛΑΤΦΟΡΜΕΣ ΣΥΝΕΡΓΑΣΙΑΣ (Collaboration Platforms)

Οι πλατφόρμες συνεργασίας παρέχουν όλα τα απαραίτητα εργαλεία για την συνεργασία μεταξύ των επιχειρήσεων. Αυτό μπορεί να γίνεται είτε μέσω συγκεκριμένου συνεργατικού σχεδίου, είτε παρέχοντας υποστήριξη μέσω μιας εικονικής ομάδας συμβούλων. Επιχειρηματικές δυνατότητες προκύπτουν κατά τη διαχείριση της πλατφόρμας (αμοιβές συμμετοχής και χρησιμοποίησης) και κατά την πώληση εξειδικευμένων εργαλείων (π.χ. για σχεδίαση, ροή πληροφοριών, διαχείριση κειμένων, κλπ.). Παραδείγματα υπάρχουν στα προϊόντα και υποπροϊόντα προγραμμάτων από Παγκόσμιο Δίκτυο Μηχανολογίας (Global Engineering Network) όπως είναι το Deutsche Telecom/Globana's ICS, το πρόγραμμα ESPRIT GENIAL και άλλα ερευνητικά προγράμματα για τρισδιάστατες συνεργατικές σχεδιάσεις.

### 1.3.10 ΑΝΑΖΗΤΗΣΗ ΠΛΗΡΟΦΟΡΙΩΝ - ΥΠΗΡΕΣΙΕΣ ΕΜΠΙΣΤΟΣΥΝΗΣ (Information Brokerage - Trust and other Services)

Ένα μεγάλος εύρος από νέες υπηρεσίες πληροφόρησης έχει δημιουργηθεί ώστε να προσθέσει αξία στα τεράστια ποσά δεδομένων που είναι διαθέσιμα στα ανοικτά δίκτυα όπως είναι η αναζήτηση πληροφοριών π.χ. το Yahoo (http://www.yahoo.com), δημιουργία προφίλ πελατών, συμβουλές για επενδύσεις, κλπ. Συνήθως οι συμβουλές και

πληροφορίες πληρώνονται άμεσα είτε μέσω συνδρομής ή με πληρωμή ανάλογη της χρήσης (pay-per-use). Μια πιο ειδική κατηγορία είναι η υπηρεσίες εμπιστοσύνης, όπως αυτές παρέχονται από διάφορες αρχές πιστοποίησης, από ηλεκτρονικούς συμβολαιογράφους και από έμπιστους τρίτους φορείς. Έσοδα προκύπτουν από συνδρομές και αμοιβές από τη χρήση των υπηρεσιών καθώς και από πωλήσεις λογισμικού ή ακόμα και συμβουλών. Παράδειγμα παροχέα έμπιστων υπηρεσιών είναι η Belsign (http://www.belsign.be). Διάφορες εταιρίες συμβούλων και έρευνας αγορών προσφέρουν σήμερα υπηρεσίες πληροφοριών για εμπορικές επιχειρήσεις μέσω Διαδικτύου. Η μηχανές αναζήτησης είναι μια ειδική κατηγορία υπηρεσιών πληροφόρησης, που βασίζονται στη διαφήμιση σαν βασική πηγή εσόδων. Μεσιτικές υπηρεσίες πληροφόρησης για υποστήριξη διαπραγματεύσεων μεταξύ των επιχειρήσεων έχουν αναπτυχθεί από τα προγράμματα ESPRIT CASBA και MEMO.

## 1.4 ΚΩΔΙΚΕΣ ΠΙΣΤΟΠΟΙΗΣΗΣ ΤΑΥΤΟΤΗΤΑΣ ΜΗΝΥΜΑΤΩΝ

Η πιστοποίηση ταυτότητας του περιεχομένου των μηνυμάτων είναι ιδιαίτερα σημαντική όταν υπάρχει κίνδυνος αμελούς ή σκόπιμης τροποποίησης. Αυτό το κομμάτι περιγράφει τις διάφορες κρυπτογραφικές διαδικασίες που μπορούν να χρησιμοποιηθούν για να παραγάγουν έναν ασφαλή κώδικα πιστοποίησης ταυτότητας μηνυμάτων (MAC) για τα μηνύματα που διαβιβάζονται πέρα από τα δίκτυα υπολογιστών. Η παραγωγή της MAC είναι ένα ουσιαστικό μέρος της διαδικασίας των ψηφιακών υπογραφών.

Η γενεά της MAC επιτυγχάνεται με το μετασχηματισμό ενός μηνύματος με τρόπο τέτοιο που να παράγει ένα σχετικά μικρό στοιχείο το οποίο θα εξαρτάται εξ ολοκλήρου από το περιεχόμενο μηνυμάτων. Στην χρήση, η MAC επισυνάπτεται ή ενσωματώνεται στο διαβιβασθέν μήνυμα: ο παραλήπτης επαναλαμβάνει τη διαδικασία παραγωγής της MAC μετά από το λαμβανόμενο μήνυμα, και ελέγχει ότι η υπολογισμένη MAC είναι ίδια με αυτήν που παρέχεται το μήνυμα. Η MAC μπορεί επίσης να αναφερθεί ως "αφομοίωση μηνυμάτων".

Τα κριτήρια σχεδίου για έναν αλγόριθμο της MAC είναι:

- Η διαδικασία πρέπει να είναι υπολογιστικά ιδιαίτερα αποδοτική, προκειμένου να ελαχιστοποιηθούν τα γενικά έξοδα στο σύστημα μηνύματος.

- Ο αλγόριθμος πρέπει να είναι αρκετά σύνθετος για να καταστήσει υπολογιστικά απραγματοποίητη την παραγωγή ενός ψεύτικου μηνύματος που ταιριάζει με τη γνωστή MAC, προκειμένου να ελαχιστοποιηθεί ο κίνδυνος σκόπιμης τροποποίησης μηνυμάτων.

- Ο αλγόριθμος πρέπει να λειτουργήσει όπως μια μονόδρομη λειτουργία, δηλ. θα πρέπει να είναι αδύνατον να συναγάγεται οποιοδήποτε μέρος του μηνύματος από τη MAC.

- Τέλος ο αλγόριθμος πρέπει να είναι ισχυρός για να εξασφαλίσει ότι η μικρότερη πιθανή αλλαγή στο μήνυμα (η παραμικρή τροποποίηση) ανιχνεύεται ακριβώς.

### 1.4.1 ΠΡΟΤΥΠΟ ISO 9797

Η οργάνωση διεθνών προτύπων (ISO) έχει παράγει πρότυπα, **ISO 9797**, το οποίο προσδιορίζει την παραγωγή της MAC. Τα πρότυπα περιλαμβάνουν τη χρήση κάποιου συμμετρικού κρυπτογραφικού αλγορίθμου (π.χ. **DES**) αλλά δεν προσδιορίζουν κάποιον ιδιαίτερο. Η παραγωγή της MAC επιτυγχάνεται ως εξής:

- Εάν είναι απαραίτητο, το κείμενο μηνυμάτων να είναι παραγεμισμένο σε ένα κατάλληλο μήκος που χρησιμοποιεί δυαδικές μηδενικές τιμές, προκειμένου να γίνει το μήκος μηνυμάτων ένα πολλαπλάσιο του κρυπτογραφικού βασικού μήκους **ν**. Μια εναλλακτική μέθοδος στα πρότυπα επιτρέπει την επισύναψη ενός δυαδικού ένα (1), έπειτα παραγεμίζει με το δυαδικό μηδέν (0).
- Το στοιχείο διαιρείται επάνω σε **ν** - ομάδες δεδομένων δυαδικών ψηφίων.
- Ένα αρχικό πλήκτρο τυχαία ή ψευδο-τυχαία παράγεται.
- Η πρώτη ομάδα δεδομένων του μηνύματος κρυπτογραφείται χρησιμοποιώντας το αρχικό πλήκτρο, παράγοντας μια ομάδα δεδομένων του κρυπτογραφήματος στο

ίδιο μέγεθος όπως της εισόδου.

- Το κρυπτογράφημα ως αποτέλεσμα της προηγούμενης διαδικασίας κρυπτογράφησης είναι αποκλειστικό χρησιμοποιείται ως είσοδος στον επόμενο κύκλο της κρυπτογράφησης όπως ανωτέρω.
- Αυτή η διαδικασία επαναλαμβάνεται για κάθε ομάδα δεδομένων στο μήνυμα έως ότου κρυπτογραφηθεί και η τελευταία ομάδα δεδομένων και το κρυπτογράφημα ως αποτέλεσμα της κρυπτογράφησης της τελικής ομάδας δεδομένων του μηνύματος είναι η MAC (τα πρότυπα επιτρέπουν ένα **μ** - MAC δυαδικών ψηφίων με τη χρησιμοποίηση των **leftmost** δυαδικών ψηφίων **μ**).
  Η παραγωγή της MAC του ISO 9797 είναι αποτελεσματική στις περισσότερες κυβερνητικές εφαρμογές.

### 1.4.2 ΠΡΟΤΥΠΟ ΠΙΣΤΟΠΟΙΗΣΗΣ ΤΑΥΤΟΤΗΤΑΣ ANSI X9.9

Το Αμερικανικό Εθνικό Ίδρυμα Προτύπων (Ansi) έχει δημοσιεύσει πρότυπα πιστοποίησης ταυτότητας μηνυμάτων για τους χρηματοδοτικούς οργανισμούς που μπορούν να παράγουν **32-bit, 48-bit**, ή **64-bit MACs**. Τα πρότυπα επιτρέπουν την εκλεκτική πιστοποίηση ταυτότητας, δηλ. την πιστοποίηση ταυτότητας των μερών ενός μηνύματος, καθώς επίσης και ολόκληρων μηνυμάτων. Ο **X9.9** αλγόριθμος πιστοποίησης ταυτότητας είναι ίδιος με αυτόν που καθορίζεται στα πρότυπα του ISO 9797, που χρησιμοποιούν έναν **64-bit** κρυπτογραφικό αλγόριθμο και **32-.,48-**, ή **64-bit MACs**. Το **X9.9** είναι κατάλληλο για εκείνες τις κυβερνητικές εφαρμογές που απαιτούν ένα μέτριο επίπεδο πιστοποίησης ταυτότητας.

## 1.5 ΕΜΠΙΣΤΟΙ ΤΡΙΤΟΙ ΦΟΡΕΙΣ (TRUSTED THIRD PARTIES)

Οι χρήστες σε ένα διανεμημένο σύστημα πρέπει συχνά να επικυρώσουν τους χρήστες Η/Υ ή τα μηνύματα. Η διαχείριση των δικτύων υπηρεσιών ασφάλειας θα μπορούσε να παρασχεθεί κεντρικά μέσω της χρήσης των γνωστών κεντρικών υπολογιστών πιστοποίησης ταυτότητας ή **Trusted Third Parties (TTPs)**. Ένα **TTP**

μπορεί να παρέχει διάφορες υπηρεσίες πιστοποίησης ταυτότητας:

- πιστοποίηση ταυτότητας ενός χρήστη σε ένα σύστημα, για να παρέχει τη διαβεβαίωση ότι ο χρήστης είναι πραγματικά αυτός που ισχυρίζεται.
- πιστοποίηση ταυτότητας ενός συστήματος σε έναν χρήστη, για να παρέχει την διαβεβαίωση της ταυτότητας του συστήματος.
- παραγωγή και διανομή των κοινών κρυπτογραφικών πλήκτρων περιόδου επικοινωνίας.
- πιστοποίηση ταυτότητας των κατώτερων κεντρικών υπολογιστών πιστοποίησης ταυτότητας, σε ένα ιεραρχικό δίκτυο.
- διαιτησία των διαφωνιών σχετικά με την αυθεντικότητα μηνυμάτων και
- εγκαταστάσεις για να ανακαλέσει τα πιστοποιητικά ταυτότητας και τα πλήκτρα περιόδου επικοινωνίας.

### 1.5.1 ΠΙΣΤΟΠΟΙΗΣΗ ΤΑΥΤΟΤΗΤΑΣ ΧΡΗΣΤΩΝ ΑΠΟ ΕΜΠΙΣΤΟ ΤΡΙΤΟ ΦΟΡΕΑ

Οι κρυπτογραφικές τεχνικές είναι ένα ουσιαστικό μέρος των λειτουργιών **TTP**. Η ακεραιότητα, η επικαιρότητα, και η εμπιστευτικότητα των μηνυμάτων μεταξύ ενός κεντρικού υπολογιστή ασφάλειας και των συμμετεχόντων συστημάτων χρηστών Η/Υ πρέπει να βεβαιωθούν συνολικά για τον κεντρικό υπολογιστή πιστοποίησης ταυτότητας που εμπιστεύονται. Το **TTP** πρέπει πρώτα να προσδιορίσει και να επικυρώσει έναν χρήστη με τη βοήθεια της επαλήθευσης κωδικού πρόσβασης, των σημείων, των έξυπνων καρτών, ή των ψηφιακών τεχνικών υπογραφών. Μόλις επικυρωθεί ο χρήστης, το **TTP** μπορεί να παράγει τα πλήκτρα περιόδου επικοινωνίας άμεσα και να τα διαβιβάσει στο χρήστη και στο σύστημα στο οποίο ο χρήστης επιδιώκει την πρόσβαση, ή μπορεί να χορηγήσει ένα εισιτήριο ή ένα πιστοποιητικό που περιέχουν τα πλήκτρα περιόδου επικοινωνίας και επιτρέπουν στον κάτοχο να αποκτήσει πρόσβαση στο σύστημα στόχων για μια καθορισμένη χρονική περίοδο.

### 1.5.2 ΤΟ ΣΥΣΤΗΜΑ ΚΕΡΒΕΡΟΣ (Kerberos)

**Kerberos** είναι ένα παράδειγμα ενός συστήματος **TTP**. Χρησιμοποιεί DES και

είναι βασισμένο στη χρήση ενός κεντρικού υπολογιστή πιστοποίησης ταυτότητας **Kerberos (KAS)**, και ενός κεντρικού υπολογιστή Ticket-Granting **(TGS)** όπου και τα δύο είναι εμπιστευόμενες οντότητες σε ένα δίκτυο. Ένας χρήστης μοιράζεται ένα προσχεδιασμένο μυστικό πλήκτρο με το **KAS** για την αρχική πιστοποίηση ταυτότητας. Μόλις επικυρωθεί ο χρήστης, στα συστήματα **KAS** παίρνει ένα εισιτήριο που ισχύει για μια χρονική περίοδο και που εξουσιοδοτεί το φορέα για να λάβει άλλα εισιτήρια που περιέχουν τα πλήκτρα περιόδου επικοινωνίας από τα **TGS.** Τα εισιτήρια που χορηγούνται από το **TGS** είναι περιορισμένης διάρκειας, δείχνουν την ημερομηνία και το χρόνο του ζητήματος και της ισχύος του εισιτηρίου, και περιέχουν το προσδιοριστικό του χρήστη και τα συμμετρικά πλήκτρα περιόδου επικοινωνίας.

### 1.5.3 ΤΟ ΠΡΟΤΥΠΟ ANSI X9.17

Τα πρότυπα **ANSI X9.17** στη βασική διαχείριση ενσωματώνουν τη χρήση ενός βασικού κέντρου μεταφράσεων **Key Translation Center (KTC)** που παρέχει τις υπηρεσίες πιστοποίησης ταυτότητας. Η διαδικασία πιστοποίησης ταυτότητας χρησιμοποιεί τη συμμετρική κρυπτογράφηση **(Symmetric Encryption-DES)** για να παρέχει τα εμπιστευμένα μονοπάτια μεταξύ του **KTC** και των οντοτήτων δικτύων. Χρησιμοποιεί τη MAC που προσδιορίζεται στα πρότυπα **Ansi X9.9** για την πιστοποίηση ταυτότητας μηνυμάτων.

### 1.5.4 ΥΠΗΡΕΣΙΕΣ ΤΟΥ ISO TTP

Ο **ISO** έχει αυτήν την περίοδο τα σχέδια εργασίας των **Trusted Third Party** για τα δίκτυα διασύνδεσης ανοικτών συστημάτων (Open Systems Interconnect-OSI), και τα πρότυπα του **ISO 11770-3** προσδιορίζουν το ρόλο μιας συγκεκριμένης μορφής **TTP** αποκαλούμενης αρχή **(Certification Authority-CA)** πιστοποίησης.

Η βασική λειτουργία του **ISO TTP** περιλαμβάνει: πιστοποίηση ταυτότητας των οντοτήτων που χρησιμοποιούν τις υπηρεσίες του **TTP**, υπογραφή, σφράγιση και ηλεκτρονικό έγγραφο πριν από τη μετάδοση, εγγραφή του εγγράφου, πιστοποίηση των γραμματοσήμων χρόνου και ημερομηνίας ενός εγγράφου και πιστοποίηση του περιεχομένου ενός εγγράφου.

Το **TTP** θα παράγει τα πιστοποιητικά ασφάλειας για τις οντότητες δικτύων πριν από οποιαδήποτε χρήση των ασυμμετρικών βασικών ζευγαριών. Το πιστοποιητικό θα έχει μια καθορισμένη περίοδο. Μια ιεραρχία **CAs** μπορεί να υπάρξει για να παρέχει τις υπηρεσίες πιστοποίησης ταυτότητας στα μεγαλύτερα δίκτυα.

## 1.6 ΒΙΟΜΕΤΡΙΚΗ

Η βιομετρική τεχνολογία μπορεί να χρησιμοποιηθεί για να επικυρώσει ένα πρόσωπο με τη μέτρηση μερικών προσωπικών ιδιοτήτων. Οι μετρήσεις ιδιοτήτων καταχωρούνται σε έναν πίνακα ή μια βάση δεδομένων αναφοράς και ελέγχονται κάθε φορά που επιδιώκει να αποκτήσει πρόσβαση ο χρήστης. Γενικά οι βιομετρικές τεχνικές πιστοποίησης ταυτότητας είναι, ακόμα σε ένα αρχικό στάδιο ανάπτυξης. Δύο ζητήματα είναι σημαντικά στην πιστοποίηση ταυτότητας: αρχικά ένας εξουσιοδοτημένος χρήστης δεν πρέπει να αμφισβητήσει λανθασμένα την πρόσβαση, και δεύτερον ένας αναρμόδιος χρήστης δεν πρέπει να επιτραπεί να αποκτήσει πρόσβαση.

Στην περίπτωση των τεχνικών πιστοποίησης ταυτότητας που περιγράφονται στα προηγούμενα τμήματα, τα ποσοστά σφάλματος είναι χαρακτηριστικά εξαιρετικά χαμηλά ή ανύπαρκτα δεδομένου ότι οι σταθερές τιμές ανταλλάσσονται σύμφωνα με έναν προσδιορισμένο τύπο ή έναν αλγόριθμο. Στην περίπτωση της βιομετρικής, εντούτοις, τα χαρακτηριστικά που μετρισύνται μπορούν νόμιμα να αλλάξουν, και πρέπει να ληφθούν μέριμνες για αυτές τις παραλλαγές ώστε να ελαχιστοποιήσουν τις ψεύτικες απορρίψεις. Δύο κοινά μέτρα της ποιότητας που συνδέονται συχνά με τις βιομετρικές συσκευές είναι το λανθασμένο ποσοστό αποδοχής (**False Acceptance Rate-FAR**) και το (**False Reject Rate-FRR**).

### 1.6.1 ΔΑΚΤΥΛΙΚΑ ΑΠΟΤΥΠΩΜΑΤΑ

Τα δακτυλικά αποτυπώματα έχουν γίνει αποδεκτά προσδιορίζοντας τα άτομα για περισσότερα από ένα εκατό έτη. Οι σαρωτές δακτυλικών αποτυπωμάτων είναι αυτή την χρονική περίοδο στην αγορά. Είναι μικροί και φτηνοί να χρησιμοποιηθούν ως συσκευές

πιστοποίησης ταυτότητας και να ελέγξουν την πρόσβαση στα συγκροτήματα ηλεκτρονικών υπολογιστών. Οι σαρωτές ενσωματώνουν την τεχνολογία απεικόνισης για να συλλάβουν τις λεπτομέρειες δακτυλικών αποτυπωμάτων, χρησιμοποιούν την ικανότητα επεξεργασίας ώστε να αναλυθεί το δακτυλικό αποτύπωμα και να εξαχθούν οι βασικές παράμετροι, και τη λογική για να μεταφέρουν αυτές τις τιμές σε ένα σύστημα ελέγχου πρόσβασης. Το σύστημα χρησιμοποιεί τις καταχωρημένες παραμέτρους και αρνείται ή εγκρίνει την πρόσβαση ανάλογα με την περίπτωση.

### 1.6.2 ΑΝΙΧΝΕΥΣΕΙΣ ΦΩΝΗΣ

Τα χαρακτηριστικά της φωνής ενός χρήστη μπορούν να χρησιμοποιηθούν για να προσδιορίσουν ένα άτομο ακόμη και αν αυτά αλλάζουν κατά τη διάρκεια του χρόνου ή λόγω κάποιας ασθένειας. Η τεχνολογία για να συλλάβει την ομιλία και να προσδιορίσει τα μεμονωμένα χαρακτηριστικά είναι ώριμη αν και οι παρούσες εμπορικές συσκευές είναι ακόμα αρκετά ακριβές. Ο χρήστης λέει μια γνωστή λέξη ή μια φράση σε ένα μικρόφωνο, και ένας επεξεργαστής εξάγει τα βασικά χαρακτηριστικά που μπορούν έπειτα να συγκριθούν.

### 1.6.3 ΠΡΟΤΥΠΑ ΑΜΦΙΒΛΗΣΤΡΟΕΙΔΩΝ

Το πίσω μέρος του ανθρώπινου ματιού ποικίλλει από το ένα άτομο στο άλλο, με τον ίδιο σχεδόν τρόπο όπως τα δακτυλικά αποτυπώματα. Οι συσκευές ταιριάσματος προτύπων αμφιβληστροειδών απαιτούν από το χρήστη να εξεταστεί από μια οπτική μονάδα, η οποία χαρτογραφεί τον αμφιβληστροειδή με την χρήση μιας ακτίνας φωτός και παράγει τα χαρακτηριστικά που επικυρώνουν το πρόσωπο. Αυτή η τεχνολογία απαιτεί ογκώδη εξοπλισμό ακρίβειας και ταιριάζει περισσότερο στην ασφάλεια εγκαταστάσεων.

### 1.6.4 ΠΡΟΤΥΠΑ PALM PATTERNS (ΑΝΑΓΝΩΡΙΣΗΣ ΠΑΛΑΜΗΣ)

Η μορφή ενός χεριού ποικίλλει από ένα άτομο σε άλλο με τον ίδιο τρόπο όπως ένα δακτυλικό αποτύπωμα και μπορεί να χρησιμοποιηθεί ομοίως για να επικυρώσει ένα

πρόσωπο. Ο εξοπλισμός τείνει να είναι φυσικά ογκώδης και ταιριάζει έτσι καλύτερα στον έλεγχο της πρόσβασης στην ασφάλεια εγκαταστάσεων παρά στις εφαρμογές πρόσβασης σε υπολογιστές.

### 1.6.5 ΑΝΑΛΥΣΗ ΓΡΑΦΗΣ

Οι κινήσεις μιας πέννας όταν ένας χρήστης γράφει μια συγκεκριμένη λέξη ή μια υπογραφή μπορούν να μετρηθούν ακριβώς από την άποψη της απόστασης, της γωνίας, της πίεσης, και της ταχύτητας. Αυτές οι παραμετρικές τιμές ποικίλλουν ευρέως από χρήστη σε χρήστη για μια δεδομένη λέξη, και μπορούν να μετρηθούν σχετικά απλά και φτηνά χρησιμοποιώντας ένα αντικείμενο του εξοπλισμού που περιέχει τους αισθητήρες και τα επιταχύμετρα θέσης. Η σύλληψη της γραπτής λέξης εκτελείται από μια μονάδα που περιέχει μια ειδική πέννα και που γράφει χαρακτηριστικά στην επιφάνεια. Οι τιμές που προσδιορίζονται από τη διαδικασία καταχωρούνται και συγκρίνονται ενάντια σε έναν πίνακα αναφοράς για την πιστοποίηση ταυτότητας χρηστών.

### 1.6.6 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΠΛΗΚΤΡΟΛΟΓΙΩΝ

Όταν ο κώδικας Μορς χρησιμοποιήθηκε ευρέως για τις επικοινωνίες, οι χειριστές θα μπορούσαν να αναγνωρίσουν έναν βασικό χειριστή Μορς από το μεμονωμένο ύφος του. Ένα παρόμοιο χαρακτηριστικό έχει βρεθεί για να ισχύει για τη μεμονωμένη χρήση ενός πληκτρολογίου υπολογιστή. Η πιστοποίηση ταυτότητας χρηστών μπορεί να επιτευχθεί με το ταίριασμα των συγχρονισμών μεταξύ των ζευγαριών χαρακτήρων ενάντια στο καταχωρημένο σχεδιάγραμμα του χρήστη. Αυτή η τεχνική είναι κατάλληλη για την εφαρμογή σε ένα ευφυές τερματικό, αλλά δεν μπορεί να χρησιμοποιηθεί για να επικυρώσει τους απομακρυσμένους χρήστες μέσα στο δίκτυο.

# 2

# ΑΣΦΑΛΕΙΑ ΣΥΝΑΛΛΑΓΩΝ

## ΕΙΣΑΓΩΓΗ

Μέσω της διάδοσης του Διαδικτύου (Internet), οι επιχειρήσεις και οι καταναλωτές κατάφεραν να επικοινωνήσουν τόσο σε εθνικό όσο και σε παγκόσμιο επίπεδο. Οι παράγοντες που λειτούργησαν θετικά στην υιοθέτηση αυτού του τρόπου επικοινωνίας είναι το χαμηλό κόστος, η εύκολη πρόσβαση, η γρήγορη και συνεχής ενημέρωση.

Αντίστοιχα όμως εμφανίστηκαν και οι αρνητικές επιπτώσεις της χρήσης του ηλεκτρονικού εμπορίου και η πιο σημαντική με την οποία θα ασχοληθούμε είναι η ασφάλεια των συναλλαγών. Το θέμα της ασφάλειας ανησύχησε τόσο τους καταναλωτές όσο και τις επιχειρήσεις λόγω των συχνών περιπτώσεων καταστροφής δεδομένων, εξαπάτησης ή κλοπής χρημάτων, παραποίησης εγγράφων, υποκλοπής προσωπικών ή οικονομικών πληροφοριών (π.χ. αριθμοί πιστωτικών καρτών), και άλλων τέτοιων παραδειγμάτων που έχουν διαδραματιστεί κατά των πρωταρχικών εφαρμογών του ηλεκτρονικού εμπορίου.

Στο παρόν κεφάλαιο παρουσιάζονται αναλυτικά και περιγραφικά οι τεχνολογικές λύσεις που υιοθετούνται για την ασφάλεια των συναλλαγών, η πολιτική αυτής και οι

διαδικασίες που πρέπει να ακολουθηθούν για ένα ολοκληρωμένο σύστημα ηλεκτρονικού εμπορίου.

## 2.1 ΑΠΕΙΛΕΣ ΚΑΙ ΕΠΙΘΕΣΕΙΣ

Η ασφάλεια ενός συστήματος ηλεκτρονικού εμπορίου αποτελεί πρωταρχική προϋπόθεση για την επιτυχή λειτουργία του. Τα δεδομένα που ανταλλάσσονται στις διάφορες επιχειρηματικές δραστηριότητες είναι ιδιαίτερα ευαίσθητα και κατά συνέπεια ευάλωτα σε επιθέσεις και απειλές μέσω διαδικτύου. Παρακάτω παρατίθεται μια λίστα κινδύνων:

- Πρόσβαση χωρίς εξουσιοδότηση σε δικτυακούς πόρους.
- Καταστροφή πληροφοριών και δικτυακών πόρων.
- Μεταβολή, είσοδος και μετατροπή πληροφοριών.
- Αποκάλυψη πληροφοριών σε μη εξουσιοδοτημένα άτομα.
- Πρόκληση διάρρηξης και διακοπής δικτυακών υπηρεσιών.
- Κλοπή πληροφοριών και δικτυακών πόρων.
- Άρνηση λήψης υπηρεσιών και άρνηση αποστολής ή λήψης πληροφοριών.
- Ισχυρισμός κατοχής υπηρεσιών χωρίς άδεια.
- Αποκάλυψη προς τρίτους κατά τη διάρκεια της συναλλαγής εμπιστευτικών στοιχείων (όπως ο αριθμός της πιστωτικής κάρτας στην οποία χρεώνεται μία συναλλαγή, το πλήθος των αντικειμένων που παραγγέλλονται, κλπ.).

Είναι ιδιαίτερα σημαντικό να κατανοούνται οι κίνδυνοι και να αντιμετωπίζονται στα σημερινά περιβάλλοντα υπολογιστών. Έτσι ο διαχειριστής (manager) ασφαλείας μιας επιχείρησης θα είναι σε θέση να επιλέξει κατάλληλα και με καλό λόγο κόστους / απόδοσης, συστήματα που ελέγχουν και προστατεύουν τις πληροφορίες μιας επιχείρησης. Οι βασικότερες μέθοδοι προστασίας συστημάτων που εφαρμόζονται σήμερα είναι οι εξής:

- Ασφάλεια βασισμένη στην εμπιστοσύνη.
- Ασφάλεια μέσω απόκρυψης.
- Σύστημα Password.

Η δημιουργία ασφαλούς περιβάλλοντος ηλεκτρονικού εμπορίου σημαίνει προστασία των δικτυακών πόρων και οντοτήτων από ενδεχόμενες απειλές και εγγύηση τουλάχιστον του ίδιου επιπέδου ασφαλείας με το συμβατικό εμπόριο. Συνεπώς το μέλλον

του ηλεκτρονικού εμπορίου συνδέεται άμεσα με την ικανοποιητική λύση του προβλήματος της ασφάλειας.

## 2.2 ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ

### 2.2.1 Η ΣΗΜΑΣΙΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΓΙΑ ΤΙΣ ΕΦΑΡΜΟΓΕΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ

Δεδομένου ότι έχουν αναπτυχθεί πολλές ιστορίες γύρω από την ασφάλεια στο ηλεκτρονικό εμπόριο, το γεγονός αυτό έχει σαν αποτέλεσμα την επιφυλακτική αντιμετώπισή του από ένα μεγάλο μέρος του αγοραστικού και επιχειρηματικού κόσμου. Υπάρχουν πράγματι πολλοί λόγοι που το Διαδίκτυο διαφέρει και κατά συνέπεια απαιτεί ιδιαίτερη προσοχή:

- **Ο φυσικός κόσμος ενδιαφέρεται για ασφάλεια.**

  Πολλά από τα θέματα που αποκαλούνται «προβλήματα ασφαλείας» για το ηλεκτρονικό εμπόριο είναι ακριβώς ανάλογα με επιχειρηματικά θέματα του πραγματικού κόσμου. Για παράδειγμα μπορεί κάποιος να θέλει συγκεκριμένα είδη των επιχειρηματικών του επικοινωνιών να είναι ιδιωτικά, μπορεί να απαιτεί να πληρωθεί μετρητοίς ή να ζητάει προσωπικές υπογραφές στα συμβόλαια κλπ. Αυτές οι απαιτήσεις και τα μέσα που χρησιμοποιούνται για να ικανοποιηθούν έχουν αναπτυχθεί εδώ και χιλιάδες χρόνια κατά τη διάρκεια της ιστορίας του εμπορίου. Στο Διαδίκτυο τα θέματα αυτά αντιμετωπίζονται μέσα σε ένα διαφορετικό περιβάλλον και γίνονται προσπάθειες ώστε να γίνουν σαφή και κατανοητά καθώς και να αναπτυχθούν νέες λύσεις σε σύντομο σχετικά χρονικό διάστημα.

- **Οι υπολογιστές είναι διασυνδεδεμένοι.**

  Στην αρχή της ιστορίας των υπολογιστών κάποιος έπρεπε να είναι στο ίδιο δωμάτιο με τον υπολογιστή για να το χρησιμοποιήσει ή τουλάχιστον σε ένα άμεσα συνδεδεμένο τερματικό. Εφόσον λοιπόν μόνο έμπιστοι χρήστες είχαν πρόσβαση στα δωμάτια και στα τερματικά, η ασφάλεια του ίδιου του συστήματος δεν ήταν τόσο σημαντική. Στο Διαδίκτυο όμως, επιτρέπεται σε οποιονδήποτε στον κόσμο να χρησιμοποιήσει τους υπολογιστές ενός οργανισμού. Έτσι έχει δημιουργηθεί μια «τρύπα» στην ασφάλεια του οργανισμού και πρέπει οι αρμόδιοι

να είναι πολύ προσεκτικοί κατά τη σχεδίαση, υλοποίηση και λειτουργία του συστήματος τους για να διασφαλιστούν.

- **Το δίκτυο είναι δημόσιο.**

  Ένα διαδίκτυο είναι μια διασυνδεδεμένη ομάδα δικτύων και το Διαδίκτυο (με κεφαλαίο το Δ) είναι το μεγαλύτερο διασυνδεδεμένο δίκτυο δεδομένων στον κόσμο. Τα ανεξάρτητα δίκτυα ανήκουν σε χιλιάδες διαφορετικούς οργανισμούς και φορείς και δεν υπάρχει κανένας κεντρικός έλεγχος του ίδιου του δικτύου. Αυτό που κρατά το Διαδίκτυο ενωμένο είναι μια συμφωνία με κοινά πρωτόκολλα που χρησιμοποιούνται και στο γεγονός ότι τα δίκτυα επιτρέπουν την κίνηση μεταξύ τους. Με την πάροδο των χρόνων, οι τεχνολογίες και οι οργανισμοί άλλαξαν έτσι ώστε τώρα να απαιτείται το απόρρητο των συνδιαλέξεων.

- **Το δίκτυο είναι ψηφιακό.**

  Ακόμα και να έχει κάποιος πρόσβαση στο τηλεφωνικό σύστημα είναι δύσκολο ή τουλάχιστον χρονοβόρο να πάρει χρήσιμες πληροφορίες ακούγοντας τηλεφωνικές συνδιαλέξεις. Ένα δίκτυο υπολογιστών, δίνει τη δυνατότητα σε κάποιον να παρακολουθήσει πολλές συζητήσεις ταυτόχρονα. Επιπλέον, ο υπολογιστής μπορεί να ψάχνει τις συνδιαλέξεις για συγκεκριμένες φράσεις, όπως οι αριθμοί πιστωτικών καρτών χωρίς ο εισβολέας να χρειάζεται να κάνει κάποια παραπάνω δουλειά.

- **Οι υπολογιστές συλλέγουν πληροφορίες.**

  Υποθέτοντας ότι ένας πωλητής έχει ένα αρχείο για κάθε πελάτη του και ότι ένα στοιχείο σε κάθε αρχείο είναι ο αριθμός πιστωτικής κάρτας του πελάτη. Ένας εισβολέας με πρόσβαση στο χώρο που κρατάει ο πωλητής τα αρχεία του μπορεί να πάει σε καθένα από αυτά και να συλλέξει μια λίστα από αριθμούς πιστωτικών καρτών. Αν από την άλλη έχει απλώς μια απλή σελίδα όπου καταγράφει όλους τους πελάτες του και τους αριθμούς πιστωτικών καρτών τους τότε η δουλειά των εισβολέων είναι ακόμα πιο εύκολη. Τα υπολογιστικά συστήματα είναι συνήθως έτσι: οι επιθυμητές (και ευαίσθητες) πληροφορίες είναι εύκολα προσπελάσιμες ενώ υπάρχουν προγράμματα που μπορούν να χρησιμοποιηθούν για αναζητήσεις.

- **Οι υπολογιστές μπορούν να προγραμματιστούν.**
  Όπως έχει ήδη αναφερθεί ένα από τα προβλήματα είναι ότι οι υπολογιστές μπορούν να χρησιμοποιηθούν από τους εισβολείς για να ψάξουν μέσα από δεδομένα για χρήσιμες πληροφορίες. Επίσης οι υπολογιστές μπορούν να

προγραμματιστούν και για άλλες παράνομες δραστηριότητες: για επιβεβαίωση εκατοντάδων παράνομων παραγγελιών, ή για εύρεση τρόπων πρόσβασης σε άλλα υπολογιστικά συστήματα. Οι πιο έμπειροι εισβολείς μπορούν να γράψουν και να διανείμουν προγράμματα σε αρχάριους εισβολείς κάνοντας τους επικίνδυνους.

- **Χωρίς ασφάλεια, οι απάτες με υπολογιστές είναι ανεξιχνίαστες.**

  Σε ένα όχι ασφαλές υπολογιστικό σύστημα μια επίθεση μπορεί να μην αφήσει ίχνη. Τα εγκλήματα στο φυσικό κόσμο πάντα αφήνουν κάποιες φυσικές αποδείξεις (ένας μάρτυρας, δαχτυλικά αποτυπώματα, εικόνες σε κάμερες ασφαλείας κλπ.). Τα υποσυστήματα ασφαλείας και τα κρυπτογραφικά συστήματα προστατεύουν το σύστημα και παρέχουν κάποια ίχνη για το ποιες ενέργειες εκτελέστηκαν και από ποιον. Επειδή ολόκληρο το περιβάλλον δημιουργείται στον υπολογιστή πρέπει επίσης να αναπτυχθούν και αυτά τα υποσυστήματα για να εξασφαλισθεί η προστασία του συστήματος.

- **Οι υπολογιστές δεν είναι αντικαταστάτες τους ανθρώπου.**

  Από πολλές απόψεις, η λήψη παραγγελιών με τη βοήθεια υπολογιστή είναι φθηνότερη και πιο αποδοτική από το να έχουμε κάποιον υπάλληλο να απαντάει στο τηλέφωνο και να καταγράφει την παραγγελία. Από την άλλη βέβαια ο υπάλληλος είναι πιο ευέλικτος στην επικοινωνία του με ένα πελάτη ή μπορεί να εντοπίσει κάτι ασυνήθιστο στις παραγγελίες. Οι μηχανές δεν έχουν αυτή την ευελιξία. Τέλος είναι πιθανόν κάποιοι άνθρωποι να είναι πιο πρόθυμοι να πουν ψέματα σε ένα υπολογιστικό σύστημα παρά σε ένα άτομο, με αποτέλεσμα οι ενδεχόμενοι εισβολείς να είναι πολλοί περισσότεροι.

- **Το Διαδίκτυο δείχνει «ανώνυμο».**

  Με πολλούς τρόπους, η επικοινωνία μέσω του Διαδικτύου φαίνεται πιο θεωρητική, πιο απρόσωπη ή λιγότερο πραγματική από την επικοινωνία πρόσωπο με πρόσωπο ή από την επικοινωνία μέσω τηλεφώνου. Αυτό σημαίνει ότι κάποιοι άνθρωποι μπορεί να προσπαθήσουν να εξαπατήσουν ή να μπερδέψουν ένα μακρινό web site, όταν δεν θα μπορούσαν να σκεφθούν να κάνουν κάτι ανάλογο σε ένα γειτονικό μαγαζί. Αντιστρόφως, η απόσταση αυτή σημαίνει ότι το πιο σημαντικό είναι οι καταναλωτές να είναι σίγουροι ότι επικοινωνούν με την επιχείρηση που θέλουν. Είναι δύσκολο στον πραγματικό κόσμο να ξεγελαστεί κάποιος έτσι ώστε να νομίζει ότι βρίσκεται σε ένα γνωστό κατάστημα, αλλά μια τέτοια παραπλάνηση είναι πολύ πιο εύκολη στο δίκτυο. Ακόμα όμως και στο

φυσικό κόσμο, μπορούν να προκύψουν προβλήματα: υπάρχουν περιστατικά όπου είχαν εγκατασταθεί παράνομα ATMs για συλλογή αριθμών λογαριασμών και PINs.

- **Το εμπόριο πληροφοριών είναι διαφορετικό.**

  Πολλές από τις απαιτήσεις ασφαλείας βρίσκουν εφαρμογή στο εμπόριο πληροφοριών. Οι διακινούμενες πληροφορίες είναι πολύ εύκολο να αντιγραφούν, να μεταβληθούν και να διανεμηθούν. Όταν στέλνει κάποιος πληροφορίες θέλει να παραδοθούν μόνο στον αγοραστή και όχι στον οποιοδήποτε που «ακούει» παράνομα. Στο φυσικό κόσμο ο ταχυδρόμος μπορεί να αντιγράψει ένα περιοδικό, αλλά και να το κάνει, αυτό απαιτεί αρκετή προσπάθεια, όταν η αντιγραφή μιας ηλεκτρονικής έκδοσης του περιοδικού απαιτεί ελάχιστη προσπάθεια. Οι αγοραστές πληροφοριών τώρα, θέλουν να είναι σίγουροι ότι η πληροφορία που έλαβαν είναι ακριβώς αυτή που στάλθηκε. Απαιτεί αρκετή προσπάθεια για να σταματήσει και να μεταβάλλει κάποιος ένα μέρος ενός μηνύματος στο φυσικό κόσμο, ενώ είναι πολύ εύκολο να το κάνει ηλεκτρονικά. Οι πωλητές πληροφοριών θέλουν συνήθως την άμεση αποστολή τους ώστε να μη χρειάζονται περαιτέρω έλεγχοι, όπως γίνεται στις ταχυδρομικές παραγγελίες λιανικών πωλήσεων.

- **Το νομικό σύστημα πρέπει να αναδιοργανωθεί.**

  Πολλά από τα θέματα που αναφέρθηκαν παραπάνω βρίσκονται στην αρμοδιότητα του νομικού συστήματος. Όμως το νομικό σύστημα βασίζεται σε διάφορες φυσικές αποδείξεις (χαρτογραφημένα συμβόλαια, υπογραφές, διευθύνσεις, κλπ.) κατά την εξέταση κάθε υπόθεσης. Έτσι παίρνεται σαν δεδομένο ότι είναι δύσκολο να πλαστογραφηθεί η υπογραφή ενός ατόμου και άρα μπορεί να αποδειχτεί ότι κάποιος δεν υπέγραψε κάτι αν η υπογραφή φαίνεται να μην είναι σωστή. Τι όμως υποκαθιστά την υπογραφή στο ηλεκτρονικό εμπόριο, Στις περισσότερες περιπτώσεις (αν όχι σε όλες), χρησιμοποιούνται ψηφιακές υπογραφές. Πρόκειται βέβαια για μια σχετικά νέα τεχνολογία που απαιτεί κάποια προσπάθεια για να κατανοηθούν τα «λεπτά» σημεία της. Επίσης, πολλά άλλα νομικά θέματα εμπλέκονται καθώς οι τεχνολογίες αλλάζουν.

- **Υπάρχουν συγκεκριμένα σημεία επιθέσεων.**

  Τα υπολογιστικά συστήματα έχουν αποδειχθεί αρκετά ευαίσθητα σε επιθέσεις, έτσι θα πρέπει να δοθεί ιδιαίτερη προσοχή με τα νέα συστήματα ηλεκτρονικού

εμπορίου. Η ασφάλεια στο Διαδίκτυο έχει απασχολήσει τα πρωτοσέλιδα των «New York Times» και της «Wall Street Journal», έτσι ώστε αρκετοί άνθρωποι (και πωλητές και αγοραστές) να ενημερωθούν σχετικά με ζητήματα ασφαλείας. Ακόμα και αν οι κίνδυνοι φαίνονται μικρότερης σημασίας από ότι στον πραγματικό κόσμο, σήμερα επικρατεί η αντίληψη ότι οι κίνδυνοι είναι πιο σοβαροί και είναι ιδιαίτερα σημαντικό να ληφθούν υπόψη τόσο στο σχεδιασμό όσο και στην υλοποίηση των συστημάτων ηλεκτρονικού εμπορίου.

## 2.3 ΒΑΣΙΚΕΣ ΣΥΝΙΣΤΩΣΕΣ ΑΣΦΑΛΕΙΑΣ

Πολλές φορές έχει ακουστεί ότι είναι προτιμότερο να αντιμετωπίζεται η ασφάλεια σαν πρόβλημα διαχείρισης κινδύνων. Αυτό είναι αληθές για τρεις λόγους. Πρώτον, η ασφάλεια που θέλει κανείς εξαρτάται από τι προσπαθεί να προστατέψει. Δεύτερον, επιπρόσθετη ασφάλεια σχεδόν πάντα έρχεται με επιπρόσθετο κόστος, προβλήματα, καθυστερήσεις. Τρίτον, δεν έχει νόημα να είναι η ασφάλεια κάποιου τμήματος ενός συστήματος πολύ πιο δυνατή από ότι σε ένα άλλο τμήμα, αφού μια αλυσίδα είναι τόσο δυνατή όσο ο πιο αδύναμος κρίκος της.

Στην πραγματικότητα, η ασφάλεια αποτελεί κυριότητα ολόκληρου του συστήματος. Η ασφάλεια μιας τράπεζας, για παράδειγμα, εξαρτάται από το θησαυροφυλάκιο, τους φύλακες, τις βιντεοκάμερες, τους αισθητήρες κίνησης, την ετοιμότητα των υπαλλήλων, από τις διαδικασίες λειτουργίας όλου του εξοπλισμού και από τις διαδικασίες χειρισμού προβλημάτων. Παρόμοια, η ασφάλεια των συστημάτων ηλεκτρονικού εμπορίου απαιτεί την απαραίτητη τεχνολογία, αλλά επίσης απαιτεί πλήρη γνώση του τι προστατεύεται, καθώς επίσης προσεκτικό έλεγχο και λειτουργία από τους ανθρώπους που τα χειρίζονται.

### Τεχνολογία

Στην ουσία, οι τεχνολογικές συνιστώσες είναι τα εργαλεία που πρέπει να χρησιμοποιηθούν για την κατασκευή ενός ασφαλούς συστήματος. Αυτές οι συνιστώσες περιλαμβάνουν μηχανισμούς κρυπτογράφησης, πρωτόκολλα ασφαλών επικοινωνιών, τρόπους αποθήκευσης ευαίσθητων πληροφοριών κ.α. Οι περισσότερες συζητήσεις σχετικά με την ασφάλεια, ειδικά στο ηλεκτρονικό εμπόριο, εστιάζονται σ' αυτές τις συνιστώσες.

**Πολιτικές και διαδικασίες**

Μια πολιτική ασφαλείας καθορίζει τι προστατεύει και γιατί. Περιγράφει τις απειλές για το σύστημα οι οποίες πρέπει να αντιμετωπιστούν. Έτσι πρέπει να σχεδιαστεί ένα υποσύστημα ασφαλείας για την προστασία της εφαρμογής καθώς επίσης να αξιολογηθούν τα αποτελέσματα της υλοποίησης για να εξακριβωθεί αν ικανοποιούνται οι απαιτήσεις ασφαλείας. Η πολιτική μπορεί επίσης να χρησιμοποιηθεί σαν οδηγός αξιολόγησης για το αν το σύστημα λειτουργεί σωστά ή όχι. Φυσικά, η πολιτική μπορεί να εξελιχθεί με την πάροδο του χρόνου, με αντίστοιχες αλλαγές στην υλοποίηση των υποσυστημάτων ασφαλείας. Είναι ιδιαίτερα σημαντικό για την πολιτική ασφαλείας να εξελίσσεται παράλληλα με τις αλλαγές στις επιχειρήσεις, αφού τέτοιες αλλαγές μεταβάλλουν τη φύση των εμπλεκόμενων κινδύνων. Οι διαδικασίες καταγράφουν πως το σύστημα πρέπει να λειτουργεί για να βρίσκεται σε συμφωνία με την πολιτική. Η καταγραφή τους επιτρέπει να γίνονται πάντα οι σωστές ενέργειες, αντί να γίνονται όταν (ή αν) κάποιος θυμηθεί να τις κάνει.

**Προσωπικό**

Συχνά λέγεται ότι οι άνθρωποι αποτελούν το ποιο αδύναμο σημείο στην ασφάλεια ενός υπολογιστικού συστήματος αφού μπορούν να ξεγελασθούν, να επηρεασθούν ή να εξαναγκασθούν ώστε να βοηθήσουν εισβολείς. Ακόμα μπορεί και να μην γνωρίζουν τι κάνουν. Γι' αυτό είναι απαραίτητη η κατάλληλη εκπαίδευση τους σε θέματα ασφαλείας. Οποιοσδήποτε εμπλέκεται στο σύστημα πρέπει να γνωρίζει την πολιτική ασφαλείας, τους μηχανισμούς που χρησιμοποιούνται για την υλοποίηση της πολιτικής και τις ευθύνες του για την ασφαλή φύλαξη των πληροφοριών.

## 2.3.1 ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΣΥΣΤΗΜΑΤΩΝ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ

Για την δημιουργία ασφαλούς περιβάλλοντος ηλεκτρονικού εμπορίου υπάρχει μια διαδικασία κινήσεων. Οι κινήσεις αυτές θεωρούνται απαιτήσεις αφού αλλιώς το σύστημα υπολειτουργεί. Οι απαιτήσεις αυτές χωρίζονται σε πέντε ενότητες:

- Έλεγχος αυθεντικότητας (Authentication).
- Εξουσιοδότηση (Authorization).

- Εμπιστευτικότητα (Confidentiality).
- Ακεραιότητα (Integrity).
- Μη αποποίηση ευθύνης (Non-repudation).

Οι αρχές ασφαλείας του ηλεκτρονικού εμπορίου βασίζονται σ' αυτές τις πέντε βασικές απαιτήσεις οι οποίες εξαρτώνται άμεσα η μία από την άλλη. Οι απαιτήσεις αυτές πρέπει να συμβαδίζουν και με την πολιτική ασφαλείας που έχει επιλεγεί για το σύστημα.

### 2.3.2 ΕΛΕΓΧΟΣ ΑΥΘΕΝΤΙΚΟΤΗΤΑΣ (Authentication)

Ο έλεγχος της αυθεντικότητας αποσκοπεί στην εξακρίβωση της ταυτότητας, την οποία ισχυρίζεται ότι έχει ένας χρήστης έτσι ώστε να αποκλείονται οι περιπτώσεις της «ψηφιακής πλαστοπροσωπίας». Όλα τα μέρη που εμπλέκονται στη συναλλαγή πρέπει να αισθάνονται ότι οι επικοινωνίες σε ένα δικτυωμένο περιβάλλον γίνονται μεταξύ των μελών με τα οποία πιστεύουν ότι συνεργάζονται εργασιακά. Ο έλεγχος της αυθεντικότητας του χρήστη γίνεται πριν την έναρξη οποιασδήποτε ηλεκτρονικής συναλλαγής και υλοποιείται με τη χρήση διαφόρων τεχνολογιών. Πιο συγκεκριμένα, τα συστήματα ασφαλείας επιτυγχάνουν την πιστοποίηση επαληθεύοντας πληροφορίες που ο χρήστης παρέχει, με αυτές που το σύστημα ήδη ξέρει για το χρήστη. Οι μέθοδοι αυθεντικότητας βασίζονται στους ακόλουθους παράγοντες:

- Τη γνώση κάποιου τύπου ιδιοκτησιακών πληροφοριών, όπως είναι τα *passwords*.
- Κατοχή κάποιου τύπου ιδιοκτησιακής πληροφορίας όπως ένα *κλειδί* ή μια *κάρτα*.
- Παρουσίαση κάποιου τύπου βιομετρικών χαρακτηριστικών, όπως είναι ένα *δακτυλικό αποτύπωμα*.
- Απόδειξη ότι *ένα έμπιστο τρίτο μέλος* έχει ήδη εγκαταστήσει πιστοποίηση για αυτόν που τη διεκδικεί.

Για να εξακριβωθεί η ταυτότητα ενός χρήστη, αυτοί οι παράγοντες πρέπει να ληφθούν υπόψη σε συνδυασμό μεταξύ τους παρά ξεχωριστά. Μερικές κοινές μέθοδοι για συστήματα ασφάλειας δικτύων που χρησιμοποιούνται για να επιτύχουν αυθεντικότητα των χρηστών, περιλαμβάνουν passwords, προσωπικούς αριθμούς αναγνώρισης (Personal Identification Numbers-PINs), ψηφιακές υπογραφές και πιστοποιητικά.

### 2.3.3 ΕΞΟΥΣΙΟΔΟΤΗΣΗ (Authorization)

Η εξουσιοδότηση περιλαμβάνει τον έλεγχο πρόσβασης σε συγκεκριμένες πληροφορίες και υπηρεσίες όταν η ταυτότητα του χρήστη εξακριβωθεί. Δηλαδή εξουσιοδότηση σημαίνει παραχώρηση δικαιωμάτων από τον ιδιοκτήτη στο χρήστη. Για παράδειγμα, ο πελάτης εξουσιοδοτεί τον έμπορο ώστε ο τελευταίος να ελέγξει αν ο αριθμός της πιστωτικής κάρτας είναι έγκυρος και αν τα χρήματα στο λογαριασμό μπορούν να καλύψουν το ποσό των συναλλαγών. Η εξουσιοδότηση στην ουσία περιορίζει τις ενέργειες ή τις λειτουργίες που τα εξουσιοδοτημένα μέλη μπορούν να πραγματοποιήσουν σε ένα δικτυωμένο περιβάλλον.

Αυτοί οι περιορισμοί βασίζονται στο επίπεδο ασφαλείας του πιστοποιημένου μέλους. Η εξουσιοδότηση αποτελείται από μηχανισμούς ελέγχου πρόσβασης, δικτυακούς πόρους και δικαιώματα πρόσβασης. Τα δικαιώματα πρόσβασης περιγράφουν προνόμια πρόσβασης ή άδειες σχετικά με τις συνθήκες κάτω από τις οποίες διάφορες οντότητες μπορούν να έχουν πρόσβαση σε δικτυακούς πόρους και πώς αυτές οι οντότητες επιτρέπεται να μπουν σ' αυτούς τους δικτυακούς πόρους. Παραδείγματα προνομίων ή αδειών είναι:

- ✓ Δημιουργία ή καταστροφή.
- ✓ Διάβασμα, φυλλομέτρηση (browsing) ή γράψιμο.
- ✓ Προσθήκη, διαγραφή ή μετατροπή περιεχομένου.
- ✓ Εισαγωγή-εξαγωγή.
- ✓ Εκτέλεση.

Τα προνόμια αυτά μπορούν να ελεγχθούν από έναν απλό χρήστη ή από το διαχειριστή μέσω μιας λίστας ελέγχου πρόσβασης. Η λίστα καταγράφει τις άδειες των εξουσιοδοτημένων χρηστών. Οι υπηρεσίες εξουσιοδότησης επιβάλλονται αρχικά από τις υπηρεσίες ελέγχου πρόσβασης. Η εξουσιοδότηση επίσης σχετίζεται άμεσα με την ηλεκτρονική δημοσίευση και με την προστασία των πνευματικών δικαιωμάτων.

### 2.3.4 ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ (Confidentiality)

Η εμπιστευτικότητα είναι συνυφασμένη με την αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας, παρέχεται μέσω κρυπτογράφησης και είναι απαραίτητο στοιχείο της ιδιωτικότητας του χρήστη (user privacy). Για το ηλεκτρονικό εμπόριο, η

εμπιστευτικότητα αποτελεί ύψιστης σημασίας συστατικό στην προστασία των οικονομικών δεδομένων ενός οργανισμού ή μιας εταιρείας, των πληροφοριών ανάπτυξης προϊόντων, των οργανωτικών δομών, και διαφόρων άλλων τύπων προσωπικών πληροφοριών από μη εξουσιοδοτημένη πρόσβαση.

Σε ένα περιβάλλον ηλεκτρονικού εμπορίου, πληροφορίες εξαρτώμενες από το χρόνο μπορεί να είναι επίσης ένα κρίσιμο θέμα των εμπιστευτικών υπηρεσιών. Μια λίστα τιμών ή μια αναφορά μπορεί να είναι πολύ εμπιστευτικές για κάποιο συγκεκριμένο χρονικό διάστημα, και ελεύθερα διαθέσιμες αμέσως μετά. Για να συμβιβαστούν αυτές οι ανάγκες, πολιτικές ελέγχου της ροής της πληροφορίας πρέπει να περιλαμβάνονται στην εμπιστευτικότητα καθώς και στον έλεγχο αυθεντικότητας. Οι πολιτικές αυτές καθορίζουν όχι μόνο πότε ένα αντικείμενο θα ανακοινωθεί, αλλά ποια τιμή θα καθοριστεί και ποιος θα το χρεωθεί. Σε επιχειρήσεις με οικονομία βασισμένη σε πληροφορίες, οι συνέπειες ενός κενού στην εμπιστευτικότητα μπορεί να είναι καταστροφικές. Η εμπιστευτικότητα πρέπει να εξασφαλίζει ότι:

- η πληροφορία δεν μπορεί να διαβαστεί, αντιγραφεί, μετατραπεί ή αποκαλυφθεί χωρίς την απαραίτητη εξουσιοδότηση και
- οι επικοινωνίες μέσω των δικτύων δεν μπορούν να διακοπούν.

Τεχνικές κρυπτογράφησης και κωδικοποίησης έχουν σχεδιαστεί για να ικανοποιούν αυτές τις απαιτήσεις.

### 2.3.5 ΑΚΕΡΑΙΟΤΗΤΑ (Integrity)

Ακεραιότητα σημαίνει αποφυγή μη εξουσιοδοτημένης τροποποίησης των δεδομένων κατά τη μεταφορά τους στο δίκτυο και αυτό διασφαλίζεται με διάφορες μεθόδους (π.χ. ψηφιακές υπογραφές). Υπάρχουν μέθοδοι που ελέγχουν αν ένα μήνυμα έχει μεταβληθεί τη στιγμή της μεταφοράς. Τα συστήματα ηλεκτρονικού εμπορίου πρέπει να χρησιμοποιούν τέτοιες μεθόδους ώστε να μπορούν να διασφαλίσουν ότι τα δεδομένα φτάνουν στον προορισμό τους όπως ακριβώς στάλθηκαν. Οι υπηρεσίες ακεραιότητας θα πρέπει να προστατεύουν από μετατροπές στα δεδομένα αλλά επίσης και προσθέσεις, αφαιρέσεις και αναδιατάξεις μερών των δεδομένων.

### 2.3.6 ΜΗ ΑΠΟΠΟΙΗΣΗ ΕΥΘΥΝΗΣ (Non-repudiation)

Μη αποποίηση ευθύνης σημαίνει ότι κανένας από τους συναλλασσόμενους δεν πρέπει να έχει τη δυνατότητα να αρνηθεί τη συμμετοχή του σε μια συναλλαγή. Οι υπηρεσίες μη αποποίησης ευθύνης πρέπει, αν ερωτηθούν από ένα τρίτο μέλος, να μπορούν να αποδείξουν την προέλευση, μεταφορά, παράδοση και μετάδοση των δεδομένων. Η ανάγκη για τέτοιες υπηρεσίες αντικατοπτρίζει τις ατέλειες σε κάθε περιβάλλον επικοινωνίας, είτε είναι δικτυωμένο είτε όχι, και φανερώνει το γεγονός ότι απαιτούνται κατάλληλοι μηχανισμοί ασφαλείας για την πραγματοποίηση κρίσιμων και ζωτικής σημασίας συναλλαγών και επικοινωνιών.

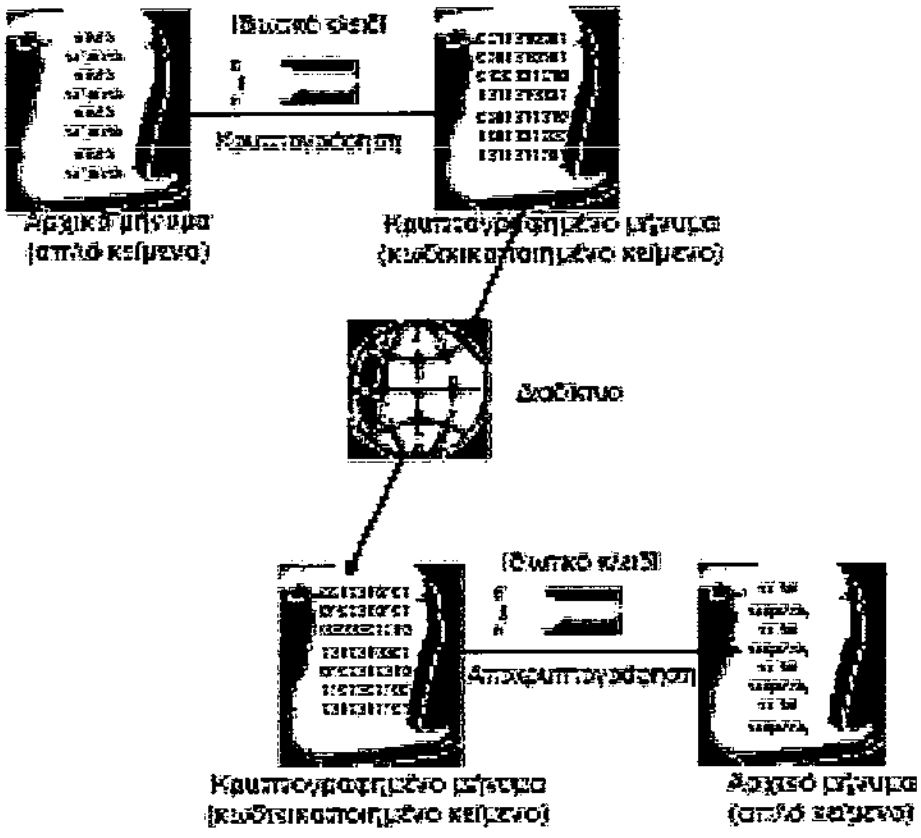
## 2.4 ΑΣΦΑΛΕΙΑ ΣΥΝΑΛΛΑΓΩΝ

### 2.4.1 ΣΥΜΜΕΤΡΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ ΚΑΙ ΚΡΥΠΤΟΓΡΑΦΙΑ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ

Η κρυπτογράφηση χρησιμοποιείται για να καλύψει την ανάγκη εμπιστευτικότητας με σκοπό το ασφαλές ηλεκτρονικό εμπόριο. Στοιχειώδες συστατικό ενός συστήματος κρυπτογράφησης είναι το κλειδί, μια σειρά από bits συγκεκριμένου μήκους.

Στην παραδοσιακή κρυπτογραφία, ο αποστολέας και ο παραλήπτης ενός μηνύματος γνωρίζουν και χρησιμοποιούν το ίδιο μυστικό κλειδί. Αυτή η μέθοδος είναι γνωστή σαν συμμετρική κρυπτογραφία. Η ακαταλληλότητα της μεθόδου έγκειται στο ότι αδυνατεί να προσφέρει πρακτικά ασφαλή διαχείριση κλειδιών σε δημόσια δίκτυα με πληθώρα χρηστών. Αν χρησιμοποιηθούν κοινά κλειδιά για δύο ανταποκριτές, τότε καταλήγουμε στην ανεπιθύμητη κατάσταση να μπορεί ο ένας να διαβάζει τα μηνύματα που απευθύνονται στον άλλον.

Το σχήμα συμμετρικής κρυπτογραφίας αντιμετωπίζει πρόβλημα και στο θέμα της αυθεντικοποίησης, μιας και είναι αδύνατο να αποδειχτεί η ταυτότητα αποστολέα και παραλήπτη του μηνύματος. Εφόσον τόσο ο ανταποκριτής Α όσο και ο Β μοιράζονται το ίδιο κλειδί, μπορούν προφανώς να στείλουν κρυπτογραφημένο μήνυμα και να ισχυριστούν ότι το έστειλε ο άλλος. Αυτή η έμφυτη ασάφεια πάνω στο ποιος δημιούργησε το μήνυμα αδυνατεί να ικανοποιήσει την απαίτηση για μη αποποίηση ευθύνης.



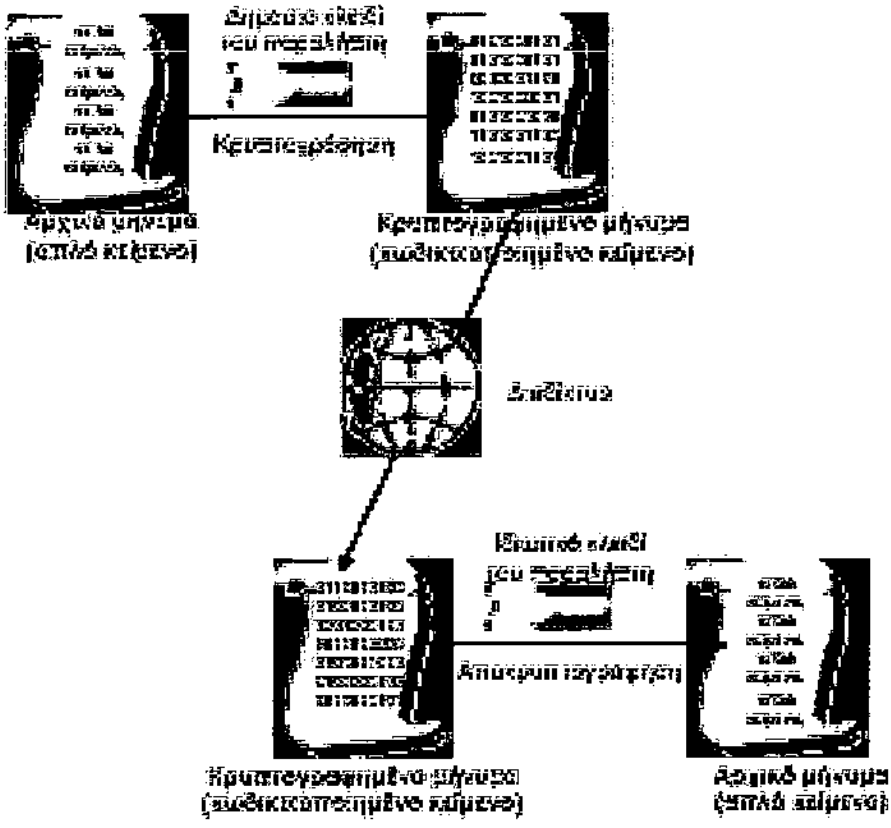
**Σχήμα 1: Συμμετρική κρυπτογραφία.**

Τη λύση έρχεται να δώσει η ασύμμετρη κρυπτογραφία ή κρυπτογραφία δημόσιου κλειδιού. Το δημόσιο κλειδί δημοσιεύεται (π.χ. με e-mail, σε κάποιον εξυπηρετητή ή μέσω υπηρεσιών καταλόγου δημοσίων κλειδιών τις οποίες προσφέρουν οι Αρχές Πιστοποίησης) ενώ το ιδιωτικό παραμένει μυστικό. Η ανάγκη για τον παραλήπτη και τον αποστολέα να διαμοιραστούν απόρρητη πληροφορία ικανοποιείται πλέον. Ο οποιοσδήποτε μπορεί να στείλει εμπιστευτικά μήνυμα απλά κάνοντας χρήση του δημόσιου κλειδιού, αλλά το μήνυμα μπορεί να αποκρυπτογραφηθεί μόνο από το ιδιωτικό κλειδί, που είναι στην κατοχή του νόμιμου παραλήπτη. Τα κλειδιά μπορούν να χρησιμοποιηθούν για να:

- Παρέχουν εμπιστευτικότητα μηνύματος.
- Αποδεικνύουν την αυθεντικότητα του δημιουργού του μηνύματος.

Στην πρώτη περίπτωση ο αποστολέας χρησιμοποιεί το δημόσιο κλειδί του παραλήπτη για να κρυπτογραφήσει ένα μήνυμα, έτσι ώστε αυτό να παραμείνει εμπιστευτικό μέχρι να αποκωδικοποιηθεί από τον παραλήπτη με το ιδιωτικό κλειδί του.

Στη δεύτερη περίπτωση, ο αποστολέας κρυπτογραφεί ένα μήνυμα χρησιμοποιώντας το ιδιωτικό του κλειδί, ένα κλειδί το οποίο μόνο αυτός γνωρίζει.



**Σχήμα 2: Ασύμμετρη κρυπτογραφία.**

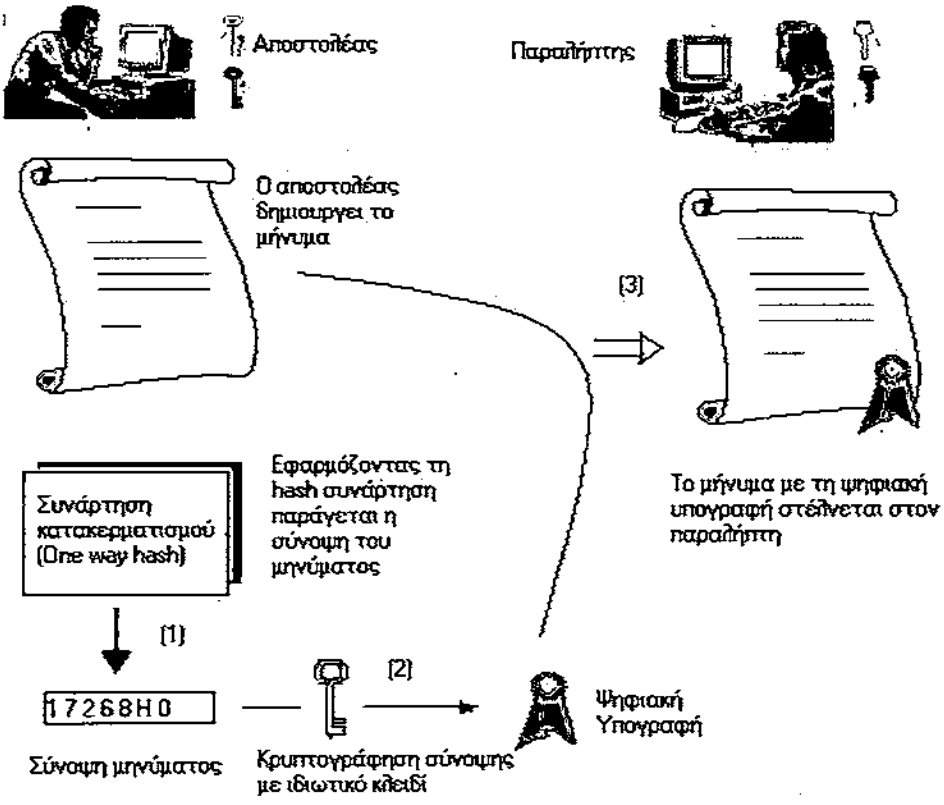
Η ασφάλεια παύει να υπάρχει συνήθως όταν ένας μη εξουσιοδοτημένος χρήστης αποκτήσει ένα ιδιωτικό κλειδί ή κωδικό. Η πλημμελής προστασία του ιδιωτικού κλειδιού (π.χ. αποθήκευση στο δίσκο Η/Υ συνδεδεμένου στο Διαδίκτυο) δεν αποτελεί, σε καμία περίπτωση, μειονέκτημα των τεχνολογιών Διαδικτύου. Κάθε τεχνολογία είναι πεπερασμένη, οπότε ο παράγοντας άνθρωπος οφείλει να κάνει το αυτονόητο. Να προστατέψει το ιδιωτικό του κλειδί.

## 2.4.2 · ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ

Οι ασύμμετροι αλγόριθμοι είναι υπολογιστικά αργοί για την κρυπτογράφηση ενός ολόκληρου μηνύματος. Έστω λοιπόν ότι ο Α επιθυμεί να στείλει υπογεγραμμένο έγγραφο ή μήνυμα στον Β. Το πρώτο βήμα είναι γενικά να εφαρμόσει μια hash

συνάρτηση στο μήνυμα και να δημιουργήσει ένα message digest. Το message digest είναι συνήθως αισθητά μικρότερο από το πρωτότυπο μήνυμα.

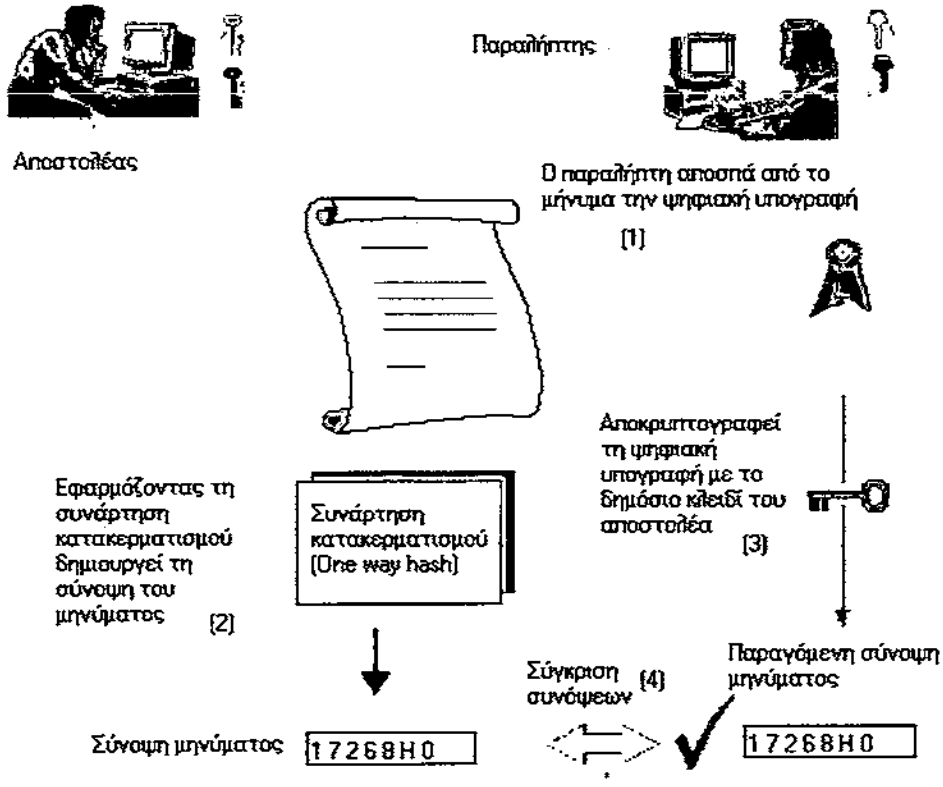
- Εφαρμόζει, πρώτα απ' όλα, την ίδια hash συνάρτηση με τον Α στο μήνυμα που παρέλαβε (το οποίο επαναλαμβάνουμε είναι κρυπτογραφημένο ή απλό κείμενο). Δημιουργεί έτσι τη δική του εκδοχή για το ορθό message digest.




**Σχήμα 3: Ψηφιακή υπογραφή.**

- Στη συνέχεια αποκρυπτογραφεί τη ψηφιακή υπογραφή την οποία παρέλαβε συνημμένη με το μήνυμα χρησιμοποιώντας το δημόσιο κλειδί του Α. Η διαδικασία αυτή οδηγεί στην αναπαραγωγή του message digest το οποίο δημιούργησε ο Α. Ο Β έχει τώρα στη διάθεση του δύο message digests. Τα συγκρίνει και αν ταιριάζουν, αυθεντικοποίησε επιτυχώς τη ψηφιακή υπογραφή του Α. Αν όχι, υπάρχουν λίγες πιθανές εξηγήσεις. Είτε κάποιος προσποιείται τον Α, ή το μήνυμα μεταβλήθηκε από τη στιγμή που το υπέγραψε ο Α, ή υπήρξε λάθος στη μετάδοση

Επαλήθευση Ψηφιακής Υπογραφής




**Σχήμα 4: Επαλήθευση Ψηφιακής υπογραφής**

### 2.4.3 ΨΗΦΙΑΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ ΚΑΙ ΑΡΧΕΣ ΠΙΣΤΟΠΟΙΗΣΗΣ

Το πρόβλημα στο μοντέλο δημόσιου κλειδιού είναι η σύνδεση οντότητας (χρήστη, εμπόρου, επιχείρησης κ.α.) με το δημόσιο κλειδί της. Έστω ότι ο Α υπογράφει έγγραφα με ένα ζευγάρι κλειδιών που ισχυρίζεται ότι είναι του Β. Τη λύση δίνουν ψηφιακά έγγραφα τα οποία καλούνται ψηφιακά πιστοποιητικά και τα οποία συσχετίζουν μια οντότητα με ένα συγκεκριμένο δημόσιο κλειδί. Τα ψηφιακά πιστοποιητικά χρησιμοποιούνται τυπικά, για να δημιουργήσουν αίσθημα εμπιστοσύνης στη νομιμότητα ενός δημόσιου κλειδιού. Είναι ουσιαστικά ψηφιακές υπογραφές που προστατεύουν τα δημόσια κλειδιά από παραχάραξη, λανθασμένη αναπαράσταση ή μετατροπή. Η επαλήθευση μιας ψηφιακής υπογραφής λοιπόν, μεταφράζεται σαν έλεγχος εγκυρότητας του πιστοποιητικού για το εμπλεκόμενο δημόσιο κλειδί.

Από τη στιγμή που δημιουργεί κάποιος το ζευγάρι δημόσιου και ιδιωτικού κλειδιού του, επιφορτίζεται με την προστασία του ιδιωτικού κλειδιού του. Μένει να αποφασίσει με ποιον τρόπο θα διανείμει το δημόσιο κλειδί του στους ανταποκριτές του. Η λύση

«ηλεκτρονικό ταχυδρομείο» κρίνεται απαγορευτική μιας και ενέχει τον κίνδυνο να ξεχαστεί κάποιος εκτός λίστας διευθύνσεων, ενώ αδυνατεί να επιτρέψει σε νέους χρήστες να γίνουν ανταποκριτές με δική τους πρωτοβουλία. Άλλο σημαντικό μειονέκτημα της λύσης αυτής είναι ο μικρός βαθμός αξιοπιστίας που προσφέρει όσον αφορά στην αυθεντικοποίηση.

Ένας καλύτερος, αξιόπιστος τρόπος διανομής δημόσιων κλειδιών είναι η χρήση μιας Αρχής Πιστοποίησης (Certification Authority). Μια αρχή πιστοποίησης θα δεχτεί το δημόσιο κλειδί του χρήστη σε συνδυασμό με κάποιο είδος απόδειξης της ταυτότητάς του (ποικίλει ανάλογα με την κλάση του πιστοποιητικού) και θα λειτουργήσει σαν τόπος απόθεσης ψηφιακών πιστοποιητικών. Οι άλλοι μπορούν τώρα να επαληθεύουν το δημόσιο κλειδί του χρήστη απευθυνόμενοι στην αρχή πιστοποίησης. Μπορούν δηλαδή να θεωρούν δεδομένο ότι ο χρήστης είναι αυτός που ισχυρίζεται ότι είναι. Για να είναι παγκοσμίως αποδεκτά αυτά τα ψηφιακά πιστοποιητικά πρέπει να εκδίδονται από μια ουδέτερη αρχή και να βρίσκονται σε συμφωνία με τα διεθνή πρότυπα. Φορείς που εκδίδουν ψηφιακά πιστοποιητικά (Αρχές Πιστοποίησης - Certification Authorities) είναι οι Verisign, Cybertrust, Nortel, Globalsign κ.α. Το στάνταρτ πρότυπο πιστοποιητικών δημοσίου κλειδιού είναι το **X.509** το οποίο αποτελείται από:

- Το διακεκριμένο όνομα του κατόχου του.
- Το δημόσιο κλειδί του.
- Την ταυτότητα του χορηγού του πιστοποιητικού και τη ψηφιακή υπογραφή του.
- Ένα κωδικό (serial number) που δίνεται από το χορηγό.
- Μια χρονική περίοδο εγκυρότητας του πιστοποιητικού.

Οι αρχές πιστοποίησης είναι απαραίτητο να λειτουργούν συνετά. Να σιγουρεύουν ότι οι συσχετισμοί προσώπων είναι εξαντλητικά ελεγμένοι και άρα αντανακλούν την πραγματικότητα (π.χ. έλεγχος ταυτότητας, διαβατηρίου κατά τη φυσική παρουσία των ενδιαφερομένων). Ας σημειωθεί ότι η έκδοση ψηφιακού πιστοποιητικού από τις αρχές πιστοποίησης δεν είναι δωρεάν. Η τιμή αυξάνει όσο μεγαλύτερη είναι η κλάση του πιστοποιητικού. Οι αρχές πιστοποίησης φέρουν επίσης την ευθύνη συντήρησης και διάθεσης μιας Λίστας Απόσυρσης Πιστοποιητικών (Certification Revocation List), από την οποία ενημερώνονται οι χρήστες για το ποια πιστοποιητικά δεν είναι πλέον έγκυρα. Οι λίστες απόσυρσης πιστοποιητικών δεν περιέχουν ληγμένα πιστοποιητικά διότι τα τελευταία έχουν ενσωματωμένο μηχανισμό λήξης. Περιέχουν, ωστόσο πιστοποιητικά που χάθηκαν, κλάπηκαν ή παύουν να ισχύουν γενικά.

### 2.4.4 ΔΙΑΧΕΙΡΙΣΗ ΚΛΕΙΔΙΩΝ

Διαχείριση κλειδιών ονομάζουμε τη δημιουργία, μεταφορά, αποθήκευση και διαγραφή των κλειδιών. Προφανώς ο αριθμός των πιθανών κλειδιών για κάθε δεδομένη εφαρμογή πρέπει να είναι εξαιρετικά μεγάλος. Διαφορετικά, ένας εισβολέας θα μπορούσε να σπάσει το σύστημα δοκιμάζοντας όλα τα πιθανά κλειδιά. Έστω, ότι ο αριθμός των πιθανών κλειδιών είναι πράγματι εξαιρετικά μεγάλος αλλά κάποια από αυτά τα κλειδιά φέρουν μεγαλύτερη πιθανότητα να παραχθούν από κάποια άλλα. Μια τέτοια κατάσταση αποτελεί πρόβλημα. Συνεπώς πρέπει να χρησιμοποιηθεί μια γεννήτρια τυχαίων ή ψευδοτυχαίων αριθμών για τη δημιουργία κλειδιών. Τα συμμετρικά κλειδιά που πρόκειται να χρησιμοποιηθούν για μικρές χρονικές περιόδους μπορούν να κρυπτογραφηθούν από συμμετρικά κλειδιά που ισχύουν για μεγάλες χρονικές περιόδους και να ανταλλαχθούν κρυπτογραφημένα. Τα κλειδιά που χρησιμοποιούνται για την κρυπτογράφηση των κλειδιών μπορούν να διανεμηθούν χειρονακτικά ή μπορούν με τη σειρά τους να κρυπτογραφηθούν από άλλα χειρονακτικά διανεμημένα συμμετρικά κλειδιά.

**Αλγόριθμοι Κρυπτογράφησης**

Ο **DES** (Data Encryption Standard) ανήκει στην κατηγορία των συμμετρικών αλγορίθμων. Ο DES έχει ερευνηθεί και μελετηθεί τα τελευταία 20 χρόνια και είναι σίγουρα ο πιο γνωστός και ευρύτατα χρησιμοποιημένος αλγόριθμος στον κόσμο. Οι λειτουργίες του είναι σχετικά γρήγορες και δουλεύουν καλά ακόμα και για μεγάλα έγγραφα.

Μια παραλλαγή του DES η οποία χρησιμοποιείται σήμερα είναι ο **Triple-DES** που λογικά είναι πιο αργός, έχοντας όμως μέγεθος κλειδιού 168 bits είναι πολύ δύσκολο να «σπαστεί». Ο Triple-DES κρυπτογραφεί κάθε μήνυμα χρησιμοποιώντας τρία διαφορετικά κλειδιά και άρα απαιτεί τρεις φορές περισσότερο χρόνο από τον DES.

Ο **RC2** είναι ένας αλγόριθμος γρηγορότερος από τον DES, ο οποίος έχει σχεδιαστεί ως αντικαταστάτης του. Έχει τη δυνατότητα να είναι περισσότερο ή λιγότερο ασφαλής από τον DES σε εξαντλητικές αναζητήσεις κλειδιού χρησιμοποιώντας κατάλληλα κλειδιά μεταβλητού μεγέθους.

Ο **RC4** σχεδιάστηκε από τον Ron Rivest και χρησιμοποιεί και αυτός κλειδιά μεταβλητού μεγέθους. Ανεξάρτητοι αναλυτές εξέτασαν αναλυτικά τον αλγόριθμο και τον

θεώρησαν ασφαλή. Χρησιμοποιείται για ασφαλείς επικοινωνίες όπως στην κρυπτογράφηση της πληροφορίας κατά την επικοινωνία με ασφαλή web site (πρωτόκολλο SSL).

Ο **IDEA** δημιουργήθηκε το 1991 και σχεδιάστηκε με σκοπό την αποδοτικότητα σε επίπεδο λογισμικού. Προσφέρει πολύ δυνατή κρυπτογράφηση κάνοντας χρήση κλειδιού 128 bits.

Ο **Diffie-Hellman** αλγόριθμος αναπτύχθηκε περί το 1976 από τους Diffie και Hellman και επιτρέπει σε δύο άτομα να ανταλλάξουν με ασφαλή τρόπο ένα μυστικό κλειδί σε ένα μη ασφαλές μέσο.

Ο **DSA** αναπτύχθηκε με βάση το λεγόμενο αλγόριθμο El Gamal. Το σχήμα των ψηφιακών υπογραφών χρησιμοποιεί το ίδιο είδος κλειδιών με τον Diffie-Hellman.

## 2.5 ΣΥΣΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Το Διαδίκτυο είναι γνωστό για την αφοσίωσή του σε ανοιχτά πρότυπα. Αυτή η υποστήριξη στα ανοιχτά πρότυπα, σε συνδυασμό με την ανοιχτή ανταλλαγή πληροφορίας πάνω από το Διαδίκτυο, ίσως οδηγήσει στη σκέψη ότι Διαδίκτυο και ασφάλεια είναι όροι αμοιβαία αποκλειόμενοι. Κάτι τέτοιο απέχει από την πραγματικότητα. Το Διαδίκτυο έχει εξοπλιστεί με ποικιλία στάνταρτ που καλύπτουν πολλά επίπεδα δικτύωσης, από ασφάλεια σε επίπεδο πακέτου μέχρι ασφάλεια σε επίπεδο εφαρμογών. Αν επιμένει κανείς να θεωρεί το Διαδίκτυο ανασφαλές μέσο λόγω της αποκεντρωμένης φύσης του, αξίζει να σημειωθεί ότι τα δεδομένα που εμπλέκονται σε συναλλαγές μπορούν να διασφαλιστούν κάνοντας χρήση ενός ικανού αριθμού στάνταρτ. Τα στάνταρτ που καλύπτονται εδώ κατηγοριοποιούνται σύμφωνα με το αν παρέχουν ασφάλεια σύνδεσης ή ασφάλεια εφαρμογών. Στάνταρτ όπως το Secure Sockets Layer (SSL) έχουν σχεδιαστεί με σκοπό να επιτύχουν ασφαλή επικοινωνία στο Διαδίκτυο, αν και το SSL χρησιμοποιείται κυρίως για web εφαρμογές. Το Secure HTTP (S-HTTP) και το Secure MIME (S/MIME), από την άλλη πλευρά, στοχεύουν στην παροχή αυθεντικοποίησης και εμπιστευτικότητας στις εφαρμογές (το S-HTTP για web εφαρμογές και το S/MIME για ηλεκτρονικό ταχυδρομείο και συναφείς εφαρμογές). Το SET προχωρά ένα βήμα περισσότερο προσφέροντας ασφάλεια στις συναλλαγές ηλεκτρονικού εμπορίου.

### 2.5.1 ΑΣΦΑΛΕΙΑ ΣΤΙΣ ΕΦΑΡΜΟΓΕΣ ΠΑΓΚΟΣΜΙΟΥ ΙΣΤΟΥ (web εφαρμογές): S-HTTP και SSL

Η ασφάλεια των web εφαρμογών περιστρέφεται γύρω από δύο πρωτόκολλα, το S-http και το SSL, τα οποία προσφέρουν αυθεντικοποίηση για εξυπηρετητές (servers) και φυλλομετρητές (browsers), καθώς επίσης εμπιστευτικότητα και ακεραιότητα δεδομένων για επικοινωνίες μεταξύ web εξυπηρετητή και φυλλομετρητή.

Το τρέχον αναγνωρισμένο πρωτόκολλο ασφαλούς επικοινωνίας στο web είναι το SSL της Netscape το οποίο και χρησιμοποιείται μέχρι σήμερα για την αποστολή εμπιστευτικών δεδομένων στο Διαδίκτυο όπως στοιχεία πιστωτικών καρτών. Το SSL προστατεύει το κανάλι επικοινωνίας λειτουργώντας χαμηλότερα στο μοντέλο διαστρωμάτωσης δικτύου. Είναι συνεπώς ανεξάρτητο εφαρμογής και επιτρέπει σε πρωτόκολλα όπως τα HTTP (HyperText Tranfer Protocol), Telnet και FTP (File Transfer Protocol) να «κάθονται» διαφανώς πάνω του. Το SSL χρησιμοποιεί τεχνικές ασύμμετρης κρυπτογράφησης στην αρχική «χειραψία», ώστε να επιτευχθούν οι ακόλουθοι στόχοι:

- ✓ Ο εξυπηρετητής ή και ο πελάτης (προαιρετικά) αυθεντικοποιούνται μέσω των ψηφιακών πιστοποιητικών.
- ✓ Εξυπηρετητής και πελάτης συμφωνούν στη χρήση ενός συγκεκριμένου κλειδιού (session key) με το οποίο θα κρυπτογραφηθεί το υπόλοιπο της συναλλαγής. Το κλειδί κρυπτογραφείται με το δημόσιο κλειδί του εξυπηρετητή και στέλνεται στον πελάτη. Σημειώνεται επίσης ότι το κλειδί αλλάζει από σύνδεση σε σύνδεση.

### 2.5.2 ΑΣΦΑΛΕΙΑ ΣΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΤΑΧΥΔΡΟΜΕΙΟ: PEM, S/MIME και PGP

Μια ποικιλία πρωτοκόλλων ασφαλείας έχουν προταθεί για το ηλεκτρονικό ταχυδρομείο στο Διαδίκτυο, αλλά μόνο ένα ή δύο έχουν γνωρίσει ευρεία αποδοχή. Το Privacy Enhanced Mail (PEM) είναι ένα στάνταρτ για την ασφάλεια ηλεκτρονικού ταχυδρομείου χρησιμοποιώντας συμμετρική ή ασύμμετρη κρυπτογραφία. Το PEM έχει φθίνουσα πορεία διότι αδυνατεί να διαχειριστεί το νεώτερο πολυμελές ηλεκτρονικό ταχυδρομείο (multipart e-mail) το οποίο υποστηρίζεται από το MIME (Multipurpose

Internet Mail Extensions), ενώ απαιτεί αυστηρή ιεραρχία αρχών πιστοποίησης για να εκδώσει κλειδιά.

Το S/MIME είναι ένα πρωτόκολλο που προσθέτει ψηφιακές υπογραφές και κρυπτογράφηση στα Διαδικτυακά MIME μηνύματα. Το MIME είναι το επίσημο στάνταρτ για εκτεταμένο Διαδικτυακό ηλεκτρονικό ταχυδρομείο. Καθορίζει τη δομή του κυρίου μέρους ενός ηλεκτρονικού μηνύματος. Το S/MIME βασίζεται στη χρήση ενός ψηφιακού φακέλου (digital enveloppe). Το μήνυμα κρυπτογραφείται με ένα συμμετρικό αλγόριθμο, όπως DES ή RC2. Το συμμετρικό κλειδί κρυπτογραφείται με το δημόσιο κλειδί του παραλήπτη οπότε μαζί με το κρυπτογραφημένο μήνυμα τοποθετούνται στο ψηφιακό φάκελο και στέλνονται στον παραλήπτη. Το S/MIME έχει υιοθετηθεί από πλήθος ηγετικών παραγωγών στο δικτυακό και διαμηνυματικό χώρο, όπως οι ConnectSoft, Frontier, FTP Software, Microsoft, Lotus, Secure Ware, VeriSign, Netscape και Novell. Αποτελεί λοιπόν δοκιμασμένο υπόβαθρο για την ανάπτυξη συστήματος ηλεκτρονικού ταχυδρομείου στα πλαίσια εφαρμογών ηλεκτρονικού εμπορίου.

Μια δημοφιλής εφαρμογή που αναπτύχθηκε με σκοπό την ασφάλεια μηνυμάτων και αρχείων είναι το Pretty Good Privacy (PGP). Είναι ίσως η ευρύτερα διαδεδομένη εφαρμογή ασφαλείας για ηλεκτρονικό ταχυδρομείο στο Διαδίκτυο. Το PGP (Pretty Good Privacy) είναι πακέτο λογισμικού που παρέχει ρουτίνες κρυπτογράφησης για e-mail και εφαρμογές αποθήκευσης αρχείων. Το PGP απαρτίζεται από υπάρχοντα κρυπτοσυστήματα και πρωτόκολλα κρυπτογράφησης. Τρέχει σε διάφορες πλατφόρμες. Προσφέρει κρυπτογράφηση μηνύματος, ψηφιακές υπογραφές, συμπίεση δεδομένων και e-mail συμβατότητα.

### 2.5.3 FIREWALLS

Ο έλεγχος πρόσβασης πραγματοποιείται για να ικανοποιήσει την απαίτηση αυθεντικότητας με σκοπό το ασφαλές ηλεκτρονικό εμπόριο. Τα Firewalls καθιστούν δυνατό τον έλεγχο πρόσβασης.

Firewall ονομάζεται ένας μηχανισμός ασφάλειας, που ελέγχει την κυκλοφορία της πληροφορίας μεταξύ ενός τοπικού δικτύου και του Διαδικτύου και προστατεύει από εξωτερικές απειλές και παραβιάσεις. Χρησιμοποιείται για να ελέγχει όλες τις συνδέσεις δικτύου που γίνονται σε έναν οργανισμό, να απαγορεύει μερικές από αυτές και να

κρατάει αρχεία όλης της κίνησης, όπου προσπάθειες για παραβιάσεις μπορούν να καταγραφούν. Τα firewalls μπορούν να απομονώσουν επιλεκτικά του υπολογιστές από το διαδίκτυο. Ένα firewall δημιουργεί έναν τομέα ασφάλειας που περικλείει όλους τους υπολογιστές που είναι συνδεδεμένοι σ' αυτόν. Μέσα στον τομέα μπορεί να υποτεθεί ότι οι υπολογιστές που περιλαμβάνει μπορούν να χρησιμοποιηθούν μόνο από άτομα που έχουν φυσική πρόσβαση.

Υποθέτοντας τώρα ότι το λογισμικό στους υπολογιστές αυτούς δεν περιέχει ιούς ή «δούρειους ίππους», και ότι οι χρήστες με φυσική πρόσβαση δεν θα εισάγουν τέτοιες απειλές, η πιστοποίηση του χρήστη και ο έλεγχος πρόσβασης μπορούν να είναι αξιόπιστοι.

Γενικά υπάρχουν δύο είδη firewalls αυτά που λαμβάνουν αποφάσεις στο επίπεδο της μεταγωγής πακέτων (packet filters) και αυτά που ενεργούν στο επίπεδο των εφαρμογών (proxies). Φυσικά πολλά προϊόντα καλύπτουν και τις δύο κατηγορίες αλλά ο διαχωρισμός εξακολουθεί να υπάρχει μια και τα κριτήρια ασφάλειας είναι διαφορετικά για κάθε κατηγορία.

Ένας περιορισμός των firewalls είναι ότι οι αποφάσεις καλύπτουν τα πρωτόκολλα και όχι τη χρήση των πρωτοκόλλων. Ένα proxy firewall χρησιμοποιείται για αυτές ακριβώς τις περιπτώσεις, όπου απαιτείται εξειδικευμένη γνώση της ίδιας της εφαρμογής.

Ένα καλό παράδειγμα αποτελεί το sendmail (πρόγραμμα για την παραλαβή και αποστολή ηλεκτρονικού ταχυδρομείου) που έχει μια μακρά παράδοση προβλημάτων ασφάλειας. Με ένα packet filter firewall έχουμε την επιλογή να αφήσουμε να περάσουν τα πακέτα του ηλεκτρονικού ταχυδρομείου αποδεχόμενοι την πιθανότητα να έχουμε προβλήματα ασφάλειας λόγω του sendmail ή να απαγορεύσουμε τη μεταφορά αυτών των πακέτων με απώλεια της υπηρεσίας του ηλεκτρονικού ταχυδρομείου. Και οι δύο εναλλακτικές λύσεις είναι εξίσου απαράδεκτες. Στο συγκεκριμένο παράδειγμα, χρειαζόμαστε ένα πρόγραμμα που να μπορεί να παραλαμβάνει μηνύματα ηλεκτρονικού ταχυδρομείου και να τα τοποθετεί σε ένα γνωστό μέρος από όπου μπορούν να προωθηθούν στο sendmail για επεξεργασία. Αντικαθιστώντας το sendmail με ένα άλλο μικρότερο πρόγραμμα επιτυγχάνουμε τα εξής:

Επιθέσεις που στηρίζονται σε γνώση της συμπεριφοράς του sendmail αποτυγχάνουν μια και δεν επικοινωνούν πλέον κατευθείαν με το sendmail. Το νέο πρόγραμμα (με το proxy) μπορεί να τρέχει με ελάχιστα προνόμια μια και απλά αποθηκεύει τα μηνύματα σε αρχεία. Άρα και να μπορέσει κάποιος να κοροϊδέψει το proxy, δε θα πετύχει πολλά. Αντίθετα το sendmail τρέχει με προνόμια διαχειριστή (administrator).

Η μειωμένη λειτουργικότητα συνεπάγεται μειωμένη πολυπλοκότητα. Έτσι είναι πιο εύκολο να πραγματοποιηθεί μια εκτεταμένη και αναλυτική εξέταση του proxy για να βρεθούν πιθανά προβλήματα ασφάλειας. Φυσικά ένα proxy firewall πρέπει πάντοτε να συνοδεύεται από κάποιο μηχανισμό ελέγχου στην πρόσβαση από το Διαδίκτυο στο εσωτερικό δίκτυο. Αυτό συνήθως επιτυγχάνεται με ένα packet filter firewall. Αν όμως δεχτούμε ότι τα εσωτερικά μηχανήματα επικοινωνούν με το Διαδίκτυο αποκλειστικά και μόνο μέσω proxies, μπορούμε να αποφύγουμε τη χρήση του packet filter με το να δώσουμε διευθύνσεις στα μηχανήματα του εσωτερικού δικτύου, που να είναι άχρηστες στο Διαδίκτυο. Έτσι το εξωτερικό μηχάνημα δεν έχει τρόπο να στείλει πακέτα σε εσωτερικά μηχανήματα παρά μόνο στο proxy firewall. Για το σκοπό αυτό υπάρχουν ειδικές κλάσεις διευθύνσεων που είναι εγγυημένα μη διαδρομίσιμες (unroutable).

Αυτό που είναι όμως αναμφισβήτητο είναι ότι αν δε γίνει σωστή εγκατάσταση, ένα firewall μπορεί να κάνει περισσότερο κακό παρά καλό, δίνοντας μια αδικαιολόγητη αίσθηση ασφάλειας. Η κακή εγκατάσταση μπορεί επίσης να δημιουργήσει προβλήματα στους χρήστες, όπως καθυστερήσεις, διακοπές στις συνδέσεις και γενικά απρόβλεπτη συμπεριφορά. Τα firewalls έχουν δεχτεί κριτική όσον αφορά στη δυσκολία χρήσης τους.

Επίσης, δεν παρέχουν προστασία από επιθέσεις προερχόμενες από χρήστη εντός του τοπικού δικτύου. Τέλος, απαιτείται συνεχής επαγρύπνηση και τακτικοί έλεγχοι στα αρχεία που κρατάει το firewall αφού προσπάθειες για παραβιάσεις καταγράφονται στα αρχεία του.

# 3

# ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ

## ΕΙΣΑΓΩΓΗ

Η εγκαθίδρυση του ηλεκτρονικού έμπορίου και η ευρεία χρησιμοποίησή του στον κόσμο των επιχειρήσεων, έφερε στο προσκήνιο την έννοια της πρόληψης όσον αφορά τη διασφάλιση της σωστής λειτουργίας του. Αποτέλεσμα ήταν ο καθορισμός ενός ιδιαίτερα συγκεκριμένου στόχου. Της ανάπτυξης ενός δυνατού συστήματος προστασίας που θα συνδυάζει αρμονικά την τεχνολογία, τη νομοθεσία και το εξειδικευμένο ανθρώπινο δυναμικό, ανάλογα με τις απαιτήσεις κάθε εφαρμογής.

Στο παρόν κεφάλαιο, αναλύεται η νέα θέση CPO στις εταιρείες, ο ρόλος των φυσικών προσώπων - κλειδιών που τις καλύπτουν, των υπευθύνων για την αστυνόμευση των αρχείων, το σχέδιο ασφαλείας πάνω στο οποίο βασίζονται και δρουν, καθώς και οι μορφές εισβολέων που καλούνται να αντιμετωπίσουν, κυρίως με βάση τα κίνητρα και τις μεθόδους τους. Τέλος, επισημαίνονται τα κενά της νομοθεσίας που παρατηρούνται καθώς και οι προσπάθειες να προταθούν συμπληρωματικά μέτρα και ελεγκτικοί μηχανισμοί απέναντι στη διαφύλαξη της ιδιωτικής ζωής.

## 3.1 ΣΧΕΔΙΑΣΜΟΣ ΑΣΦΑΛΕΙΑΣ

Ο σχεδιασμός ασφαλείας πρέπει να αποτελεί μέρος κάθε εφαρμογής ηλεκτρονικού εμπορίου. Είναι σημαντικό όμως να λαμβάνεται υπόψη από την αρχή του σχεδιασμού της εφαρμογής, γιατί είναι πολύ πιο δαπανηρό να προστεθεί ασφάλεια κατά τη διάρκεια της. Υπάρχουν πέντε βασικά βήματα για το σχεδιασμό της ασφάλειας των συστημάτων ηλεκτρονικού εμπορίου:

- Καθορισμός της πολιτικής ασφαλείας.
- Προσθήκη των απαραίτητων μηχανισμών ασφαλείας στην εφαρμογή.
- Σχεδιασμός της ασφάλειας του φυσικού, δικτυακού και υπολογιστικού περιβάλλοντος του συστήματος.
- Ανάπτυξη μηχανισμών ανάδρασης, επίβλεψης και περιοδικού ελέγχου για παρατήρηση της ορθής λειτουργίας του συστήματος.
- Χρήση των αποτελεσμάτων της ανάδρασης, επίβλεψης και περιοδικού ελέγχου για βελτίωση του σχεδιασμού, υλοποίησης και λειτουργίας του συστήματος.

### 3.1.1 ΚΑΘΟΡΙΣΜΟΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

Το πρώτο βήμα στο σχεδιασμό ασφαλείας είναι ο καθορισμός της πολιτικής ασφαλείας. Η πολιτική θα πρέπει να καλύπτει όλο το σύστημα, περιλαμβάνοντας συστήματα πληροφοριών (δίκτυα και υπολογιστές), δεδομένα (πληροφορίες ανάπτυξης, παραγωγής και αποθήκευσης) και ανθρώπινο δυναμικό (χειριστές, προσωπικό συντήρησης, πελάτες). Επιπλέον θα πρέπει να περιέχει αναφορές για το τι προστατεύεται, τι είδος προστασίας χρειάζεται, ποιος είναι υπεύθυνος για τα διάφορα μέρη του συστήματος, για την απαραίτητη εκπαίδευση, και τι είδος επίβλεψης και περιοδικού ελέγχου απαιτείται.

### 3.1.2 ΣΧΕΔΙΑΣΜΟΣ ΤΟΥ ΠΕΡΙΒΑΛΛΟΝΤΟΣ

Το δεύτερο βήμα είναι ο σχεδιασμός του περιβάλλοντος της εφαρμογής. Ο σχεδιασμός του περιβάλλοντος περιλαμβάνει όλες τις συνιστώσες έξω από την ίδια

την εφαρμογή, όπως είναι οι υπολογιστές, τα λειτουργικά συστήματα, τα δίκτυα και οι φυσικές εγκαταστάσεις. Συχνά το περιβάλλον μπορεί να παρέχει κάποιες δυνατότητες προστασίας της εφαρμογής, έτσι ώστε η εφαρμογή να μη χρειάζεται να τις αντιγράψει. Αξίζει να σημειωθεί όμως ότι τέτοιες δυνατότητες πρέπει να καταγράφονται έτσι ώστε η εφαρμογή να μπορεί να επαναδημιουργηθεί οπουδήποτε εμφανισθεί ανάγκη. Σε άλλες περιπτώσεις το ίδιο το περιβάλλον πρέπει να δεσμεύει την εφαρμογή με διάφορους τρόπους ή να απαιτεί ειδικές μεθόδους ασφαλείας να λαμβάνονται από την εφαρμογή αν δεν περιλαμβάνονται από το περιβάλλον.

Στην πράξη ο σχεδιασμός του περιβάλλοντος και ο σχεδιασμός των μηχανισμών ασφαλείας της εφαρμογής θα πρέπει να αλληλεπιδρούν με χρήσιμο τρόπο. Μερικά προβλήματα ασφαλείας είναι ευκολότερο να λυθούν από την εφαρμογή παρά από το περιβάλλον και το αντίστροφο. Σε μερικές περιπτώσεις, ειδικά στο σχεδιασμό των προϊόντων, η εφαρμογή μπορεί να επιβάλλει κάποιες απαιτήσεις στο περιβάλλον στο οποίο θα χρησιμοποιηθεί. Τελικά το πιο σημαντικό θέμα κατά την ανάπτυξη του σχεδίου ασφαλείας είναι ο σχεδιασμός ολόκληρου του συστήματος (εφαρμογής και περιβάλλοντος).

### 3.1.3 ΣΧΕΔΙΑΣΜΟΣ ΤΩΝ ΜΗΧΑΝΙΣΜΩΝ ΑΣΦΑΛΕΙΑΣ ΤΗΣ ΕΦΑΡΜΟΓΗΣ

Το τρίτο βήμα στο σχεδιασμό ασφαλείας είναι η παροχή μηχανισμών ασφαλείας για την ίδια την εφαρμογή. Ο γενικός σχεδιασμός της εφαρμογής μαζί με την πολιτική ασφαλείας θα πρέπει να παρέχει τις απαιτήσεις για το τι προστατεύεται και να δίνει μια καθοδήγηση για το είδος της προστασίας που χρειάζεται. Το σχέδιο ασφαλείας τότε μπορεί να χρησιμοποιήσει διάφορες συνιστώσες τεχνολογιών όπως συστήματα κρυπτογράφησης, πιστοποίησης και εξουσιοδότησης. Επιπρόσθετα σ' αυτούς τους γενικούς μηχανισμούς για έλεγχο της πρόσβασης στις πληροφορίες, μπορεί να υπάρχουν και κάποιες ειδικές απαιτήσεις της ίδιας της εφαρμογής.

### 3.1.4 ΕΠΙΒΛΕΨΗ ΚΑΙ ΠΕΡΙΟΔΙΚΟΣ ΕΛΕΓΧΟΣ

Πέρα από τις ειδικές απαιτήσεις της εφαρμογής, η ασφάλεια απαιτεί μηχανισμούς ανάδρασης ώστε να εξασφαλίζεται ότι οι μηχανισμοί ασφαλείας

λειτουργούν σωστά, μηχανισμούς αποθήκευσης ώστε να περιορίζεται η έκταση της ζημιάς, και μηχανισμούς ανάκτησης όταν παρουσιάζεται το πρόβλημα. Στον ηλεκτρονικό χώρο, αυτοί οι έλεγχοι αναλαμβάνονται από μηχανισμούς παρακολούθησης, ελέγχου ταχύτητας και υπηρεσίες πελατών. Η πληροφορία που παρέχεται από αυτούς τους μηχανισμούς μπορεί να χρησιμοποιηθεί με διάφορους τρόπους: για επαναλειτουργία σε περίπτωση προβλήματος, για έλεγχο ώστε να εξασφαλίζεται ότι οι επιθέσεις ήταν ανεπιτυχείς, για επιβεβαίωση ότι η λειτουργία συμφωνεί με την πολιτική ασφαλείας, και για αξιολόγηση αν η πολιτική ασφαλείας, ο σχεδιασμός και οι μηχανισμοί είναι αποτελεσματικοί για την εφαρμογή.

Ειδικοί στην ασφάλεια υπολογιστών συχνά επισημαίνουν ότι η ασφάλεια πρέπει να περικλείει ολόκληρο το σύστημα. Οι σχεδιαστές και οι χειριστές μιας υπηρεσίας πρέπει να λαμβάνουν σοβαρά υπόψη τους θέματα σχετικά με την εφαρμογή και τους κινδύνους πριν αποφασίσουν για το επίπεδο της ασφάλειας που θα παρέχεται, και εσωτερικά σε κάθε επίπεδο πρέπει να σκεφθούν τη σχετιζόμενη δύναμη των μηχανισμών ασφαλείας που θα αναπτυχθούν.

### 3.1.5 ΑΝΑΘΕΣΗ ΡΟΛΩΝ ΚΑΙ ΥΠΕΥΘΥΝΟΤΗΤΩΝ

Πολύ σημαντικό μέρος του σχεδιασμού της πολιτικής ασφαλείας είναι οι ρόλοι, οι δραστηριότητες και οι αντίστοιχες υπευθυνότητες (του κάθε ρόλου) που πρέπει να ανατεθούν σε πρόσωπα - κλειδιά για την ορθή λειτουργία ενός συστήματος ηλεκτρονικού εμπορίου. Αυτά τα πρόσωπα - κλειδιά, χαρακτηρίζονται από τις εταιρείες ως cpo. Η θέση cpo είναι σχετικώς νέα θέση στις περισσότερες εταιρείες και οι αρμοδιότητες της δεν είναι πάντα καθορισμένες. Έτσι η αλληλεπίδραση με τις επίκαιρες πληροφορίες είναι ουσιώδη. Στηρίζουν κυρίως δραστηριότητες όπως το καθήκον το οποίο συνδυάζει τους νόμους και το μάρκετινγκ, εναρμονίζουν και θέτουν σε εφαρμογή τακτικές και ενέργειες, παρακολουθούν παλιά και νέα προϊόντα, υπηρεσίες και συστήματα ώστε να διασφαλίζεται ο σεβασμός των προσωπικών δεδομένων, δημιουργούν γέφυρα με IT μεταξύ ασφαλιστών, αγοραστών και σωματειακών καθοδηγητών, βρίσκουν και θέτουν κανόνες για τον χειρισμό προτύπων δομής ελέγχου προσωπικών δεδομένων, παρεμβαίνουν στην εμπόδιση ή αντιγραφή των πληροφοριών από τα μέσα μαζικής ενημέρωσης, εξασφαλίζουν ότι οι εταιρείες συμμορφώνονται με τους ισχύοντες νόμους, μεταφέρουν προτάσεις για κανονισμούς στην Διοίκηση, κρατούν τους υπαλλήλους ενήμερους για τις εξελίξεις που λαμβάνουν χώρα και οι οποίες τους αφορούν, ενημερώνουν την εταιρεία για τις εξελίξεις των

οργανώσεων, προλαμβάνοντας τις παρεμβάσεις από τα κυβερνητικά σώματα προτείνουν, σχεδιάζουν και διαβιβάζουν στρατηγικές Και τέλος διατηρούν τη συνέπεια, την αξιοπιστία, και την εμπιστοσύνη μέσα και έξω από τον οργανισμό.

Καθώς οι βιομηχανίες καλύπτουν μερικώς όλα τα παραπάνω ζητήματα, οι CPO πρέπει να προετοιμάζονται να πλησιάσουν βιομηχανικά θέματα σε επίσημο και ανεπίσημο περιβάλλον σε εθνική και διεθνή κλίμακα. Το γεγονός αυτό δεν αφήνει αδιάφορες βεβαίως τις εταιρείες που συνεργάζονται ήδη με τους CPO, η ενημέρωση, η παρακολούθηση των εξελίξεων σε όποιο επίπεδο, θα πρέπει να είναι παράλληλη και με απόλυτη συνεργασία.

Η συμμετοχή στις θέσεις των CPO σε μια εταιρεία προϋποθέτει την διασφάλιση προσωπικών δεδομένων εσωτερικά και εξωτερικά της εταιρείας ώστε να πετύχουν αντάξια δημόσια και πελατειακή αναγνώριση ως «οδηγοί της διασφάλισης». Επίσης προσφέρει προσωπική και επαγγελματική ανάπτυξη και χαρίζει στους CPO την εμπειρία που χρειάζονται για να γίνουν ειδικοί στην διακυβέρνηση της αρένας της διασφάλισης προσωπικών δεδομένων.

Η δουλειά ενός CPO μπορεί να συμπεριλαμβάνει την διατήρηση της ασφάλειας της λειτουργίας της εταιρείας μακριά από εισβολείς εντός ή εκτός. Επιπλέον συμμετέχουν στην ανάπτυξη μιας ασφαλούς αστυνόμευσης σχεδιασμένης να διατηρεί τα αρχεία στην μέγιστη ασφαλή περιοχή ενός δικτύου, είτε είναι είτε όχι προσβάσιμο, χωρίς να χρησιμοποιεί το δίκτυο.

Ένας καλός CPO είναι τεχνικός, δικηγόρος, καλός ομιλητής και σε πολλούς τομείς ειδικός. Έτσι δεν είναι έκπληξη ότι για όλους αυτούς τους ρόλους το να βρεθεί κατάλληλο πρόσωπο είναι δύσκολο. Μπορεί να χρειαστούν μερικά χρόνια. Σύμφωνα με την Διασφάλιση Προσωπικών Δεδομένων και τις Αμερικανικές Επιχειρήσεις η υποστήριξη οργανισμών είναι δουλειά του Κοινωνικού Δικαίου, γι' αυτό πολλές (χιλιάδες) εταιρείες θα χρειαστούν CPO μέσα στο 2004.

Ένας τρόπος για να προσλάβει μια εταιρεία CPO είναι αρχικά να εκπαιδεύσει κάποιον που είναι στο υπάρχον προσωπικό του νομικού τμήματος. Το Σωματείο των Υπαλλήλων της Διασφάλισης (ACPO) πραγματοποιεί ειδικά μαθήματα και σεμινάρια ώστε να μπορεί να υποσχεθεί ότι ο CPO είναι κατάλληλο πρόσωπο και να τον εξοπλίσει σωστά. Εφόσον είναι ήδη στον χώρο του δίνεται η ευκαιρία να αξιοποιήσει τις γνώσεις που έχει και απόκτησε για ένα συγκεκριμένο του αντικείμενο: τους στόχους και τις ιδέες της εταιρείας στην οποία εργάζεται.

Αν κάποια εταιρεία αποφασίσει να ψάξει γενικά στην αγορά εργασίας ή σε κάποια άλλη εταιρεία για να προσλάβει έναν CPO, θα πρέπει η εταιρεία αυτή να ακολουθεί όρους διασφάλισης που να σχετίζονται με την δική της. Υπάρχει η εταιρεία **Πρωτοπόροι της Διασφάλισης** (Privacy Leaders) η οποία ειδικεύεται στην

εύρεση CPO. Η ίδρυση της έγινε το 1991 – πριν ακόμα αρχίσουν τα «ιδιαίτερα» προβλήματα που εμφανίζονται τώρα στις εταιρείες-.

Σε μεγαλύτερες εταιρείες η διοίκηση μπορεί να επιλέξει να τοποθετήσει CPO σε μικρότερους τομείς ή να δημιουργήσει ένα ολόκληρο τμήμα Πρωτοπόρων διασφάλισης (Privacy Leaders). Οι λίστες των υποψηφίων CPO μπορούν να συμπληρώσουν και να δώσουν έμφαση σε κάθε τμήμα των μεγαλύτερων εταιρειών. Μπορούν ακόμα να βοηθήσουν στο να βρεθεί το κατάλληλο άτομο για τη θέση CPO, ή την θέση **affairs officer, chief public policy officer, chief e-security** και άλλα. Οι εταιρείες πρέπει να έχουν υπ' όψιν τους ότι η πληρωμή ενός CPO είναι μηναία, ποσοστιαία και ανάλογα τον πελάτη. Ειδικά για τα διευθυντικά στελέχη τα οποία έχουν σημαντική θέση στην εταιρεία τα χρηματικά οφέλη είναι αρκετά μεγάλα. Επιπλέον για οτιδήποτε συμβεί αναφέρονται κατευθείαν στον πρόεδρο της εταιρείας ή στον CEO (Chiff Executive Officer).Η εταιρεία μπορεί να έχει περισσότερα πλεονεκτήματα από τα συνηθισμένα αν θελήσει να προσλάβει κάποιον ψάχνοντας στην αγορά εργασίας και όχι σε άλλη εταιρεία. Σημαντικοί λόγοι ύπαρξης των CPO είναι επιπλέον οι γνώσεις τους για νομικά, οικονομικά, και θέματα πληροφορικής όπως αναπτύσσονται παρακάτω:

- νέοι κανονισμοί της κυβέρνησης: HIPAA (Health Insurance Portability and Accountability Act), COPPA (Children's Online Privacy Protection Act ) κτλ,
- νομοθεσία εσωτερικού και εξωτερικού: GLB (Gramm-leach-Bliley Act),
- ανάπτυξη καταναλωτικού ενδιαφέροντος και προσωπικής δραστηριότητας,
- επιχειρηματικό περιβάλλον εξελισσόμενο από παραδοσιακό σε online,
- ανάπτυξη διαφόρων κατηγοριών ενέργειας και άλλων ιδιωτικών διεκδικήσεων.

Οι cpo κατατάσσονται ανάλογα με τον ρόλο και την υπευθυνότητα σε τέσσερις βασικές κατηγορίες όπου ανάλογα την θέση βλέπουμε και τι περιλαμβάνει η δραστηριότητα τους.

**Υπεύθυνος Ασφαλείας**

- έγκαιρη και αποτελεσματική αντιμετώπιση περιστατικών ασφαλείας και ατυχημάτων ή έκτακτων γεγονότων.
- τη διαχείριση των δικαιωμάτων προσπέλασης.
- τη δημιουργία σχεδίου για την εκπαίδευση και ενημέρωση του υπόλοιπου προσωπικού.
- τη σύνταξη αναφορών για την ασφάλεια του συστήματος ανά τακτά χρονικά διαστήματα.

- την έγκαιρη ενημέρωση του σχετικά με οποιεσδήποτε αλλαγές που μπορούν να επηρεάσουν την ασφάλεια του συστήματος όπως διακοπές για συντήρηση ή επισκευή, πρόσληψη προσωπικού, αλλαγές στον εξοπλισμό κλπ.

**Διαχειριστής Συστήματος**

- διαχείριση του υλικού και του εξοπλισμού του συστήματος και την καταγραφή του.
- διαχείριση (σε συνεργασία με τον Υπεύθυνο Ασφαλείας) των δικαιωμάτων προσπέλασης.
- επίβλεψη του συστήματος για την ορθή του λειτουργία και το χειρισμό σε περίπτωση δυσλειτουργιών.
- έγκαιρη ενημέρωση του σχετικά με οποιεσδήποτε αλλαγές που μπορούν να επηρεάσουν την ασφάλεια του συστήματος όπως διακοπές για συντήρηση ή επισκευή, πρόσληψη προσωπικού, αλλαγές στον εξοπλισμό κλπ.

**Διοικητικός Υπεύθυνος**

Πρόκειται για το πρόσωπο που επικοινωνεί με τη διοίκηση και το προσωπικό του συστήματος.

- επίβλεψη του Υπεύθυνου Ασφαλείας και του Διαχειριστή Συστήματος.
- μεταφορά των οδηγιών της διοίκησης στο υπόλοιπο προσωπικό.
- παρακολούθηση της σωστής ολοκλήρωσης των προβλεπόμενων διαδικασιών.
- διατήρηση του ηθικού του προσωπικού σε ικανοποιητικό επίπεδο, ενός πολύ σημαντικού παράγοντα για την ασφάλεια του συστήματος.

**Χειριστές Συστήματος**

Είναι υπεύθυνοι για την εκπλήρωση των καθηκόντων που τους ανατίθενται από τον Υπεύθυνο Ασφαλείας και το Διαχειριστή Συστήματος.

- αναφορά περιστατικών σχετικών με την ασφάλεια του συστήματος και συνεισφορά τους στην επίλυσή τους.
- ενημέρωση για θέματα ασφαλείας.
- ακριβής τήρηση των κανονισμών του συστήματος.
- αποφυγή δραστηριοτήτων που μπορούν να επιφέρουν δυσλειτουργίες στο σύστημα.

## 3.2 ΚΡΙΣΙΜΑ ΖΗΤΗΜΑΤΑ

Μέρος του σχεδιασμού μιας κατάλληλης πολιτικής ασφαλείας είναι να αναγνωρισθεί ποιο επίπεδο προστασίας αποτελεί εγγύηση ενάντια σε κάθε είδος απειλής. Χωρίς πλήρη κατανόηση των πλεονεκτημάτων των διαφόρων κριτηρίων ασφαλείας είναι αδύνατον να αξιολογηθούν οι επιλογές από επιχειρηματική σκοπιά. Παρακάτω θα αναλυθούν οι απειλές της ασφάλειας υπολογιστών και θα αξιολογηθούν τα μέσα που μειώνουν αυτές τις απειλές.

### 3.2.1 ΕΧΘΡΟΙ

Το πρώτο βήμα είναι να αναγνωρισθούν ποιοι είναι οι «εχθροί». Οι άνθρωποι συχνά ξεκινούν εστιάζοντας στους τύπους επιθέσεων και στη ζημιά που προκύπτει αλλά μεγάλη σημασία έχουν και τα μέσα που χρησιμοποιούνται για την επίθεση. Έτσι έχουμε:

**Crackers**

Οι crackers αρέσκονται στο να εισβάλλουν σε υπολογιστικά συστήματα για βανδαλισμούς ή για επίδειξη. Χρησιμοποιούν υπάρχοντα προϊόντα επίθεσης από το δίκτυο ή από περιοδικά. Συνήθως δεν έχουν δυνατούς υπολογιστικούς πόρους και οι προθέσεις συχνά δεν είναι εχθρικές. Ωστόσο, προκαλούν ουσιαστικές ζημιές, είτε προκαλώντας βανδαλισμούς στο σύστημα, είτε διακόπτοντας λειτουργίες ή καταναλώνοντας το χρόνο του προσωπικού του συστήματος στην προσπάθεια τους να καταλάβουν ποια είναι η ζημιά και να την διορθώσουν.

**Ερευνητές (Researchers)**

Ένας ερευνητής μπορεί να εργαστεί πολύ σκληρά στην προσπάθεια του να ανακαλύψει αδυναμίες σε πρωτόκολλα ασφαλείας και στη συνέχεια εκδίδει τα αποτελέσματα του στο Διαδίκτυο. Οι αποκαλύψεις προκαλούν αμηχανία αλλά οδηγούν έμμεσα σε πιο ασφαλή συστήματα. Οι ερευνητές έχουν τυπικά πρόσβαση σε ουσιώδης υπολογιστικούς πόρους, από δίκτυα με ανενεργούς δικτυωμένους υπολογιστές έως ειδικού σκοπού hardware ή supercomputers.

**Εγκληματίες (Criminals)**

Ακόμα και χωρίς το Διαδίκτυο υπάρχει ένα μεγάλο μέρος υπαλλήλων με εγκληματική δράση που προκαλεί αδυναμίες σε υπολογιστικά συστήματα. Επειδή τα βασικά χαρακτηριστικά του Διαδικτύου είναι η μεγάλη διάδοση και η ανωνυμία, έχει γίνει πολύ ελκυστικό μέρος για «εγκλήματα». Τα δικτυακά εγκλήματα εκτείνονται από απλές απάτες με κλοπή αριθμών πιστωτικών καρτών έως προσεκτικές επιθέσεις για πρόσβαση σε χρήμα ή πληροφορίες. Οι εγκληματίες μπορεί να μην έχουν τους πόρους για να σπάσουν σχήματα κρυπτογράφησης, αλλά μπορούν εύκολα να δωροδοκήσουν υπαλλήλους ή άλλο προσωπικό με πρόσβαση σε συστήματα ηλεκτρονικού εμπορίου. Πρόθεση τους είναι το οικονομικό όφελος.

**Ανταγωνιστές (Competitors)**

Ένας ανταγωνιστής μπορεί να μην μπει σε υπολογιστικό σύστημα για να κλέψει χρήματα ή να καταστρέψει αρχεία, αλλά η πρόσβαση στις λίστες των πελατών ή σε διάφορα επιχειρηματικά σχέδια είναι πολύτιμες γι' αυτόν. Επιπρόσθετα, ένας ανταγωνιστής που γνωρίζει τις αδυναμίες στην ασφάλεια κάποιων συστημάτων μπορεί να χρησιμοποιήσει τις πληροφορίες σε καταστάσεις ανταγωνιστικών πωλήσεων ή για να δημιουργήσει κακή δημοσιότητα για τους κατόχους των συστημάτων. Παρόλο που οργανισμοί μπορεί να έχουν μεγάλους πόρους, δεν αρέσκονται να δαπανήσουν μεγάλα ποσά με παράνομους ή ανήθικους τρόπους.

**Κυβερνήσεις (Governments)**

Σε μια έντονα ανταγωνιστική παγκόσμια οικονομία, όλο και περισσότερα κρατικά πρακτορεία πληροφοριών εργάζονται για το οικονομικό πλεονέκτημα της εγχώριας βιομηχανίας στην κατανάλωση των εξωτερικών βιομηχανιών. Τέτοιοι οργανισμοί εστιάζονται σε πληροφορίες ιδιοκτησιακών σχεδίων, οικονομικές πληροφορίες και ακριβείς πληροφορίες για καταστάσεις ανταγωνιστικών πωλήσεων. Τα κρατικά πρακτορεία πληροφοριών έχουν τεράστιους πόρους στη διάθεσή τους.

**Εσωτερικοί εχθροί**

Δυσαρεστημένοι ή άπληστοι υπάλληλοι μπορούν να αποτελέσουν την πιο σοβαρή απειλή για την ασφάλεια των συστημάτων ηλεκτρονικού εμπορίου. Οι «εσωτερικοί εχθροί» εξ ορισμού έχουν πρόσβαση σε ευαίσθητα συστήματα και πληροφορίες. Υπάρχουν διάφοροι τεχνικοί τρόποι για τη διαφύλαξη των συστημάτων όπως

συσκευές προστασίας, αλλά, διασταυρούμενοι έλεγχοι και καλές υπαλληλικές σχέσεις είναι απαραίτητες. Μια από τις σπουδαιότερες αποφάσεις κατά το σχεδιασμό μιας εφαρμογής είναι κατά πόσο η ασφάλεια προσανατολίζεται προς τις εξωτερικές απειλές και κατά πόσο προς τις εσωτερικές απειλές.

**Οποιοσδήποτε με φυσική πρόσβαση**

Οποιοσδήποτε με φυσική πρόσβαση σε υπηρεσίες αποτελεί απειλή για την ασφάλεια. Συνεργεία καθαρισμού, προσωπικό διανομών, επισκέπτες και προσωρινοί εργάτες έχουν πρόσβαση αλλά δεν αποτελούν αντικείμενο παρακολούθησης και ελέγχου στον ίδιο βαθμό με το προσωπικό πλήρους απασχόλησης.

### 3.2.2 ΑΠΕΙΛΕΣ

Παίρνοντας μια ιδέα για το ποιοι είναι οι πιθανοί εισβολείς σε ένα σύστημα ηλεκτρονικού εμπορίου, μπορεί κανείς να υποθέσει και ποιες είναι οι πιθανές επιθέσεις. Για παράδειγμα, οι επικοινωνίες πάνω από δημόσια δίκτυα εκτίθενται σε πολλούς κινδύνους, όπως παρακολούθηση, υποκλοπές κλπ. Επιπλέον, οι υπολογιστές του πελάτη και του εξυπηρετητή μπορεί να δεχτούν επίθεση ενώ και η ίδια η εφαρμογή μπορεί να αποτελέσει αντικείμενο επίθεσης. Ακολουθούν τα είδη επιθέσεων σε τέτοια συστήματα.

**Διακοπή υπηρεσιών**

Αυτός ο τύπος προβλήματος μπορεί να προκληθεί από «κρέμασμα» του εξοπλισμού, όπως είναι σφάλματα στους δίσκους στους υπολογιστές ή στο δίκτυο. Για παράδειγμα, ένας εισβολέας μπορεί να βάλει έναν ιό στο λειτουργικό σύστημα ενός εξυπηρετητή –πιθανότατα κάποιον άσχετο με την εφαρμογή ηλεκτρονικού εμπορίου- για να οδηγήσει το σύστημα σε κατάρρευση. Σε μια τέτοια επίθεση δεν αποκαλύπτετε καμιά ιδιωτική πληροφορία αλλά οι επιθέσεις έχουν σχέση με την αποδοτική λειτουργία των επιχειρήσεων.

**Κλοπή και απάτη**

Ένας χρήστης χωρίς εξουσιοδότηση μπορεί να είναι ικανός να αποκτήσει κέρδη ή υπηρεσίες παράνομα. Αυτό γίνεται όταν αποτυγχάνει η πιστοποίηση, οπότε ένας χρήστης χωρίς εξουσιοδότηση υποδύεται με επιτυχία έναν εξουσιοδοτημένο χρήστη. Για παράδειγμα, ένας εισβολέας μαντεύοντας passwords αποκτά πρόσβαση στο

λογαριασμό κάποιου άλλου χρήστη. Σε πιο πολύπλοκη κατάσταση ο χρήστης μπορεί να κατασκευάσει όχι εξουσιοδοτημένα κουπόνια πληρωμών.

**Κατάχρηση**

Πληρωμές από νόμιμους χρήστες μπορεί να κατευθυνθούν σε μη εξουσιοδοτημένα μέλη. Παρόλο που αυτό είναι αρκετά δύσκολο όταν χρησιμοποιούνται πιστωτικές κάρτες, άλλα συστήματα πληρωμών μπορεί να είναι πιο ευάλωτα. Για παράδειγμα, ένας πωλητής που εμφανίζεται να είναι νόμιμος ίσως να πουλήσει πρόσβαση στα περιεχόμενα άλλου πωλητή. Έτσι η πληρωμή θα πάει σε λάθος πρόσωπο χωρίς ο αγοραστής να γνωρίζει την παραπλάνηση αυτή.

**Παραποίηση δεδομένων**

Τα αρχεία που κρατάει το σύστημα μπορεί να καταστραφούν ή να καταστούν αναξιόπιστα. Αυτό μπορεί να προκληθεί από κάποιο ιό ή από αποτυχία του συστήματος ή από μια ενεργή επίθεση. Μια τέτοια επίθεση μπορεί να πάρει διάφορες μορφές: ο εισβολέας μεταβάλλει νόμιμα αρχεία ή εισάγει λανθασμένες πληροφορίες στο σύστημα. Ένα πρόβλημα με «μολυσμένα» δεδομένα μπορεί να παραμένει πέρα από κάθε τροποποίηση. Για παράδειγμα, αν τα αρχεία μιας επιχείρησης χαθούν, οποιοσδήποτε που είναι γνώστης του προβλήματος μπορεί να προκαλέσει συναλλαγές γνωρίζοντας ότι τα αρχεία δεν μπορούν να χρησιμοποιηθούν για άμυνα του συστήματος.

**Κλοπή των αρχείων**

Ένας εισβολέας μπορεί να αποκτήσει πρόσβαση στα αρχεία μιας επιχείρησης, σε εμπιστευτικές πληροφορίες του συστήματος ή σε ιδιωτικές πληροφορίες σχετικά με τους πελάτες της. Για παράδειγμα, ένας εισβολέας μπορεί να κλέψει αρχεία πελατών που ίσως να περιέχουν αριθμούς πιστωτικών καρτών.

**Μετατροπή περιεχομένου**

Οι εισβολείς μπορούν μπουν σε ένα σύστημα και να μεταβάλλουν το περιεχόμενο του, όπως π.χ. να μπουν σε κάποιο web site και να ζωγραφίσουν πάνω στις εικόνες του.

**Μεταμφίεση**

Οι εισβολείς δημιουργούν ένα παρόμοιο web site γεγονός που τραβά την προσοχή ανυποψίαστων χρηστών, οδηγώντας τους σε λάθος ιστοσελίδες. Οι μέθοδοι που χρησιμοποιούνται για τα παραπάνω είδη επιθέσεων είναι πολύπλοκοι και διαφέρουν. Ακολουθούν κάποιοι μηχανισμοί επιθέσεων που μπορούν να συνδυαστούν με διάφορους τρόπους.

**Μη εξουσιοδοτημένη ακρόαση**

Ένας εισβολέας ακούει τα μηνύματα που διακινούνται στο δίκτυο. Τα μηνύματα αυτά μπορεί να είναι κρυπτογραφημένα ή όχι, αλλά ακόμα και να είναι μπορούν να καταγραφούν και να αναλυθούν αργότερα.

**Ανάλυση της κυκλοφορίας**

Ο εισβολέας μαθαίνει ότι συγκεκριμένοι πελάτες επικοινωνούν με συγκεκριμένους εξυπηρετητές. Ιστορικά, η ανάλυση της κυκλοφορίας έχει αποδειχθεί πολύτιμη για στρατιωτικές και διπλωματικές καταστάσεις. Για παράδειγμα, μια ξαφνική αύξηση στην κυκλοφορία των μηνυμάτων μεταξύ της βάσης και των μονάδων της στο πεδίο της μάχης, μπορεί να σημαίνει ότι επίκειται επίθεση, ακόμα και αν τα μηνύματα δεν μπορούν να αποκωδικοποιηθούν. Σε εμπορικές καταστάσεις, είναι σημαντικό να γνωρίζει κάποιος ότι δύο υποτιθέμενοι ανταγωνιστές επικοινωνούν μεταξύ τους. Τα περισσότερα συστήματα ηλεκτρονικού εμπορίου, ή γενικά τα δικτυακά συστήματα δεν κάνουν καμιά προσπάθεια για να αποφύγουν την ανάλυση της κυκλοφορίας.

**Κρυπτανάλυση**

Ένας εισβολέας προσπαθεί να αποκωδικοποιήσει τα κρυπτογραφημένα μηνύματα. Υπάρχουν πολλές διαφορετικές τεχνικές που ανήκουν σ' αυτήν την κατηγορία όπως δυναμικές προσπάθειες ευρέσεως των κλειδιών κρυπτογράφησης, επιθέσεις σε αδυναμίες πρωτοκόλλων και αλγορίθμων και επιθέσεις σε συστήματα παραγωγής και διανομής κλειδιών.

**Επιθέσεις πιστοποίησης**

Ο εισβολέας υποδύεται ότι είναι ο εξυπηρετητής με τον οποίο νομίζει ο χρήστης ότι επικοινωνεί ή υποδύεται ότι είναι νόμιμος πελάτης. Πρόκειται επίσης για ευρεία

κατηγορία που περιλαμβάνει εύρεση των passwords, κλοπή των νόμιμων πιστοποιητικών των χρηστών κ.α.

**Επιθέσεις αντικατάστασης**

Ο εισβολέας αντικαθιστά ολόκληρο ή μέρος ενός μηνύματος με κάτι άλλο.

**Μη ανιχνεύσιμη εισβολή**

Ένας εισβολέας επιτίθεται στο σύστημα για λίγο κάθε φορά έτσι ώστε να μην μπορεί να εντοπιστεί. Έτσι, αν ο εισβολέας κατέχει πολλούς κλεμμένους αριθμούς πιστωτικών καρτών χρησιμοποιεί τον καθένα μόνο μια φορά.

## 3.3 ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ

Το έγγραφο αυτό αποτελείται κυρίως από την πολιτική ασφάλειας, την περιγραφή της υφιστάμενης κατάστασης της υποδομής από τη σκοπιά της ασφάλειας, τις απαιτήσεις ασφάλειας, το πλάνο υλοποίησης και την περιγραφή των διαδικασιών συνεχούς επισκόπησης και αναθεώρησης του σχεδίου ασφάλειας.

**Πολιτική ασφάλειας *(Security Policy)***

Πρόκειται για ένα σύνολο κανόνων, οι οποίοι προσδιορίζουν επακριβώς το ρόλο κάθε εμπλεκόμενου μέσα σε μία εταιρία ή έναν οργανισμό, τις αρμοδιότητες, τις ευθύνες και τα καθήκοντά του.

Μια πολιτική ασφαλείας πρέπει να περιλαμβάνει τα ακόλουθα στοιχεία:

**Αγαθά** *(Assets)*: πρόκειται για τις οντότητες (πχ υλικό, λογισμικό, πληροφορίες κλπ) του πληροφοριακού συστήματος που έχουν αξία και πρέπει να προστατευθούν

**Ρόλους και αρμοδιότητες** *(Roles and Responsibilities)*: πρόκειται για τους ρόλους, αρμοδιότητες, καθήκοντα, ευθύνες για θέματα που αφορούν το πληροφοριακό σύστημα και την ασφάλειά του

**Στόχους** *(Security policy objectives)*: πρόκειται για τον στόχο (ή τους στόχους) ασφαλείας που καθορίζει συνοπτικά την εστίαση της πολιτικής και θέτει περιορισμούς

**Πεδίο εφαρμογής της πολιτικής ασφαλείας** *(Scope of Security Policy)*: πρόκειται για την εμβέλεια, την έκταση και το χώρο που αφορά η πολιτική ασφαλείας

**Οδηγίες, κατευθυντήριες γραμμές** *(Guidelines)*: γενικές αρχές και κανόνες, που διέπουν την κατάρτιση της πολιτικής ασφάλειας.

**Πολιτισμικές Αξίες, νομοθεσία, άλλες πολιτικές** *(Cult πολιτικές (Cult, other policies)*: πρόκειται για το σύνολο των πεποιθήσεων, αξιών, αρχών, πολιτικών, κωδίκων δεοντολογίας, νόμων που συνθέτουν την κουλτούρα του οργανισμού και του περιβάλλοντος αυτού και ανατροφοδοτούν τους μηχανισμούς του μέσω μιας διαδικασίας συνεχούς εκμάθησης

**Υλοποίηση και εφαρμογή της πολιτικής ασφαλείας - Ενημέρωση και συμμόρφωση** *(Implementation and application of the security policy – Awareness, enforcement, breach)*: πρόκειται για το οργανωτικό πλαίσιο ρόλων, αρμοδιοτήτων, κανονισμών, επιτροπών για την υλοποίηση και εφαρμογή της πολιτικής ασφαλείας, για την ενημέρωση του προσωπικού σχετικά με την συμμόρφωση και τις ενέργειες που λαμβάνονται στην περίπτωση παραβίασης της πολιτικής ασφαλείας

**Επισκόπηση και αναθεώρηση της πολιτικής** *(Review and audit)*: πρόκειται για την τακτική επισκόπηση και αναθεώρηση της πολιτικής σύμφωνα με τις εκάστοτε συνθήκες ώστε να είναι επίκαιρη και να καλύπτει το σύνολο των δομικών στοιχείων του πληροφοριακού συστήματος και των διαδικασιών διαχείρισης

### 3.3.1 ΣΧΕΔΙΟ ΕΚΤΑΚΤΗΣ ΑΝΑΓΚΗΣ

Στο σχέδιο έκτακτης ανάγκης, το οποίο συμπληρώνει το σχέδιο ασφάλειας, προβλέπονται μέτρα που στοχεύουν στα ακόλουθα:

- Ελαχιστοποίηση διακοπών της κανονικής λειτουργίας.
- Περιορισμός της έκτασης των ζημιών και καταστροφών, και αποφυγή πιθανής κλιμάκωσης αυτών.
- Εγκατάσταση εναλλακτικών μέσων λειτουργίας εκ των προτέρων.
- Εκπαίδευση, εξάσκηση και εξοικείωση του ανθρώπινου δυναμικού με διαδικασίες έκτακτης ανάγκης.
- Δυνατότητα ταχείας και ομαλής αποκατάστασης της λειτουργίας.
- Ελαχιστοποίηση των οικονομικών επιπτώσεων.

Το σχέδιο έκτακτης ανάγκης πρέπει να προσδιορίζει τους πιθανούς κινδύνους και γενικότερα τα κριτήρια που καθορίζουν την κατάσταση ως έκτατη και

επιβάλλουν την ενεργοποίηση του σχεδίου. Πρέπει να υπάρχουν σαφείς και γραπτές διαδικασίες που να θέτουν τον οργανισμό σε κατάσταση έκτακτης ανάγκης και να επιτρέπουν εφαρμογή του σχεδίου.

Το σχέδιο έκτακτης ανάγκης πρέπει να προσδιορίζει τις σημαντικές λειτουργίες (critical functions and systems) και τα αντίστοιχα συστήματα του οργανισμού, τη στρατηγική προστασίας τους (protection strategy) και την προτεραιότητα με την οποία θα τεθούν σε εφαρμογή οι δραστηριότητες του οργανισμού στο εναλλακτικό σύστημα. Επίσης, το σχέδιο πρέπει να περιέχει μια κατάσταση με τα μέλη του προσωπικού που θα κληθούν στην περίπτωση καταστροφής καθώς και τα τηλέφωνα των προμηθευτών υλικού και λογισμικού, των σημαντικών πελατών, των ατόμων που βρίσκονται σε διαφορετικές εγκαταστάσεις που θα χρησιμοποιηθούν από την επιχείρηση για τη συνέχιση της λειτουργίας της. Επίσης το σχέδιο θα πρέπει να περιέχει διαδικασίες για υπολογισμό της ζημιάς από την καταστροφή του συντελέστηκε. Ακόμα θα πρέπει να περιέχει έναν κατάλληλο χρόνο-προγραμματισμό με σαφή ανάθεση καθηκόντων για την αποκατάσταση της λειτουργίας του οργανισμού.

Σε πρώτη φάση, το σχέδιο έκτακτης ανάγκης πραγματεύεται την ανάκαμψη ύστερα από φυσικές καταστροφές (φωτιές, πλημμύρες, σεισμούς, κτλ.). Η προτεινόμενη λύση είναι η τοποθέτηση συναγερμών. Οι συναγερμοί χρησιμοποιούνται τόσο για την ανίχνευση εισβολών στα συστήματα, όσο και για την ανίχνευση επικείμενης ζημιάς λόγω φυσικών φαινομένων. Όσον αφορά τις εισβολές, χρησιμοποιούνται αυτοματοποιημένα και βασισμένα σε λογισμικό συστήματα ανίχνευσης, συστήματα συναγερμού που βασίζουν τη λειτουργία τους σε αισθητήρες, οι οποίοι - με τη σειρά τους - δίνουν τακτικές αναφορές στα κέντρα ελέγχου, και συστήματα στα οποία κάθε αισθητήρας αντιδρά άμεσα, όταν εντοπίζει ίχνη εισβολής. Ακόμα, όσον αφορά την αντιμετώπιση φυσικών φαινομένων, χρησιμοποιούνται ειδικές συσκευές φιλτραρίσματος, όπως είναι τα φίλτρα αέρος, που περιορίζουν τις ζημιές από τον καπνό και από άλλα βλαβερά αέρια, τα φίλτρα πακέτων, που περιορίζουν τη ροή των μη εξουσιοδοτημένων πακέτων στα εσωτερικά δίκτυα της εταιρίας ή του οργανισμού, και τα φίλτρα θορύβου, που ελαττώνουν το άκουσμα εξωτερικών θορύβων. Επίσης, για τους περιβαλλοντικούς ελέγχους υπάρχουν συσκευές ή μέθοδοι που ελέγχουν τη θερμοκρασία, την πίεση, την υγρασία και άλλους περιβαλλοντικούς παράγοντες. Το σχέδιο έκτακτης ανάγκης, άλλωστε,

έρχεται να καλύψει τα κενά που πιθανόν να έχει αφήσει το σχέδιο ασφάλειας. Ένα άλλο ενδεχόμενο που καλύπτει το σχέδιο έκτακτης ανάγκης είναι αυτό της διακοπής στην παροχή ηλεκτρικού ρεύματος. Για την αντιμετώπιση αυτού του προβλήματος χρησιμοποιούνται ειδικές γεννήτριες, οι οποίες παρέχουν συνεχώς ενέργεια σε ζωτικά τμήματα του εξοπλισμού. Οι γεννήτριες αυτές είναι ιδιαίτερα χρήσιμες σε περιπτώσεις όπου συμβαίνουν συχνά blackouts και υπάρχει κίνδυνος απώλειας σημαντικών πληροφοριών. Τέλος, στο σχέδιο έκτακτης ανάγκης περιλαμβάνονται και τα μέτρα για τον έλεγχο της φυσικής πρόσβασης. Παραδείγματα είναι οι φύλακες, οι προστατευτικοί φράχτες, τα βιομετρικά συστήματα και τα συστήματα συναγερμού σε πόρτες και δωμάτια. Η φυσική ασφάλεια είναι δαπανηρή, ενώ ποτέ δεν είναι τέλεια. Χωρίς φυσική ασφάλεια όμως, όλοι οι άλλοι τύποι προστασίας των πληροφοριών έρχονται σε δεύτερη μοίρα. Η όσο το δυνατόν καλύτερη φυσική προστασία εμποδίζει την πραγματοποίηση επιθέσεων από το εσωτερικό μιας εταιρίας ή ενός οργανισμού, οι οποίες (επιθέσεις) υποβοηθούνται από ειδικούς εξώτερικούς παράγοντες.

Το σχέδιο έκτακτης ανάγκης αντιμετωπίζει όμως και άλλες περιπτώσεις, όπως είναι αυτή της διατήρησης αντιγράφων. Η αποθήκευση των πιο σημαντικών αντιγράφων του λογισμικού του συστήματος είναι πολύ σπουδαία υπόθεση. Για το λόγο αυτό, συνιστάται τα αντίγραφα να φυλάσσονται φρουρούμενα σε άλλα κτίρια. Τα μέρη αυτά διακρίνονται στις εξής δύο κατηγορίες: *cold sites* (ή shells) και *hot sites*. Τα πρώτα είναι, στην ουσία, εγκαταστάσεις όπου υπάρχει παροχή ηλεκτρικής ενέργειας και κλιματισμός. Στις εγκαταστάσεις αυτές θα μπορεί να εγκαθίσταται ένα υπολογιστικό σύστημα, όμοιο ακριβώς με αυτό που λειτουργεί στα κυρίως κτίρια, το οποίο θα μπορεί να τίθεται άμεσα σε λειτουργία, κάθε φορά που κάτι τέτοιο θα κρίνεται απαραίτητο.

Τα *hot sites*, από την άλλη, είναι και αυτά εγκαταστάσεις, στις οποίες όμως υπάρχει ήδη εγκατεστημένο ένα υπολογιστικό σύστημα, το οποίο είναι και ανά πάσα στιγμή έτοιμο για λειτουργία και χρήση. Το σύστημα αυτό διαθέτει περιφερειακά, τηλεπικοινωνιακές γραμμές, γεννήτριες, και, ακόμα και προσωπικό για να το χειριστεί άμεσα, σε περίπτωση έκτακτης ανάγκης. Για την ενεργοποίηση ενός *hot site*, αρκεί να φορτωθούν τα δεδομένα και το αντίγραφο του λογισμικού του συστήματος, στοιχεία που βρίσκονται - όπως είπαμε - αποθηκευμένα μακριά από τα κεντρικά κτίρια της εταιρίας ή του οργανισμού.

### 3.3.2 ΤΑ ΒΑΣΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΗΣ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

Για να τεθεί σε πλήρη λειτουργία η πολιτική ασφαλείας πρέπει να πληρούνται τα παρακάτω βασικά χαρακτηριστικά:

- Απαιτεί ***συμμόρφωση από το προσωπικό του οργανισμού***. Το έγγραφο της πολιτικής θα πρέπει να είναι στη διάθεση όλου του προσωπικού.
- Εκφράζει ***γενικότερες απόψεις ή αρχές*** του οργανισμού.
- Είναι ***σαφής*** ώστε να μην παρουσιάζονται δυσκολίες στην κατανόηση και εφαρμογή της και ***εφαρμόσιμη*** από άποψη κόστους.
- Είναι ***γενικεύσιμη*** ώστε η εφαρμογή της να είναι επεκτάσιμη σε μελλοντικά συστήματα που ενδεχομένως ενταχθούν στο πληροφοριακό σύστημα του οργανισμού.
- Είναι ***απαλλαγμένη από μη απαραίτητους τεχνικούς όρους και εξειδικευμένες αναφορές*** ώστε να μην καθίσταται δύσκολη στην εφαρμογή της και εξαρτημένη από τεχνολογικές επιλογές καθώς και να μην τροποποιείται συχνά, παρά μόνο όταν συμβαίνουν σημαντικές αλλαγές στα εξής :

1. Στην οργανωτική δομή και στην κουλτούρα του οργανισμού.
2. Στις απαιτήσεις ασφαλείας.
3. Στις τεχνολογικές εξελίξεις.

✓ **Υφιστάμενη κατάσταση**

Η υπολογιστική και επικοινωνιακή υποδομή εξετάζεται σε σχέση με τις ***αδυναμίες***, τους ***κινδύνους*** που παρουσιάζονται και τα ***μέτρα ασφάλειας***, τα οποία έχουν ήδη υλοποιηθεί με σκοπό την αντιμετώπιση των αδυναμιών και των κινδύνων του πληροφοριακού συστήματος. Βάση για την εξέταση της υφιστάμενης κατάστασης μπορεί να αποτελέσει και η ανάλυση επικινδυνότητας. Τα υφιστάμενα μέτρα ασφάλειας αξιολογούνται.

✓ **Απαιτήσεις Ασφάλειας**

Προσδιορίζονται οι απαιτήσεις ασφάλειας με τη βοήθεια ειδικών μεθόδων ανάλυσης και καταγραφής απαιτήσεων. Ο προσδιορισμός των απαιτήσεων μπορεί να βασίζεται στην ανάλυση επικινδυνότητας, το τελευταίο στάδιο της οποίας είναι εκείνο της ανάλυσης μέγιστου κέρδους - ελάχιστου κόστους (cost benefit analysis) από την

εφαρμογή των διαφόρων μέτρων ασφαλείας. Τα μέτρα ασφάλειας πρέπει να προσφέρουν ασφάλεια αντίστοιχη της αξίας του πληροφοριακού συστήματος καθώς και της σοβαρότητας των κινδύνων που αντιμετωπίζει.

Τα ***μέτρα ασφαλείας*** αντανακλούν τη διασφάλιση των βασικών απαιτήσεων ασφαλείας και περιλαμβάνουν αναλυτικούς ***κανόνες*** και ***οδηγίες*** για την επίτευξη των στόχων ασφαλείας (βασικών και επιμέρους) που έχουν τεθεί. Τα μέτρα ασφαλείας του πληροφοριακού συστήματος μπορούν να αναλυθούν στις παρακάτω βασικές κατηγορίες:

| **Βασικές κατηγορίες μέτρων ασφάλειας του πληροφοριακού συστήματος** | **Επιμέρους κατηγορίες των βασικών μέτρων ασφάλειας του ΠΣ** |
|---|---|
| *Οργάνωση και διαχείριση της ασφάλειας του πληροφοριακού συστήματος* | Σχεδιασμός της ασφάλειας του ΠΣ<br>Κώδικας δεοντολογίας.<br>Έλεγχος, επιθεώρηση και εποπτεία της ασφάλειας του ΠΣ.<br>Ρόλοι και αρμοδιότητες υλοποίησης και διαχείρισης της ασφάλεια του ΠΣ.<br>Τεκμηρίωση και εγχειρίδια χρήσης των διαδικασιών και λειτουργιών σχετικά με την ασφάλεια του ΠΣ.<br>Εκπαίδευση, ευαισθητοποίηση, ενημέρωση χρηστών. |
| *Ασφάλεια ανάπτυξης και συντήρησης του πληροφοριακού συστήματος* | Ανάπτυξη και συντήρηση εφαρμογών (Application development and maintenance).<br>Διαχείριση της υποστήριξης και απόκτησης υλικού και λογισμικού από προμηθευτές (Vendor support – contracts and reliability).<br>Απογραφή του υλικού και λογισμικού και διαχείριση των αλλαγών (Hardware and software inventory). |
| *Φυσική ασφάλεια* | Ασφάλεια κτιριακών εγκαταστάσεων.<br>Ασφάλεια εξοπλισμού πληροφορικής και τηλεπικοινωνιακής υποδομής.<br>Προστασία από φυσικές καταστροφές (Environmental controls). |
| *Ασφάλεια της υπολογιστικής και τηλεπικοινωνιακής υποδομής* | Μηχανισμοί εξασφάλισης ακεραιότητας και εμπιστευτικότητας των δεδομένων.<br>Κατηγοριοποίηση, ταξινόμηση των δεδομένων (Classification of data/ information). |

| | |
|---|---|
| | Διαδικασίες διαχείρισης εφεδρικών αντιγράφων ασφαλείας.<br>Διαδικασίες αντιμετώπισης ιομορφών .<br>Διαδικασίες διαχείρισης συνθηματικών.<br>Ασφάλεια εφαρμογών-λογισμικού.<br>Ασφάλεια λειτουργικών συστημάτων και βάσεων δεδομένων.<br>Ασφάλεια δικτύων και τηλεπικοινωνιών και ασφάλεια κατά τη σύνδεση στο Internet.<br>Έλεγχος προσπέλασης του ΠΣ.<br>Μηχανισμοί καταγραφής συμβάντων και περιστατικών και ανίχνευσης και αντιμετώπισης προσπαθειών παραβίασης της ασφάλειας του ΠΣ. |
| *Ανάκαμψη από καταστροφές* | Σχέδιο έκτακτης ανάγκης. |

✓ **Πλάνο Υλοποίησης**

Τον προσδιορισμό των απαιτήσεων ασφάλειας ακολουθεί η υλοποίησή τους. Το σχετικό πλάνο υλοποίησης αναφέρεται στον καταμερισμό αρμοδιοτήτων και ευθυνών των εμπλεκόμενων, στην κατάτμηση του έργου υλοποίησης σε επιμέρους εργασίες και στον χρονοπρογραμματισμό τους.

✓ **Συνεχής Επισκόπηση – Αναθεώρηση**

Προσδιορισμός διαδικασιών για την τακτική ενημέρωση του ίδιου του σχεδίου ασφάλειας. Η επανεξέταση όλων των ελέγχων, καθώς και των λειτουργιών, αποτελεί σημαντικό βήμα προς τη θωράκιση των συστημάτων επιχειρήσεων και οργανισμών, και την ενίσχυση των αμυντικών μηχανισμών τους. Άλλωστε, η τεχνολογία εξελίσσεται με τόσο γρήγορο ρυθμό, που ακόμα και η παραμικρή αλλαγή θα πρέπει να αντικατοπτρίζεται άμεσα στα μέτρα ασφάλειας που τελικά υιοθετούνται. Από την άλλη, αυτό δε σημαίνει απαραίτητα ότι θα υπάρχουν συνεχείς αλλαγές στην πολιτική ασφάλειας, ούτε ότι θα αλλάζουν κάθε τόσο τα καθήκοντα των χρηστών και λοιπών εμπλεκομένων. Αντιθέτως, όλοι καλούνται να τηρούν πιστά τις οδηγίες που τους έχουν δοθεί, και να φροντίζουν ώστε να

ελαχιστοποιούν τα λάθη τους. Επίσης, έχει τεράστια σημασία η καλλιέργεια ενός κλίματος εμπιστοσύνης και αμοιβαίας κατανόησης ανάμεσα στο σύνολο του ανθρώπινου δυναμικού που έρχεται είτε έμμεσα, είτε άμεσα σε επαφή με τα συστήματα πληροφορικής και τηλεπικοινωνιών μέσα σε μία επιχείρηση ή σε έναν οργανισμό.

## 3.4 ΠΑΡΑΔΕΙΓΜΑΤΑ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟ INTERNET ΥΠΑΡΧΟΥΝ ΣΤΙΣ ΠΑΡΑΚΑΤΩ ΔΙΕΥΘΥΝΣΕΙΣ

1. Lancaster University Electronic Information Systems Security Policy
http://www.lancs.ac.uk/homepage/webmenus/e-security

2. Murdoch University – Office of Information Technology Services – IT Security Policy
http://wwwits2.murdoch.edu.au/security/policy.html

3. Kansas Information Resources Council- Security Policy and Procedures for the Kanwin Network
http://www.ink.org/public/kirc/refpg2.htm#BM4220

4. Janet Security Policy
http://www.ja.net/documents/JANET_security_policy.html

5. Acme Agency Business Contingency Plan Model
http://www.ink.org/public/kirc/modelpln.htm

## 3.5 ΣΥΜΠΛΗΡΩΜΑΤΙΚΑ ΜΕΤΡΑ ΠΟΥ ΠΡΕΠΕΙ ΝΑ ΛΗΦΘΟΥΝ ΩΣ ΠΡΟΣ ΤΗ ΝΟΜΟΘΕΣΙΑ

Είναι γνωστό, και ισχύει ιδιαίτερα στη χώρα μας, ότι η αξία του νόμου φαίνεται κυρίως στην εφαρμογή του. Ως προς αυτό το κριτήριο, οι νέες τεχνολογίες της πληροφορίας βάζουν σε δοκιμασία μεγάλα τμήματα της παραδοσιακής νομοθεσίας. Η ποινική νομοθεσία στα προηγμένα κράτη διευρύνεται ώστε να περιλάβει νέου τύπου αδικήματα, αλλά για την αποτελεσματική εφαρμογή της χρειάζεται ακόμη κατάλληλη εκπαίδευση αστυνομικών και δικαστικών αρχών, των ίδιων των χρηστών

των νέων τεχνολογιών, παράλληλη εισαγωγή τεχνικών και οργανωτικών μέτρων ασφάλειας και μέτρα για την επιτάχυνση της διεθνούς συνεργασίας.

Με την εισαγωγή της ψηφιακής τεχνολογίας και των ηλεκτρονικών υπολογιστών σε κάθε σπίτι και σε κάθε τομέα της κοινωνικής ζωής (οικονομία, υγεία, πολιτική, περιβάλλον, μεταφορές, ψυχαγωγία κ.τ.λ.) προσωπικά δεδομένα θα μεταφέρονται μέσω ηλεκτρονικών δικτύων και θα γίνονται αντικείμενο επεξεργασίας για ποικίλους σκοπούς σε πρωτοφανή κλίμακα. Αυστηρές νομοθεσίες για την προστασία των προσωπικών δεδομένων είναι απαραίτητες ώστε να εξασφαλιστεί η συναίνεση και συμμετοχή των πολιτών στην εισαγωγή των νέων τεχνολογιών. Οι βασικές αρχές των νομοθεσιών αυτών είναι ήδη γνωστές. Περιέχονται σε όλες τις ισχύουσες Ευρωπαϊκές νομοθεσίες, στη Σύμβαση 108 του Συμβουλίου της Ευρώπης και την Πρόταση Οδηγίας της Ευρωπαϊκής Ένωσης. Είναι όμως βέβαιο ότι η νομοθεσία γενικού περιεχομένου, όπως οι προαναφερθείσες, είναι μεν απαραίτητη αλλά δεν είναι αρκετή για να εξασφαλίσει τον επιδιωκόμενο στόχο, δηλαδή την προστασία του πολίτη. Θα χρειαστεί και μια σειρά από συμπληρωματικά μέτρα.

### 3.5.1 ΣΥΜΠΛΗΡΩΜΑΤΙΚΑ ΜΕΤΡΑ

Η όποια γενική νομοθεσία πρέπει να συνοδεύεται από νομοθετήματα τομεακού χαρακτήρα. Η ραγδαία εξάπλωση των νέων τεχνολογιών σε όλους τους τομείς της κοινωνικής και οικονομικής ζωής, δημιουργεί ειδικές, χωριστές ανάγκες για την προστασία των προσωπικών δεδομένων ανάλογα με τις ιδιαιτερότητες του κάθε τομέα. Από το 1981 το Συμβούλιο της Ευρώπης έχει υιοθετήσει μια σειρά από Συστάσεις που καλύπτουν τις ιατρικές βάσεις δεδομένων, την κοινωνική ασφάλιση, το μάρκετινγκ, τα δεδομένα για τους εργαζομένους, την εμπορευματοποίηση των δεδομένων του δημοσίου τομέα, τα δεδομένα της αστυνομίας, τα δεδομένα της έρευνας και της στατιστικής, τις τηλεπικοινωνίες. Πρόταση τομεακής Οδηγίας για τα ψηφιακά τηλεπικοινωνιακά δίκτυα έχει ήδη υποβληθεί από την Ευρωπαϊκή Επιτροπή. Παράλληλα γενικού χαρακτήρα η πρόταση Οδηγίας της Ευρωπαϊκής Ένωσης ζητάει από τα κράτη μέλη να ενθαρρύνουν τις επαγγελματικές οργανώσεις να υιοθετήσουν τομεακούς κώδικες δεοντολογίας, ενώ αφήνει ανοιχτό το ενδεχόμενο νέων τομεακών νομοθετικών προτάσεων.

Τα νομοθετήματα και οι κώδικες δεοντολογίας τομεακού χαρακτήρα, έχουν ένα κοινό χαρακτηριστικό, ότι στο βαθμό που εκπονούνται σε στενή συνεργασία με ενδιαφερομένους φορείς, συμβάλλουν αποφασιστικά στην ευαισθητοποίηση των χρηστών των προσωπικών δεδομένων σε κάθε τομέα. Έχουν όμως και μια θεμελιώδη

διαφορά, ότι τα πρώτα έχουν νομική ισχύ δημοσίου δικαίου, ενώ οι δεύτεροι επαφίονται στη νομιμοφροσύνη των μελών των επαγγελματικών οργανώσεων και στην αποφασιστικότητα εθελοντικών διαχειριστικών οργάνων όσον αφορά την επιβολή κυρώσεων. Κι αν σε ορισμένα κράτη μέλη της Ευρωπαϊκής Ένωσης όπως η Ολλανδία, υπάρχει επιτυχής παράδοση τέτοιων μορφών αυτοδιαχείρισης, η αποτελεσματικότητά τους σε χώρες της Νότιας Ευρώπης και ειδικά στην Ελλάδα, όπου και οι ίδιοι οι νόμοι συχνά δεν εφαρμόζονται, είναι εξαιρετικά αμφίβολη. Χρειάζεται νομοθετική παρέμβαση με τη μεγαλύτερη δυνατή συμμετοχή των ενδιαφερομένων φορέων, τόσο για την πληρότητα του νομοθετήματος όσο και για την ενημέρωση των χρηστών των προσωπικών δεδομένων.

Κεφαλαιώδους σημασίας είναι ο ρόλος της υπηρεσίας ελέγχου που προβλέπεται από όλες τις ευρωπαϊκές νομοθεσίες . Η υπηρεσία αυτή ελέγχει κατά κανόνα τόσο τον ιδιωτικό όσο και τον δημόσιο τομέα, επομένως πρέπει να είναι ουσιαστικά ανεξάρτητη από την Κυβέρνηση. Σε περίπτωση αμφισβητήσεων, τον τελευταίο ρόλο έχει η δικαστική εξουσία και όχι ο Υπουργός Δικαιοσύνης. Η υπηρεσία ελέγχου πρέπει να έχει εξουσίες τόσο κατασταλτικές (άσκηση ελέγχου, απαγόρευση παράνομης επεξεργασίας δεδομένων, προσφυγή στη δικαιοσύνη), όσο και προληπτικές (έκδοση ερμηνευτικών εγκυκλίων, οργάνωση εκπαιδευτικών σεμιναρίων, θεσμοθετημένο διάλογο με τις ομάδες των χρηστών, συμβολή στη σύνταξη κωδικών δεοντολογίας). Πρέπει ακόμα να έχει στη διάθεσή της επαρκή μέσα ώστε να ασκήσει επιτυχώς τα καθήκοντά της. Σημαντική είναι η περίπτωση του σκανδάλου της εμπορευματοποίησης προσωπικών δεδομένων του δημοσίου στη Νότια Ουαλία της Αυστραλίας, που αποκαλύφθηκε το 1990 - 1992, από την αρμόδια υπηρεσία ελέγχου, που είχε πενιχρά μέσα (π.χ. συνολικό προσωπικό 6 ατόμων), αλλά από την Ανεξάρτητη Επιτροπή εναντίον της Διαφθοράς που έχει ετήσιο προϋπολογισμό άνω των 100 εκατομ. δολαρίων. Πρέπει επίσης η υπηρεσία ελέγχου να έχει πρόσβαση στη δημοσιότητα και κυρίως στα μέσα μαζικής ενημέρωσης και στο Κοινοβούλιο. Τέλος, στις αρμοδιότητες της υπηρεσίας ελέγχου πρέπει να περιλαμβάνεται και η συνεργασία με τις αντίστοιχες υπηρεσίες άλλων κρατών.

Τελικός κριτής της σωστής εφαρμογής του νόμου και αρμόδιος για την επιβολή κυρώσεων είναι ο δικαστής. Και αν οι υπηρεσίες ελέγχου διαθέτουν στο στελεχιακό τους δυναμικό τόσο νομομαθείς όσο και ειδικούς της πληροφορικής, που εξειδικεύονται στην εφαρμογή του νόμου με την πείρα που αποκτούν, οι δικαστές σπάνια διαθέτουν ειδικές γνώσεις του δικαίου της πληροφορικής ή των εφαρμογών της σε όλες τις πτυχές της κοινωνικής και οικονομικής ζωής. Για τη διαπίστωση της νομιμότητας συγκεκριμένης επεξεργασίας δεδομένων ο νόμος δεν περιέχει πάντοτε ρητές προϋποθέσεις, αλλά παραπέμπει στην συγκριτική εκτίμηση των συμφερόντων τόσο των προσώπων που αφορά η επεξεργασία όσο και των χρηστών που προβαίνουν

στην επεξεργασία. Κάποια επιμόρφωση των δικαστών θα ήταν επομένως εξαιρετικά χρήσιμη.

Με την εξάπλωση της χρήσης των νέων τεχνολογιών της πληροφορίας σε παγκόσμιο επίπεδο και των δυνατοτήτων κατάχρησης των προσωπικών δεδομένων, το πλέον αποτελεσματικό όπλο είναι η συμμετοχή της κοινωνίας. Ο πολίτης πρέπει να μάθει με σαφήνεια και χωρίς υπερβολές, ποια είναι τα σχετικά οφέλη, ποια τα δικαιώματά του και ποιοι οι κίνδυνοι από την επεξεργασία των προσωπικών του δεδομένων. Οι χρήστες πρέπει να ενημερωθούν για τις υποχρεώσεις που επιβάλλει η νομοθεσία. Το ζητούμενο είναι να φτάσουμε στο σημείο όπου σε συνθήκες ελεύθερου ανταγωνισμού ο πολίτης θα προτιμά εκείνες τις υπηρεσίες (τηλεπικοινωνιών, πιστωτικών καρτών, πωλήσεων από απόσταση, ιατρικής περίθαλψης, κ.τ.λ.) που θα σέβονται και θα προστατεύουν τα προσωπικά δεδομένα. Ο υψηλότερος βαθμός ενδιαφέροντος των πολιτών παρατηρείται στη Γερμανία και αυτό έχει συμβάλλει στη θέσπιση αυστηρής νομοθεσίας. Είναι ενδιαφέρουσα η διαφορά ανάμεσα στο πνεύμα της γερμανικής νομοθεσίας που στηρίζει τη νομιμότητα της επεξεργασίας προσωπικών δεδομένων κυρίως στη συναίνεση του πολίτη και της γαλλικής νομοθεσίας, όπου η νομιμότητα στηρίζεται στην έγκριση της υπηρεσίας ελέγχου. Για να είναι σε θέση να εκτιμήσει τις περιστάσεις και να συναινέσει, ο πολίτης πρέπει να είναι ενημερωμένος. Και αυτό φυσικά είναι υποχρέωση του κράτους.

Η εξέλιξη των νέων τεχνολογιών πληροφορίας και τηλεπικοινωνιών, καθιστά ολοένα και δυσκολότερο τον έλεγχο της επεξεργασίας των προσωπικών δεδομένων με παραδοσιακούς τρόπους, καθώς η ποσότητα των δεδομένων που γίνονται αντικείμενο επεξεργασίας, ο συνολικός αριθμός των χρηστών τέτοιων δεδομένων και η ταχύτητα μεταφοράς των δεδομένων μέσω τηλεπικοινωνιών δικτύων αυξάνονται ραγδαίως. Η λύση του προβλήματος βρίσκεται στην ίδια την τεχνολογία. Είναι τεχνικά δυνατό στο σχεδιασμό του λογισμικού που χρησιμοποιείται για την επεξεργασία των προσωπικών δεδομένων, για σκοπούς π.χ. εργασιακούς, ιατρικής περίθαλψης, εμπορικών συναλλαγών κ.τ.λ. να περιλαμβάνονται κανόνες για την αποτελεσματική προστασία των προσωπικών δεδομένων, που θα επιτρέπουν δηλαδή επεξεργασία προσωπικών δεδομένων στο βαθμό που είναι απολύτως αναγκαίος για τους συγκεκριμένους σκοπούς, που θα σβήνουν ή παγώνουν τα δεδομένα όταν δεν απαιτούνται πλέον για τους σκοπούς αυτούς, που θα επιτρέπουν την πρόσβαση μόνο σε εξουσιοδοτημένα πρόσωπα, που θα διευκολύνουν την παρακολούθηση της πορείας των δεδομένων προς τους διάφορους αποδέκτες – χρήστες.

Ειδικό λογισμικό είναι δυνατό να κατασκευαστεί και για τις ανάγκες των υπηρεσιών ελέγχου, έτσι ώστε να επιταχύνεται ο έλεγχος των δηλώσεων επεξεργασίας που υποβάλλουν οι χρήστες και τις οποίες επιβάλλουν οι περισσότερες

ευρωπαϊκές νομοθεσίες. Είναι προφανές ότι η βιομηχανία του λογισμικού θα προχωρήσει προς αυτή την κατεύθυνση όταν υπάρξει σχετική ζήτηση στην αγορά. Και η ζήτηση θα υπάρξει όταν η προστασία των προσωπικών δεδομένων θα είναι μέρος του κοινωνικού προβληματισμού και μέρος της εμπορικής πολιτικής των επιχειρήσεων. Σε ένα άλλο κλάδο του δικαίου, εκείνο της προστασίας της πνευματικής ιδιοκτησίας, όπου τα οικονομικά συμφέροντα για την προστασία των ηλεκτρονικών πνευματικών έργων (βάσεων δεδομένων, υπηρεσιών ψυχαγωγίας, MULTIMEDIA) είναι ήδη ισχυρά, έχουν γίνει σημαντικά βήματα από την ίδια την τεχνολογία. Για την προστασία των προσωπικών δεδομένων κάποιες μελέτες τεχνολογικού χαρακτήρα έχουν προγραμματιστεί στα πλαίσια του προγράμματος της Ε.Ε. για την ασφάλεια των πληροφοριών, που έχει ως στόχο την επίτευξη του τρίπτυχου «εμπιστευτικότητα, πληρότητα, διαθεσιμότητα» για τις ηλεκτρονικές πληροφορίες.

Οι ανθρώπινες δραστηριότητες που περιλαμβάνουν επεξεργασία δεδομένων (ή τουλάχιστον ορισμένες από αυτές που θα θεωρηθούν εν δυνάμει περισσότερο επιβλαβείς), θα πρέπει να συνοδεύονται από έκθεση των επιπτώσεων της συγκεκριμένης επεξεργασίας για τα προσωπικά δεδομένα. Αυτό ήδη συμβαίνει με τη προστασία του περιβάλλοντος. Σύμφωνα με το άρθρο 130 Ρ παράγρ.2 της Ενιαίας Πράξης, όπως έχει ενσωματωθεί στη Συνθήκη για τη Ευρωπαϊκή, «οι ανάγκες στον τομέα της προστασίας του περιβάλλοντος πρέπει να λαμβάνονται υπόψη στον καθορισμό και την εφαρμογή των άλλων πολιτικών της Κοινότητας». Κάτι ανάλογο θα χρειαστεί και για τα προσωπικά δεδομένα και θα συμβάλλει θετικά στο έργο των υπηρεσιών ελέγχου, στην άσκηση των δικαιωμάτων τους από τους ίδιους τους πολίτες και στη συνειδητοποίηση των χρηστών.

Η θέσπιση τομεακών νομοθετημάτων, η κατάλληλη υποστήριξη των υπηρεσιών ελέγχου, η επιμόρφωση των δικαστών, η συνειδητοποίηση των πολιτών, η παραγωγή κατάλληλου λογισμικού, η έκθεση για τις επιπτώσεις της επεξεργασίας των προσωπικών δεδομένων, θα έχουν μικρή αποτελεσματικότητα αν είναι δυνατή η ανεξέλεγκτη επεξεργασία προσωπικών δεδομένων σε κάποιες τρίτες χώρες. Τεχνικά αυτό είναι εξαιρετικά εύκολο, ενώ ο πλήρης προληπτικός έλεγχος της εξαγωγής δεδομένων είναι αδύνατος. Δειγματοληπτικός έλεγχος ή κυρώσεις για παράνομη εξαγωγή που αποκαλύπτεται εκ των υστέρων έχουν βέβαια και κάποια προληπτική επίδραση, αλλά πιθανότατα αφορούν μόνο την κορυφή του παγόβουνου.

Η Ευρώπη προηγείται σημαντικά, σε ό,τι αφορά την νομοθεσία προστασίας των προσωπικών δεδομένων, όλων ανεξαιρέτως των τρίτων κρατών, συμπεριλαμβανομένων των κυρίων ανταγωνιστών της στον τομέα των τεχνολογιών πληροφόρησης των ΗΠΑ, της Ιαπωνίας και των κρατών της Άπω Ανατολής. Αν η κατάσταση αυτή παραμείνει τότε θα κινδυνεύουν σοβαρά όχι μόνο η ιδιωτική ζωή

και τα δικαιώματα των Ευρωπαίων πολιτών αλλά και η ανταγωνιστικότητα των Ευρωπαϊκών εταιριών που επεξεργάζονται προσωπικά δεδομένα και που αφ' ενός υποχρεώνονται να λάβουν μέτρα προστασίας που έχουν οικονομικό κόστος και αφ' ετέρου δεν έχουν το δικαίωμα να κάνουν χρήση προσωπικών δεδομένων με την ευχέρεια των ανταγωνιστών τους στις τρίτες χώρες. Ήδη παρατηρούνται θετικές εξελίξεις σε ορισμένες τρίτες χώρες, που είναι αποτέλεσμα και της πρότασης Οδηγίας. Στο QUEBEC το πεδίο εφαρμογής του νόμου διευρύνθηκε και περιλαμβάνει τώρα και τον ιδιωτικό τομέα. Η θέσπιση νομοθεσίας στη Ν.Ζηλανδία επιταχύνθηκε από την πρόταση Οδηγίας .Νομοθεσία πολύ παραπλήσια με την πρόταση Οδηγίας εξετάζεται στο HONG-KONG. Στις ΗΠΑ το ζήτημα της προστασίας της ιδιωτικής ζωής έρχεται σιγά σιγά στο προσκήνιο. Τέλος, για την παρακολούθηση των τρίτων χωρών στο ζήτημα της επεξεργασίας προσωπικών δεδομένων, ιδιαίτερα χρήσιμη είναι η εργασία κάποιων ιδιωτικών φορέων από τους οποίους ο πιο γνωστός ονομάζεται PRIVACY INTERNATIONAL και καλύπτει ευρύτατο αριθμό κρατών.

Απολύτως αποτελεσματική για τον πολίτη είναι η προστασία όταν τα προσωπικά του δεδομένα δεν γίνονται αντικείμενα επεξεργασίας. Ο πολίτης θα πρέπει να έχει δικαίωμα επιλογής ανάμεσα σε λύσεις που περιλαμβάνουν και σε λύσεις που δεν περιλαμβάνουν επεξεργασία προσωπικών δεδομένων ( π.χ. ανάμεσα σε πληρωμή με πιστωτική κάρτα και τοις μετρητοίς). Από τη σκοπιά των χρηστών θα πρέπει να αποφεύγεται η επεξεργασία προσωπικών δεδομένων χωρίς σοβαρό λόγο για την επεξεργασία προσωπικών δεδομένων (και φυσικά να ακολουθούνται οι επιταγές του νόμου, εφόσον γίνεται τέτοια επεξεργασία). Οι δυνατότητες των νέων τεχνολογιών δεν αποτελούν επαρκή λόγο για την επεξεργασία προσωπικών δεδομένων, αλλά εργαλείο που θα πρέπει να χρησιμοποιείται όταν τέτοια επεξεργασία είναι απαραίτητη.

Στις περισσότερες χώρες του κόσμου και δυστυχώς στη χώρα μας, η προστασία των προσωπικών δεδομένων δεν έχει βρεθεί μέχρι τώρα στ' επίκεντρο της επικαιρότητας και του δημοσίου ενδιαφέροντος. Η ευκαιρία δίνεται τώρα, που τα προγράμματα εργασίας της Ευρωπαϊκής Ένωσης, για την Κοινωνία της Πληροφορίας των ΗΠΑ για την Εθνική Υπ. Πληροφοριών, παίρνουν συγκεκριμένη μορφή.

## 3.6 ΕΞΕΛΙΞΗ ΤΟΥ ΘΕΣΜΙΚΟΥ ΕΛΕΓΧΟΥ ΤΗΣ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

Νομοθέτες και επιστημονική κοινότητα συνέκλιναν στην παραδοχή ότι οι ουσιαστικές ρυθμίσεις μπορούν να αποδειχτούν κενές περιεχομένου και στερούμενες ρυθμιστικής ικανότητας, εάν δεν συνοδεύονται από διατάξεις και διαδικασίες που διασφαλίζουν τη διαφάνεια των πληροφοριακών ροών και τη άσκηση ελέγχου.

- **Το δικαίωμα πρόσβασης του πολίτη**. Πολλοί, θεωρούν την άσκηση του ελέγχου δικαίωμα και καθήκον του ατόμου. Όλες οι εθνικές νομοθεσίες κατοχυρώνουν το δικαίωμα πρόσβασης του ιδιώτη, δηλαδή το δικαιωμά του να μαθαίνει ποιες προσωπικές του πληροφορίες αποτελούν αντικείμενο συλλογής, επεξεργασίας και μετάδοσης σε τρίτους. Ο ιδιώτης μπορεί μάλιστα να επέμβει στη διαμόρφωση των πληροφοριών αυτών στο βαθμό που δικαιούται να ζητήσει τη διόρθωση, συμπλήρωση, τροποποίηση, διευκρίνιση ή διαγραφή των ανακριβών, ασαφών ή αναληθών πληροφοριών που αφορούν το πρόσωπό του.

Παρά τη σημασία του δικαιώματος αυτού δε μπορεί ωστόσο να μη σημειωθεί ότι ασκήθηκε ή ασκείται σπανιότατα, μην αγγίζοντας καν το ποσοστό του 10% σε σχέση με το σύνολο των ατόμων, πληροφορίες των οποίων είναι καταχωρημένες σε ιδιωτικά και δημόσια αρχεία. Αυτό είναι κατά κάποιο τρόπο φυσιολογικό, αν λάβουμε υπόψη ότι στις κοινωνίες της πληροφορίας όπου η συλλογή, παροχή κι εν γένει κυκλοφορία πληροφοριών έχει καταστεί φαινόμενο καθημερινό, θα ήταν παράδοξο να περιμένει κανείς από το μέσο πολίτη να απευθύνεται συχνά σε δημόσιες αρχές και ιδιώτες για να ενημερωθεί για την πορεία των πληροφοριών του. Η στάση αυτή εξηγείται, αν αναλογιστεί κανείς ότι τα πλέον ενδιαφέροντα για τον πολίτη αρχεία όπως π.χ. τα αρχεία της αστυνομίας είναι απροσπέλαστα γι' αυτόν. Οι σχετικές νομοθεσίες συνήθως προβλέπουν εξαιρέσεις από το δικαίωμα πρόσβασης, όταν πιθανολογείται ότι η άσκησή του μπορεί να θέσει σε κίνδυνο το δημόσιο συμφέρον, τη δημόσια τάξη, την εθνική ασφάλεια και άμυνα, τη δημόσια υγεία κ.α.

Εξάλλου είναι αμφίβολο αν ο μεμονωμένος πολίτης είναι σε θέση να ελέγξει την πληροφοριακή συμπεριφορά της διοίκησης ή μιας ιδιωτικής επιχείρησης. Υπό τις συνθήκες της ηλεκτρονικής επεξεργασίας προσωπικών δεδομένων η διάσταση μεταξύ των γνώσεων του πολίτη κι αυτών του τεχνικού είναι προφανώς μεγάλη. Ο ιδιώτης παραμένει ένας outsider, από τον οποίο λείπουν οι απαραίτητες πληροφορίες

που θα του επέτρεπαν να αναλύσει τις δραστηριότητες του δημοσίου και του ιδιωτικού τομέα σε σχέση με την επεξεργασία προσωπικών πληροφοριών. Επιπλέον, μη γνωρίζοντας την πολύπλοκη δομή της δημόσιας διοίκησης είναι δύσκολο γι' αυτόν να κατανοήσει τις λεπτομέρειες της ηλεκτρονικής επεξεργασίας των προσωπικών του πληροφοριών αλλά και το σύνολο των συνεπειών αυτής.

- **Η ανάγκη ύπαρξης ενός ειδικού και ανεξάρτητου ελεγκτικού μηχανισμού.**

Το βασικό μειονέκτημα του ατομικού ελέγχου εντοπίζεται στο γεγονός ότι αφορά μια ατομική περίπτωση. Μόνο μια συνολική θεώρηση κι επιθεώρηση της διαδικασίας επεξεργασίας των προσωπικών πληροφοριών αλλά και της οργάνωσης της διοικητικής αρχής ή επιχείρησης, που προβαίνει σε αυτή, επιτρέπει τη συναγωγή σχετικά ασφαλών συμπερασμάτων αναφορικά με τη νομιμότητα της όλης διαδικασίας. Το δικαίωμα πρόσβασης, έστω και σε κατάσταση αδράνειας, αναπτύσσει βέβαια μια προληπτική ενέργεια, η αποτελεσματική εφαρμογή της νομοθεσίας όμως προϋποθέτει τη θέσπιση του θεσμικού ελέγχου της προστασίας προσωπικών πληροφοριών.

Ο νομοθέτης άλλων χωρών δεν εμπιστεύτηκε την αποστολή αυτή σε κανένα από τους παραδοσιακούς μηχανισμούς ελέγχου. Το αντικείμενο ήταν νέο, συνεχώς εξελισσόμενο και με πολλές ιδιαιτερότητες. Το ελεγκτικό όργανο έπρεπε να κατέχει ένα ευρύ πεδίο ειδικών γνώσεων για να διεξάγει αποτελεσματικά τον έλεγχο των συστημάτων πληροφορικής. Οι υφιστάμενες διοικητικές υπηρεσίες, τα δικαστήρια και το κοινοβούλιο εξαιτίας του όγκου και της φύσης των υπολοίπων καθηκόντων τους, θα ήταν αδύνατο να ανταποκριθούν στα καθήκοντα και στον τρόπο εργασίας μιας αρχής ελέγχου της προστασίας προσωπικών πληροφοριών.

Τα νέα προβλήματα επιζητούσαν όχι μόνο νέους ρυθμιστικούς κανόνες αλλά και νέα εργαλεία για την επίλυσή τους. Η ίδρυση των νέων αρχών αποτελούσε μια ένδειξη των ελλειμμάτων του κλασσικού συστήματος δικαιϊκού και πολιτικού ελέγχου και συνιστούσε ταυτόχρονα μια ομολογία της ανεπάρκειας των παραδοσιακών ελεγκτικών μηχανισμών στις βιομηχανικές κοινωνίες με ταχεία ανάπτυξη στις νέες τεχνολογίες. Η ύπαρξη μιας ιδιαίτερης ανεξάρτητης αρχής ελέγχου αντανακλούσε, σε μεγάλη έκταση, τη δυσκολία του Κοινοβουλίου να ασκήσει τις ελεγκτικές του αρμοδιότητες σε έναν τομέα τόσο ζωτικό για τη δομή και την εξέλιξη της κοινωνίας.

## 3.7 ΣΥΜΠΕΡΑΣΜΑΤΙΚΕΣ ΕΠΙΣΗΜΑΝΣΕΙΣ

Πέρα από το

σημεία αυτά θα μπορούσαν να είναι:

- Η έκταση του πεδίου εφαρμογής του σχετικού νόμου, ο οποίος ασφαλώς πρέπει να περιλαμβάνει το σύνολο ανεξαιρέτως των αρχείων του δημόσιου και του ιδιωτικού τομέα, να κατοχυρώνει την προστασία τόσο από την ηλεκτρονική όσο και από την παραδοσιακή επεξεργασία και να προβλέπει όσο το δυνατό λιγότερες και σαφώς ορισμένες εξαιρέσεις.
- Η ανεξαρτησία και η αποτελεσματικότητα του οργάνου που θα αναλάβει τον κεντρικό ρόλο της εποπτείας της εφαρμογής του νόμου. Η ανεξαρτησία προϋποθέτει τη θέσπιση όλων των απαραίτητων προσωπικών και λειτουργικών εγγυήσεων απέναντι κυρίως από την εκτελεστική εξουσία ενώ η αποτελεσματικότητα κρίνεται από την απονομή πραγματικής ισχύος στις αποφάσεις του και τη χορήγηση ικανής τεχνικής υποστήριξης στο έργο του.
- Ο κατά το μέτρο του δυνατού περιορισμός της προσφυγής σε διακρίσεις των πληροφοριών και αναλογικά την αποφυγή ρυθμίσεων που θα στηρίζονται σε τέτοιες διακρίσεις, αλλά αντίθετα την εξεύρεση στενής οργανικής σύνδεσης της φύσης των επεξεργαζομένων πληροφοριών με το σκοπό της επεξεργασίας τους, ως κριτήριο και όριο της νομιμότητάς της.
- Η ουσιαστική διασφάλιση της εγκυρότητας της συναίνεσης του προσώπου για την επεξεργασία πληροφοριών που το αφορούν και η πραγματική κατοχύρωση της ελευθερίας του να χορηγεί ή μη τη συναίνεσή του.
- Τέλος, απαραίτητη φαίνεται η γενίκευση του συστήματος της δήλωσης ίδρυσης αρχείων πληροφοριών και ο περιορισμός του συστήματος της αίτησης στις ελάχιστες και ιδιαίτερα σημαντικές περιπτώσεις, διαφορετικά είναι βέβαιο, ότι με την εισαγωγή των τεχνολογιών της πληροφορίας και επικοινωνίας σε όλους τους τομείς της ανθρώπινης δραστηριότητας και με την ίδρυση εκατομμυρίων αρχείων πληροφοριών, το όποιο όργανο ελέγχου πολύ σύντομα θα βρίσκεται σε αδυναμία να ανταποκριθεί στα καθήκοντά του και να παρακολουθήσει την πραγματικότητα οπότε και ο έλεγχος και η διαφάνεια δεν θα είναι παρά μια μακρινή ουτοπία.

Η διαφύλαξη της ιδιωτικής ζωής είναι η μόνη άμυνα μιας πολιτισμένης κοινωνίας ελεύθερων ανθρώπων να κρατήσει την ταυτότητά της , αφού τελικά ελευθερία δεν είναι παρά αυτό που βιώνουμε καθημερινά, ενώ πολιτισμός ο σεβασμός της.

# 4

# ΘΕΩΡΗΤΙΚΗ ΚΑΙ ΝΟΜΟΛΟΓΙΑΚΗ ΕΠΕΞΕΡΓΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

## ΕΙΣΑΓΩΓΗ

Η τεχνολογία μας θέτει συνεχώς νέα ηθικά και νομικά ζητήματα. Ακόμα κι αν επικρατεί μια γενική κοινωνική άποψη, όσον αφορά ένα συγκεκριμένο ηθικό ζήτημα, η συμμόρφωση προς ένα γενικά αποδεκτό δεδομένο είναι προαιρετική, εκτός και αν ο νόμος το επιβάλλει. Η έλευση της «ηλεκτρονικής εποχής» δεν πέρασε απαρατήρητη από τη νομική επιστήμη, η οποία ήδη από τη δεκαετία του '70 έθεσε τη βάση για την αντιμετώπιση του προβλήματος που ήγειρε η χρήση της πληροφόρησης.

## 4.1 ΘΕΩΡΗΤΙΚΗ ΚΑΙ ΝΟΜΟΛΟΓΙΑΚΗ ΕΠΕΞΕΡΓΑΣΙΑ ΤΟΥ ΔΙΚΑΙΩΜΑΤΟΣ ΑΥΤΟΔΙΑΘΕΣΗΣ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΠΛΗΡΟΦΟΡΙΩΝ.

Τόσο ο εθνικός νομοθέτης όσο και η νομολογία αναζήτησαν κατ' αρχήν στο θεμελιώδη νόμο μια πρώτη ένδειξη για τη στάση που θα ήταν ενδεδειγμένο να

τηρηθεί. Ωστόσο τα περισσότερα εθνικά Συντάγματα, ακόμη και σήμερα, στερούνται μιας ρητής, ειδικής διάταξης - εξαίρεση αποτελούν τα Συντάγματα της Ολλανδίας (αρθ. 10 παρ. 2,3 με ειδικότερη συγκεκριμένη αναφορά στο δικαίωμα γνώσης και επανόρθωσης των δεδομένων), Πορτογαλίας (αρθ. 26 παρ. 2 διάταξη που εντάσσεται στο δικαίωμα προστασίας του απορρήτου της ιδιωτικής ζωής και επιφυλάσσεται υπέρ του νόμου ως προς την πρόβλεψη αποτελεσματικών εγγυήσεων έναντι της καταχρηστικής χρήσης πληροφοριών που αφορούν πρόσωπα), Ισπανίας (αρθ. 18 παρ.4) – που θα καταγραφεί κάποιο νέο δικαίωμα ή τουλάχιστον θα δηλώνει ότι ο συντακτικός νομοθέτης δεν είναι ανυποψίαστος για τους κινδύνους που συνεπάγεται το φαινόμενο στην πλήρη του ανάπτυξή.

Το Ελληνικό Σύνταγμα παραμένει μέχρι σήμερα εξίσου «σιωπηρό» είναι βέβαια αληθές ότι τα ασαφή εννοιολογικά όρια της έννοιας «ιδιωτική ζωή» φαίνονται ικανά να συμπυκνώσουν και να εκφράσουν το πιο ενδόμυχο, απόκρυφο δέος που μπορεί να αισθάνεται ο πολίτης έναντι της ηλεκτρονικής καταγραφής των στοιχείων της προσωπικότητας του που εμφανίζονται ενδιαφέροντα (ή μη) για το κοινωνικό σύνολο.

Άλλωστε η απουσία νομοθετικού ορισμού του δικαιώματος εκδηλώνει ίσως την πρόθεση του νομοθέτη να ικανοποιήσει την ανάγκη κάθε ατόμου να διάγει την ιδιωτική ζωή, που επιθυμεί. Αυτή η ανάγκη είναι τόσο προφανής, που αυτό και μόνο φαίνεται ν' αρκεί για να δικαιολογήσει την απουσία κάθε ορισμού. Η οποιαδήποτε αναζήτηση ενός σκληρού πυρήνα του δικαιώματος αποβαίνει κατ' επέκταση μάταιη, και όχι μόνο για τους προαναφερόμενους λόγους. Μια επιπλέον αδυναμία σχετίζεται με την ίδια τη νομική φύση του δικαιώματος ως μη απολύτου, καθώς το αντικείμενο του, η προστασία της προσωπικότητας, δε νοείται εκτός του κοινωνικού περιβάλλοντος μέσα στο οποίο αυτή αναπτύσσεται. Συνεπώς, η «αντοχή» του όποιου σκληρού πυρήνα της αποβαίνει ιδιαίτερα ευάλωτη σε εξαιρετικές περιστάσεις και προσδίδονται ιδιαίτερα ελαστικά όρια στα άξια έννομης προστασίας συμφέροντα που η ιδιωτική ζωή «στεγάζει». Η θεώρηση αυτή τείνει το περιεχόμενο του δικαιώματος, ως τόπο σύγκρουσης μεταξύ του δικαιώματος του ατόμου στο απόρρητο της ζωής του να διατηρεί απρόσιτα από τη γνώση και τη χρήση των τρίτων ορισμένα στοιχεία του ατομικού βίου, και του δικαιώματος της ολότητας για ενημέρωση πάνω σε κάποιον ουσιώδη λόγο δημοσίου συμφέροντος. Και είναι αλήθεια, αυτός ο κοινός τόπος προβληματισμού της θεωρίας, εδώ και κάποια χρόνια, δεν καταλήγει σε μια

οριοθέτηση του χώρου ιδιωτικής και δημόσιας ζωής ελλείψει αποδεκτών και αδιαμφισβήτητων κριτηρίων.

Οι έσχατοι κίνδυνοι για την προστασία της ιδιωτικής ζωής προσέδωσαν νέα διάσταση στο θεωρητικό διάλογο. Η αντιπαράθεση μέχρι τώρα ως προς τη «γραμμή οριοθέτησης» της σύγκρουσης έλαβε το χαρακτήρα εγγυητικής υποχώρησης του δικαιώματος ιδιωτικού βίου το οποίο αποστερούνταν βαθμιαία ζωτικού χώρου και αμυντικού προσανατολισμού. Η στρατηγική που αναπτύχθηκε ζήτησε πρόσθετη νομική βάση την ελεύθερη ανάπτυξη της προσωπικότητας, ξεκινώντας από τη βάση ότι τα δεδομένα προσωπικού χαρακτήρα εκδηλώνουν –σκιαγραφούν – εξατομικεύουν την ανάπτυξη της προσωπικότητας στη φυσική, πνευματική, ψυχική, κοινωνική, οικονομική, πολιτιστική και ηθική διάσταση της και ότι σε ένα φιλελεύθερο Κράτος Δικαίου η αξιοπρέπεια του ατόμου ταυτίζεται με την ελεύθερη ανάπτυξη της προσωπικότητας και κατ' επέκταση, με το δικαίωμα των ατόμων στον αυτοκαθορισμό τους, στην ελεύθερη «συνδρομή» τους στη διαμόρφωση της εικόνας που το κοινωνικό περιβάλλον σχηματίζει γι' αυτούς.

Με τη σειρά της, η ελεύθερη ανάπτυξη της προσωπικότητας δεν ολοκληρώνεται και δε διασφαλίζεται χωρίς την ύπαρξη μια «σφαίρας» απρόσιτης σε τρίτους, η έλλειψη της οποίας στερεί τη δυνατότητα επιλογής ελεύθερης προσωπικής απόφασης, αλλά και κάθε ανεξάρτητη αντίδραση στην κρατική και ιδιωτική δραστηριότητα. Οι δυνατότητες που παρουσιάζει η σύγχρονη τεχνολογία, εύκολης πρόσβασης στο αρχείο, διασύνδεσης με άλλες βάσεις δεδομένων, μακροχρόνιας αποθήκευσης πληροφοριών, απειλούν να εξουδετερώσουν τον εγγυητικό χαρακτήρα των δικαιωμάτων. Τον κίνδυνο αυτό επισημαίνει ενδεικτικά το ισπανικό Σύνταγμα: αρθ.18, ο νόμος θα περιορίσει τη χρήση της πληροφόρησης, για να εξασφαλίσει την τιμή, το προσωπικό και οικογενειακό απόρρητο των πολιτών και την πλήρη άσκηση των δικαιωμάτων τους. Η σύνδεση αυτή της τιμής και του προσωπικού απορρήτου των πολιτών καθιστά την ιδιωτική ζωή ένα δικαίωμα σταυροδρόμι, στο οποίο συγκλίνουν όλα εκείνα τα έννομα συμφέροντα του πολίτη, που κωδικοποιημένα μέσα από την καταγραφή προσωπικών δεδομένων υπόκεινται στην απειλή καταχρηστικής χρήσης και επεξεργασίας τους.

Ερχόμαστε έτσι στο κυρίαρχο στοιχείο του δικαίου της προστασίας του πολίτη από την ηλεκτρονική επεξεργασία των πληροφοριών, δηλαδή το χαρακτήρα του ως μηχανισμού κατανομής των πληροφοριών. Η θέση αυτή αναδεικνύει

- ✓ την ύπαρξη ενός θεμιτού σκοπού (finalite), ο οποίος θα προβλέπεται από το νόμο και θα προωθεί τη συλλογή πληροφοριών είτε ως αντικείμενο της διοικητικής δράσης είτε ως μέσο κατανομής γνώσεων για την ευδοκίμηση της, ενώ παράλληλα θα εμποδίζει την επέλευση ανεπιθύμητων επεμβάσεων στην ιδιωτική σφαίρα,
- ✓ την κατοχύρωση συγκεκριμένων υποκειμενικών δικαιωμάτων με συγκεκριμένο περιεχόμενο, ώστε να επιτρέψουν στους πολίτες να πληρούν τις ελάχιστες διαδικαστικές προϋποθέσεις για να ασκήσουν το δικαίωμα τους στον αυτοκαθορισμό.

Οι νεώτερες αυτές κατακτήσεις της θεωρίας προϋποθέτουν την αποκατάσταση της «πληροφοριακής ισορροπίας» ως εκδήλωση της αρχής της πρακτικής αρμονίας των δικαιωμάτων μεταξύ καταχωρούμενου ατόμου και του φορέα χρήσεως της τεχνολογίας, η οποία επιτυγχάνεται με την παροχή δικαιώματος πρόσβασης του πρώτου στις πληροφορίες που το αφορούν. Το δικαίωμα αυτό αναλύεται:
α)στο δικαίωμα γνώσης του ενδιαφερόμενου ως προς την ύπαρξη των στοιχείων και β)στο δικαίωμα διαφάνειας των κυκλωμάτων πληροφόρησης.

Πέρα από τη διατύπωση ορισμένων αξιωματικών θέσεων, θεωρία και νομολογία καταπιάστηκαν με το ζήτημα των θεμιτών περιορισμών του δικαιώματος αυτοκαθορισμού προσωπικών δεδομένων – προστασίας της ιδιωτικής ζωής, βρίσκοντας μάλιστα απρόσμενους αρωγούς τη νομολογία των οργάνων της ΕΣΔΑ.

Σημειώνουμε την αναφορά στο ότι, το περιοριστικό μέτρο πρέπει να κρίνεται αναγκαίο σε μια δημοκρατική κοινωνία για την εθνική ή δημόσια ασφάλεια, την προάσπιση της τάξεως καθώς και την πρόληψη ποινικών παραβάσεων. Επίσης κανόνες αναγκαστικού δικαίου θέτουν τα άρθρα 14 (απαγόρευση διακρίσεων) και 18 (οι περιορισμοί πρέπει να υπηρετούν τον σκοπό για τον οποίο καθιερώθηκαν). Η προσβολή του δικαιώματος στην ιδιωτική ζωή (άρθρο 8 ΕΣΔΑ) λόγω της αποκάλυψης, αθέμιτης χρήσης, αλλά και άρνησης πρόσβασης στα δεδομένα που αφορούν τον πολίτη αποτελεί ήδη απόηχο μιας μακράς νομολογίας των οργάνων της ΕΣΔΑ. Χαρακτηριστικές και ιδιαίτερα ενδιαφέρουσες είναι οι σχετικά πρόσφατες αποφάσεις Z.v. Finland, M.v.Sweden, που αφορούν την δημόσια αποκάλυψη ιατρικών δεδομένων.

Παραδείγματος χάρη δεδομένα που διατηρούνταν για λόγους εθνικής ασφάλειας αφορά η υπόθεση:Patrick Martin vs Switzerland. Ο αιτών προέβαλε στην Επιτροπή ότι η άρνηση των αρχών, είτε να του επιτρέψουν να έχει πρόσβαση στο αρχείο του

μετά τη λήξη της μυστικής παρακολούθησης του από την ελβετική αστυνομία είτε να το καταστρέψουν, ερχόταν σε ευθεία αντίθεση με το άρθρο 8 ΕΣΔΑ. Η επιτροπή επανέλαβε την αιτιολογία της Leander v. Sweden η οποία έθεσε και την αρχή, ότι η διατήρηση από το μυστικό αρχείο της αστυνομίας καθώς και η κοινοποίηση από αυτήν δεδομένων προσωπικού χαρακτήρα, όταν συνοδεύεται από την άρνηση προς τον ενδιαφερόμενο να τα αντικρούσει, συνιστά παραβίαση του δικαιώματος στην ιδιωτική ζωή.

Ωστόσο στην εν λόγω περίπτωση η περαιτέρω αρχειοθέτηση των δεδομένων σύμφωνα με την εθνική νομοθεσία τα εξασφάλιζε από οποιαδήποτε πρόσβαση τρίτου. Η προστασία της εθνικής ασφάλειας συγκαταλέγεται μεταξύ των θεμιτών σκοπών περιορισμού, διασφαλίζει με άλλα λόγια την απαραίτητη ισορροπία μεταξύ της εθνικής ασφάλειας και του δικαιώματος του αιτούντος για σεβασμό της ιδιωτικής του ζωής. Όπως και σε προηγούμενες αποφάσεις, η Επιτροπή σημειώνει ότι στο πλαίσιο της εθνικής ασφάλειας αναγνωρίζεται στα κράτη ένα ευρύ περιθώριο εκτίμησης καθώς οι εθνικές αρχές βρίσκονται σε καλύτερη θέση να εκτιμήσουν την αναγκαιότητα λήψης των περιοριστικών μέτρων.

Πιο συγκεκριμένα, ο περιορισμός οφείλει να ανταποκρίνεται σε ένα συμβατό νομικό θεμέλιο. Η αρχή της νομιμότητας αξιώνει, εν προκειμένω την ύπαρξη τυπικού νόμου για τα κύρια στοιχεία της ρύθμισης και τη μεγαλύτερη δυνατή διασφάλιση δημοσιότητας και σαφήνειας .Η νομική βάση περιορισμού οφείλει να διακρίνεται για την καθαρότητα της και να περιλαμβάνει μόνο εκείνη τη χρήση ή επεξεργασία που ανταποκρίνεται στην αναγκαία αξίωση πληροφόρησης των δημοσίων αρχών που είναι απαραίτητη για την αποτελεσματική εκπλήρωση της αποστολής τους. Η καθαρότητα ισοδυναμεί με επαρκή και συγκεκριμένο καθορισμό των στόχων χρήσης καθώς και των αποδεκτών συλλεγόμενων δεδομένων. Η θέση αυτή επιλύει και το πρόβλημα του θεμιτού της διασύνδεσης βάσεων δεδομένων μεταξύ τους, αν και η λειτουργία αυτή θα αντιστρατευόταν την αρχή της ειδικότητας, διότι κατά τον τρόπο αυτό δε θα ήταν αδιανόητη η παρέκκλιση από τον ειδικό τρόπο χρήσεως και η καταχρηστική επεξεργασία τους για σκοπούς άλλους από τους αρχικά προβλεπόμενους. Συνεπώς, η αρχή της «πληροφοριακής διάκρισης των εξουσιών». Η οργανική και λειτουργική διάκριση της Διοίκησης διαγράφει τα πλαίσια δράσης της, άρα θεμιτής συλλογής και χρήσης των δεδομένων για τη συγκεκριμένη και απολύτως αναγκαία εξυπηρέτηση ειδικών σκοπών. Η αρχή της αναγκαιότητας εμποδίζει κάθε

άλλη επέμβαση που εξυπηρετεί άλλους σκοπούς και άλλες ανάγκες, εφ' όσον αυτή δεν προβλέπεται νομοθετικά.

Τελευταίο σε αναφορά, αλλά όχι και σε σημασία, στοιχείο αποτελεί η αρχή της αναλογικότητας κατά την οποία, δεν είναι θεμιτή κάθε συλλογή, χρήση, αποθήκευση, επεξεργασία, όταν αυτή οδηγεί σε υπέρμετρα, δυσανάλογο περιορισμό ή διακινδύνευση του δικαιώματος της ιδιωτικότητας ενόψει του δηλούμενου σκοπού. Είναι εντούτοις αναμφισβήτητο ότι η εκτίμηση του βαθμού διακινδύνευσης των ατομικών ελευθεριών δε μπορεί να εγγραφεί εκ των προτέρων σε ένα γενικό ή ειδικό νόμο προστασίας ή σε οποιοδήποτε δεοντολογικό κώδικα συμπεριφοράς. Η τελική στάθμιση των συμφερόντων προϋποθέτει αξιολόγηση του συνολικού περιβάλλοντος και η χρήση των συλλεγόμενων δεδομένων, εμπίπτει στην εφαρμογή των θεσπισμένων γενικών αρχών ως περιπτωσιολογικός έλεγχος δράσης, μέρος του οποίου έχει εναποτεθεί στις Αρχές Ελέγχου, όργανα σχεδόν πάντοτε εκτεθειμένα εκτός των διοικητικών δομών. Απαραίτητο εχέγγυο νομιμοποίησης του έργου τους κρίνεται ότι είναι η ικανότητα τους να αποτελούν όργανα διαλόγου και σύνθεσης των διαπλεκόμενων κατ' ουσίαν συμφερόντων.

Η φύση του ελέγχου δεν οργανώνεται, ούτε άλλωστε θα είχε και νόημα να οργανωθεί, ως κατασταλτική μόνον. Οι Αρχές ελέγχου καλούνται να εξειδικεύσουν τις δυνατότητες παρέμβασης τους σε ρυθμιστικές, γνωμοδοτικές, ελεγκτικές, διαμεσολαβητικές αρμοδιότητες.

## 4.2 ΔΙΕΘΝΕΙΣ ΟΨΕΙΣ ΤΗΣ ΠΡΟΒΛΗΜΑΤΙΚΗΣ

Η βασική φιλοσοφία που επεκτάθηκε, για τη ρύθμιση των συγκρούσεων που ανακύπτουν με αφορμή τη χρήση της πληροφορικής στο δημόσιο τομέα και τους κινδύνους που αυτή συνεπάγεται για την ελεύθερη ανάπτυξη της προσωπικότητας και την άσκηση των ελευθεριών του πολίτη τεκμηριώνεται με την αναφορά σε διεθνή κείμενα προστασίας των διακυβευόμενων αγαθών. Ορισμένα από αυτά καθώς κωδικοποιούν το σκληρό πυρήνα των αρχών προστασίας και των δικαιωμάτων του ατόμου, αποτελούν σύμφωνα με τη Σύμβαση εφαρμογής Schengen το ελάχιστο κανονιστικό περιεχόμενο ενός εθνικού νομοθετήματος προστασίας των προσωπικών πληροφοριών .

Τα διεθνή αυτά κείμενα, ανεξάρτητα από την ονομασία τους τη νομική τους φύση και το γεωγραφικό εύρος τους εμφανίζουν ως κοινό χαρακτηριστικό, την προσπάθεια εναρμόνισης των γενικών αρχών προστασίας και αντιμετώπισης του προβλήματος της διασυνοριακής ροής δεδομένων. Στο ζήτημα αυτό οι δυσκολίες ήταν αξεπέραστες. Οι χώρες του Τρίτου Κόσμου ελάχιστα αγωνιούσες για την εξέλιξη του προβλήματος καθώς και ισχυρότατα συμφέροντα, πολυεθνικής εμβέλειας, πίσω από την αρχή του οικονομικού φιλελευθερισμού κατέστησαν την διαπραγμάτευση εξαιρετικά ενδιαφέρουσα. Θα προηγηθεί η αναφορά στις «*κατευθυντήριες αρχές*» του Οργανισμού Ηνωμένων Εθνών, (με κριτήριο το βαθμό της οικουμενικότητας τους), στις «*κατευθυντήριες γραμμές*» του ΟΟΣΑ, για να καταλήξουμε στα επίμαχα και νομικά κρίσιμα ζητήματα που θίγουν η Ευρωπαϊκή Σύμβαση 108/1981 του Συμβουλίου της Ευρώπης σε συνδυασμό με την ειδική θεματική σύσταση R 87(15). Επίσης θα συζητηθεί η δυνατότητα άμεσης εφαρμογής, της πρόσφατης οδηγίας 95/46/ΕΚ ως οργανικού μέρους της προστασίας των δεδομένων κατά τη χρήση τους για τους σκοπούς της Σύμβασης Schengen.

## 4.2.1 «ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΑΡΧΕΣ» ΤΟΥ ΟΡΓΑΝΙΣΜΟΥ ΗΝΩΜΕΝΩΝ ΕΘΝΩΝ

Την 14η Δεκεμβρίου 1990 η Γενική Συνέλευση των Ηνωμένων Εθνών ενέκρινε το σχέδιο απόφασης της Επιτροπής των δικαιωμάτων του ανθρώπου, με τίτλο «*Κατευθυντήριες αρχές προστασίας προσωπικών δεδομένων σε αυτοματοποιημένα αρχεία*». Το κείμενο προτρέπει τα κράτη - μέλη να υιοθετήσουν μια νομοθεσία που θα ενσωματώνει τις ελάχιστες αρχές προστασίας των προσωπικών δεδομένων. Το πεδίο εφαρμογής τους καλύπτει τα αυτοματοποιημένα και χειρόγραφα αρχεία δημοσίου και ιδιωτικού τομέα. Τις αρχές που το σχέδιο καθιερώνει τις συναντά κανείς ευρύτατα τόσο στις εργασίες του ΟΟΣΑ όσο και σ' αυτές του Συμβουλίου της Ευρώπης:

- Καταδικάζει τη συλλογή δεδομένων όταν αυτά προέρχονται από μέσα αθέμιτα ή παράνομα (περιορισμοί ως προς τη συλλογή αρ. 1).
- Καταδικάζει την απόκτηση και χρήση δεδομένων αντίθετων προς τους σκοπούς και τις αρχές της Χάρτας των Ηνωμένων Εθνών.
- Υπογραμμίζει την ανάγκη ποιότητας και ακρίβειας των δεδομένων .

- Επιβεβαιώνει την αρχή της ειδικότητας των σκοπών της συλλογής.
- Ως προς την ατομική συμμετοχή του πολίτη καθιερώνει το δικαίωμα πρόσβασής του, ανεξάρτητα από την εθνικότητα ή την κατοικία του και προβλέπει δυνατότητα προσφυγής.
- Απαγορεύει τη συλλογή ευαίσθητων δεδομένων (φυλετική ή εθνική καταγωγή, χρώμα, σεξουαλική ζωή, πολιτικές γνώμες, θρησκευτικές ή φιλοσοφικές πεποιθήσεις, ένταξη σωματειακή ή συνδικαλιστική).
- Ως προς τις εξαιρέσεις, τις αποδέχεται εφ' όσον αυτές είναι αναγκαίες για την προστασία της εθνικής ασφάλειας, δημόσιας τάξης, υγείας , ηθικής, δικαιωμάτων και ελευθεριών. Οι εξαιρέσεις επιτρέπουν τη συλλογή και χρήση ονομαστικών-ευαίσθητων δεδομένων, όταν ο σκοπός της δράσης μπορεί να χαρακτηριστεί ως συμβατός με τα διεθνή κείμενα προστασίας των ανθρωπίνων δικαιωμάτων.
- Το άρθρο 8 προβλέπει κυρώσεις για την παραβίαση των αρχών προστασίας.
- Περιορίζει τη διασυνοριακή ροή δεδομένων, όταν η χώρα που τα εισάγει δεν παρουσιάζει «ουσιαστικά ισοδύναμες εγγυήσεις» με αυτές της χώρας εξαγωγής (άρθρο 9).

### 4.2.2 ΟΙ «ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΓΡΑΜΜΕΣ» ΤΟΥ ΟΟΣΑ

Κοινός τόπος της φιλοσοφίας που διέπει τόσο τις εργασίες του ΟΟΣΑ όσο και του Συμβουλίου της Ευρώπης είναι η πρόσκληση προς τα Κράτη – Μέλη να συμβάλλουν στην κατοχύρωση της εναρμόνισης αρχών προστασίας αν και ο πρώτος οργανισμός δήλωσε κυρίως τις προσπάθειες ανάπτυξης του εμπορίου και οικονομικής συνεργασίας με απώτερο στόχο την ελεύθερη κυκλοφορία της πληροφόρησης. Οι γραμμές του ΟΟΣΑ, αν και δεν είναι νομικά δεσμευτικές, μπορούν ωστόσο να θεωρηθούν ως ένα καλό παράδειγμα δικαίου με την έννοια ότι η ύπαρξή τους αποτελεί ένδειξη μιας ορισμένης διεθνούς συναίνεσης των δυτικών χωρών ως προς τον τρόπο αντιμετώπισης των προβλημάτων που ανακύπτουν από τη χρήση της πληροφορικής, την άσκηση των ελευθεριών και τη διεθνή ανταλλαγή ονομαστικών δεδομένων. Σημείο αναφοράς αποτελεί το άρθρο 18, διάταξη που στη βάση της οριοθετείται μια ορισμένη ισορροπία, ώστε μια εθνική νομοθεσία προστασίας της

ιδιωτικής ζωής να μη θέτει μη αναγκαίους περιορισμούς στη διασυνοριακή κυκλοφορία των δεδομένων, εκτός αν πρόκειται για τις ιδιαίτερες εγγυήσεις προστασίας των ευαίσθητων δεδομένων της χώρας εξαγωγής.

Οι «κατευθυντήριες γραμμές» εφαρμόζονται τόσο στο δημόσιο όσο και στον ιδιωτικό τομέα. Ωστόσο η Σύμβαση ρυθμίζει μόνο τα αυτοματοποιημένα αρχεία, αν και υπάρχει η δυνατότητα, επέκτασης, των ρυθμίσεων της και στα μη αυτοματοποιημένα. Με τον τρόπο αυτό, ανταποκρίνεται καλύτερα στο γεγονός ότι είναι δύσκολο να υπάρξει νομοθετική διάκριση μεταξύ αυτοματοποιημένης και μη επεξεργασίας, καθώς και στο ότι, ο κύριος του αρχείου θα μπορούσε να υπεκφύγει της εφαρμογής των κανόνων προσφεύγοντας σε μη αυτοματοποιημένες μεθόδους επεξεργασίας για αθέμιτους σκοπούς.

Τέλος, η Σύμβαση ορίζει ότι κάθε Κράτος οφείλει να βάλει σε εφαρμογή όλα τα αναγκαία μέτρα υλοποίησης των θεμελιωδών αρχών. Με άλλα λόγια, η Σύμβαση δεν είναι αύτεκτέλεστη, αλλά και δεν αποτελεί απλώς ένα κείμενο προγραμματικού χαρακτήρα. Έξαρχο είναι το στοιχείο της «προτροπής» για ρύθμιση, είτε μέσω της κρατικής και νομοθετικής εξουσίας είτε μέσω αυτορύθμισης.

### 4.2.3 ΕΙΔΙΚΕΣ ΑΡΧΕΣ ΠΡΟΣΤΑΣΙΑΣ – ΕΞΑΙΡΕΣΕΙΣ

Οι αρχές εμπνέονται από την ιδέα, ότι τα προσωπικά δεδομένα πρέπει ν' αποκτώνται με θεμιτά μέσα και δεν πρέπει ν' αποτελούν αντικείμενο επεξεργασίας παρά μόνο για νόμιμους σκοπούς. Τα δεδομένα πρέπει να είναι πρόσφορα, ακριβή, ενημερωμένα, επίκαιρα και δεν μπορούν να διατηρούνται ονομαστικά πέρα από μια αναγκαία διάρκεια για την εκπλήρωση των σκοπών για τους οποίους έχει γίνει η καταγραφή. Πάνω στην ίδια βάση στηρίζεται η λήψη μέτρων ασφάλειας για την προστασία των καταχωρούμενων δεδομένων έναντι τυχαίας καταστροφής ,απώλειας ή αυθαίρετης πρόσβασης, τροποποίησης, διάδοσής τους, καθώς και η αρχή της διαφάνειας που αντιτίθεται στην ίδρυση μυστικών αρχείων. Η Σύμβαση προβλέπει ιδιαίτερες εγγυήσεις για την προστασία μιας σειράς ευαίσθητων δεδομένων, που περιλαμβάνουν τη φυλετική καταγωγή, τις πολιτικές και θρησκευτικές πεποιθήσεις, δεδομένα που σχετίζονται με την υγεία, και τη σεξουαλική ζωή, καθώς αυτά αφορούν την πιο απρόσιτη σφαίρα ιδιωτικής ζωής. Επίσης οι ποινικές καταδίκες, που θίγουν την τιμή και την υπόληψη. Οι εγγυήσεις αυτές τάσσονται ως νόμιμη προϋπόθεση της

αυτοματοποιημένης επεξεργασίας των δεδομένων αυτών. Οι συντάκτες της Σύστασης του ΟΟΣΑ ακολουθούν την άποψη που υποστηρίζεται ευρέως από εγκυρότατους ακαδημαϊκούς κύκλους και από την αμερικανική νομοθεσία για την προστασία της ιδιωτικής ζωής, ότι μόνο το πλαίσιο επεξεργασίας και η χρήση των δεδομένων μπορούν να καταστήσουν ένα δεδομένο «ευαίσθητο» και άρα άξιο προστασίας και όχι η φύση τους αυτή καθ' εαυτή (Principe de finalite).

Πιο αποτελεσματικό μέσο για τη διασφάλιση των αρχών είναι η άσκηση ατομικού ελέγχου. Αυτή συνίσταται σε μια πλειάδα δικαιωμάτων μεταξύ των οποίων το δικαίωμα στην πληροφόρηση του ατόμου ως προς την ύπαρξη του αυτοματοποιημένου αρχείου, τους βασικούς σκοπούς του, καθώς και την ταυτότητα του κυρίου του αρχείου. Το δικαίωμα αυτό μετουσιώνεται στην ύπαρξη δικαιώματος πρόσβασης και γνωστοποίησης των δεδομένων που το αφορούν, εφόσον αυτά υπάρχουν. Τέλος, προβλέπεται δικαίωμα διόρθωσης των εσφαλμένων δεδομένων και εξάλειψης εκείνων που έγιναν αντικείμενο επεξεργασίας κατά παράβαση.

Οι εξαιρέσεις ορίζονται κατά τρόπο περιοριστικό και αποκλειστικό και πρέπει να προβλέπονται από ένα τυπικό νόμο αποκλείοντας κατ' αυτόν τον τρόπο κάθε κανονιστική διάταξη.

Στη θεωρία εκφράστηκε σοβαρός σκεπτικισμός για τον τρόπο διατύπωσης των εξαιρέσεων. Για παράδειγμα ειδική εξαίρεση από τα δικαιώματα που αναγνωρίζει το άρθρο 8 επιτρέπεται, κατόπιν ειδικής νομοθετικής διάταξης, για τα αυτοματοποιημένα αρχεία που χρησιμοποιούνται για στατιστικούς σκοπούς ή για την προαγωγή της επιστημονικής έρευνας, εφόσον η χρήση τους δεν προβάλλει προφανείς κινδύνους για την ιδιωτική ζωή των ενδιαφερομένων προσώπων.

Η Σύμβαση καθιερώνει, τέλος, τη συνεργασία μεταξύ των συμβαλλόμενων κρατών και πρόσβαση στα πρόσωπα που διαμένουν στην αλλοδαπή και θέλουν ν' ασκήσουν στην επικράτεια ενός κράτους τα δικαιώματα που τους αναγνωρίζει το άρθρο 8 έπειτα από κατάθεση αίτησης στην αρμόδια Αρχή του κράτους διαμονής τους. Για τις περιπτώσεις συνεργασίας κρατών απαγορεύεται ρητά η κατάχρηση του σκοπού μετάδοσης των πληροφοριών και προβλέπεται υποχρέωση εχεμύθειας των εμπλεκόμενων προσώπων. Το επόμενο άρθρο ορίζει τις περιπτώσεις, όπου είναι δυνατή η άρνηση διεθνούς συνεργασίας, όταν η αίτηση είναι αβάσιμη, απαράδεκτη ή η ικανοποίησή της είναι ασύμβατη με την ασφάλεια ή τη δημόσια τάξη, καθώς και τις θεμελιώδης ελευθερίες που προστατεύονται στο συμβαλλόμενο αυτό κράτος.

Η Σύμβαση προβλέπει ειδικό όργανο, τη «Συμβουλευτική Επιτροπή», για τη διατύπωση γνώμης ως προς τις αναγκαίες τροποποιήσεις της. Η Ευρωπαϊκή Σύμβαση του 1981 φιλοδοξεί ν' αποτελέσει όργανο ευρύτερης εμβέλειας επιτρέποντας, και σε Κράτη μη Μέλη του Συμβουλίου της Ευρώπης την προσχώρηση σ' αυτήν .

## 4.2.4 Η ΣΥΣΤΑΣΗ R(8715) ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ ΤΗΣ ΕΥΡΩΠΗΣ ΓΙΑ ΤΗ ΡΥΘΜΙΣΗ ΤΗΣ ΧΡΗΣΗΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΣΤΟΝ ΑΣΤΥΝΟΜΙΚΟ ΤΟΜΕΑ

Η Ευρωπαϊκή Σύμβαση του 1981 ρυθμίζοντας με τρόπο ενιαίο τη χρήση των δεδομένων στον δημόσιο και ιδιωτικό τομέα χαρακτήριζε μια προηγούμενη γενιά εθνικών νομοθετημάτων, σύμφωνα με τις οποίες η διάκριση της χρήσης των δεδομένων αποκρυσταλλωνόταν σε τυπικές, γραφειοκρατικές ιδιαιτερότητες νόμιμης συγκρότησης του αρχείου. Η σύγχρονη τάση διακρίνεται, αντίθετα, από ειδικές διατάξεις που αφορούν ειδικούς τομείς δραστηριότητας (νόμοι δεύτερης γενιάς), με σκοπό να προσφέρουν μία συμπληρωματική προστασία Η τάση αυτή ακολουθήθηκε από την επιτροπή εμπειρογνωμόνων για τη προστασία δεδομένων του Συμβουλίου της Ευρώπης. Ο μη δεσμευτικός χαρακτήρας των Συστάσεων δεν εμπόδισε τα κράτη να διατυπώσουν επιφυλάξεις ως προς την ισχύ τους αναγνωρίζοντας τουλάχιστον σ' αυτές μία ιδιάζουσα νομικοπολιτική βαρύτητα.

Η ίδια σκέψη αυτή κυριαρχεί και στην ειδική Σύσταση R (87)15. Η επιτροπή εμπειρογνωμόνων διευκρινίζει ότι οι τιθέμενες αρχές προσφέρουν ελάχιστες εγγυήσεις. Η εξισορρόπηση των διακυβευόμενων συμφερόντων διαρθρώνει τις διατάξεις της Σύστασης: αφ' ενός του ατόμου για την προστασία της ιδιωτικής του ζωής και αφ' ετέρου του κοινωνικού συμφέροντος για την διατήρηση της δημόσιας τάξης. Η σύγκρουση αυτή καθιστά το ζήτημα της στάθμισης εξαιρετικά λεπτό, καθώς η διαφύλαξη των κοινωνικών αγαθών αποτελεί πρωταρχική κρατική λειτουργία.

Σε κάθε Κράτος – Μέλος προβλέπεται σύσταση ανεξάρτητης Αρχής ελέγχου, επιφορτισμένης με την τήρηση των αρχών και την διατύπωση προτάσεων ως προς τη χρήση νέων τεχνικών μέσων επεξεργασίας. Ιδιαίτερης σημασίας είναι η ανάγκη δήλωσης των μόνιμων αυτοματοποιημένων αρχείων στην Αρχή ελέγχου. Η δήλωση αυτή πρέπει να είναι πλήρης, όσον αφορά τη φύση του αρχείου, το υπεύθυνο όργανο της επεξεργασίας, τους σκοπούς του αρχείου, και τους πιθανούς αποδέκτες

κοινοποίησης των δεδομένων. Ως προς τη συλλογή δεδομένων, το στοιχείο που αξίζει προσοχής είναι η εξειδίκευση των σκοπών επεξεργασίας και η ενημέρωση του προσώπου, εν αγνοία του οποίου συλλέχθηκαν προσωπικά του δεδομένα από τη στιγμή που η γνωστοποίησης αυτή δεν απειλεί να βλάψει το αντικείμενο της αστυνομικής δραστηριότητας.

Επίσης το αρ. 2,4 απαγορεύει τη συλλογή δεδομένων για πρόσωπα, με αποκλειστικό αίτιο τη φυλετική τους καταγωγή, τις συγκεκριμένες θρησκευτικές τους πεποιθήσεις, τη σεξουαλική τους συμπεριφορά ή τις πολιτικές τους γνώμες. Εξαιρετικά η συλλογή αυτή μπορεί να πραγματοποιηθεί, αν είναι απολύτως αναγκαία για τις ανάγκες της συγκεκριμένης έρευνας.

Όσον αφορά την καταγραφή των δεδομένων, επαναλαμβάνονται οι αξιώσεις ποιότητας των δεδομένων, της αναγκαιότητας και της ειδικότητας των σκοπών.

Η Αρχή θέτει αυστηρούς όρους (νόμιμο συμφέρον) για την κοινοποίηση ονομαστικών πληροφοριών. Απαγορεύεται κατ' αρχήν η κοινοποίηση εκτός της αστυνομίας σε άλλα δημόσια όργανα και σε ιδιώτες. Η διασυνοριακή μετάδοση πληροφοριών πρέπει να περιορίζεται μεταξύ αστυνομικών αρχών και να βασίζεται σε σαφή νομική διάταξη, από το εσωτερικό ή το διεθνές δίκαιο. Σε κάθε άλλη περίπτωση επιτρέπεται εφόσον είναι απαραίτητη για την πρόληψη ενός σοβαρού κινδύνου ή για την καταστολή σοβαρής ποινικής παράβασης και στο μέτρο που δεν είναι αντίθετη προς τις διατάξεις εσωτερικού δικαίου που προστατεύουν το ενδιαφερόμενο πρόσωπο.

Κάθε πρόσωπο μπορεί κατ' αρχήν ν' ασκήσει τα δικαιώματα πρόσβασης και διόρθωσης των δεδομένων. Τα δικαιώματα αυτά μπορούν ν' αποτελέσουν αντικείμενο περιορισμών στο μέτρο που αυτοί καθίστανται απαραίτητοι για την εκπλήρωση νόμιμου καθήκοντος της αστυνομίας ή για την προστασία του ενδιαφερόμενου προσώπου ή των δικαιωμάτων και ελευθεριών τρίτου. Η άρνηση ή ο περιορισμός των δικαιωμάτων αυτών πρέπει ν' απαντάται αιτιολογημένα, σε γραπτή μορφή. Εντούτοις, ακόμη και η αιτιολογία μπορεί να παραλείπεται, στο μέτρο που αυτό καθίσταται απαραίτητο για την εκπλήρωση νόμιμου καθήκοντος της αστυνομίας ή αναγκαίο για την προστασία των δικαιωμάτων τρίτου.

Το άρθρο 7 αναγνωρίζει την αρχή της περιορισμένης διατήρησης των δεδομένων στο χρόνο και το άρθρο 8 θέτει τους κανόνες των εγγυήσεων ασφάλειας του αρχείου.

Έχουμε λοιπόν καταρχήν το γενικό πλαίσιο της Ευρωπαϊκής Σύμβασης του 1891, το οποίο εξειδικεύεται, συμπληρώνεται ή τροποποιείται κατά περίπτωση από την ειδική Σύσταση. Η συνδυασμένη εφαρμογή των αρχών τους αποτελεί την εφαρμογή Schengen. Η διεθνής αυτή Σύμβαση εμπνέεται από το ίδιο διεθνές περιβάλλον, ανυψώνοντας και τη νομική σημασία της Σύστασης, καθώς η παραπομπή σ' αυτήν λαμβάνει χώρα παγκοσμίως.

Τέλος, Σύσταση αφήνει ανοικτή τη δυνατότητα για τα Κράτη - Μέλη επέκτασης των αρχών της

- στη συλλογή, καταγραφή και χρήση δεδομένων προσωπικού χαρακτήρα για σκοπούς που συνδέονται με την κρατική ασφάλεια,
- στη διατήρηση χειρόγραφων αρχείων ώστε να μην καταστρατηγείται το πλαίσιο προστασίας καθώς και
- στα νομικά πρόσωπα.

## 4.2.5 ΟΔΗΓΙΑ 95/46/ΕΚ: ΚΟΙΝΟΤΙΚΟΠΟΙΗΣΗ ΜΙΑΣ ΠΤΥΧΗΣ ΤΗΣ ΕΣΩΤΕΡΙΚΗΣ ΑΣΦΑΛΕΙΑΣ ΤΗΣ ΕΥΡΩΠΗΣ

Εντοπίζοντας την προβληματική μας στη χρήση προσωπικών δεδομένων για σκοπούς που σχετίζονται με τη δράση της αστυνομίας φάνηκε καθαρά ένα κανονιστικό πλαίσιο σαφές και κοινά αποδεκτό σε ευρωπαϊκή κλίμακα, ικανό να εξασφαλίσει ένα ελάχιστο επίπεδο προστασίας. Η περιπετειώδης έκδοση της οδηγίας 95/46/ΕΚ «τάραξε τα ύδατα»: το κείμενο της δεν έχει ακόμη αποτελέσει αντικείμενο εκτενούς αποτίμησης, ωστόσο η ύπαρξη της αναγκάζει σε επανεξέταση του μέχρι σήμερα, κεκτημένου. Στο σημείο αυτό δε θα προχωρήσουμε σε ανάλυση των διατάξεων της Οδηγίας, πρώτον διότι το ελληνικό νομοσχέδιο σε μεγάλο βαθμό εμπνέεται από το κείμενο της, αναπαράγει τους ορισμούς και τις αρχές της και άρα η αναλυτική παρουσίαση στερείται αναγκαιότητας. Δεύτερον, διότι κατά σαφή διάταξη της οι κανόνες της δεν εφαρμόζονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα όταν αυτή πραγματοποιείται στο πλαίσιο δραστηριοτήτων που δεν εμπίπτουν στο πεδίο εφαρμογής του κοινοτικού δικαίου.

Με μια πρώτη ανάγνωση εξαιρούνται από το πεδίο προστασίας της όλες οι προβλέψεις για την επεξεργασία δεδομένων στα πλαίσια διακυβερνητικής συνεργασίας σε τομείς ποινικού δικαίου. Το εννοιολογικό εύρος των όρων που

χρησιμοποιούνται φαίνεται ν' αφήνει ένα κάποιο νομοθετικό κενό για τη χρήση δεδομένων που αποσκοπεί στη διαφύλαξη της δημόσιας τάξης. Το άρθρο 3 παρ. 2 Οδηγίας εντάσσεται προφανώς στη λογική εναρμόνισης των νομοθεσιών για την προστασία των δεδομένων ως όρου για την πραγμάτωση της ενιαίας εσωτερικής αγοράς. Κατά συνέπεια, η Οδηγία λειτουργεί αυστηρά εντός της κοινοτικής αρμοδιότητας και δεν υπεισέρχεται σε ρύθμιση τομέων που εκφεύγουν της κοινοτικής δράσης. Η οδηγία χρησιμοποιήθηκε από τον έλληνα νομοθέτη ως γενεσιουργός λόγος και βάση της ρυθμιστικής εμβέλειας του διαβήματος του.

## 4.3 ΕΝΙΑΙΟΣ ΕΜΠΟΡΙΚΟΣ ΚΩΔΙΚΑΣ

Οι ιδιωτικές επιχειρήσεις και οι ελεύθερες αγορές αναπτύσσονται όπου υπάρχουν ευρέως αποδεκτά νόμιμα πλαίσια που υποστηρίζουν τις εμπορικές συναλλαγές. Οι ηλεκτρονικές συναλλαγές πρέπει επίσης να υποστηρίζονται σε παγκόσμια κλίμακα.

Είναι αναγκαίο να αναπτυχθούν πρόσθετες πρότυπες διατάξεις και ενιαίες θεμελιώδεις αρχές με σκοπό την εξάλειψη των κανονιστικών φραγμών και τη διευκόλυνση του ηλεκτρονικού εμπορίου με:

- Την ενθάρρυνση της αναγνώρισης εκ μέρους των κυβερνήσεων, την αποδοχή και την διευκόλυνση των ηλεκτρονικών επικοινωνιών.
- Τη διατύπωση σαφών διεθνών κανόνων προκειμένου να υποστηριχθεί η αποδοχή των ηλεκτρονικών υπογραφών και άλλων διαδικασιών επαλήθευσης και,
- Την προώθηση της ανάπτυξης αποτελεσματικών μηχανισμών για την επίλυση διαφωνιών σχετικά με παγκόσμιες εμπορικές συναλλαγές.

Η διεθνής εξάπλωση του ηλεκτρονικού εμπορίου και η διασφάλιση του εξαρτάται επίσης από τις δυνατότητες που έχουν οι συμμετέχοντες να δημιουργήσουν ένα λογικά ασφαλές πλαίσιο όσον αφορά την ευθύνη τους για οποιαδήποτε ζημιά που μπορεί να προκύψει από τις πράξεις τους.

## 4.4 ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΝΕΥΜΑΤΙΚΩΝ ΔΙΚΑΙΩΜΑΤΩΝ

Για την προώθηση του εμπορίου στο internet οι πωλητές πρέπει να γνωρίζουν ότι η πνευματική τους ιδιοκτησία δεν θα κλαπεί και οι αγοραστές πρέπει να γνωρίζουν ότι αποκτούν αυθεντικά προϊόντα.

Κατά συνέπεια είναι αναγκαία η νομοθεσία για την σαφή προστασία των δικαιωμάτων του δημιουργού και των εμπορικών σημάτων ώστε να αποτραπεί η απάτη. Παρ' όλο που η τεχνολογία μπορεί να συμβάλλει στην καταπολέμηση της πειρατείας στο Διαδίκτυο, χρειάζεται και ένα αποτελεσματικό νομικό πλαίσιο για την παροχή αποτελεσματικών νομικών προσφυγών σε περίπτωση τέλεσης των αδικημάτων αυτών. Το θέμα αυτό χρειάζεται να αντιμετωπισθεί από τέσσερις διαφορετικές προοπτικές:

1. Επαρκής νομοθετική κατοχύρωση των δικαιωμάτων πνευματικής ιδιοκτησίας.
2. Καθιέρωση κατάλληλων ρυθμίσεων για την χορήγηση αδειών.
3. Εφαρμογή διαδικασιών διαχείρισης.
4. Χρήση τεχνικών μηχανισμών προστασίας.

## 4.5. ΚΑΤΟΧΥΡΩΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

Η χρήση ισχυρών μηχανισμών κρυπτογράφησης που εξασφαλίζουν την εμπιστευτικότητα ευαίσθητων εμπορικών και προσωπικών στοιχείων αποτελεί έναν από τους θεμελιώδεις λίθους της διασφάλισης προσωπικών δεδομένων. Οι αποκλίνοντες εθνικοί νόμοι που περιορίζουν τη χρήση, εξαγωγή, εισαγωγή και προσφορά τεχνολογιών και προϊόντων κρυπτογράφησης προσθέτουν σοβαρά εμπόδια στην ανάπτυξη του ηλεκτρονικού εμπορίου. Οι κυβερνήσεις πρέπει να αναπτύξουν πολιτικές με στόχο την εξασφάλιση της ελεύθερης κυκλοφορίας τεχνολογιών και προϊόντων κρυπτογράφησης, διασφαλίζοντας ταυτόχρονα τη δημόσια ασφάλεια.

Ειδικότερο ζήτημα είναι εκείνο των ψηφιακών υπογραφών. Οι πρωτοβουλίες στον τομέα αυτό πρέπει να έχουν ως στόχο την εξασφάλιση ενός κοινού νομικού πλαισίου που θα περιλαμβάνει τη νομική αναγνώριση των ψηφιακών υπογραφών

στην ενιαία αγορά και τον καθορισμό των ελάχιστων κριτηρίων για τις αρχές πιστοποίησης.

Βασική είναι η ανάγκη να διασφαλιστεί το δικαίωμα προάσπισης της ιδιωτικότητας του ατόμου, ενώ παράλληλα να αποφεύγονται εμπόδια στη διασυνοριακή παροχή υπηρεσιών ηλεκτρονικού εμπορίου. Παραμένει να εξετασθεί κατά πόσο χρειάζονται πρόσθετα ρυθμιστικά μέτρα, προκειμένου να αντιμετωπισθούν ειδικά ζητήματα που προκύπτουν από τις εξελίξεις του ηλεκτρονικού εμπορίου. Ιδιαίτερα, χρειάζεται να διασφαλιστούν οι αρχές της προστασίας της ιδιωτικότητας στους τομείς των συστημάτων ηλεκτρονικών πληρωμών, της φορολογίας και των συστημάτων διαχείρισης των δικαιωμάτων του δημιουργού.

## 4.6 Η ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ

**Ιδιωτικότητα και προσωπικά δεδομένα:**

Ο όρος ιδιωτικότητα πρέπει να γίνει αντιληπτός ως περιγραφικός όρος αλλά και ως αίτημα και δικαίωμα. Η ιδιωτικότητα δεν πρέπει να συγχέεται ή να ταυτίζεται με τον ιδιωτικό βίο. Η ιδιωτικότητα κατά μετάφραση του privacy, δηλώνει στην προκειμένη περίπτωση το δικαίωμα να προσδιορίζω ποιες πληροφορίες που με αφορούν θα καταστούν γνωστές στο περιβάλλον καθώς και να γνωρίζω ποιοι , από ποιες πηγές και για ποιο σκοπό διαθέτουν πληροφορίες για το άτομο μου. Πρόκειται ειδικότερα για τη λεγόμενη πληροφοριακή ιδιωτικότητα (informational privacy) ή το δικαίωμα πληροφοριακού αυτοκαθορισμού. Τα προσωπικά δεδομένα δεν πρέπει ομοίως να ταυτίζονται ή να συγχέονται με τα απόρρητα δεδομένα. Για τον καθορισμό μιας πληροφορίας ως προσωπική ,καθοριστική είναι η οποιαδήποτε σύνδεση άμεση ή έμμεση, με ένα πρόσωπο. Η ηλεκτρονική διεύθυνση συνιστά αναμφίβολα προσωπικό δεδομένο έστω και έμμεσο, με την έννοια ότι κάθε ηλεκτρονική διεύθυνση συνδέεται πάντα με ένα όνομα ή μια φυσική διεύθυνση. Τα προσωπικά δεδομένα συλλέγονται με cookies που επιτρέπουν την εκπόνηση προφίλ χρηστών ακόμη και εάν δεν είναι δυνατός ο προσδιορισμός της ταυτότητας του χρήστη ως φυσικού προσώπου.

**Ηλεκτρονικό εμπόριο και προσβολή της ιδιωτικότητας:**

Το εμπορικό Διαδίκτυο προσφέρει πολλές δυνατότητες στους εμπόρους όπως μικρό σχετικά κόστος, κατάργηση των αποστάσεων, δυνατότητα προσέγγισης εκατομμυρίων προσώπων και ιδίως δυνατότητα να φέρνει σε επαφή εμπόρους και καταναλωτές σε όλον τον κόσμο με σελίδες ανοιχτές επί 24ωρου βάσεως. Η πληθώρα προσφοράς και ζήτησης θα μπορούσαν να καταστήσουν δυσκολότερη τη σχέση πελατείας στο διαδίκτυο. Αυτό δεν συμβαίνει καθώς η τεχνολογία επιτρέπει πολύ πιο εύκολα από ότι στον πραγματικό κόσμο να προσδιορίζεται η ταυτότητα του αντισυμβαλλόμενου καταναλωτή, να ορίζεται το προφίλ του (ακόμα και εν αγνοία του) και να γίνεται πιστός πελάτης μετά την πρώτη επαφή. Η αμφίδρομη λειτουργία του δικτύου συνιστά μια εξαιρετική βάση για τη συλλογή δεδομένων. Η συλλογή, χρήση και εκμετάλλευση δεδομένων φαίνεται να καθιστά ένα τρόπο χρηματοδότησης υπηρεσιών Διαδικτύου.

**Οι προσωπικές πληροφορίες δεν είναι συναλλακτικό αγαθό:**

Ως στοιχείο της προσωπικότητας κάθε προσώπου η ιδιωτικότητα είναι δικαίωμα και όχι εμπόρευμα. Το γεγονός ότι οι συναλλαγές λαμβάνουν χώρα σε ένα ηλεκτρονικό περιβάλλον δεν συνεπάγεται αναίρεση των θεμελιωδών αξιών και κανόνων, όπου ένα εξωδικτυακό παρελθόν που βασίζεται στην ασφάλεια δικαίου και στην εγγύηση των δικαιωμάτων, έχει κληροδοτήσει στην Κοινωνία της πληροφορίας .

Το Διαδίκτυο και το ηλεκτρονικό εμπόριο δεν είναι ένας αναρχικός χώρος στον οποίο δεν εφαρμόζονται κανόνες και δεν υπάρχει θέση για τα δικαιώματα. Σημείο αφετηρίας είναι ότι οι νομικοί κανόνες που διέπουν τον φυσικό κόσμο πρέπει να είναι εφαρμόσιμοι και στον ηλεκτρονικό τομέα. Το ερώτημα που τίθεται είναι εάν το υφιστάμενο πλαίσιο κανόνων μπορεί να επιλύσει ικανοποιητικά τα ζητήματα προστασίας της ιδιωτικότητας.

**Τα ιδιαίτερα προβλήματα του ενδοδικτυακού χώρου:**

Τα ιδιαίτερα χαρακτηριστικά των τεχνολογιών που υποστηρίζουν το ηλεκτρονικό εμπόριο θέτουν ορισμένα πρόσθετα προβλήματα. Στο ηλεκτρονικό εμπόριο δεν έχουμε την κλασική δομή συναλλαγής με δυο αντισυμβαλλόμενους. Τα συστήματα που συμμετέχουν στη συναλλαγή (ISP, Internet access provider, carrier, search engines, payment gateways) και οι νέες δυνατότητες προκαλούν νέους κινδύνους για την ιδιωτικότητα. Ο πολλαπλασιασμός των ενδιάμεσων στη ροή των δεδομένων που προκύπτει από το ηλεκτρονικό εμπόριο υπογραμμίζει την ανάγκη να

# 5

# ΝΟΜΙΚΑ ΘΕΜΑΤΑ

## ΕΙΣΑΓΩΓΗ

Η δημιουργία ενός «ψηφιακού παγκόσμιου πολιτισμού» που χαρακτηρίζει το νέο αιώνα είχε ως συνέπεια το παγκόσμιο επιχειρηματικό ενδιαφέρον για τη χρησιμοποίηση του διαδικτύου ως ισχυρό μέσο επικοινωνίας και συναλλαγών μεταξύ επιχειρήσεων (business to business) ή από την επιχείρηση προς τον καταναλωτή (business to consumer). Στο κεφάλαιο αυτό γίνεται αναφορά στην προσπάθεια προσαρμογής του νομικού κόσμου στα νέα δεδομένα που δημιουργήθηκαν με την εξάπλωση της ηλεκτρονικής πληροφορίας, προκειμένου να εγκαθιδρυθεί εκείνο το νομικό πλαίσιο που θα διευκολύνει τις ηλεκτρονικές συναλλαγές και θα προστατεύσει το σύγχρονο χρήστη του Internet.

## 5.1 ΤΡΟΠΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΤΟΥ ΦΑΙΝΟΜΕΝΟΥ ΤΗΣ ΠΑΡΑΒΙΑΣΗΣ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ.

Η προστασία ενός Πληροφοριακού Συστήματος μπορεί να επιτευχθεί με δυο βασικές δράσεις:

- Με τη συστηματική παρέμβαση του κοινωνικού συνόλου και την αξίωση θεσμικής εξασφάλισης των δικαιωμάτων των πολιτών, διαμέσου των μηχανισμών της νομοθετικής εξουσίας. Η δράση αυτή μπορεί να προωθηθεί με την ενημέρωση και την ευαισθητοποίηση των πολιτών σε θέματα που αφορούν τις πιθανές αρνητικές επιπτώσεις από την ανάπτυξη της Πληροφορικής. Απαραίτητο συμπλήρωμα είναι η προώθηση της ελεύθερης διακίνησης των πληροφοριών, ώστε να μην τίθενται αδικαιολόγητοι φραγμοί στις θετικές επιπτώσεις αντίστοιχα.

- Με την συγκρότηση πλαισίου γενικών αρχών και την ενεργοποίηση τεχνικών ρυθμίσεων που επιτρέπουν στα Πληροφοριακά Συστήματα να είναι εναρμονισμένα με τις κυρίαρχες απόψεις του κοινωνικού συνόλου. Η δράση αυτή μπορεί να προωθηθεί με την ανάπτυξη τεχνικών και μεθοδολογιών ικανών να εγγυηθούν ότι τα αυτοματοποιημένα Πληροφοριακά Συστήματα εξυπηρετούν στόχους συμβατούς με αυτούς του κοινωνικού συνόλου και καλύπτουν όλες τις τεχνικές προδιαγραφές που αφορούν στην ασφάλειά τους.

Από την περιγραφή των δυο παραπάνω δράσεων προκύπτει ότι η ασφάλεια είναι τεχνικός στόχος για την προστασία κάθε πληροφοριακού συστήματος. Είναι φανερό ότι το απαιτούμενο επίπεδο της ασφάλειας ενός Πληροφοριακού Συστήματος δεν είναι συγκεκριμένο για όλα τα συστήματα, αλλά εξαρτάται κυρίως από τη φύση των διαχειριζόμενων δεδομένων, καθώς και από το συγκεκριμένο χώρο - χρονικό περιβάλλον. Συγκεκριμένα:

Υπάρχουν δεδομένα τα οποία χαρακτηρίζονται ως άξια προστασίας μόνο σε ένα συγκεκριμένο Πληροφοριακό Σύστημα. Τα δεδομένα αυτά αποκαλούνται **ευπαθή δεδομένα**. Υπάρχουν επίσης, δεδομένα τα οποία είναι κοινά αποδεκτό είτε ότι πρέπει

να προστατεύονται είτε ότι δεν πρέπει καν να συλλέγονται, γιατί αντιπροσωπεύουν σημαντικές προσωπικές αξίες ενός εκάστου μέλους του κοινωνικού συνόλου. Η προστασία των δεδομένων αυτών δεν εξαρτάται από το τεχνολογικό περιβάλλον στο οποίο χρησιμοποιούνται. Τα δεδομένα αυτά αποκαλούνται **εγγενώς ευπαθή δεδομένα**. Τέτοιου είδους δεδομένα μπορούν να είναι είτε όσα αφορούν στις φιλοσοφικές ή πολιτικές απόψεις ή στις θρησκευτικές πεποιθήσεις ενός ατόμου (των οποίων η συλλογή και επεξεργασία θεωρείται ότι δεν είναι επιτρεπτή), είτε όσα αφορούν στην κατάσταση της υγείας ενός ατόμου (των οποίων η συλλογή και επεξεργασία είναι αποδεκτή υπό όρους).

Η διασύνδεση κρατικών αρχείων (υπουργεία, εφορίες, τράπεζες, οργανισμοί κοινωνικής ασφάλισης, αστυνομία κ.λ.π.) και η διασταύρωση προσωπικών δεδομένων συντελεί μεν στην πάταξη της γραφειοκρατίας και στον διοικητικό εκσυγχρονισμό, ενέχει όμως παράλληλα το ενδεχόμενο καταχρήσεων σε βάρος του πολίτη. Τέτοιου είδους παραβάσεις έγιναν ήδη και σχεδιάζονται ακόμη περισσότερες και στη χώρα μας, χωρίς δυστυχώς να συναντήσουν ανάλογες αντιδράσεις από οικείους κοινωνικούς φορείς. Χαρακτηριστικά παραδείγματα αποτελούν η αυθαίρετη σύνδεση του ύψους των τηλεφωνικών λογαριασμών ελευθέρων επαγγελματιών με τη φορολογική ικανότητά τους, η διασταύρωση των σχετικών στοιχείων ταυτότητας με τον αριθμό φορολογικού μητρώου από το σύστημα TAXIS κ.λ.π.

Στα πλαίσια αυτά λοιπόν, προβάλλει η ανάγκη θέσπισης ενός αποτελεσματικού συστήματος τεχνικών διασφαλίσεων, (κρυπτογράφηση δεδομένων, κωδικοποίηση, επίπεδα πρόσβασης ανά κατηγορία υπαλλήλου κ.λ.π) και η **θέσπιση καταλλήλων νομικών διατάξεων** για την προστασία των πληροφοριών προσωπικού χαρακτήρα οι οποίες διακινούνται μέσω τηλ/κών δικτύων και υπηρεσιών.

## 5.2 Η ΚΟΙΝΩΝΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

Η έννοια της «Κοινωνίας της Πληροφορίας» είναι δύσκολο να προσδιοριστεί λόγω του ευρύτατου φάσματος που αυτή καλύπτει καθώς και των διαρκών μεταβολών στις οποίες υφίσταται. Προσπάθεια να δοθεί ένας ορισμός έγινε από το Ευρωπαϊκό

Κοινοβούλιο με τις οδηγίες 98/34/ΕΚ, 98/48/ΕΚ και 2000/31/ΕΚ, στις οποίες ως υπηρεσία της Κοινωνίας της Πληροφορίας περιγράφεται «κάθε υπηρεσία που παρέχεται έναντι αμοιβής με ηλεκτρονικά μέσα εξ αποστάσεως και κατόπιν προσωπικής επιλογής ενός αποδέκτη υπηρεσιών» και «ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά» (2000/31/ΕΚ).

Άρα με λίγα λόγια, η Κοινωνία της Πληροφορίας είναι το σύνολο των βιοτικών σχέσεων που γεννιούνται μέσα στη νέα τεχνολογία της πληροφορικής και εξαρτώνται από αυτή.

## 5.3 ΔΙΑΔΙΚΤΥΟ

Νόμος παγκοσμίως εφαρμοστέος που να ρυθμίζει τη νέα κοινωνική πραγματικότητα του διαδικτύου δεν υπάρχει. Εφαρμόζονται όμως διατάξεις που ρυθμίζουν τα υπόλοιπα μέσα επικοινωνίας ή συγκεκριμένες πτυχές του διαδικτύου.

Το δίκτυο εν γένει είναι μια ομάδα υπολογιστών συνδεδεμένων μεταξύ τους και η οποία επιτρέπει σε πολλούς ανθρώπους να επικοινωνούν ο ένας με τον άλλο, να μοιράζονται ταυτόχρονα πληροφορίες και εξοπλισμό.

Το διαδίκτυο ή Internet είναι ένα απεριόριστο δίκτυο διασυνδεδεμένων δικτύων υπολογιστών, στο οποίο έχουν πρόσβαση οι πάντες χωρίς διάκριση. Ονομάζεται και Net (δίκτυο) ή Information Syberhighway (Λεωφόρος των πληροφοριών) ή Cyberspace (Κυβερνοχώρος). Χαρακτηριστικό του είναι ότι εάν κάποιο τμήμα του καταστραφεί, τότε οι πληροφορίες ακολουθούν άλλο δρόμο που παρακάμπτει το κατεστραμμένο τμήμα. Τη διεύθυνση της κυκλοφορίας των πληροφοριών στο διαδίκτυο την επιτελεί ένας ειδικός υπολογιστής, εξυπηρετητής - Router.

Οι εφαρμογές του διαδικτύου είναι το ηλεκτρονικό ταχυδρομείο (e-mail), οι ταχυδρομικοί κατάλογοι (mailing lists), ο παγκόσμιος ιστός (World Wide Web), οι ομάδες συζητήσεων και οι δίαυλοι συνομιλιών (newsgroups - chat rooms), το πρωτόκολλο μεταφοράς αρχείου (File Transfer Protocol), ο τηλεχειρισμός υπολογιστή (Telnet), η τηλεφωνία και τηλεδιάσκεψη, η ραδιοφωνική αναμετάδοση προγραμμάτων.

## 5.4 ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

Ηλεκτρονικό εμπόριο είναι η πραγματοποίηση εμπορικών συναλλαγών βασισμένη σε ηλεκτρονικά μέσα που υποστηρίζουν κείμενο, ήχο και εικόνα. Διακρίνεται σε έμμεσο (offline), κατά το οποίο η παραγγελία υλικών αγαθών διεξάγεται ηλεκτρονικά, αλλά η παράδοση ακολουθεί τους παραδοσιακούς τρόπους (π.χ. ταχυδρομείο) και σε άμεσο (online), που όλα τα στάδια (παραγγελία, πληρωμή και παράδοση άυλων αγαθών και υπηρεσιών π.χ. λογισμικό, οπτικοακουστικό υλικό) ολοκληρώνονται ηλεκτρονικά.

## 5.5 ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ

Η ταχύτητα επέκτασης του διαδικτύου, δραστηριοποίησε διεθνείς οργανισμούς, την Επιτροπή Ευρωπαϊκών Κοινοτήτων και τις κυβερνήσεις διαφόρων χωρών προκειμένου να ορίσουν το νομικό πλαίσιο των ηλεκτρονικών συναλλαγών. Στο διεθνή χώρο η Επιτροπή Διεθνούς Εμπορικού Δικαίου των Ηνωμένων Εθνών (UNCITRAL) συνέταξε το 1996 τον Πρότυπο Νόμο για το ηλεκτρονικό εμπόριο ρυθμίζοντας ζητήματα όπως η εξομοίωση των ηλεκτρονικών πληροφοριών με έγγραφα υλικής υπόστασης, η νομική ισχύς της ηλεκτρονικής υπογραφής, η εγκυρότητα των ηλεκτρονικών κειμένων, ο τόπος, ο χρόνος και η απόδειξη παραλαβής του ηλεκτρονικού μηνύματος. Παρ' όλ'αυτά, ο παραπάνω νόμος θεωρείται αδύναμος και εμφανίζει περιορισμένη εφαρμογή.

Το 1999, το Ευρωπαϊκό Κοινοβούλιο εξέδωσε την υπ'αρ.2000/31/EC Οδηγία η οποία τέθηκε σε ισχύ στις 17.07.2000. Η Οδηγία αυτή καθιέρωσε την αρχή της ελευθερίας σύναψης ηλεκτρονικών συμβάσεων και την αρχή της χώρας προέλευσης, το οποίο σημαίνει ότι το δίκαιο που διέπει τις συναλλαγές με ηλεκτρονικά μέσα είναι το δίκαιο της χώρας εγκατάστασης του φορέα παροχής υπηρεσιών. Η Ελλάδα με την έκδοση του υπ'αρ. 150/2001 π.δ. προσαρμόστηκε με την Οδηγία καθιερώνοντας το Ν.2672/1999 για τις ηλεκτρονικές υπογραφές, το Ν.2251/1994 για την προστασία των

καταναλωτών καθώς και ειδικότερους νόμους, όπως το Ν.2121/1993 για την πνευματική ιδιοκτησία.

### 5.5.1 ΤΟ ΠΕΔΙΟ (ΜΗ) ΕΦΑΡΜΟΓΗΣ ΤΟΥ ΕΛΛΗΝΙΚΟΥ ΝΟΜΟΣΧΕΔΙΟΥ ΣΤΟΝ ΑΣΤΥΝΟΜΙΚΟ ΤΟΜΕΑ (Ιούλιος 1996)

Η ρύθμιση των σχέσεων που απορρέουν από τη χρήση της πληροφορικής στον αστυνομικό τομέα δεν έχει επιτευχθεί επαρκώς. Ενώ οι ισχύουσες διατάξεις για το νομικό καθεστώς των υπηρεσιών ασφαλείας δε διακρίνονται για τη σαφήνεια και την προβλεψιμότητα των συνεπειών τους, η εφαρμογή της διεθνούς αστυνομικής συνεργασίας, αύξησε τα υπάρχοντα θεσμικά ελλείμματα.

Οι ελπίδες εναποτέθηκαν στη θέσπιση ενός νόμου για την προστασία των προσωπικών πληροφοριών, δεδομένου του πολλαπλασιασμού των κινδύνων για την προστασία της ιδιωτικότητας και της ευρείας δυνατότητας πρόσβασης, ανταλλαγής, αποθήκευσης, επεξεργασίας και διασύνδεσης αρχείων που ανέδειξε η χρήση ηλεκτρονικής υποστήριξης. Ο προσδιορισμός του ορίου επεξεργασίας δεδομένων προσωπικού χαρακτήρα προϋποθέτει το συνδυασμό δύο αρχών:

1. (την αρχή) της νομιμότητας, αναγκαία συνέπεια κατά το αρθ. 8 ΕΣΔΑ, με το οποίο επιβάλλεται η ύπαρξη νόμου για την διατήρηση και λειτουργία αρχείου στο δημόσιο τομέα.

2. (την αρχή) της θεμιτής επεξεργασίας.

Η προσφυγή σε ένα γενικό νόμο προστασίας των πληροφοριών δε δικαίωσε απόλυτα τις προσδοκίες κάλυψης ενός κενού μνήμης του δημοκρατικού πολιτεύματος έναντι της ανάπτυξης της ***«ηλεκτρονικής μνήμης»***, εφόσον δε στάθηκε ικανή να καλύψει τους κινδύνους που απορρέουν, όταν ως κύριος του αρχείου νομιμοποιείται η αστυνομική αρχή. Επισήμανε απλώς την ανάγκη ασφαλιστικών ρητρών. Μια γενική επισκόπηση, των ευρωπαϊκών νομοθεσιών επιβεβαίωσε, την ύπαρξη μιας κοινής φιλοσοφίας βασιζόμενη σε 10 αρχές που εξειδικεύουν τη φιλοσοφία αυτή.

Πρόκειται: **α)** για την αρχή της κοινωνικής αποδοχής της συλλογής, **β)** της περιορισμένης συλλογής, **γ)** της ποιότητας των δεδομένων, **δ)** της εξειδίκευσης των

σκοπών συλλογής και επεξεργασίας, ε) της περιορισμένης χρήσης, στ) την αρχή των εγγυήσεων ασφάλειας, ζ) την αρχή της διαφάνειας, η) της περιορισμένης διατήρησης στο χρόνο, θ) την αρχή της υπευθυνότητας, ι) της ατομικής συμμετοχής.

### 5.5.1.1 Η ΚΟΙΝΩΝΙΚΗ ΑΠΟΔΟΧΗ ΤΗΣ ΣΥΛΛΟΓΗΣ

Η εφαρμογή αυτής της αρχής προϋποθέτει την ταξινόμηση της προσωπικής πληροφορίας και την απαγόρευση συλλογής ορισμένων κατηγοριών δεδομένων. Η στάση αυτή μπορεί να θεωρηθεί αυστηρή, καθώς άλλες νομοθεσίες δεν προβαίνουν σε έναν αποκλεισμό «ευαίσθητων» πληροφοριών, αλλά συνδέουν άμεσα τη συλλογή της οποιασδήποτε πληροφορίας με το βαθμό αναγκαιότητας. Παρ' όλο που ο Έλληνας νομοθέτης αναγνωρίζει την ύπαρξη «ευαίσθητων δεδομένων», το σχέδιο νόμου προβλέπει κατ' εξαίρεση τη σύσταση και λειτουργία αρχείων επεξεργασίας ευαίσθητων δεδομένων, όταν η επεξεργασία εκτελείται από δημόσια αρχή στο πλαίσιο της προβλεπόμενης από το νόμο αρμοδιότητάς της και αφορά εξακρίβωση εγκλημάτων, ποινικές παραβάσεις και καταδίκες ή ζητήματα εθνικής ασφάλειας.

Η Σύμβαση Schengen αποκτά λόγο ύπαρξης στο θέμα της διασυνοριακής κυκλοφορίας αλλοεθνών, αποκλείοντας όμως κάθε καταχώρηση που συνδέεται με «ευαίσθητα δεδομένα» όπως αυτά ορίζονται στο άρθρο 6 Ευρωπαϊκής Σύμβασης 108/1981.

### 5.5.1.2 Η ΑΡΧΗ ΤΗΣ ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΣΥΛΛΟΓΗΣ

Η αρχή αυτή προσομοιάζει με την προηγούμενη, καθώς επιβάλλει περιορισμούς στη συλλογή των προσωπικών δεδομένων σε ό,τι είναι απολύτως αναγκαίο. Επιπλέον, επιβάλλει ορισμένους κανόνες ως προς τις μεθόδους συλλογής. Αυτές πρέπει να είναι νόμιμες και θεμιτές, ενώ οι πληροφορίες πρέπει, να συλλέγονται μετά από προηγούμενη ενημέρωση ή συγκατάθεση του ενδιαφερόμενου.

Ο νομοθέτης εξαιρεί από το δικαίωμα γνώσης τα σχετικά στοιχεία, όταν αυτά ορίζονται από ειδικό νόμο, και το υποκείμενο ενημερώνεται μόνο για καταχώρηση την δεδομένων που το αφορούν, καθώς και για την πηγή των σχετικών πληροφοριών.

### 5.5.1.3 Η ΑΡΧΗ ΤΗΣ ΠΟΙΟΤΗΤΑΣ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

Σύμφωνα με την αρχή αυτή τα συλλεγόμενα δεδομένα πρέπει να είναι επίκαιρα, ακριβή και πρόσφορα προς τους σκοπούς, για τους οποίους χρησιμοποιούνται. Παράλληλα η αρχή αυτή σημασιοδοτεί το περιεχόμενο του δικαιώματος πρόσβασης και του ελεγκτικού ρόλου που ανατίθεται στην Αρχή ελέγχου. Η αρχή αυτή διατυπώνεται σαφώς στο 2 παρ. 1γ΄του νομοσχεδίου. Η εξαίρεση του άρθρου 6 παρ. 3, εντούτοις, επιφέρει μια «ρωγμή»: επιτρέπει την καταχώρηση δεδομένων που δεν είναι απολύτως εξακριβωμένα, στις περιπτώσεις που αυτό επιβάλλεται για την εξυπηρέτηση σκοπών, γεγονός που δημιουργεί εύλογα ερωτηματικά για το βαθμό αξιοπιστίας των συλλεγομένων πληροφοριών που κατέχουν οι αστυνομικές αρχές και τους κινδύνους που πιθανό ν' απορρέουν από τη χρήση τους.

### 5.5.1.4 Η ΑΡΧΗ ΤΗΣ ΕΞΕΙΔΙΚΕΥΣΗΣ ΤΩΝ ΣΚΟΠΩΝ

Οι σκοποί που συνάπτονται με τα συλλεγόμενα δεδομένα πρέπει ν' αποτελούν αντικείμενο ειδικού καθορισμού το αργότερο τη στιγμή της συλλογής. Ζήτημα που συναρτάται με το αν οι βάσεις δεδομένων αστυνομικού χαρακτήρα δηλώνονται στην υπεύθυνη Αρχή, εξειδικεύοντας στη δήλωση αυτή, τους σκοπούς επεξεργασίας. Συνήθως το αρχείο ιδρύεται χωρίς άδεια και εκφεύγει του ελέγχου δήλωσης από την Επιτροπή για την προστασία των δεδομένων.

Οι πληροφορίες που δίνονται στο κοινό περιλαμβάνουν, το σκοπό σύστασης του αρχείου, τις καταχωρημένες κατηγορίες πληροφοριών και τους παραλήπτες, τις συνθήκες άσκησης του δικαιώματος πρόσβασης και τροποποίησης. Οι σκοποί επεξεργασίας πρέπει να εξειδικευθούν, ώστε να παράσχουν κριτήρια νομιμότητας της συλλογής των επιμέρους δεδομένων.

Η Σύμβαση Εφαρμογής κηρύσσει αδύνατη την αντιγραφή της καταχώρησης από το εθνικό τμήμα του συστήματος πληροφοριών σε άλλα εθνικά αρχεία δεδομένων. Εξαίρεση από την αρχή της εξειδίκευσης σύμφωνα με τη Σύμβαση γίνεται εφόσον αυτή αιτιολογείται από την ανάγκη προλήψεως επικείμενης σοβαρής απειλής κατά της δημόσιας τάξης και ασφάλειας.

Γενικά, η εφαρμογή των διατάξεων της Σύμβασης δημιουργεί έναν ευρύτατο ορίζοντα «ασφάλειας» που ελαχιστοποιεί τον κίνδυνο νομιμοποίησης της πιθανής διάχυσης των πληροφοριών σε τρίτους. Κρίσιμη ασφαλώς δεν είναι η δημιουργία ενός συγκεκριμένου κανόνα, αλλά η επαλήθευση του στην πράξη: κατά συνέπεια, το μείζον βάρος επωμίζεται η Αρχή ελέγχου.

### 5.5.1.5 Η ΑΡΧΗ ΤΟΥ ΠΕΡΙΟΡΙΣΜΟΥ ΚΑΤΑ ΤΗ ΧΡΗΣΗ

Τα ονομαστικά δεδομένα που συγκεντρώνονται δεν ενδείκνυται να κοινοποιηθούν σε άλλους ούτε να χρησιμοποιηθούν για σκοπούς άλλους από αυτούς που εξειδικεύθηκαν κατά τη συλλογή, εφ' όσον το υποκείμενο δεν συγκατατίθεται ή δεν το επιτρέπει κάποιος κανόνας δικαίου. Η εμπιστευτικότητα της συλλογής επιβάλλει καταρχήν τη μη διάδοση τους, εκτός αν οι σκοποί που θα εξυπηρετούσε η μετάδοση αυτή είναι οι ίδιοι με τους αρχικά καθορισμένους.

Το νομοσχέδιο εισάγει τη δυνατότητα διασύνδεσης βάσεων δεδομένων, η οποία γνωστοποιείται στην Αρχή Ελέγχου με δήλωση των υπεύθυνων επεξεργασίας των αρχείων ώστε να παραχωρηθεί η άδεια της.

Ως προς τη διασυνοριακή ροή δεδομένων η Σύμβαση Εφαρμογής Schengen επιβάλλει κάποιες ιδιαίτερες αξιώσεις: οριοθετεί γεωγραφικά τη διαβίβαση μόνο στις χώρες που είναι συμβαλλόμενα μέλη της και ιδίως αποκλείει κάθε διαβίβαση, όταν αυτή πραγματοποιείται μεταξύ μερών που δεν έχουν θέσει σε εφαρμογή ένα νομοθετικό επίπεδο προστασίας των δεδομένων τουλάχιστον ίσου προς την Σύμβαση του Συμβουλίου της Ευρώπης και τη Σύσταση R(87)15 της Επιτροπής Υπουργών.

### 5.5.1.6 Η ΑΡΧΗ ΤΩΝ ΕΓΓΥΗΣΕΩΝ ΑΣΦΑΛΕΙΑΣ

Η ηλεκτρονική διαχείριση συνεπάγεται κινδύνους απώλειας, καταστροφής, αλλοίωσης των δεδομένων καθώς και κινδύνους μη επιτρεπόμενης πρόσβασης και διάδοσης τους. Η έννοια της «ασφάλειας» περιχαρακώνει την εμπιστευτικότητα και την ακεραιότητα των δεδομένων. Οι μορφές προστασίας, που μπορεί να λαμβάνει, αφορούν ηλεκτρονικά μέτρα (π.χ. κωδικοποίηση).

Η Σύμβαση Εφαρμογής προβλέπει έλεγχο των εγκαταστάσεων, έλεγχο των μέσων αποθήκευσης ,καταχωρήσεως, χρήσεως, προσβάσεως, διαβιβάσεως, εισαγωγής και μεταφοράς των δεδομένων.

### 5.5.1.7 Η ΑΡΧΗ ΤΗΣ ΔΙΑΦΑΝΕΙΑΣ

Το υποκείμενο δύσκολα μπορεί ν' ασκήσει το δικαίωμα στην πρόσβαση και την επανόρθωση των δεδομένων που το αφορούν, για αυτό και απαντάται συχνά η υποχρέωση για το φορέα συλλογής να ενημερώσει το υποκείμενο για την ύπαρξη συγκεκριμένου αρχείου που τον αφορά, καθώς και για τα δικαιώματά του.

Είναι ευνόητη η πρόσκρουση της αρχής αυτής σε εξαιρέσεις, όταν ορισμένα αρχεία, δεν είναι προσιτά στο κοινό. Η γνωστοποίηση προς την Αρχή Ελέγχου, της λειτουργίας αρχείου από τον υπεύθυνο επεξεργασίας θα καταχωρείται, σε Μητρώο αρχείων που διατηρεί η ίδια. Δεν απαιτείται καταχώρηση όταν το αρχείο προβλέπεται από το νόμο ως αντικείμενο της αρμοδιότητας δημόσιας αρχής ή υπηρεσίας.

### 5.5.1.8 Η ΑΡΧΗ ΤΗΣ ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΔΙΑΤΗΡΗΣΗΣ ΣΤΟ ΧΡΟΝΟ

Η αρχή αυτή εμφανίζεται ως συνώνυμη του «δικαιώματος στη λήθη». Η απεριόριστη χρονικά διατήρηση των δεδομένων συνεπάγεται προφανείς κινδύνους όπως να καταστήσει τα δεδομένα ανακριβή. Επιπλέον, τα ανακριβή δεδομένα συνδεόμενα με περιόδους της ζωής του υποκειμένου παρωχημένες, κινδυνεύουν να

οδηγήσουν στη δημιουργία τεράστιων βάσεων δεδομένων, όπου θα βρίσκονται ανάμικτα, χωρίς συστηματική δομή και για ακαθόριστους σκοπούς.

Τα άρθρα 112, 113 της Σύμβασης εφαρμογής, ορίζουν συγκεκριμένες προθεσμίες διατήρησης των δεδομένων. Αν για παράδειγμα καταχωρούνται με τον σκοπό αναζήτησης προσώπων, διατηρούνται μόνο κατά το χρονικό διάστημα που είναι απαραίτητο, με δυνατότητα εξέτασης της ανάγκης φύλαξης τους μετά τρία χρόνια από την ενσωμάτωση τους.

Το νομοσχέδιο γενικά δεν περιέχει ακριβείς χρονικούς προσδιορισμούς. Το κάθε στοιχείο πρέπει να προβλεφθεί από ειδική νομοθετική διάταξη, ειδάλλως θα επαφίεται στην εκτίμηση του υπεύθυνου επεξεργασίας. Η παρατήρηση αυτή αποτελεί επιβεβαίωση της μη προβλεψιμότητας των διατάξεων του νομοσχεδίου.

### 5.5.1.9 Η ΑΡΧΗ ΤΗΣ ΥΠΕΥΘΥΝΟΤΗΤΑΣ

Η επιβολή των υποχρεώσεων στο συλλέγοντα τα δεδομένα και η αναγνώριση δικαιωμάτων στο θιγόμενο πρόσωπο συμπληρώνονται στις ευρωπαϊκές νομοθεσίες με τον προσδιορισμό του «κυρίου του αρχείου», πρόσωπο στο οποίο συγκεντρώνεται η νομική υποχρέωση τήρησης των κανόνων που αφορούν την προστασία της ιδιωτικής ζωής.

Σύμφωνα με τη Σύμβαση είναι μία η οριζόμενη εθνική Αρχή, αυτή που αναλαμβάνει την κεντρική αρμοδιότητα για το εθνικό τμήμα του Συστήματος Πληροφοριών Schengen, διαμέσου της οποίας πραγματοποιούνται οι καταχωρήσεις και η οποία είναι υπεύθυνη.

### 5.5.1.10 Η ΑΡΧΗ ΤΗΣ ΑΤΟΜΙΚΗΣ ΣΥΜΜΕΤΟΧΗΣ

Η Σύμβαση Schengen αναγνωρίζει μία σειρά δικαιωμάτων του ατόμου: δικαίωμα πρόσβασης, διόρθωσης και δικαίωμα δικαστικής αρωγής για την υλοποίηση τους. Ο χαρακτήρας του δικαιώματος «πρόσβασης δεν είναι νομικά ακριβής. Επομένως, η άσκησή του στην πλειονότητα των ευρωπαϊκών νομοθεσιών είναι έμμεση με εξαίρεση

την Αυστρία, όπου ορίζεται ως άμεση, εφόσον έχει προηγηθεί αίτηση ενημέρωσης στον υπεύθυνο για την επεξεργασία δεδομένων.

Συμβαίνει συχνά, η αρμόδια αστυνομική αρχή να αρνηθεί την παροχή πληροφορίας, εάν «η γνώση του περιεχομένου της από τον ενδιαφερόμενο μπορεί να δυσχεράνει την έρευνα, την πρόληψη επικίνδυνων επιθέσεων ή την πρόληψη οργανωμένου εγκλήματος».

Γενικά η ανακοίνωση πληροφοριών προς το ενδιαφερόμενο άτομο απορρίπτεται αν είναι ικανή να βλάψει την εκτέλεση του νομίμου έργου της καταχωρήσεως ή την προστασία των δικαιωμάτων και ελευθεριών τρίτων.

### 5.5.2 Η ΑΡΧΗ ΕΛΕΓΧΟΥ

Εγγυητικός παρανομαστής της αναφοράς στην προστασία δεδομένων είναι η καθιέρωση μιας ανεξάρτητης Αρχής ελέγχου η οποία τάσσεται από τη Σύμβαση ως αναγκαίος όρος νομιμοποίησης του Συστήματος Πληροφοριών, επαφίεται στους ορισμούς του εθνικού νομοθέτη και διέπεται από φάσμα αρμοδιοτήτων.

Η ελληνική πρόβλεψη του σχεδίου νόμου περιέβαλε το θεσμό με όλα τα εχέγγυα διοικητικής αυτονομίας, προσωπικής και λειτουργικής ανεξαρτησίας των μελών του, ενώ έδωσε θεσμική και κοινωνική ευρύτητα στο ρόλο του. Η αναγκαιότητα ύπαρξής του όμως δεν εγγυάται απαραίτητα την αποτελεσματικότητα διαχείρισης και νομιμοποίησης του Συστήματος.

## 5.6 ΗΛΕΚΤΡΟΝΙΚΑ ΕΓΓΡΑΦΑ

### 5.6.1 ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΚΑΙΟΠΡΑΞΙΑ

Η ηλεκτρονική δικαιοπραξία διενεργείται με ηλεκτρονικό έγγραφο μέσω μηχανικών μέσων και υπογράφεται από τον δηλούντα.

### 5.6.2 ΣΥΝΑΨΗ ΣΥΜΒΑΣΕΩΝ ΜΕΣΩ INTERNET

Οι ηλεκτρονικές συμβάσεις πραγματοποιούνται μεταξύ του προμηθευτή των αγαθών ή των υπηρεσιών και του αγοραστή - χρήστη. Για τη σύναψη έγκυρων ηλεκτρονικών συμβάσεων πρέπει να ισχύουν τα εξής στοιχεία: **πρόταση** για σύναψη σύμβασης, **αποδοχή** της και **απόδειξη** λήψεως της αποδοχής. Προηγείται όμως η **ηλεκτρονική δήλωση βούλησης**, δηλαδή η εξωτερίκευση της πραγματικής θέλησης του υποκειμένου.

Προϋποθέσεις της έγκυρης ηλεκτρονικής δήλωσης βουλήσεως είναι: α) η πράξη βούλησης του δηλούντος, β) η συνείδηση των συνεπειών της δήλωσης και γ) η δικαιοπρακτική βούληση (δηλαδή η αποδοχή των έννομων συνεπειών της). Όπου ο νόμος το απαιτεί, χρησιμοποιείται η «ηλεκτρονική υπογραφή» σε αντικατάσταση της ιδιόχειρης.

Στις εμπορικές συναλλαγές ο παραλήπτης της ηλεκτρονικής δήλωσης βουλήσεως πρέπει να δημοσιοποιήσει την ηλεκτρονική του διεύθυνση και μέσω αυτής να συναλλάσσεται. Ειδική ρύθμιση χρειάστηκε στις διασυνοριακές συναλλαγές μέσω διαδικτύου σχετικά με το ποια εθνική νομοθεσία θα εφαρμοστεί. Τα κράτη - μέλη της ΕΕ εφαρμόζουν την υπ'αρ.2000/31/EC Οδηγία, η οποία βασίζεται στην αρχή της χώρας προέλευσης με αποτέλεσμα η σύμβαση, να διέπεται από το δίκαιο της χώρας όπου είναι "εγκατεστημένος" ο φορέας παροχής της υπηρεσίας.

## 5.7 ΗΛΕΚΤΡΟΝΙΚΕΣ ΠΛΗΡΩΜΕΣ

### 5.7.1 ΜΕ ΠΙΣΤΩΤΙΚΗ ΚΑΡΤΑ

Η χρησιμοποίηση πιστωτικής κάρτας στο διαδίκτυο ελλοχεύει πολλούς κινδύνους για τον κάτοχο αυτής, όπως ο κίνδυνος υποκλοπής των δεδομένων ή του αριθμού της κάρτας, ή ανάληψη από τον προμηθευτή ποσού μεγαλύτερου από το συμφωνηθέν. Στην προσπάθειά τους τα πιστωτικά ιδρύματα (π.χ. τράπεζες) για να προλάβουν τη μη

εξουσιοδοτημένη χρήση της πιστωτικής κάρτας χρησιμοποιούν την κρυπτογραφική μέθοδο

Η τράπεζα πληρώνει μόνο όταν έχει μια έγκυρη εντολή από τον κάτοχο της κάρτας. Επομένως, η ευθύνη μετατίθεται στην τράπεζα χωρίς να αξιώνει τα χρήματα από τον κάτοχο. Η υποχρέωση του κατόχου είναι να ειδοποιήσει την τράπεζα για την απώλεια ή υποκλοπή της κάρτας του μέσα σε ορισμένο χρονικό διάστημα. Σε περίπτωση που διαπιστωθεί δόλος από τον κάτοχο, η τράπεζα δικαιούται να ζητήσει αποζημίωση αν και συνήθως τέτοιου είδους περιστατικά οφείλονται σε αμέλεια. Ο έμπορος που συναλλάσσεται χωρίς τη χρησιμοποίηση συστημάτων ασφαλείας, φέρει την ευθύνη για την υποκλοπή των δεδομένων της κάρτας και επομένως η τράπεζα δεν εγγυάται την πληρωμή του.

### 5.7.2 ΜΕ ΗΛΕΚΤΡΟΝΙΚΑ ΜΕΣΑ Η ΗΛΕΚΤΡΟΝΙΚΟ ΔΙΑΜΕΣΟΛΑΒΗΤΗ

Η πληρωμή με ηλεκτρονικά μέσα γίνεται με τη διαμεσολάβηση κάποιας επιχείρησης μεταξύ αγοραστή και πωλητή. Ενημερώνεται για τα προσωπικά στοιχεία και των δύο πλευρών, τους χορηγεί από ένα μυστικό κωδικό αριθμό με τον οποίο γίνονται αναγνωρίσιμοι στις ηλεκτρονικές τους συναλλαγές και συνάπτει τη μεταξύ τους σύμβαση. Ο πωλητής αποστέλλει το λογαριασμό του πελάτη για πληρωμή στο διαμεσολαβητή, αυτός με τη σειρά του χρεώνει το λογαριασμό της κάρτας του αγοραστή και όταν το ποσό είναι διαθέσιμο, αφαιρεί το ύψος της προμήθειάς του για τη διαμεσολάβηση και το υπόλοιπο το αποδίδει στο δικαιούχο (πωλητή).

### 5.7.3 ΜΕ «ΗΛΕΚΤΡΟΝΙΚΟ ΧΡΗΜΑ» (e-money)

Το «ηλεκτρονικό χρήμα» βασίζεται στην ανταλλαγή πραγματικού χρήματος με εικονικά «κυβερνονομίσματα» (cybermoney) των οποίων η ύπαρξη πιστοποιείται από σχετικό λογισμικό που ενημερώνει τον πωλητή για το χρηματικό υπόλοιπο του πελάτη.

## 5.8 ΠΡΟΣΤΑΣΙΑ ΣΥΜΒΑΛΛΟΜΕΝΟΥ ΚΑΤΑΝΑΛΩΤΗ

Στο χώρο του ηλεκτρονικού εμπορίου ως καταναλωτής νοείται ο χρήστης και επομένως προστατεύεται αυτόματα από το δίκαιο των καταναλωτών και ιδιαίτερα από το Ν.2254/1994. Οι όροι των συναλλαγών είναι προκαθορισμένοι, αφορούν το σύνολο, δε διαπραγματεύονται ατομικά και ο καταναλωτής, τους αποδέχεται με την υπογραφή του. Στις ηλεκτρονικές συμβάσεις, οι όροι είναι δεσμευτικοί για τους καταναλωτές, κατά συνέπεια πριν βάλουν την υπογραφή τους, θα πρέπει να έχουν ενημερωθεί από τον πωλητή για την ύπαρξή τους και να τους διαβάσουν προσεκτικά, ώστε να διαπιστωθούν έγκαιρα καταχρηστικοί όροι (π.χ. όροι που περιορίζουν την ευθύνη του προμηθευτή για καλυμμένα ελαττώματα του προϊόντος).

Αν παρ'όλ'αυτά διαπιστωθούν καθυστερημένα καταχρηστικοί όροι επέρχεται η ακυρότητα της σύμβασης. Ο Ν. 2254/1994 παρέχει στον καταναλωτή το *δικαίωμα πληροφόρησης* πριν την υπογραφή της σύμβασης καθώς και το *δικαίωμα υπαναχώρησής* του από τη σύμβαση μέσα σε ορισμένη προθεσμία χωρίς περαιτέρω έξοδα, ενώ για τον προμηθευτή απαγορεύει αντίστοιχη ακύρωση από τη μεριά του

## 5.9 ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Τα φυσικά ή νομικά πρόσωπα προστατεύονται από την επεξεργασία δεδομένων προσωπικού χαρακτήρα με βάση την υπ'αρ.95/46/ΕΚ και το Ν.2472/1997, ενώ αρμόδιοι για την επίλυση σχετικών ζητημάτων που προκύπτουν στη χώρα μας είναι η Αρχή της Προστασίας Προσωπικών Δεδομένων καθώς και οργανισμοί όπως ο παγκόσμιος Οργανισμός για την Οικονομική Συνεργασία και Ανάπτυξη (ΟΟΣΑ). Για να καταστεί αυτό δυνατό, η Αρχή τηρεί «μητρώο αποχής», στο οποίο εγγράφονται όσοι επιθυμούν τα δεδομένα τους να μη γίνουν αντικείμενο επεξεργασίας και να μην τους αποστέλλονται διαφημιστικά μηνύματα.

## 5.10 ΔΙΑΦΗΜΙΣΗ ΣΤΟ INTERNET

Η διαφήμιση στο Internet γίνεται είτε μέσω μίας ιστοσελίδας (www.) είτε μέσω του ηλεκτρονικού ταχυδρομείου (e-mail) ενώ πολλές φορές δημιουργεί προβλήματα τριών (3) κυρίως μορφών.

### 5.10.1 ΑΝΕΠΙΘΥΜΗΤΗ ΑΠΟΣΤΟΛΗ ΗΛΕΚΤΡΟΝΙΚΩΝ ΔΙΑΦΗΜΙΣΤΙΚΩΝ ΜΗΝΥΜΑΤΩΝ (junk mail spamm).

Αντιμετωπίζεται από το ελληνικό δίκαιο με την απαγορευτική διάταξη του αρ. 9 του Ν.2251/1994 και από την Οδηγία της ΕΕ με την πρόβλεψη των λεγόμενων «μητρώων αποχής», τα οποία υποχρεούται να σέβονται οι αποστολείς των διαφημίσεων και να μην αποστέλλουν διαφημιστικά μηνύματα σε όσους έχουν εγγραφεί στη συγκεκριμένη λίστα.

### 5.10.2 ΤΟ ΔΥΣΔΙΑΚΡΙΤΟ ΤΟΥ ΔΙΑΦΗΜΙΣΤΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΤΟΥ ΜΗΝΥΜΑΤΟΣ.

Συχνά αποστέλλονται διαφημιστικά μηνύματα με τη μορφή δημοσιογραφικής ή επιστημονικής έρευνας χωρίς να είναι ευδιάκριτος ο διαφημιστικός τους χαρακτήρας. Από αυτή την ενέργεια ο χρήστης προστατεύεται μέσω της αρχής του ευδιάκριτου διαχωρισμού μεταξύ διαφημιστικού μηνύματος και επιστημονικού κειμένου, η οποία απαγορεύει την αποστολή ανάλογων μηνυμάτων.

### 5.10.3 ΠΑΡΑΠΛΑΝΗΤΙΚΗ, ΑΘΕΜΙΤΗ ΚΑΙ ΣΥΓΚΡΙΤΙΚΗ ΔΙΑΦΗΜΙΣΗ.

Παραπλανητική θεωρείται η διαφήμιση που δημιουργεί πλάνη στους καταναλωτές (π.χ. τιμές ή προσφορές που δεν ισχύουν). Αθέμιτη είναι η διαφήμιση που προσβάλλει τα χρηστά ήθη (π.χ. όταν εξωθεί σε εγκληματικές πράξεις).

Συγκριτική είναι η διαφήμιση κατά την οποία συγκρίνονται ανοιχτά η ποιότητα και οι τιμές παρεμφερών προϊόντων άλλων προμηθευτών. Και οι τρεις κατηγορίες απαγορεύονται με εξαίρεση την τελευταία που επιτρέπεται μόνο στην Ελλάδα αλλά με προϋποθέσεις.

## 5.11 ΠΝΕΥΜΑΤΙΚΗ ΙΔΙΟΚΤΗΣΙΑ

Η προστασία της πνευματικής ιδιοκτησίας στο διαδίκτυο περιφρουρήθηκε νομικά σε διεθνές επίπεδο από: τη Διεθνή Σύμβαση της Βέρνης (1886, κυρώθηκε από την Ελλάδα το 1975), τη Διεθνή Σύμβαση της Ρώμης (1961, κυρώθηκε από την Ελλάδα το 1992), τη Συμφωνία TRIPS (κυρώθηκε από την Ελλάδα με το ν.2290/1995) και τη Συνθήκη WIPO (1996). Στην Ελλάδα η προστασία της πνευματικής ιδιοκτησίας ρυθμίζεται από το Ν. 2121/1993 για την πνευματική ιδιοκτησία και τα συγγενικά δικαιώματα.

Αντικείμενο προστασίας, με βάση τις εν λόγω διατάξεις, αποτελεί το έργο ως άυλο αγαθό. Ως έργο νοείται κάθε «πρωτότυπο πνευματικό δημιούργημα λόγου, τέχνης ή επιστήμης» που εκφράζεται με οποιαδήποτε μορφή, ανεξαρτήτως αξίας. Άρα προστασία παρέχεται στα προγράμματα ηλεκτρονικών υπολογιστών, στα κείμενα που διαδίδονται μέσω Internet, στο λογισμικό εφόσον βέβαια αυτό είναι πρωτότυπο και στις βάσεις δεδομένων.

## 5.12 ΦΟΡΟΛΟΓΙΚΟ ΔΙΚΑΙΟ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

Μια από τις αλλαγές που έφερε η κοινωνία των πληροφοριών είναι το ενδιαφέρον των κυβερνήσεων να αυξήσουν τα έσοδά τους με την επιβολή φόρων και δασμών μέσω των εμπορικών συναλλαγών στο διαδίκτυο. Για να επιτευχθεί όμως αυτό πρέπει να εφαρμοστούν δύο βασικές αρχές του φορολογικού δικαίου οι οποίες είναι: α) η *αρχή της εδαφικότητας*, κατά την οποία η φορολόγηση υπολογίζεται με βάση το δίκαιο του τόπου όπου μια επιχείρηση έχει εγκατασταθεί ή ασκεί δραστηριότητα και β) η *αρχή της*

*υλικότητας*, κατά την οποία απαραίτητη προϋπόθεση φορολόγησης είναι το αντικείμενο της συναλλαγής να έχει υλική υπόσταση.

Οι Η.Π.Α. δε φορολογούν τέτοιου είδους συναλλαγές σε αντίθεση με τις ευρωπαϊκές χώρες στις οποίες γίνεται προσπάθεια φορολόγησής τους. Η Ελλάδα, όσον αφορά την άμεση φορολογία, φορολογεί τις ξένες επιχειρήσεις που έχουν έδρα σε αυτή ή ενεργούν μέσω αντιπροσώπου με έδρα στην Ελλάδα (αρ. 100 ν.2238/1994).

Αλλά και στην έμμεση φορολογία (π.χ.ΦΠΑ) παρουσιάζονται προβλήματα. Σε ΦΠΑ υπόκεινται ι η παροχή πρόσβασης στο διαδίκτυο, τα αγαθά και οι υπηρεσίες που διακινούνται μέσω διαδικτύου (online). Η Γαλλία, για παράδειγμα, επιτρέπει την επιβολή ΦΠΑ στις παροχές άυλων υπηρεσιών και καθιστά ισάξια τα ηλεκτρονικά τιμολόγια με τα χάρτινα, επιβάλλει δασμούς μόνο στην εισαγωγή «υλικών» αγαθών από το εξωτερικό, ενώ η «φόρτωση» (download) λογισμικού στην οθόνη με τη χρήση ξένου server δε δασμολογείται. Γενικά, ο ΦΠΑ βασίζεται στην αρχή της εδαφικότητας και ειδικά για τα κράτη-μέλη της Ευρωπαϊκής Ένωσης, σύμφωνα με την υπ'αρ. 77/388/ΕΟΚ Πρόταση Οδηγίας ισχύουν:

- Οι υπηρεσίες που παρέχονται από φορέα μη εγκατεστημένο στην ΕΕ σε πελάτη - χρήστη στην ΕΕ θα υπόκεινται σε ΦΠΑ γιατί ο τόπος φορολογίας είναι εντός της ΕΕ.
- Οι υπηρεσίες που παρέχονται από φορέα εγκατεστημένο στην ΕΕ σε πελάτη - χρήστη μη εγκατεστημένο στην ΕΕ δε θα υπόκεινται στο ΦΠΑ της ΕΕ, αφού ο τόπος φορολογίας (έδρα του πελάτη - χρήστη) βρίσκεται εκτός της ΕΕ.
- Οι υπηρεσίες που παρέχονται από φορέα εγκατεστημένο στην ΕΕ σε πελάτη - χρήστη στην ΕΕ θα υπόκεινται σε ΦΠΑ.
- Οι υπηρεσίες που παρέχονται από φορέα εγκατεστημένο στην ΕΕ σε πελάτη - χρήστη μέσα στο ίδιο κράτος, υπόκεινται στον τρόπο επιβολής ΦΠΑ ο οποίος εφαρμόζεται στο συγκεκριμένο κράτος.

# ΠΑΡΑΡΤΗΜΑ 1

# ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

## 1. ΠΑΡΟΥΣΙΑΣΗ ΤΗΣ ΑΡΧΗΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Η Αρχή Προστασίας Δεδομένων έχει ως αποστολή της την εποπτεία της εφαρμογής του ν.2472/97 και άλλων ρυθμίσεων που αφορούν στην προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και την άσκηση των αρμοδιοτήτων που της ανατίθενται κατά περίπτωση. Κεντρικό πρόβλημα είναι η διασφάλιση της ανεξαρτησίας της Αρχής Προστασίας Δεδομένων. Από θεσμική άποψη η "ανεξαρτησία" της Αρχής θεμελιώνεται: α) στην επιλογή του μοντέλου της Ανεξάρτητης Διοικητικής Αρχής, και β) στην εμπλοκή του Κοινοβουλίου στη διαδικασία της επιλογής των μελών της Αρχής.

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα είναι προσανατολισμένη στο πρότυπο της Ανεξάρτητης Διοικητικής Αρχής. Διακηρύσσεται η προσωπική και λειτουργική ανεξαρτησία των μελών της και κατοχυρώνεται η μη υπαγωγή της λειτουργίας της σε οποιονδήποτε διοικητικό έλεγχο. Για λόγους συνταγματικής τάξης προβλέπεται η υπαγωγή της στον Υπουργό Δικαιοσύνης. Η Αρχή μπορεί να επιλέγει η ίδια τα στελέχη της Γραμματείας της ενώ έχει δικό της προϋπολογισμό.

Η εμπλοκή του Κοινοβουλίου στη διαδικασία της επιλογής των μελών μιας αρχής αποτελεί για την ελληνική έννομη τάξη νέο στοιχείο. Η συμμετοχή των δύο κοινοβουλευτικών οργάνων, της Επιτροπής Θεσμών και Διαφάνειας και της Διάσκεψης των Προέδρων, στην επιλογή των μελών της Αρχής αποσκοπεί στην εξασφάλιση της διαφάνειας και στο δημοκρατικό έλεγχο. Η συμμετοχή των κοινοβουλευτικών οργάνων σε συνδυασμό με την υποχρέωση της Αρχής να ανακοινώνει στη Βουλή παραβάσεις της νομοθεσίας και να υποβάλλει στον Πρόεδρό της ετήσια έκθεση για την "εκτέλεση της αποστολής" της συνδέει την Αρχή με το Κοινοβούλιο, αυξάνει τη νομιμοποίησή της και ενισχύει τη θέση και την ανεξαρτησία της έναντι της εκτελεστικής εξουσίας.

Μεταξύ των βασικών υποχρεώσεων των υπεύθυνων επεξεργασίας είναι η υποβολή γνωστοποίησης αρχείων και επεξεργασιών προς την Αρχή. Για τη διευκόλυνσή τους και την αποφυγή οικονομικής επιβάρυνσής τους, η Αρχή κατάρτισε και διένειμε έντυπα γνωστοποίησης, συνοδευόμενα από οδηγίες.

Η Αρχή ανέπτυξε επίσης σημαντικές πρωτοβουλίες σχετικές με την προστασία δεδομένων προσωπικού χαρακτήρα στους τομείς της Κοινωνίας της Πληροφορίας, της άμεσης προώθησης προϊόντων και υπηρεσιών, των Τηλεπικοινωνιών και των μέσων μαζικής ενημέρωσης.

Συγκρότησε και συμμετείχε σε ομάδες εργασίας με σκοπό την ανάλυση των κινδύνων και των προβλημάτων προστασίας προσωπικών δεδομένων που προκύπτουν από τις υπηρεσίες Διαδικτύου και το ηλεκτρονικό εμπόριο και την αναζήτηση λύσεων στον τομέα αυτό.

Επίσης, η Αρχή, στο πλαίσιο των γνωμοδοτικών της αρμοδιοτήτων, συνέβαλλε στις εργασίες εναρμόνισης της ελληνικής νομοθεσίας με την Οδηγία 97/66/ΕC του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου, που ολοκληρώθηκαν με την ψήφιση του νόμου 2774/99 σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα.

Τέλος, η Αρχή συμμετέχει σε διεθνή όργανα – επιτροπές και παρακολουθεί τις διεθνείς εξελίξεις στον τομέα της προστασίας των προσωπικών δεδομένων. Αναφορικά με την εφαρμογή της οδηγίας 95/46/ΕΚ από τις χώρες της Ευρωπαϊκής Ένωσης διαπιστώνεται το παράδοξο ότι οι χώρες με τη μεγαλύτερη παράδοση στην προστασία των προσωπικών δεδομένων παρουσιάζουν αξιοσημείωτη καθυστέρηση στη σχετική εναρμόνιση της νομοθεσίας τους. Εκπρόσωποι της Αρχής συμμετέχουν και στην ομάδα εργασίας που προβλέπεται από το άρθρο 29 της οδηγίας, την οποία απασχολεί το θέμα του επιπέδου προστασίας δεδομένων στις Ηνωμένες Πολιτείες και της διαβίβασης προσωπικών δεδομένων από την Ένωση προς τις Η.Π.Α. Συμμετοχή έχει να επιδείξει η Αρχή και στην Κοινή Αρχή Ελέγχου του Πληροφοριακού Συστήματος Σένγκεν καθώς και στην Κοινή Εποπτική Αρχή για τον έλεγχο της Europol (ΚΕΑ).

Αξιοσημείωτες εξελίξεις έλαβαν χώρα και στο πλαίσιο διεθνών οργανισμών, όπως το Συμβούλιο της Ευρώπης, τον Οργανισμό Οικονομικής Συνεργασίας και Ανάπτυξης, τον Παγκόσμιο Οργανισμό Εμπορίου και τον Παγκόσμιο Οργανισμό Πνευματικής Ιδιοκτησίας, καθώς και σε υπό προσχώρηση στην Ε.Ε. τρίτες χώρες όπως οι ΗΠΑ, ο Καναδάς, η Ιαπωνία και η Αυστραλία.

## 2. ΣΥΝΕΝΤΕΥΞΗ ΓΚΡΙΤΖΑΛΗ

Πέρα από τη συλλογή πληροφοριών, ηλεκτρονικά sites, βιβλία και γενικά έντυπο υλικό, θεωρήθηκε απαραίτητο να απαντηθούν άμεσα κάποια καίρια ερωτήματα σχετικά με την ιδιωτικότητα, από έναν άνθρωπο ο οποίος γνωρίζει σε

βάθος το θέμα. Η επιλογή έγινε βάσει απλών κριτηρίων. Το συγκεκριμένο άτομο θα έπρεπε να έχει μελετήσει το αντικείμενο, να είναι καταρτισμένος, να έχει περάσει από θέση τέτοια, ώστε οι απαντήσεις του να έχουν κύρος, τεκμηρίωση, εγκυρότητα και φυσικά να είναι δεκτικός στην προσέγγισή μας για μια σειρά ερωτήσεων. Θεωρήσαμε οπότε ως καταλληλότερο άνθρωπο τον Κο Γκρίτζαλη, ο οποίος ήταν μέλος της Ελληνικής Αρχής Προστασίας Προσωπικών Δεδομένων μέχρι την 31η Αυγούστου 2002, έχει ασχοληθεί με τη συγγραφή βιβλίων σχετικών με το privacy και γενικά με την ασφάλεια των πληροφοριακών συστημάτων. Επίσης έχει υπάρξει καθηγητής Πληροφορικής στο ΤΕΙ Αθηνών, στο Πανεπιστήμιο Αιγαίου και στο Οικονομικό Πανεπιστήμιο Αθηνών.

Η πρώτη επικοινωνία μαζί του έγινε σε διαπροσωπικό επίπεδο, μόνο που δεν έγινε δυνατή η διεξαγωγή της συνέντευξης τη συγκεκριμένη μέρα. Λίγο καιρό αργότερα οι ερωτήσεις εστάλησαν μέσω email και οι απαντήσεις δόθηκαν κάποιες μέρες μετά με τον ίδιο τρόπο. Παρακάτω παραθέτουμε το αποτέλεσμα της συγκεκριμένης προσπάθειας.

## ΣΥΝΤΟΜΟ ΒΙΟΓΡΑΦΙΚΟ

Δρ. Στέφανος Γκρίτζαλης: Καθηγητής Εφαρμογών τμήματος Πληροφορικής ΤΕΙ Αθήνας
Επίκουρος Καθηγητής (ΠΔ 407/80) τμήματος Πληροφοριακών και Επικοινωνιακών Συστημάτων Πανεπιστημίου Αιγαίου
Καθηγητής τμήματος Πληροφορικής Οικονομικού Πανεπιστημίου Αθηνών
Πρώην μέλος της Αρχής Προστασίας Προσωπικών Δεδομένων

## Η ΣΥΝΕΝΤΕΥΞΗ

**1. Υπάρχουν συγκεκριμένα προσωπικά δεδομένα ή είναι αόριστη έννοια;**

- *"Ορίζεται επακριβώς στο πρώτο άρθρο του νόμου 2472/97".* Αντικείμενο του παρόντος νόμου είναι η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα, για την προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής .

## 2. Υπάρχει θεσμοθετημένο νομοθετικό πλαίσιο; Ποια η διαφορά Ελλάδας με το εξωτερικό;

- *"Ο νόμος 2472/97 αποτελεί το βασικό Ελληνικό κείμενο. Επικουρικά ισχύει και ο νόμος 2774/99. Στην Ευρωπαϊκή Ένωση υπάρχει η Οδηγία 95/46."*

Στο άρθρο 2 του νόμου 2472/97 αναφέρονται τα «Δεδομένα προσωπικού χαρακτήρα» τα οποία είναι κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων. Δεν θεωρούνται προσωπικά δεδομένα τα στατιστικά στοιχεία στα οποία δεν μπορούν να προσδιορισθούν τα υποκείμενα των δεδομένων.

Τα «Ευαίσθητα δεδομένα» που αναφέρονται στα δεδομένα που αφορούν τη φυλετική προέλευση, τα πολιτικά φρονήματα, τις θρησκευτικές πεποιθήσεις, τη συμμετοχή σε συνδικαλιστική οργάνωση, την υγεία, τη ερωτική ζωή, καθώς και τα σχετικά με ποινικές διώξεις ή καταδίκες.

Σαν «Υποκείμενο των δεδομένων», θεωρείται το φυσικό πρόσωπο του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί, ιδίως βάσει αριθμού ταυτότητας. Η «Επεξεργασία δεδομένων προσωπικού χαρακτήρα» είναι κάθε εργασία που πραγματοποιείται, από το Δημόσιο ή νομικό πρόσωπο και εφαρμόζεται σε δεδομένα προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώρηση και η τροποποίηση.

Το «Αρχείο δεδομένων προσωπικού χαρακτήρα» είναι τα δεδομένα προσωπικού χαρακτήρα, τα οποία αποτελούν αντικείμενο επεξεργασίας και τα οποία τηρούνται είτε από το δημόσιο ή από νομικό πρόσωπο δημοσίου δικαίου. Η «Διασύνδεση» είναι η μορφή επεξεργασίας στην οποία γίνεται η συσχέτιση των δεδομένων ενός αρχείου με δεδομένα αρχείου που τηρούνται από άλλον ή άλλους υπεύθυνους επεξεργασίας.

Ο «Υπεύθυνος επεξεργασίας» είναι οποιοσδήποτε καθορίζει τον σκοπό και τον τρόπο επεξεργασίας των δεδομένων προσωπικού χαρακτήρα.

Ο «Εκτελών την επεξεργασία» είναι οποιοσδήποτε επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό υπεύθυνου επεξεργασίας, όπως φυσικό ή νομικό πρόσωπο δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός.

Ο «Τρίτος» θεωρείται κάθε φυσικό πρόσωπο, δημόσια αρχή που δεν έχει εξουσιοδότηση στην επεξεργασία προσωπικών δεδομένων.

Ο «Αποδέκτης» είναι κάθε φυσικό ή νομικό πρόσωπο, η δημόσια αρχή ή υπηρεσία, ή οποιοσδήποτε άλλος οργανισμός, στον οποίο ανακοινώνονται τα δεδομένα, ανεξαρτήτως αν πρόκειται για τρίτο ή όχι.

Η «Συγκατάθεση» του υποκειμένου των δεδομένων είναι κάθε δήλωση βουλήσεως, που εκφράζεται με τρόπο σαφή Η ενημέρωση αυτή περιλαμβάνει πληροφόρηση τουλάχιστον για τον σκοπό της επεξεργασίας, καθώς και το όνομα, την επωνυμία και τη διεύθυνση του υπεύθυνου επεξεργασίας και του τυχόν εκπροσώπου

του. Η συγκατάθεση μπορεί να ανακληθεί οποτεδήποτε, χωρίς αναδρομικό αποτέλεσμα.

Η «Αρχή» , η Αρχή Προστασίας Δεδομένου Προσωπικού Χαρακτήρα.

**3. Με τις εταιρίες πώς λειτουργεί η Αρχή; (κάποια εταιρία απευθύνεται στην Αρχή για πρόληψη;)**

- *"Υπάρχει συγκεκριμένη διαδικασία (χρήση εντύπων), η οποία περιγράφεται στο site της Αρχής (**www.dpa.gr**)"* .Η οποία είναι η εξής:

**ΣΥΝΤΟΜΕΣ ΟΔΗΓΙΕΣ ΣΥΜΠΛΗΡΩΣΗΣ ΤΗΣ ΓΝΩΣΤΟΠΟΙΗΣΗΣ – ΑΙΤΗΣΗΣ ΑΔΕΙΑΣ**

Για τη συμμόρφωση με τις διατάξεις του ν. 2472/97 ο υπεύθυνος επεξεργασίας που επεξεργάζεται προσωπικά δεδομένα (όπως αυτά ορίζονται από το ν. 2472/97) πρέπει να ακολουθήσει τα παρακάτω βήματα:

1. Υποχρεωτική συμπλήρωση του Εντύπου 1.0 και **τουλάχιστον ενός Εντύπου 2.0.**

- Για κάθε έναν από τους σκοπούς επεξεργασίας θα πρέπει να συμπληρωθεί ένα αντίγραφο του Εντύπου 2.0. Οι κωδικοί των σκοπών επεξεργασίας που απαιτούνται για την συμπλήρωση του Εντύπου 2.0, παρατίθενται στο κείμενο με τίτλο Κωδικοί Σκοπών.

- Σε περιπτώσεις όπου η επεξεργασία των προσωπικών δεδομένων λαμβάνει χώρα σε περισσότερους από έναν διαφορετικούς γεωγραφικούς χώρους, στα πλαίσια του ίδιου οργανισμού, θα πρέπει να συμπληρωθεί το Έντυπο 3.0.

- Σε περιπτώσεις όπου λαμβάνει χώρα διασύνδεση αρχείων (έτσι όπως αυτή ορίζεται στο Άρθρο 8 του ν. 2472/97) θα πρέπει να συμπληρωθεί το Έντυπο 4.0.

- Σε περιπτώσεις όπου μέρος ή /και το σύνολο των προσωπικών δεδομένων μεταβιβάζεται σε χώρες εκτός Ευρωπαϊκής Ένωσης θα πρέπει να συμπληρωθεί το Έντυπο 5.0. Οι κωδικοί των Χωρών Κρατών εκτός Ευρωπαϊκής Ένωσης που απαιτούνται για την συμπλήρωση του Εντύπου 5.0, παρατίθενται στο κείμενο με τίτλο Κωδικοί Χωρών.

2.Υποχρεωτική ενημέρωση των υποκειμένων επεξεργασίας ακολουθώντας τις διαδικασίες που περιγράφονται στην Απόφαση της Αρχής Νο 408 και στην Κανονιστική Πράξη 1/1999.

*Επιγραμματικά αναφέρονται σε πίνακα τα είδη εντύπων, τα οποία με αναλυτικό Οδηγό Συμπλήρωσης , βρίσκονται στο site της Αρχής Διασφάλισης Προσωπικών Δεδομένων.*

| | |
|---|---|
| **1.0** | Γνωστοποίηση Τήρησης Αρχείου / Επεξεργασίας Προσωπικών Δεδομένων (Μέρος Ι) |
| **2.0** | Γνωστοποίηση Τήρησης Αρχείου Προσωπικών Δεδομένων (Μέρος ΙΙ: Σκοπού Επεξεργασίας) |
| **3.0** | Γνωστοποίηση Διευθύνσεων Τόπων Επεξεργασίας Προσωπικών Δεδομένων |
| **4.0** | Δήλωση / Αίτηση Διασύνδεσης Αρχείων (Άρθρο 8 του Ν.2472/97) |
| **5.0** | Αίτηση Άδειας Διαβίβασης Δεδομένων σε χώρες εκτός της Ε.Ε. |
| | **Παραρτήματα:** |
| **Σκοποί** | Σκοποί επεξεργασίας για το Έντυπο 2.0 |
| **Χώρες** | Κωδικοί Χωρών Κρατών εκτός της Ευρωπαϊκής Ένωσης |

**4. Η Αρχή λειτουργεί αυτόβουλα ή περιμένει καταγγελία; Ποιός είναι ο τρόπος δράσης της;**

- *"Και αυτεπάγγελτα και μετά από καταγγελία. Σε κάθε περίπτωση η συνήθης ενέργεια της Αρχής είναι η διενέργεια διοικητικού ελέγχου στα αρχεία"* .Επιπλέον η Αρχή έχει δικαίωμα πρόσβασης στα προσωπικά δεδομένα και στην συλλογή κάθε απαραίτητης πληροφορίας για τον έλεγχο της.

**5.Με ποιο τρόπο γίνεται η παραβίαση των προσωπικών δεδομένων των ατόμων; Μπορούν να παραβιάζονται εν αγνοία μας;**

- *"Αυτό χρειάζεται βιβλίο για να αναλυθεί επαρκώς. Μελετήστε το άρθρο της κας. Μήτρου στο βιβλίο Ασφάλεια Πληροφοριών: Νομικά, Τεχνικά και Κοινωνικά θέματα, Εκδόσεις ΕΠΥ».*

....«Παρά τη σημασία του δικαιώματος για προστασία των προσωπικών δεδομένων του πολίτη, δε μπορεί να μη σημειωθεί ότι ασκείται σπανιότατα, μην

αγγίζοντας καν το ποσοστό του 10% σε σχέση με το σύνολο των ατόμων, πληροφορίες των οποίων είναι καταχωρημένες σε δημόσια και ιδιωτικά αρχεία. Η αποχή αυτή μπορεί να θεωρηθεί φυσιολογική, εφόσον στις κοινωνίες της πληροφορίας όπου η συλλογή, παροχή και κυκλοφορία πληροφοριών έχει καταστεί φαινόμενο συνηθισμένο, θα ήταν παράδοξο να περιμένει κανείς από το μέσο πολίτη να ενημερώνεται για την πορεία των πληροφοριών του. Εξάλλου τα πλέον ενδιαφέροντα για τον πολίτη αρχεία όπως της αστυνομίας είναι απροσπέλαστα για αυτόν. Ο μεμονωμένος πολίτης δεν είναι σε θέση να ελέγξει την πληροφοριακή συμπεριφορά της διοίκησης ή μιας ιδιωτικής επιχείρησης. Ο ιδιώτης παραμένει ένας outsider από τον οποίο λείπουν οι απαραίτητες πληροφορίες που θα του επέτρεπαν να αναλύσει τις δραστηριότητες του δημόσιου και του ιδιωτικού τομέα σε σχέση με τη συλλογή και επεξεργασία των προσωπικών του πληροφοριών αλλά και το σύνολο των συνεπειών της.»...

...«Αν ήταν δύσκολο να ελεγχθεί η επεξεργασία των προσωπικών πληροφοριών που γινόταν στα κέντρα μηχανογράφησης, οι νέες τεχνολογικές εφαρμογές καθιστούν πλασματικό τον οποιοδήποτε έλεγχο. Οι online συνδέσεις, η τεχνική διευκόλυνση εισόδου σε διάφορα συστήματα, τα Integrated Services Digital Network (ISDN),το πάντρεμα της τεχνολογίας με τις τηλεπικοινωνίες, τα e-mail θέτουν σε αχρηστία τις ισχύουσες ρυθμίσεις για την προστασία των προσωπικών δεδομένων.»...

**6. Πόσα χρόνια υπάρχει η Αρχή, ποια είναι η σύνθεση της, πώς δημιουργήθηκε (αφορμή) , ποιες είναι οι αρμοδιότητές της, τι επιρροή έχει και γενικότερα ποια η δύναμη της;**

- *"Η Αρχή ιδρύθηκε το Νοέμβρη του 1977 και ο ρόλος και οι αρμοδιότητές της αναφέρονται λεπτομερώς στον ιδρυτικό της νόμο (2472/97). Άρθρο 16: Συγκρότηση της Αρχής".*

Η Αρχή αποτελείται από έναν δικαστικό λειτουργό βαθμού Συμβούλου της Επικρατείας ή αντίστοιχου και άνω, ως Πρόεδρο, και έξι μέλη ως εξής:α) Έναν καθηγητή ή αναπληρωτή καθηγητή ΑΕΙ σε γνωστικό αντικείμενο του δικαίου. β) Έναν καθηγητή ή αναπληρωτή καθηγητή ΑΕΙ σε γνωστικό αντικείμενο της πληροφορικής. γ) Έναν καθηγητή ή αναπληρωτή καθηγητή ΑΕΙ. δ) Τρία πρόσωπα κύρους και εμπειρίας στον τομέα της προστασίας δεδομένων προσωπικού χαρακτήρα. Ο Πρόεδρος της Αρχής διορίζεται με προεδρικό διάταγμα, που εκδίδεται με πρόταση του Υπουργικού Συμβουλίου. Με την ίδια διαδικασία επιλέγεται και διορίζεται ο αναπληρωτής του προέδρου.

Τα μέλη της Αρχής διορίζονται όταν ο Υπουργός Δικαιοσύνης υποβάλλει στον Πρόεδρο της Βουλής πρόταση για το διορισμό των έξι τακτικών μελών της Αρχής .Επιπλέον ισχύει η τετραετής θητεία των μελών και του προέδρου όπως επίσης και ο διορισμός των αναπληρωτών τους.

Επιπλέον οι αρμοδιότητες αναφέρονται στο άρθρο 19: Αρμοδιότητες

λειτουργία και αποφάσεις της Αρχής

Η Αρχή έχει τις εξής ιδίως αρμοδιότητες:

- Εκδίδει οδηγίες προς τον σκοπό ενιαίας εφαρμογής των ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.
- Καλεί τα επαγγελματικά σωματεία και τις λοιπές ενώσεις φυσικών ή νομικών προσώπων που διατηρούν αρχεία δεδομένων προσωπικού χαρακτήρα, στην κατάρτιση κωδικών δεοντολογίας για την αποτελεσματικότερη προστασία της ιδιωτικής ζωής και των εν γένει δικαιωμάτων και θεμελιωδών ελευθεριών.
- Απευθύνει συστάσεις και υποδείξεις στους υπεύθυνους, και δίνει κατά την κρίση της, δημοσιότητα σε αυτές.
- Χορηγεί τις άδειες που προβλέπουν οι διατάξεις του παρόντος νόμου και καθορίζει το ύψος των σχετικών παραβόλων.
- Καταγγέλλει τις παραβάσεις των διατάξεων του παρόντος νόμου στις αρμόδιες διοικητικές και δικαστικές αρχές.
- Επιβάλλει τις κατά το άρθρο 21 του παρόντος νόμου διοικητικές κυρώσεις.
- Αναθέτει σε μέλη της, τη διενέργεια διοικητικών εξετάσεων.
- Ενεργεί αυτεπαγγέλτως ή κατόπιν καταγγελίας διοικητικούς ελέγχους σε κάθε αρχείο. Έχει δικαίωμα προσβάσεως στα δεδομένα προσωπικού χαρακτήρα και συλλογής κάθε πληροφορίας για τους σκοπούς του ελέγχου, χωρίς να μπορεί να της αντιταχθεί κανενός είδους απόρρητο.
- Γνωμοδοτεί για κάθε ρύθμιση που αφορά την επεξεργασία και προστασία δεδομένων προσωπικού χαρακτήρα.
- Εκδίδει κανονιστικές πράξεις για τη ρύθμιση ειδικών, τεχνικών και λεπτομερειακών θεμάτων, στα οποία αναφέρεται ο παρών νόμος.
- Ανακοινώνει στη Βουλή παραβάσεις των ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.
- Συντάσσει κάθε χρόνο έκθεση για την εκτέλεση της αποστολής της κατά το προηγούμενο ημερολογιακό έτος.
- Εξετάζεται η εφαρμογή του νόμου και η προστασία των δικαιωμάτων των αιτούντων όταν αυτά θίγονται από την επεξεργασία δεδομένων που τους αφορούν και

αιτήσεις με τις οποίες ζητείται ο έλεγχος και η εξακρίβωση της νομιμότητας των επεξεργασιών αυτών και ενημερώνει τους αιτούντες για τις σχετικές ενέργειές της.

- Συνεργάζεται με αντίστοιχες αρχές κρατών μελών της Ευρωπαϊκής Ένωσης και του Συμβουλίου της Ευρώπης σε ζητήματα σχετικά με την άσκηση των αρμοδιοτήτων της.

Συμπερασματικά βλέπουμε την δύναμη και το κύρος της αρχής μετά από αυτές τις αρμοδιότητες. Το γεγονός ότι συνεργάζεται με αντίστοιχες αρχές μελών-κρατών της Ευρωπαϊκής Ένωσης, συντάσσει ετήσια έκθεση υποβαλλόμενη στον Πρόεδρο της Βουλής, οι κανονιστικές της αποφάσεις δημοσιεύονται στην εφημερίδα της κυβερνήσεως και οι υπόλοιπες ισχύουν από την κοινοποίηση τους και ακόμα κάποια ένδικα βοηθήματα κατά των αποφάσεων της Αρχής τα χρησιμοποιεί το δημόσιο. Από όλα αυτά φαίνεται η επιρροή που ασκεί η Αρχή Διασφάλισης Προσωπικών Δεδομένων.

**7. Υπάρχει προϊστάμενος; Σε ποιον αναφέρονται για ότι χρειάζεται έγκριση; Υπάρχει θέση CPO, πόσα κερδίζει σε σχέση με άλλους;**

*"Δείτε το site της Αρχής για πληροφορίες που αφορούν το Οργανόγραμμά της. Όλοι οι υπάλληλοι αμείβονται με βάση το μισθολόγιο του Δημοσίου. Υπάρχουν και μερικά ειδικά επιδόματα".*

Κατά την άσκηση των καθηκόντων τους τα μέλη της Αρχής υπακούουν στη συνείδηση τους και το νόμο. Υπόκεινται στο καθήκον εχεμύθειας. Το καθήκον εχεμύθειας υφίσταται και μετά την με οποιονδήποτε τρόπο αποχώρηση των μελών της Αρχής.

Ότι αφορά τις χρηματικές αποδοχές όπως φαίνεται στο άρθρο 18 καθορίζονται οι μηνιαίες αποδοχές του προέδρου και των μελών της Αρχής καθώς και η αποζημίωση τους για κάθε συνεδρίαση, κατά παρέκκλιση από κάθε άλλη διάταξη. Στους αναπληρωτές καταβάλλεται το ένα τρίτο (1/3) των μηνιαίων αποδοχών των μελών της Αρχής και αποζημίωση για κάθε συνεδρίαση στην οποία μετέχουν. Οι διατάξεις για τις δαπάνες κινήσεως των μετακινουμένων προσώπων με εντολή του Δημοσίου για εκτέλεση υπηρεσίας που ισχύουν κάθε φορά έχουν εφαρμογή και για την μετακίνηση των μελών και των υπαλλήλων της Γραμματείας της Αρχής. Ο Πρόεδρος της Αρχής εκδίδει τις σχετικές εντολές μετακίνησης.

Για κάθε παράβαση των υποχρεώσεων τους που απορρέουν από τον παρόντα νόμο, τα μέλη της Αρχής έχουν πειθαρχική ευθύνη. Την πειθαρχική αγωγή ασκεί ενώπιον του πειθαρχικού συμβουλίου ο Υπουργός Δικαιοσύνης για τον Πρόεδρο και τα μέλη της Αρχής και ο Πρόεδρος της Αρχής για τα μέλη της.

Μέλος της Αρχής που, κατά παράβαση του παρόντος νόμου, γνωστοποιεί με οποιονδήποτε τρόπο δεδομένα προσωπικού χαρακτήρα που είναι προσιτά σε αυτό λόγω της υπηρεσίας του ή αφήνει άλλον να λάβει γνώση αυτών, τιμωρείται με φυλάκιση τουλάχιστον δύο ετών και χρηματική ποινή τουλάχιστον δυο εκατομμυρίων δραχμών έως δέκα εκατομμυρίων δραχμών. Αν όμως τέλεσε την πράξη με σκοπό να προσπορίσει στον εαυτό του ή σε άλλο αθέμιτο όφελος ή να βλάψει άλλον, επιβάλλεται κάθειρξη. Αν η πράξη του πρώτου εδαφίου τελέστηκε από αμέλεια επιβάλλεται φυλάκιση τουλάχιστον τριών μηνών και χρηματική ποινή.

## 9. Παράδειγμα στο οποίο έχει παραβιαστεί η προστασία προσωπικών δεδομένων στην Ελλάδα.

- *"Η περίπτωση των ταυτοτήτων είναι – ίσως – η πιο γνωστή και πάντως αρκετά χαρακτηριστική"*. Κατά την οποία αποφάσισε σύμφωνα με τον νόμο ότι τα ακόλουθα στοιχεία που προβλέπει το ν.δ. 127/1969 για τα αστυνομικά δελτία ταυτότητας υπερβαίνουν τον σκοπό επεξεργασίας:

1) Το δακτυλικό αποτύπωμα του υποκειμένου. Το στοιχείο αυτό δεν είναι αναγκαίο για την βεβαίωση της ταυτότητας του υποκειμένου αφού αυτή καταρχήν προκύπτει από την προβλεπόμενη φωτογραφία. Επιπλέον, το αποτύπωμα (η σήμανση) συνδέεται με την υποψία ή διαπίστωση εγκληματικής δραστηριότητας (σεσημασμένοι), η απόδοση της υπερβαίνει το αναγκαίο μέτρο και προσβάλλει την προστατευόμενη από το Σύνταγμα αξία του ανθρώπου.

2) Το ονοματεπώνυμο του/της συζύγου δεδομένου ότι ήδη από το 1983 ο γάμος δεν επιφέρει μεταβολή του επωνύμου των συζύγων.

3) Το επάγγελμα διότι δεν αποτελεί στοιχείο της φυσικής ταυτότητας, υπόκειται σε μεταβολές και δεν απηχεί απαραίτητα την πραγματικότητα σε χρόνο μεταγενέστερο αυτού της έκδοσης του δελτίου.

4) Η υπηκοότητα/ιθαγένεια, διότι εκ του νόμου δελτίο αστυνομικής ταυτότητας φέρουν μόνο οι Έλληνες πολίτες.

5) Η κατοικία, ως μη αναγκαίο και πρόσφορο (διότι υπόκειται σε αλλαγές) για την εξατομίκευση της ταυτότητας.

6) Το θρήσκευμα διότι ανάγεται στον εσωτερικό κόσμο του ατόμου και ως εκ τούτου είναι απρόσφορο και μη αναγκαίο για την εξατομίκευση της ταυτότητας.

Η επεξεργασία όλων των άνω δεδομένων δεν είναι θεμιτή και όταν ακόμη το υποκείμενο παρέχει προς τούτο τη ρητή συγκατάθεσή του διότι αντίκειται στην αρχή του σκοπού και της αναγκαιότητας. Για τους λόγους αυτούς και σύμφωνα με τις διατάξεις των άρθρων 4 παρ. 2, 15 παρ. 1, 19παρ. 1 εδ.α και γ και 21 παρ. 1$^{α}$ του

Ν.2472/1997, η αρχή έως ότου καθιερωθεί το νέου τύπου δελτίο ταυτότητας του ν 1599/1986, απευθύνει σύσταση στον υπεύθυνο επεξεργασίας του Υπουργείου Δημοσίας Τάξεως και κάθε άλλο συναρμόδιο να συμμορφωθούν προς το περιεχόμενο της παρούσας απόφασης, εκδίδοντας τις αναγκαίες οδηγίες προς τις οικείες αρχές και υπηρεσίες και εφεξής κατά την έκδοση των νέων δελτίων αστυνομικής ταυτότητας ή τυχόν αντικατάσταση των παλαιών να μη συλλέγουν (δηλαδή να μην ερωτούν, ούτε να επιτρέπουν την αναγραφή) και να μην επεξεργάζονται τα ακόλουθα στοιχεία:

1) δακτυλικό αποτύπωμα
2) όνομα και επώνυμο συζύγου
3) γένος
4) επάγγελμα
5) διεύθυνση κατοικίας
6) υπηκοότητα
7) θρήσκευμα

**10. Στατιστικά σε ποιον τομέα γίνονται οι περισσότερες παραβιάσεις στην Ελλάδα;**

- *"Δεν υπάρχουν ακόμη επαρκή στοιχεία για να εξαχθούν τέτοια συμπεράσματα. Πρέπει να παρέλθει ακόμη τουλάχιστον μια τριετία".*

**11. Η Αρχή αναφέρεται σε συγκεκριμένους τομείς π.χ. ιατρικούς ή όχι. Αν όχι ποιους τομείς περιλαμβάνει;**

- *"Καλύπτει κάθε τομέα, χωρίς καμία εξαίρεση!"* Επιπλέον σύμφωνα με το άρθρο 3 του 2472/97 το πεδίο εφαρμογής περιλαμβάνουν:

Οι διατάξεις του νόμου εφαρμόζονται στην εν όλων ή εν μέρει αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε αρχείο.

Δεν εφαρμόζονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα, η οποία πραγματοποιείται από φυσικό πρόσωπο για την άσκηση δραστηριοτήτων αποκλειστικά προσωπικών ή οικιακών.

Ο παρών νόμος εφαρμόζεται σε κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα, εφόσον αυτή εκτελείται:α) Από υπεύθυνο επεξεργασίας, εγκατεστημένο στην Ελληνική Επικράτεια όπου βάσει του δημοσίου διεθνούς δικαίου εφαρμόζεται το ελληνικό δίκαιο .β) Από υπεύθυνο επεξεργασίας μη εγκατεστημένο στην Ελληνική Επικράτεια ή σε τόπο όπου εφαρμόζεται το ελληνικό δίκαιο, όταν η επεξεργασία

αφορά υποκείμενα εγκατεστημένα στην Ελληνική Επικράτεια. Ισχύει και όταν ο υπεύθυνος επεξεργασίας καλύπτεται από ετεροδικία, ασυλία, ή άλλο λόγο που κωλύει την ποινική δίωξη. γ)Από υπεύθυνο επεξεργασίας που δεν είναι εγκατεστημένος στην επικράτεια Κράτους – Μέλους της Ευρωπαϊκής Ένωσης αλλά τρίτης χώρας και για τους σκοπούς της επεξεργασίας δεδομένων προσωπικού χαρακτήρα προσφεύγει σε μέσα, ευρισκόμενα στην Ελλάδα.

**12. Τι ξοδεύουν ή τι πρόκειται να ξοδέψουν μεγάλες εταιρίες για privacy;**

*"Γενικά, υπάρχει μια πολύ έντονη τάση. Τα τελευταία χρόνια δίνεται μεγάλη προσοχή σε τέτοια θέματα, ειδικά στις ΗΠΑ".*

**13. Τι θα πρέπει να περιέχει ένα καλό privacy statement;Ποια τα μέλη της Αρχής και που συνεδριάζει;**

*«Δύσκολη ερώτηση. Θα πρέπει, οπωσδήποτε, να είναι σύντομο και περιεκτικό, με προσεκτική διατύπωση και σαφή εννοιολογική επικέντρωση".*

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα συγκροτείται από ένα δικαστικό λειτουργό βαθμού Συμβούλου της Επικρατείας ή αντίστοιχου και άνω, ως Πρόεδρο, και έξι (6) μέλη και εξυπηρετείται από Γραμματεία. Η Γραμματεία λειτουργεί σε επίπεδο Διευθύνσεως και συγκροτείται από τρία (3) τμήματα:
Τμήμα Ελεγκτών, Τμήμα Επικοινωνίας, Τμήμα Διοικητικών και Οικονομικών Υποθέσεων.

**Πρόεδρος**
**Δημήτριος Γουργουράκης** -Αντιπρόεδρος του Αρείου Πάγου ε.τ.
(μέχρι 31/12/2002 ο κος Κωνσταντίνος Δαφέρμος -Επ.Αντιπρόεδρος του Αρείου Πάγου)

**Αναπληρωτής Πρόεδρος**
**Γεώργιος Δεληγιάννης**
Αντιπρόεδρος του Συμβουλίου της Επικρατείας
**Μαρία Παχή**- *Γραμματέας του Προέδρου*

---

**Μέλη**
**Ιωάννης Τσουκαλάς**
Καθηγητής Πληροφορικής του Πανεπιστημίου Θεσσαλονίκης.
**Σωτήριος Λύτρας**

Καθηγητής Δημοσίου Δικαίου του Πανεπιστημίου Αθηνών.
**Αθανάσιος Παπαχρίστου**
Καθηγητής Αστικού Δικαίου του Πανεπιστημίου Αθηνών.
**Νικόλαος Παπαγεωργίου**
Καθηγητής Εθνικού Μετσόβειου Πολυτεχνείου Αθηνών.
**Στυλιανός Σαρηβαλάσης**
Επίτιμος Σύμβουλος του Συμβουλίου της Επικρατείας.
**Νικόλαος Φραγκάκης**
Δικηγόρος.

*Αναπληρωματικά Μέλη της Αρχής*
**Αθανάσιος Καΐσης**
Καθηγητής του Πανεπιστημίου Θεσσαλονίκης.
**Πόπη Φουντεδάκη**
Καθηγήτρια του Παντείου Πανεπιστημίου Αθηνών.
**Αγάπιος Παπανεοφύτου**
Καθηγητής του Παντείου Πανεπιστημίου Αθηνών.
**Γραμματή Πάντζιου**
Καθηγήτρια ΤΕΙ Αθηνών.
**Χρήστος Παληοκώστας**
Επίτιμος Αρεοπαγίτης.
**Χρήστος Πολίτης**
Δικηγόρος.

---

**ΤΜΗΜΑ ΕΛΕΓΚΤΩΝ**
**Προϊστάμενος Ελεγκτών**
**Δρ.Ζορκάδης Βασίλειος**
Πληροφορικός
**Ελεγκτές**
**Δρ.Δόνος Πελοπίδας**
Νομικός
**Καμπουράκη Κωνσταντίνα**
Πληροφορικός
**Λωσταράκου Κυριακή**
Νομικός
**Μίτλεττον Φίλιππος**
Νομικός
**Μουλίνος Κωνσταντίνος**

Πληροφορικός
**Σιουγλέ Ευφροσύνη**
Πληροφορικός
**Καρβέλη Καλλιόπη**

---

**ΤΜΗΜΑ ΕΠΙΚΟΙΝΩΝΙΑΣ**

**Προϊστάμενος**
**Κοσμοπούλου Κατερίνα**
**Προσωπικό**
**Αθανασιάδης Ηλίας**
**Κουρούνη Κυριακή**
**Λογιάκη Αμαλία**

---

**ΤΜΗΜΑ ΔΙΟΙΚΗΤΙΚΩΝ & ΟΙΚΟΝΟΜΙΚΩΝ**

**Προϊστάμενος**
**Χρυσοβελίδη Αιμιλία**
**Προσωπικό**
**Κανακάκη Αγγελική**
**Τσιάβου Μαριάνθη**
**Γιαννάκη Μελπομένη**
**Μπάλλος Ιωάννης**
**Πέτρου Συμεών**
**Παπαδόπουλος Ανδρέα**

Η Αρχή συνεδριάζει τακτικώς ύστερα από πρόσκληση του Προέδρου. Συνεδριάζει εκτάκτως ύστερα από πρόσκληση του Προέδρου ή αίτηση δύο τουλάχιστον μελών της. Οι αποφάσεις της Αρχής λαμβάνονται με πλειοψηφία τουλάχιστον τεσσάρων μελών της. Σε περίπτωση ισοψηφίας υπερισχύει η ψήφος του Προέδρου ή του αναπληρωτή του.

# ΠΑΡΑΡΤΗΜΑ 2
# Ν. 2472/97

"Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα"

## ΚΕΦΑΛΑΙΟ Α'
## ΓΕΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

### Άρθρο 1
### Αντικείμενο

Αντικείμενο του παρόντος νόμου είναι η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα προς προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής.

### Άρθρο 2
### Ορισμοί

Για τους σκοπούς του παρόντος νόμου νοούνται ως:

α)"**Δεδομένα προσωπικού χαρακτήρα**", κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων. Δεν λογίζονται ως δεδομένα προσωπικού χαρακτήρα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν πλέον να προσδιορισθούν τα υποκείμενα των δεδομένων.

β)"**Ευαίσθητα δεδομένα**", τα δεδομένα που αφορούν τη φυλετική ή εθνική προέλευση, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, τη συμμετοχή σε ένωση, σωματείο και συνδικαλιστική οργάνωση, την υγεία, την κοινωνική πρόνοια και τη ερωτική ζωή, καθώς και τα σχετικά με ποινικές διώξεις ή καταδίκες.

γ)"**Υποκείμενο των δεδομένων**", το φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα, και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί, δηλαδή

μπορεί να προσδιορισθεί αμέσως ή εμμέσως, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός η περισσότερων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική.

δ)"**Επεξεργασία δεδομένων προσωπικού χαρακτήρα**" ("επεξεργασία"), κάθε εργασία ή σειρά εργασιών που πραγματοποιείται, από το Δημόσιο ή από νομικό πρόσωπο δημοσίου δικαίου ή ιδιωτικού δικαίου ή ένωση προσώπων ή φυσικό πρόσωπο με ή χωρίς τη βοήθεια αυτοματοποιημένων μεθόδων και εφαρμόζονται σε δεδομένα προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διατήρηση ή αποθήκευση, η τροποποίηση, η εξαγωγή, η χρήση, η διαβίβαση, η διάδοση ή κάθε άλλης μορφής διάθεση, η συσχέτιση ή ο συνδυασμός, η διασύνδεση, η δέσμευση (κλείδωμα), η διαγραφή, η καταστροφή.

ε)"**Αρχείο δεδομένων προσωπικού χαρακτήρα**" ("αρχείο"), σύνολο δεδομένων προσωπικού χαρακτήρα, τα οποία αποτελούν ή μπορεί να αποτελέσουν αντικείμενο επεξεργασίας, και τα οποία τηρούνται είτε από το Δημόσιο ή από νομικό πρόσωπο δημοσίου δικαίου, ή ιδιωτικού δικαίου ή ένωση προσώπων ή φυσικό πρόσωπο.

στ)"**Διασύνδεση**", μορφή επεξεργασίας που συνίσταται στην δυνατότητα συσχέτισης των δεδομένων ενός αρχείου με δεδομένα αρχείου ή αρχείων που τηρούνται από άλλον ή άλλους υπεύθυνους επεξεργασίας ή που τηρούνται από τον ίδιο υπεύθυνο επεξεργασίας για άλλο σκοπό.

ζ)"**Υπεύθυνος επεξεργασίας**", οποιοσδήποτε καθορίζει τον σκοπό και τον τρόπο επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, όπως φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός. Όταν ο σκοπός και ο τρόπος της επεξεργασίας καθορίζονται με διατάξεις νόμου ή κανονιστικές διατάξεις εθνικού ή κοινοτικού δικαίου, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια βάσει των οποίων γίνεται η επιλογή του καθορίζονται αντίστοιχα από το εθνικό ή το κοινοτικό δίκαιο.

η)"**Εκτελών την επεξεργασία**", οποιοσδήποτε επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό υπεύθυνου επεξεργασίας, όπως φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός.

θ)"**Τρίτος**", κάθε φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία, ή οποιοσδήποτε άλλος οργανισμός, εκτός από το υποκείμενο των δεδομένων, τον υπεύθυνο επεξεργασίας και τα πρόσωπα που είναι εξουσιοδοτημένα να

επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα, εφόσον ενεργούν υπό την άμεση εποπτεία ή για λογαριασμό του υπεύθυνου επεξεργασίας.

ι)"**Αποδέκτης**", το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή ή υπηρεσία, ή οποιοσδήποτε άλλος οργανισμός, στον οποίο ανακοινώνονται ή μεταδίδονται τα δεδομένα, ανεξαρτήτως αν πρόκειται για τρίτο ή όχι.

ια)"**Συγκατάθεση**" του υποκειμένου των δεδομένων, κάθε ελεύθερη, ρητή και ειδική δήλωση βουλήσεως, που εκφράζεται με τρόπο σαφή, και εν πλήρη επίγνωση, και με την οποία, το υποκείμενο των δεδομένων, αφού προηγουμένως ενημερωθεί, δέχεται να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν. Η ενημέρωση αυτή περιλαμβάνει πληροφόρηση τουλάχιστον για τον σκοπό της επεξεργασίας, τα δεδομένα ή τις κατηγορίες δεδομένων που αφορά η επεξεργασία, τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων προσωπικού χαρακτήρα, καθώς και το όνομα, την επωνυμία και τη διεύθυνση του υπεύθυνου επεξεργασίας και του τυχόν εκπροσώπου του. Η συγκατάθεση μπορεί να ανακληθεί οποτεδήποτε, χωρίς αναδρομικό αποτέλεσμα.

ιβ)"**Αρχή**", η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα που θεσπίζεται στο κεφάλαιο Δ΄ του παρόντος νόμου.

**Άρθρο 3**

**Πεδίο εφαρμογής**

Οι διατάξεις του παρόντος νόμου εφαρμόζονται στην εν όλω ή εν μέρει αυτοματοποιημένη επεξεργασία καθώς και στη μη αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε αρχείο.

Οι διατάξεις του παρόντος νόμου δεν εφαρμόζονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα, η οποία πραγματοποιείται από φυσικό πρόσωπο για την άσκηση δραστηριοτήτων αποκλειστικά προσωπικών ή οικιακών.

Ο παρών νόμος εφαρμόζεται σε κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα, εφόσον αυτή εκτελείται:

α)Από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία, εγκατεστημένο στην Ελληνική Επικράτεια ή σε τόπο όπου βάσει του δημοσίου διεθνούς δικαίου εφαρμόζεται το ελληνικό δίκαιο.

β)Από υπεύθυνο επεξεργασίας μη εγκατεστημένο στην Ελληνική Επικράτεια ή σε τόπο όπου εφαρμόζεται το ελληνικό δίκαιο, όταν η επεξεργασία αφορά υποκείμενα εγκατεστημένα στην Ελληνική Επικράτεια. Στην περίπτωση αυτή, ο υπεύθυνος επεξεργασίας οφείλει να υποδείξει με γραπτή δήλωσή του προς την Αρχή εκπρόσωπο εγκατεστημένο στην Ελληνική Επικράτεια, ο οποίος υποκαθίσταται στα δικαιώματα και υποχρεώσεις του υπεύθυνου, χωρίς ο τελευταίος αυτός να απαλλάσσεται από τυχόν ιδιαίτερη ευθύνη του. Το αυτό ισχύει και όταν ο υπεύθυνος επεξεργασίας καλύπτεται από ετεροδικία, ασυλία, ή άλλο λόγο που κωλύει την ποινική δίωξη.
γ)Από υπεύθυνο επεξεργασίας που δεν είναι εγκατεστημένος στην επικράτεια Κράτους- Μέλους της Ευρωπαϊκής Ένωσης αλλά τρίτης χώρας και για τους σκοπούς της επεξεργασίας δεδομένων προσωπικού χαρακτήρα προσφεύγει σε μέσα, αυτοματοποιημένα ή όχι, ευρισκόμενα στην Ελληνική Επικράτεια, εκτός εάν τα μέσα αυτά χρησιμοποιούνται μόνο με σκοπό τη διέλευση από αυτήν. Στην περίπτωση αυτή, ο υπεύθυνος επεξεργασίας οφείλει να υποδείξει με γραπτή δήλωσή του προς την Αρχή εκπρόσωπο εγκατεστημένο στην Ελληνική Επικράτεια, ο οποίος υποκαθίσταται στα δικαιώματα και υποχρεώσεις του υπεύθυνου, χωρίς ο τελευταίος αυτός να απαλλάσσεται από τυχόν ιδιαίτερη ευθύνη του. Το αυτό ισχύει και όταν ο υπεύθυνος επεξεργασίας καλύπτεται από ετεροδικία, ασυλία ή άλλο λόγο που κωλύει την ποινική δίωξη.

## ΚΕΦΑΛΑΙΟ Β'
## ΕΠΕΞΕΡΓΑΣΙΑ ΔΕΔΟΜΕΝΩΝ
## ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

### Άρθρο 4
### Χαρακτηριστικά δεδομένων προσωπικού χαρακτήρα

1.Τα δεδομένα προσωπικού χαρακτήρα για να τύχουν νόμιμης επεξεργασίας πρέπει :
α)Να συλλέγονται κατά τρόπο θεμιτό και νόμιμο για καθορισμένους, σαφείς και νόμιμους σκοπούς και να υφίστανται θεμιτή και νόμιμη επεξεργασία ενόψει των σκοπών αυτών.

β)Να είναι συναφή, πρόσφορα, και όχι περισσότερα από όσα κάθε φορά απαιτείται εν όψει των σκοπών της επεξεργασίας.

γ)Να είναι ακριβή και, εφόσον χρειάζεται, να υποβάλλονται σε ενημέρωση.

δ)Να διατηρούνται σε μορφή που να επιτρέπει τον προσδιορισμό της ταυτότητας των υποκειμένων τους μόνο κατά τη διάρκεια της περιόδου που απαιτείται, κατά την κρίση της Αρχής, για την πραγματοποίηση των σκοπών της συλλογής τους και της επεξεργασίας τους. Μετά την παρέλευση της περιόδου αυτής, η Αρχή μπορεί, με αιτιολογημένη απόφασή της, να επιτρέπει τη διατήρηση δεδομένων προσωπικού χαρακτήρα για ιστορικούς επιστημονικούς ή στατιστικούς σκοπούς, εφ΄ όσον κρίνει ότι δεν θίγονται σε κάθε συγκεκριμένη περίπτωση τα δικαιώματα των υποκειμένων τους ή και τρίτων. Η τήρηση των διατάξεων της παραγράφου αυτής βαρύνει τον υπεύθυνο επεξεργασίας.

Δεδομένα προσωπικού χαρακτήρα που έχουν συλλεγεί ή υφίστανται επεξεργασία κατά παράβαση της προηγούμενης παραγράφου καταστρέφονται με ευθύνη του υπεύθυνου επεξεργασίας. Η Αρχή, εάν εξακριβώσει αυτεπαγγέλτως ή μετά από σχετική καταγγελία παράβαση των διατάξεων της προηγούμενης παραγράφου, επιβάλλει την διακοπή της συλλογής ή της επεξεργασίας και την καταστροφή των δεδομένων προσωπικού χαρακτήρα που έχουν ήδη συλλεχθεί ή τύχει επεξεργασίας.

**Άρθρο 5**

**Προϋποθέσεις επεξεργασίας**

Επεξεργασία δεδομένων προσωπικού χαρακτήρα επιτρέπεται μόνον όταν το υποκείμενο των δεδομένων έχει δώσει τη συγκατάθεσή του.

Κατ' εξαίρεση επιτρέπεται η επεξεργασία και χωρίς τη συγκατάθεση, όταν:

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

β)Η επεξεργασία είναι αναγκαία για την εκπλήρωση υποχρεώσεως του υπεύθυνου επεξεργασίας, η οποία επιβάλλεται από το νόμο.

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

δ)Η επεξεργασία είναι αναγκαία για την εκτέλεση έργου δημόσιου συμφέροντος ή έργου που εμπίπτει στην άσκηση δημόσιας εξουσίας και εκτελείται από δημόσια αρχή ή έχει ανατεθεί από αυτή είτε στον υπεύθυνο επεξεργασίας είτε σε τρίτο, στον οποίο γνωστοποιούνται τα δεδομένα.

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

Η Αρχή μπορεί να εκδίδει ειδικούς κανόνες επεξεργασίας για τις πλέον συνήθεις κατηγορίες επεξεργασιών και αρχείων, οι οποίες προφανώς δεν θίγουν τα δικαιώματα και τις ελευθερίες των προσώπων στα οποία αναφέρονται τα δεδομένα. Οι κατηγορίες αυτές προσδιορίζονται με κανονισμούς που καταρτίζει η Αρχή και κυρώνονται με προεδρικά διατάγματα, τα οποία εκδίδονται με πρόταση του Υπουργού Δικαιοσύνης.

**Άρθρο 6**

**Γνωστοποίηση αρχείων**

Ο υπεύθυνος επεξεργασίας υποχρεούται να γνωστοποιήσει εγγράφως στην Αρχή, τη σύσταση και λειτουργία αρχείου ή την έναρξη της επεξεργασίας.

Με τη γνωστοποίηση της προηγούμενης παραγράφου ο υπεύθυνος επεξεργασίας πρέπει απαραιτήτως να δηλώνει:

α)Το ονοματεπώνυμο ή την επωνυμία ή τον τίτλο του, καθώς και τη διεύθυνσή του, καθώς και το ονοματεπώνυμο ή την επωνυμία ή τον τίτλο και τη διεύθυνση των προσώπων που χρησιμοποιεί για την εκτέλεση της επεξεργασίας σύμφωνα με το άρθρο 10. Εάν ο υπεύθυνος επεξεργασίας δεν είναι εγκατεστημένος στην Ελληνική επικράτεια ή σε τόπο όπου εφαρμόζεται το ελληνικό δίκαιο, θα πρέπει επιπροσθέτως να δηλώνεται το ονοματεπώνυμο ή η επωνυμία ή ο τίτλος και η διεύθυνση του εκπροσώπου του στην Ελλάδα.

β)Τη διεύθυνση όπου είναι εγκατεστημένο το αρχείο ή ο κύριος εξοπλισμός που υποστηρίζει την επεξεργασία.

γ)Την περιγραφή του σκοπού της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που περιέχονται ή πρόκειται να περιληφθούν στο αρχείο.

δ)Το είδος των δεδομένων προσωπικού χαρακτήρα που υφίστανται ή πρόκειται να υποστούν επεξεργασία ή περιέχονται ή πρόκειται να περιληφθούν στο αρχείο.
ε)Το χρονικό διάστημα για το οποίο προτίθεται να εκτελεί την επεξεργασία ή να διατηρήσει το αρχείο.
στ)Τους αποδέκτες ή τις κατηγορίες αποδεκτών στους οποίους ανακοινώνει ή ενδέχεται να ανακοινώνει τα δεδομένα προσωπικού χαρακτήρα.
ζ)Τις ενδεχόμενες διαβιβάσεις και το σκοπό της διαβίβασης δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες.
η)Τα βασικά χαρακτηριστικά του συστήματος και των μέτρων ασφαλείας του αρχείου ή της επεξεργασίας.
θ)Στην περίπτωση που η επεξεργασία ή το αρχείο εμπίπτει σε μία από τις κατηγορίες για τις οποίες η Αρχή έχει εκδώσει ειδικούς κανόνες επεξεργασίας ο υπεύθυνος επεξεργασίας καταθέτει στην Αρχή δήλωση με την οποία βεβαιώνει ότι η επεξεργασία θα διεξάγεται ή το αρχείο θα τηρείται σύμφωνα με τους ειδικούς κανόνες που έχει θεσπίσει η Αρχή, η οποία προσδιορίζει ειδικότερα τον τύπο και το περιεχόμενο της δήλωσης.

3.Τα στοιχεία της προηγούμενης παραγράφου καταχωρίζονται στο Μητρώο Αρχείων και Επεξεργασιών που τηρεί η Αρχή. Κάθε μεταβολή των στοιχείων που αναφέρονται στην παράγραφο 2 πρέπει να γνωστοποιείται εγγράφως και χωρίς καθυστέρηση από τον υπεύθυνο στην Αρχή.

**Άρθρο 7**

**Επεξεργασία ευαίσθητων δεδομένων**

Απαγορεύεται η συλλογή και η επεξεργασία ευαίσθητων δεδομένων.
Κατ΄ εξαίρεση επιτρέπεται η συλλογή και η επεξεργασία ευαίσθητων δεδομένων, καθώς και η ίδρυση και λειτουργία σχετικού αρχείου, ύστερα από άδεια της Αρχής, όταν συντρέχουν μία ή περισσότερες από τις ακόλουθες προϋποθέσεις:
α)Το υποκείμενο έδωσε τη γραπτή συγκατάθεσή του εκτός εάν η συγκατάθεση έχει αποσπασθεί με τρόπο που αντίκειται στο νόμο ή τα χρηστά ήθη ή νόμος ορίζει ότι η συγκατάθεση δεν αίρει την απαγόρευση.

β)Η επεξεργασία είναι αναγκαία για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου, εάν τούτο τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του.

γ)Η επεξεργασία αφορά αποκλειστικά δεδομένα του υποκειμένου, τα οποία δημοσιοποιεί ή του είναι αναγκαία για την αναγνώριση ή άσκηση ή υπεράσπιση δικαιώματός του ενώπιον δικαστηρίου.

δ)Η επεξεργασία αφορά θέματα υγείας και εκτελείται από πρόσωπο που ασχολείται κατ' επάγγελμα με την παροχή υπηρεσιών υγείας και υπόκειται σε καθήκον εχεμύθειας ή σε συναφείς κώδικες δεοντολογίας, υπό τον όρο ότι η επεξεργασία είναι απαραίτητη για την ιατρική πρόληψη, διάγνωση, περίθαλψη ή τη διαχείριση υπηρεσιών υγείας.

ε)Η επεξεργασία είναι απαραίτητη για την εξυπηρέτηση των αναγκών της εθνικής ασφάλειας, καθώς επίσης και για την εξυπηρέτηση των αναγκών της εγκληματολογικής ή σωφρονιστικής πολιτικής, όταν εκτελείται από δημόσια Αρχή και αφορά τη διακρίβωση εγκλημάτων, ποινικές καταδίκες και μέτρα ασφάλειας.

στ)Η επεξεργασία πραγματοποιείται για ερευνητικούς και επιστημονικούς αποκλειστικά σκοπούς και υπό τον όρο ότι τηρείται η ανωνυμία και λαμβάνονται όλα τα απαραίτητα μέτρα για την προστασία των δικαιωμάτων των προσώπων στα οποία αναφέρονται.

ζ)Η επεξεργασία αφορά δεδομένα δημοσίων προσώπων, εφόσον αυτά συνδέονται με την άσκηση δημοσίου λειτουργήματος ή τη διαχείριση συμφερόντων τρίτων, και πραγματοποιείται αποκλειστικά για την άσκηση του δημοσιογραφικού επαγγέλματος. Η άδεια της αρχής χορηγείται μόνο εφόσον η επεξεργασία είναι απολύτως αναγκαία για την εξασφάλιση του δικαιώματος πληροφόρησης επί θεμάτων δημοσίου ενδιαφέροντος καθώς και στο πλαίσιο καλλιτεχνικής έκφρασης και εφόσον δεν παραβιάζεται καθ' οιονδήποτε τρόπο το δικαίωμα προστασίας της ιδιωτικής και οικογενειακής ζωής.

Η Αρχή χορηγεί άδεια συλλογής και επεξεργασίας ευαίσθητων δεδομένων, καθώς και άδεια ιδρύσεως και λειτουργίας σχετικού αρχείου, ύστερα από αίτηση του υπεύθυνου επεξεργασίας. Εφ' όσον η Αρχή διαπιστώσει ότι πραγματοποιείται επεξεργασία ευαίσθητων δεδομένων, η γνωστοποίηση αρχείου, σύμφωνα με το άρθρο 6 του παρόντος νόμου, επέχει θέση αιτήσεως για τη χορήγηση άδειας. Η Αρχή μπορεί να επιβάλλει όρους και προϋποθέσεις για την αποτελεσματικότερη προστασία του

δικαιώματος ιδιωτικής ζωής των υποκειμένων ή τρίτων. Πριν χορηγήσει την άδεια, η Αρχή καλεί σε ακρόαση τον υπεύθυνο επεξεργασίας ή τον εκπρόσωπο του και τον εκτελούντα την επεξεργασία.

4.Η άδεια εκδίδεται για ορισμένο χρόνο, ανάλογα με τον σκοπό της επεξεργασίας. Μπορεί να ανανεωθεί ύστερα από αίτηση του υπεύθυνου επεξεργασίας.

5.Η άδεια περιέχει απαραιτήτως:
α)Το ονοματεπώνυμο ή την επωνυμία ή τον τίτλο καθώς και τη διεύθυνση του υπεύθυνου επεξεργασίας και του τυχόν εκπροσώπου του.
β)Τη διεύθυνση όπου είναι εγκατεστημένο το αρχείο.
γ)Το είδος των δεδομένων προσωπικού χαρακτήρα που επιτρέπεται να περιληφθούν στο αρχείο.
δ)Το χρονικό διάστημα για το οποίο χορηγείται η άδεια.
ε)Τους τυχόν όρους και προϋποθέσεις που έχει επιβάλει η Αρχή για την ίδρυση και λειτουργία του αρχείου.
στ)Την υποχρέωση γνωστοποίησής του ή των αποδεκτών ευθύς ως εξατομικευτούν.

6.Αντίγραφο της άδειας καταχωρίζεται στο Μητρώο Αδειών που διατηρεί η Αρχή.

7.Κάθε μεταβολή των στοιχείων που αναφέρονται στην παράγραφο 5 γνωστοποιείται χωρίς καθυστέρηση στην Αρχή. Κάθε άλλη μεταβολή, πλην της διεύθυνσης του υπευθύνου ή του εκπροσώπου του, συνεπάγεται την έκδοση νέας άδειας, εφόσον συντρέχουν οι νόμιμες προϋποθέσεις.

**Άρθρο 8**
**Διασύνδεση αρχείων**

Διασύνδεση αρχείων επιτρέπεται μόνον υπό τους όρους του παρόντος άρθρου.
Κάθε διασύνδεση γνωστοποιείται στην Αρχή με δήλωση την οποία υποβάλλουν από κοινού οι υπεύθυνοι επεξεργασίας ή ο υπεύθυνος επεξεργασίας που διασυνδέει δύο ή περισσότερα αρχεία που εξυπηρετούν διαφορετικούς σκοπούς.

Εάν ένα τουλάχιστον από τα αρχεία που πρόκειται να διασυνδεθούν περιέχει ευαίσθητα δεδομένα, ή εάν η διασύνδεση έχει ως συνέπεια την αποκάλυψη ευαίσθητων δεδομένων, ή εάν για την πραγματοποίηση της διασύνδεσης, πρόκειται να γίνει χρήση ενιαίου κωδικού αριθμού, η διασύνδεση επιτρέπεται μόνον με προηγούμενη άδεια της Αρχής (άδεια διασύνδεσης).

Η άδεια διασύνδεσης της προηγούμενης παραγράφου χορηγείται ύστερα από ακρόαση των υπεύθυνων επεξεργασίας των αρχείων και περιέχει απαραιτήτως:

α)Τον σκοπό για τον οποίο η διασύνδεση θεωρείται αναγκαία.

β)Το είδος των δεδομένων προσωπικού χαρακτήρα που αφορά η διασύνδεση.

γ)Το χρονικό διάστημα για το οποίο επιτρέπεται η διασύνδεση.

δ)Τους τυχόν όρους και προϋποθέσεις για την αποτελεσματικότερη προστασία των δικαιωμάτων και ελευθεριών και ιδίως του δικαιώματος ιδιωτικής ζωής των υποκειμένων ή τρίτων.

Η άδεια διασύνδεσης μπορεί να ανανεωθεί ύστερα από αίτηση των υπεύθυνων επεξεργασίας.

Οι δηλώσεις της παρ. 2 του παρόντος άρθρου καθώς και αντίγραφα των αδειών διασύνδεσης καταχωρίζονται στο Μητρώο Διασυνδέσεων που τηρεί η Αρχή.

**Άρθρο 9**

**Διασυνοριακή ροή δεδομένων προσωπικού χαρακτήρα**

Η διαβίβαση δεδομένων προσωπικού χαρακτήρα 2ίβαση δεδομένων προσωπικού χαρακτήρα σε χώρες της Ευρωπαϊκής Ένωσης είναι ελεύθερη. Η διαβίβαση προς χώρα που δεν ανήκει στην Ευρωπαϊκή Ένωση δεδομένων προσωπικού χαρακτήρα τα οποία έχουν υποστεί ή πρόκειται να υποστούν επεξεργασία μετά τη διαβίβασή τους, επιτρέπεται ύστερα από άδεια της Αρχής. Η Αρχή παρέχει την άδεια μόνον εάν κρίνει ότι η εν λόγω χώρα εξασφαλίζει ικανοποιητικό επίπεδο προστασίας. Προς τούτο, λαμβάνει υπ' όψη ιδίως τη φύση των δεδομένων, τους σκοπούς και τη διάρκεια της επεξεργασίας, τους σχετικούς γενικούς και ειδικούς κανόνες δικαίου, τους κώδικες δεοντολογίας, τα μέτρα ασφαλείας για την προστασία δεδομένων προσωπικού χαρακτήρα, καθώς και το επίπεδο προστασίας των χωρών προέλευσης, διέλευσης και τελικού προορισμού των δεδομένων.

Η διαβίβαση δεδομένων προσωπικού χαρακτήρα προς χώρα που δεν ανήκει στην Ευρωπαϊκή Ένωση και η οποία δεν εξασφαλίζει ικανοποιητικό επίπεδο προστασίας, επιτρέπεται κατ' εξαίρεση, με άδεια της Αρχής, εφ' όσον συντρέχει μία ή περισσότερες από τις κατωτέρω προϋποθέσεις:

α)Το υποκείμενο των δεδομένων έδωσε τη συγκατάθεσή του για τη διαβίβαση, εκτός εάν η συγκατάθεση έχει αποσπασθεί με τρόπο που να αντίκειται στο νόμο ή τα χρηστά ήθη.

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

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

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

ε)Η μετάδοση, το οποίο κατά το νόμο προορίζεται για την παροχή πληροφοριών στο κοινό και είναι προσιτό στο κοινό ή σε κάθε πρόσωπο που αποδεικνύει έννομο συμφέρον, εφόσον στη συγκεκριμένη περίπτωση πληρούνται οι νόμιμες προϋποθέσεις για την πρόσβαση στο μητρώο.

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

**Άρθρο 10**

**Απόρρητο και ασφάλεια της επεξεργασίας**

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι απόρρητη. Διεξάγεται αποκλειστικά και μόνο από πρόσωπα που τελούν υπό τον έλεγχο του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία και μόνον κατ' εντολήν του.

Για τη διεξαγωγή της επεξεργασίας ο υπεύθυνος επεξεργασίας οφείλει να επιλέγει πρόσωπα με αντίστοιχα επαγγελματικά προσόντα που παρέχουν επαρκείς εγγυήσεις από πλευράς τεχνικών γνώσεων και προσωπικής ακεραιότητας για την τήρηση του απορρήτου.

Ο υπεύθυνος επεξεργασίας οφείλει να λαμβάνει τα κατάλληλα οργανωτικά και τεχνικά μέτρα για την ασφάλεια των δεδομένων και την προστασία τους από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας. Αυτά τα μέτρα πρέπει να εξασφαλίζουν επίπεδο ασφαλείας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων που είναι αντικείμενο της επεξεργασίας. Η Αρχή παρέχει εκάστοτε οδηγίες για τον βαθμό ασφαλείας των δεδομένων καθώς και για τα μέτρα προστασίας που είναι αναγκαίο να λαμβάνονται για κάθε κατηγορία δεδομένων, εν' όψει και των τεχνολογικών εξελίξεων.

Αν η επεξεργασία διεξάγεται για λογαριασμό του υπεύθυνου από πρόσωπο μη εξαρτώμενο από αυτόν, η σχετική ανάθεση γίνεται υποχρεωτικά εγγράφως. Η ανάθεση προβλέπει υποχρεωτικά ότι ο ενεργών την επεξεργασία την διεξάγει μόνο κατ' εντολήν του υπεύθυνου και ότι οι λοιπές υποχρεώσεις του παρόντος άρθρου βαρύνουν αναλόγως και αυτόν.

## ΚΕΦΑΛΑΙΟ Γ΄

## ΔΙΚΑΙΩΜΑΤΑ ΤΟΥ ΥΠΟΚΕΙΜΕΝΟΥ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

**Άρθρο 11**

**Δικαίωμα ενημέρωσης**

Ο υπεύθυνος επεξεργασίας οφείλει, κατά το στάδιο της συλλογής δεδομένων προσωπικού χαρακτήρα, να ενημερώνει με τρόπο πρόσφορο και σαφή το υποκείμενο για τα εξής τουλάχιστον στοιχεία:

α)την ταυτότητά του και την ταυτότητα του τυχόν εκπροσώπου του.

β)τον σκοπό της επεξεργασίας.

γ)του αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων.

δ) την ύπαρξη του δικαιώματος πρόσβασης

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

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

Με απόφαση της Αρχής, ύστερα από αίτηση του υπεύθυνου επεξεργασίας, η υποχρέωση ενημέρωσης, σύμφωνα με τις παρ. 1 και 3 του παρόντος άρθρου, μπορεί να αρθεί, εν όλω ή εν μέρει, εφ' όσον η συλλογή δεδομένων προσωπικού χαρακτήρα γίνεται για λόγους εθνικής ασφάλειας ή για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων.

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

**Άρθρο 12**

**Δικαίωμα πρόσβασης**

Καθένας έχει δικαίωμα να γνωρίζει εάν δεδομένα προσωπικού χαρακτήρα που τον αφορούν αποτελούν ή αποτέλεσαν αντικείμενο επεξεργασίας. Προς τούτο, ο υπεύθυνος επεξεργασίας, έχει υποχρέωση να του απαντήσει εγγράφως.

Το υποκείμενο των δεδομένων έχει δικαίωμα να ζητεί και να λαμβάνει από τον υπεύθυνο επεξεργασίας, χωρίς καθυστέρηση και κατά τρόπο εύληπτο και σαφή, τις ακόλουθες πληροφορίες:

α)Όλα τα δεδομένα προσωπικού χαρακτήρα που το αφορούν, καθώς και την προέλευσή τους.

β)Τους σκοπούς της επεξεργασίας, τους αποδέκτες ή τις κατηγορίες αποδεκτών.

γ)Την εξέλιξη της επεξεργασίας για το χρονικό διάστημα από την προηγούμενη ενημέρωση ή πληροφόρησή του.

δ)Τη λογική της αυτοματοποιημένης επεξεργασίας.

Το δικαίωμα πρόσβασης μπορεί να ασκείται από το υποκείμενο των δεδομένων και με τη συνδρομή ειδικού.

3.Το δικαίωμα της προηγούμενης παραγράφου και τα δικαιώματα του άρθρου 13 ασκούνται με την υποβολή της σχετικής αίτησης στον υπεύθυνο της επεξεργασίας και ταυτόχρονη καταβολή χρηματικού ποσού, το ύψος του οποίου, ο τρόπος καταβολής του και κάθε άλλο συναφές ζήτημα ρυθμίζονται με απόφαση της Αρχής. Το ποσό αυτό επιστρέφεται στον αιτούντα εάν το αίτημα διόρθωσης ή διαγραφής των δεδομένων κριθεί βάσιμο είτε από τον υπεύθυνο της επεξεργασίας είτε από την Αρχή, σε περίπτωση προσφυγής του σ' αυτήν. Ο υπεύθυνος έχει υποχρέωση στην περίπτωση αυτή να χορηγήσει στον αιτούντα, χωρίς καθυστέρηση δωρεάν και σε γλώσσα κατανοητή, αντίγραφο του διορθωμένου μέρους της επεξεργασίας που τον αφορά.

4.Εάν ο υπεύθυνος επεξεργασίας δεν απαντήσει εντός δεκαπέντε (15) ημερών ή εάν η απάντησή του δεν είναι ικανοποιητική, το υποκείμενο των δεδομένων έχει δικαίωμα να προσφύγει στην Αρχή. Στην περίπτωση κατά την οποία ο υπεύθυνος επεξεργασίας αρνηθεί να ικανοποιήσει το αίτημα του ενδιαφερόμενου, κοινοποιεί την απάντησή του στην Αρχή και ενημερώνει τον ενδιαφερόμενο ότι μπορεί να προσφύγει σε αυτήν.

προώθησης πωλήσεως αγαθών ή παροχής υπηρεσιών εξ αποστάσεως. Η Αρχή τηρεί μητρώο με τα στοιχεία ταυτότητας των ανωτέρω. Οι υπεύθυνοι επεξεργασίας των σχετικών αρχείων έχουν την υποχρέωση να συμβουλεύονται πριν από κάθε επεξεργασία το εν λόγω μητρώο και να διαγράφουν από το αρχείο τους τα πρόσωπα της παραγράφου αυτής.

**Άρθρο 14**

**Δικαίωμα προσωρινής δικαστικής προστασίας**

Καθένας έχει δικαίωμα να ζητήσει από το αρμόδιο κάθε φορά δικαστήριο την άμεση αναστολή ή μη εφαρμογή πράξης ή απόφασης που τον θίγει, την οποία έχει λάβει διοικητική αρχή, νομικό πρόσωπο δημοσίου δικαίου ή ιδιωτικού δικαίου ή ένωση προσώπων ή φυσικό πρόσωπο αποκλειστικά με αυτοματοποιημένη επεξεργασία στοιχείων, εφόσον η επεξεργασία αυτή αποβλέπει στην αξιολόγηση της προσωπικότητάς του και ιδίως της αποδοτικότητάς του στην εργασία, της οικονομικής φερεγγυότητάς του, της αξιοπιστίας του και της εν γένει συμπεριφοράς του.

Το δικαίωμα του παρόντος άρθρου μπορεί να ικανοποιηθεί και όταν δεν συντρέχουν οι λοιπές ουσιαστικές προϋποθέσεις της προσωρινής δικαστικής προστασίας, όπως προβλέπονται κάθε φορά.

## ΚΕΦΑΛΑΙΟ Δ΄

## ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

**Άρθρο 15**

**Σύσταση - αποστολή - νομική φύση**

Συνιστάται Αρχή Προστασίας Δεδομένων αποστολή την εποπτεία της εφαρμογής του παρόντος νόμου και άλλων ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα καθώς και την ενάσκηση των αρμοδιοτήτων που της ανατίθενται κάθε φορά.

5.Με απόφαση της Αρχής, ύστερα από αίτηση του υπεύθυνου επεξεργασίας, η υποχρέωση πληροφόρησης, σύμφωνα με τις παρ. 1 και 2 του παρόντος άρθρου, μπορεί να αρθεί, εν όλω ή εν μέρει, εφ' όσον η επεξεργασία δεδομένων προσωπικού χαρακτήρα γίνεται για λόγους εθνικής ασφάλειας ή για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων. Στην περίπτωση αυτή ο Πρόεδρος της Αρχής ή ο αναπληρωτής του προβαίνει σε όλες τις αναγκαίες ενέργειες και έχει ελεύθερη πρόσβαση στο αρχείο.

6.Δεδομένα που αφορούν την υγεία γνωστοποιούνται στο υποκείμενο μέσω ιατρού.

**Άρθρο 13**

**Δικαίωμα αντίρρησης**

Το υποκείμενο των δεδομένων έχει δικαίωμα να προβάλλει οποτεδήποτε αντιρρήσεις για την επεξεργασία δεδομένων που το αφορούν. Οι αντιρρήσεις απευθύνονται εγγράφως στον υπεύθυνο επεξεργασίας και πρέπει να περιέχουν αίτημα για συγκεκριμένη ενέργεια, όπως διόρθωση, προσωρινή μη χρησιμοποίηση, δέσμευση, μη διαβίβαση ή διαγραφή. Ο υπεύθυνος επεξεργασίας έχει την υποχρέωση να απαντήσει εγγράφως επί των αντιρρήσεων μέσα σε αποκλειστική προθεσμία δεκαπέντε (15) ημερών. Στην απάντησή του οφείλει να ενημερώσει το υποκείμενο για τις ενέργειες στις οποίες προέβη ή, ενδεχομένως, για τους λόγους που δεν ικανοποίησε το αίτημα. Η απάντηση σε περίπτωση απόρριψης των αντιρρήσεων πρέπει να κοινοποιείται και στην Αρχή.

2.Εάν ο υπεύθυνος επεξεργασίας δεν απαντήσει εμπροθέσμως ή η απάντησή του δεν είναι ικανοποιητική, το υποκείμενο των δεδομένων έχει δικαίωμα να προσφύγει στην Αρχή και να ζητήσει την εξέταση των αντιρρήσεών του. Εάν η Αρχή πιθανολογήσει ότι οι αντιρρήσεις είναι εύλογες και ότι συντρέχει κίνδυνος σοβαρής βλάβης του υποκειμένου από την συνέχιση της επεξεργασίας, μπορεί να επιβάλλει την άμεση αναστολή της επεξεργασίας έως ότου εκδώσει οριστική απόφαση επί των αντιρρήσεων.

3.Καθένας έχει δικαίωμα να δηλώσει στην Αρχή ότι δεδομένα που τον αφορούν δεν επιθυμεί να αποτελέσουν αντικείμενο επεξεργασίας από οποιονδήποτε, για λόγους

Η Αρχή αποτελεί ανεξάρτητη δημόσια αρχή, έχει δικό της προϋπολογισμό και εξυπηρετείται από δική της γραμματεία. Η Αρχή δεν υπόκειται σε οποιονδήποτε διοικητικό έλεγχο. Κατά την άσκηση των καθηκόντων τους τα μέλη της Αρχής απολαύουν προσωπικής και λειτουργικής ανεξαρτησίας. Η Αρχή υπάγεται στον Υπουργό Δικαιοσύνης και εδρεύει στην Αθήνα.

Τον προϋπολογισμό της Αρχής εισηγείται ο Υπουργός Δικαιοσύνης, ύστερα από πρόταση της Αρχής. Ποσοστό των κάθε είδους εσόδων του Δημοσίου από την εφαρμογή του παρόντος νόμου, συμπεριλαμβανομένων των παραβόλων και προστίμων που επιβάλλει η Αρχή, διατίθεται για τις ανάγκες της Αρχής. Το ποσοστό αυτό καθορίζεται κάθε φορά με κοινή απόφαση των Υπουργών Οικονομικών και Δικαιοσύνης.

**Άρθρο 16**

**Συγκρότηση της Αρχής**

Η Αρχή συγκροτείται από έναν δικαστικό λειτουργό βαθμού Συμβούλου της Επικρατείας ή αντίστοιχου και άνω, ως Πρόεδρο, και έξι μέλη ως εξής:

α)Έναν καθηγητή ή αναπληρωτή καθηγητή ΑΕΙ σε γνωστικό αντικείμενο του δικαίου.

β)Έναν καθηγητή ή αναπληρωτή καθηγητή ΑΕΙ σε γνωστικό αντικείμενο της πληροφορικής.

γ)Έναν καθηγητή ή αναπληρωτή καθηγητή Α.Ε.Ι.

δ, ε, στ) Τρία πρόσωπα κύρους και εμπειρίας στον τομέα της προστασίας δεδομένων προσωπικού χαρακτήρα.

Ο δικαστικός λειτουργός - Πρόεδρος και οι καθηγητές - μέλη μπορεί να είναι εν ενεργεία ή μη.

2.Ο Πρόεδρος της Αρχής είναι πλήρους και αποκλειστικής απασχόλησης και διορίζεται με προεδρικό διάταγμα, που εκδίδεται με πρόταση του Υπουργικού Συμβουλίου, ύστερα από εισήγηση του Υπουργού Δικαιοσύνης. Εάν για τη θέση του Προέδρου επιλεγεί εν ενεργεία δικαστικός λειτουργός, απαιτείται απόφαση του οικείου Ανώτατου Δικαστικού Συμβουλίου. Με την ίδια διαδικασία επιλέγεται και διορίζεται ο αναπληρωτής του Προέδρου.

Τα μέλη της Αρχής διορίζονται με την εξής διαδικασία: ο Υπουργό Δικαιοσύνης υποβάλλει στον Πρόεδρο της Βουλής πρόταση για το διορισμό των έξι τακτικών μελών της Αρχής και των ισάριθμων αναπληρωτών τους. Η πρόταση περιλαμβάνει διπλάσιο αριθμό υποψηφίων. Ο Πρόεδρος της Βουλής διαβιβάζει την πρόταση στην Επιτροπή Θεσμών και Διαφάνειας, η οποία διατυπώνει γνώμη. Τα τακτικά μέλη της Αρχής και οι αντίστοιχοι αναπληρωτές τους επιλέγονται από τη Διάσκεψη των Προέδρων. Οι επιλεγέντες διορίζονται με προεδρικό διάταγμα, που εκδίδεται με πρόταση του Υπουργού Δικαιοσύνης και δημοσιεύεται στην Εφημερίδα της Κυβερνήσεως.

Ο Πρόεδρος και τα μέλη της Αρχής διορίζονται με θητεία. Η θητεία τους είναι τετραετής και μπορεί να ανανεωθεί μία μόνο φορά. Κανείς δεν μπορεί να υπηρετήσει συνολικά περισσότερο από οκτώ (8) χρόνια. Η σύνθεση των έξι μελών της Αρχής ανανεώνεται κατά το ήμισυ ανά διετία. Μετά την πρώτη συγκρότηση της Αρχής, γίνεται κλήρωση μεταξύ των έξι τακτικών μελών της, ώστε τρία να έχουν τετραετή θητεία και τρία διετή.

Ο Πρόεδρος και τα μέλη της Αρχής διορίζονται με ισάριθμους αναπληρωτές, οι οποίοι πρέπει να διαθέτουν τις αυτές ιδιότητες και προσόντα. Οι αναπληρωτές του Προέδρου και των μελών μετέχουν στις συνεδριάσεις της Αρχής μόνο σε περίπτωση προσωρινής απουσίας ή κωλύματος του αντίστοιχου τακτικού. Με απόφασή του ο Πρόεδρος της Αρχής αναθέτει ειδικά καθήκοντα στους αναπληρωτές. Η θητεία του κάθε αναπληρωτή είναι ίση με τη θητεία του αντίστοιχου τακτικού.

**Άρθρο 17**

**Κωλύματα - ασυμβίβαστα μελών της Αρχής**

Δεν μπορεί να διορισθεί μέλος της Αρχής:

α)Υπουργός, υφυπουργός, γενικός γραμματέας υπουργείου ή αυτοτελούς γενικής γραμματείας και βουλευτής.

β)Διοικητής, διευθυντής, διαχειριστής, μέλος του διοικητικού συμβουλίου ή ασκών διευθυντικά καθήκοντα εν γένει σε επιχείρηση η οποία παράγει, μεταποιεί, διαθέτει ή εμπορεύεται υλικά χρησιμοποιούμενα στην πληροφορική ή τις τηλεπικοινωνίες ή παρέχει υπηρεσίες σχετικές με την πληροφορική, τις τηλεπικοινωνίες ή την

επεξεργασία δεδομένων προσωπικού χαρακτήρα καθώς και οι συνδεόμενοι με σύμβαση έργου με τέτοια επιχείρηση.

Εκπίπτει αυτοδικαίως από την ιδιότητα του μέλους της Αρχής όποιος, μετά το διορισμό του:

α)Αποκτά μία από τις ιδιότητες που συνιστούν κώλυμα διορισμού, σύμφωνα με την προηγούμενη παράγραφο.

β)Προβαίνει σε πράξεις ή αναλαμβάνει οποιαδήποτε εργασία ή έργο ή αποκτά άλλη ιδιότητα που, κατά την κρίση της Αρχής, δεν συμβιβάζονται με τα καθήκοντά του ως μέλους της Αρχής.

Στην διαπίστωση των ασυμβίβαστων της προηγούμενης παραγράφου προβαίνει η Αρχή, χωρίς συμμετοχή του μέλους της, στο πρόσωπο του οποίου ενδέχεται να συντρέχει το ασυμβίβαστο. Η Αρχή αποφασίζει ύστερα από ακρόαση του εν λόγω μέλους. Την διαδικασία κινεί είτε ο Πρόεδρος της Αρχής είτε ο Υπουργός Δικαιοσύνης.

Απώλεια της ιδιότητας βάσει της οποίας μέλος της Αρχής διορίσθηκε, σύμφωνα με την παρ.1 του άρθρου 16 του παρόντος νόμου, συνεπάγεται την αυτοδίκαιη έκπτωσή του αν οφείλεται σε αμετάκλητη πειθαρχική ή ποινική καταδίκη.

**Άρθρο 18**

**Υποχρεώσεις και δικαιώματα μελών της Αρχής**

Κατά την άσκηση των καθηκόντων τους τα μέλη της Αρχής υπακούουν στη συνείδησή τους και το νόμο. Υπόκεινται στο καθήκον εχεμύθειας. Ως μάρτυρες ή πραγματογνώμονες μπορούν να καταθέτουν στοιχεία που αφορούν αποκλειστικά και μόνο την τήρηση των διατάξεων του παρόντος νόμου από υπεύθυνους επεξεργασίας. Το καθήκον εχεμύθειας υφίσταται και μετά την με οποιονδήποτε τρόπο αποχώρηση των μελών της Αρχής.

Με απόφαση των Υπουργών Οικονομικών και Δικαιοσύνης καθορίζονται οι μηνιαίες αποδοχές του Προέδρου και των μελών της Αρχής καθώς και η αποζημίωση τους για κάθε συνεδρίαση, κατά παρέκκλιση από κάθε άλλη διάταξη. Στους αναπληρωτές καταβάλλεται το ένα τρίτο (1/3) των μηνιαίων αποδοχών των μελών της Αρχής και αποζημίωση για κάθε συνεδρίαση στην οποία μετέχουν. Οι διατάξεις για τις δαπάνες κινήσεως των μετακινουμένων προσώπων με εντολή του Δημοσίου για εκτέλεση

υπηρεσίας που ισχύουν κάθε φορά έχουν εφαρμογή και για την μετακίνηση των μελών και των υπαλλήλων της Γραμματείας της Αρχής. Ο Πρόεδρος της Αρχής εκδίδει τις σχετικές εντολές μετακίνησης.

Για κάθε παράβαση των υποχρεώσεών τους που απορρέουν από τον παρόντα νόμο, τα μέλη της Αρχής υπέχουν πειθαρχική ευθύνη. Την πειθαρχική αγωγή ασκεί ενώπιον του πειθαρχικού συμβουλίου ο Υπουργός Δικαιοσύνης για τον Πρόεδρο και τα μέλη της Αρχής και ο Πρόεδρος της Αρχής για τα μέλη της. Το πειθαρχικό συμβούλιο συντίθεται από έναν Αντιπρόεδρο του Συμβουλίου της Επικρατείας, ως πρόεδρο, έναν Αρεοπαγίτη, ένα Σύμβουλο του Ελεγκτικού Συνεδρίου και δύο Καθηγητές Α.Ε.Ι. σε γνωστικό αντικείμενο του δικαίου. Χρέη γραμματέα του συμβουλίου εκτελεί υπάλληλος της Αρχής. Ο πρόεδρος, τα μέλη και ο γραμματέας του συμβουλίου ορίζονται με ισάριθμους αναπληρωτές. Για τα μέλη του συμβουλίου που είναι δικαστικοί λειτουργοί απαιτείται απόφαση του οικείου ανώτατου δικαστικού συμβουλίου. Το συμβούλιο συγκροτείται με απόφαση του Υπουργού Δικαιοσύνης με τριετή θητεία. Το συμβούλιο συνεδριάζει με την παρουσία τεσσάρων τουλάχιστον μελών, μεταξύ των οποίων οπωσδήποτε ο πρόεδρος ή ο αναπληρωτής του, και αποφασίζει με απόλυτη πλειοψηφία των παρόντων. Σε περίπτωση ισοψηφίας υπερισχύει η ψήφος του προέδρου. Αν υπάρχουν περισσότερες από δύο γνώμες, οι ακολουθούντες την ασθενέστερη οφείλουν να προσχωρήσουν σε μία από τις επικρατέστερες. Το πειθαρχικό συμβούλιο αποφασίζει σε πρώτο και τελευταίο βαθμό την απαλλαγή ή την παύση του εγκαλουμένου. Η αμοιβή του προέδρου, των μελών και του γραμματέα του συμβουλίου καθορίζεται με κοινή απόφαση των Υπουργών Οικονομικών και Δικαιοσύνης κατά παρέκκλιση κάθε άλλης διατάξεως.

4.Μέλος της Αρχής που, κατά παράβαση του παρόντος νόμου, γνωστοποιεί με οποιονδήποτε τρόπο δεδομένα προσωπικού χαρακτήρα που είναι προσιτά σε αυτό λόγω της υπηρεσίας του ή αφήνει άλλον να λάβει γνώση αυτών, τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών και χρηματική ποινή τουλάχιστον δύο εκατομμυρίων (2.000.000) δραχμών έως δέκα εκατομμυρίων (10.000.000) δραχμών. Αν όμως τέλεσε την πράξη με σκοπό να προσπορίσει στον εαυτό του ή σε άλλο αθέμιτο όφελος ή να βλάψει άλλον, επιβάλλεται κάθειρξη. Αν η πράξη του πρώτου εδαφίου τελέστηκε από αμέλεια επιβάλλεται φυλάκιση τουλάχιστον τριών (3) μηνών και χρηματική ποινή.

**Άρθρο 19**

**Αρμοδιότητες, λειτουργία και αποφάσεις της Αρχής**

Η Αρχή έχει τις εξής ιδίως αρμοδιότητες:

α)Εκδίδει οδηγίες προς τον σκοπό ενιαίας εφαρμογής των ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

β)Καλεί και επικουρεί τα επαγγελματικά σωματεία και τις λοιπές ενώσεις φυσικών ή νομικών προσώπων που διατηρούν αρχεία δεδομένων προσωπικού χαρακτήρα στην κατάρτιση κωδίκων δεοντολογίας για την αποτελεσματικότερη προστασία της ιδιωτικής ζωής και των εν γένει δικαιωμάτων και θεμελιωδών ελευθεριών των φυσικών προσώπων στον τομέα της δραστηριότητάς τους.

γ)Απευθύνει συστάσεις και υποδείξεις στους υπεύθυνους επεξεργασίας ή τους τυχόν εκπροσώπους τους και δίδει κατά την κρίση της δημοσιότητα σε αυτές.

δ)Χορηγεί τις άδειες που προβλέπουν οι διατάξεις του παρόντος νόμου και καθορίζει το ύψος των σχετικών παραβόλων.

ε)Καταγγέλλει τις παραβάσεις των διατάξεων του παρόντος νόμου στις αρμόδιες διοικητικές και δικαστικές αρχές.

στ)Επιβάλλει τις κατά το άρθρο 21 του παρόντος νόμου διοικητικές κυρώσεις.

ζ)Αναθέτει σε μέλος ή μέλη της τη διενέργεια διοικητικών εξετάσεων.

η)Ενεργεί αυτεπαγγέλτως ή κατόπιν καταγγελίας διοικητικούς ελέγχους σε κάθε αρχείο. Έχει προς τούτο δικαίωμα προσβάσεως στα δεδομένα προσωπικού χαρακτήρα και συλλογής κάθε πληροφορίας για τους σκοπούς του ελέγχου, χωρίς να μπορεί να της αντιταχθεί κανενός είδους απόρρητο. Κατ' εξαίρεση, η Αρχή δεν έχει πρόσβαση στα στοιχεία ταυτότητας συνεργατών που περιέχονται σε αρχεία που τηρούνται για λόγους εθνικής ασφάλειας ή για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων. Τον έλεγχο διενεργεί μέλος ή μέλη της Αρχής ή υπάλληλος της Γραμματείας, ειδικά προς τούτο εντεταλμένος από τον Πρόεδρο της Αρχής. Κατά τον έλεγχο αρχείων που τηρούνται για λόγους εθνικής ασφαλείας παρίσταται αυτοπροσώπως ο Πρόεδρος της Αρχής.

θ)Γνωμοδοτεί για κάθε ρύθμιση που αφορά την επεξεργασία και προστασία δεδομένων προσωπικού χαρακτήρα.

ι)Εκδίδει κανονιστικές πράξεις για τη ρύθμιση ειδικών, τεχνικών και λεπτομερειακών θεμάτων, στα οποία αναφέρεται ο παρών νόμος.

ια)Ανακοινώνει στη Βουλή παραβάσεις των ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.
ιβ)Συντάσσει κάθε χρόνο έκθεση για την εκτέλεση της αποστολής της κατά το προηγούμενο ημερολογιακό έτος. Στην έκθεση επισημαίνονται και οι τυχόν ενδεικνυόμενες νομοθετικές μεταβολές στον τομέα της προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Η έκθεση υποβάλλεται από τον Πρόεδρο της Αρχής στον Πρόεδρο της Βουλής και τον Πρωθυπουργό και δημοσιεύεται στην Εφημερίδα της Κυβερνήσεως με ευθύνη της Αρχής, η οποία μπορεί να δώσει και άλλου είδους δημοσιότητα στην έκθεση.
ιγ)Εξετάζει παράπονα σχετικά με την εφαρμογή του νόμου και την προστασία των δικαιωμάτων των αιτούντων όταν αυτά θίγονται από την επεξεργασία δεδομένων που τους αφορούν και αιτήσεις με τις οποίες ζητείται ο έλεγχος και η εξακρίβωση της νομιμότητας των επεξεργασιών αυτών και ενημερώνει τους αιτούντες για τις σχετικές ενέργειές της.
ιδ)Συνεργάζεται με αντίστοιχες αρχές άλλων κρατών μελών της Ευρωπαϊκής Ένωσης και του Συμβουλίου της Ευρώπης σε ζητήματα σχετικά με την άσκηση των αρμοδιοτήτων της.

Η Αρχή συνεδριάζει τακτικώς ύστερα από πρόσκληση του Προέδρου. Συνεδριάζει εκτάκτως ύστερα από πρόσκληση του Προέδρου ή αίτηση δύο τουλάχιστον μελών της. Οι αποφάσεις της Αρχής λαμβάνονται με πλειοψηφία τουλάχιστον τεσσάρων μελών της. Σε περίπτωση ισοψηφίας υπερισχύει η ψήφος του Προέδρου ή του αναπληρωτή του.
Η Αρχή καταρτίζει τον κανονισμό λειτουργίας της, με τον οποίο ρυθμίζονται ιδίως η κατανομή αρμοδιοτήτων μεταξύ των μελών της, η προηγούμενη ακρόαση των ενδιαφερομένων, θέματα πειθαρχικής διαδικασίας και ο τρόπος διεξαγωγής των κατά την περίπτωση η' της παρ. 1 του παρόντος άρθρου ελέγχων.
Η Αρχή τηρεί τα ακόλουθα μητρώα :
α)Μητρώο Αρχείων και Επεξεργασιών, στο οποίο περιλαμβάνονται τα αρχεία και οι επεξεργασίες που γνωστοποιούνται στην Αρχή.
β)Μητρώο Αδειών, στο οποίο περιλαμβάνονται οι άδειες που εκδίδει η Αρχή για την ίδρυση και λειτουργία αρχείων που περιέχουν ευαίσθητα δεδομένα.

γ)Μητρώο Διασυνδέσεων, στο οποίο περιλαμβάνονται οι δηλώσεις και οι άδειες που εκδίδει η Αρχή για τη διασύνδεση αρχείων.
δ)Μητρώο προσώπων που δεν επιθυμούν να περιλαμβάνονται σε αρχεία, τα οποία έχουν ως σκοπό την προώθηση προμήθειας αγαθών ή την παροχή υπηρεσιών εξ αποστάσεως.
ε)Μητρώο Αδειών Διαβίβασης, στο οποίο καταχωρίζονται οι άδειες διαβίβασης δεδομένων προσωπικού χαρακτήρα.
στ)Μητρώο Απόρρητων Αρχείων, στο οποίο καταχωρίζονται, με απόφαση της Αρχής ύστερα από αίτηση του εκάστοτε υπεύθυνου επεξεργασίας, αρχεία που τηρούν τα Υπουργεία Εθνικής Άμυνας και Δημόσιας Τάξης καθώς και η Εθνική Υπηρεσία Πληροφοριών, για λόγους εθνικής ασφάλειας ή για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων. Στο Μητρώο Απόρρητων Αρχείων καταχωρίζονται και οι διασυνδέσεις με ένα τουλάχιστον αρχείο της περίπτωσης αυτής.

5. Καθένας έχει πρόσβαση στα υπό στοιχεία α, β, γ, δ και ε μητρώα της προηγούμενης παραγράφου. Ύστερα από αίτηση του ενδιαφερόμενου και με απόφαση της Αρχής είναι δυνατό να επιτραπεί εν όλων ή εν μέρει, η πρόσβαση και στο Μητρώο Απόρρητων Αρχείων. Ύστερα από αίτηση του υπεύθυνου επεξεργασίας ή του εκπροσώπου του και με απόφαση της Αρχής είναι δυνατόν να απαγορευθεί, εν όλω ή εν μέρει, η πρόσβαση στο Μητρώο Αδειών Διαβίβασης, εφ' όσον από αυτήν θα προέκυπτε κίνδυνος για την ιδιωτική ζωή τρίτου, την εθνική ασφάλεια, τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων και την εκπλήρωση των υποχρεώσεων της χώρας που απορρέουν από διεθνείς συμβάσεις.

6.Ο Πρόεδρος εκπροσωπεί την Αρχή ενώπιον κάθε άλλης αρχής, καθώς και σε επιτροπές και ομάδες, συνεδριάσεις και συνόδους οργάνων της Ευρωπαϊκής Ένωσης καθώς και άλλων διεθνών οργανισμών και οργάνων που προβλέπονται από διεθνείς συμβάσεις ή στις οποίες μετέχουν εκπρόσωποι αντίστοιχων αρχών άλλων χωρών. Ο Πρόεδρος μπορεί να αναθέτει την εκπροσώπηση της Αρχής σε μέλος της, αναπληρωτή ή και υπάλληλο του κλάδου ελεγκτών της Γραμματείας.

7.Στον Πρόεδρο της Αρχής ανήκει η ευθύνη της λειτουργίας της καθώς και της λειτουργίας της Γραμματείας. Ο Πρόεδρος μπορεί να εξουσιοδοτεί μέλος της Αρχής

ή τον προϊστάμενο της Γραμματείας ή προϊστάμενο υπηρεσίας της Γραμματείας να υπογράφει με "εντολή Προέδρου" έγγραφα, εντάλματα πληρωμής ή άλλες πράξεις. Ο Πρόεδρος είναι ο διοικητικός προϊστάμενος του προσωπικού της Γραμματείας, ασκεί την έπ' αυτού πειθαρχική εξουσία και μπορεί να επιβάλλει πειθαρχική ποινή το πολύ προστίμου ίσου προς το ήμισυ των μηνιαίων αποδοχών του εγκαλουμένου.

8.Οι κανονιστικές αποφάσεις της Αρχής δημοσιεύονται στην Εφημερίδα της Κυβερνήσεως. Οι λοιπές αποφάσεις της Αρχής ισχύουν από την έκδοση ή την κοινοποίησή τους.

9.Ένδικα βοηθήματα κατά των αποφάσεων της Αρχής μπορεί να ασκεί και το Δημόσιο. Το ένδικο βοήθημα ασκεί ο κατά περίπτωση αρμόδιος υπουργός.

10.Κάθε δημόσια αρχή παρέχει τη συνδρομή της στην Αρχή.

**Άρθρο 20**

**Γραμματεία της Αρχής**

Η Αρχή εξυπηρετείται από Γραμματεία. Η Γραμματεία λειτουργεί σε επίπεδο Διευθύνσεως. Η υπηρεσιακή κατάσταση των υπαλλήλων της διέπεται από τις διατάξεις που ισχύουν εκάστοτε για τους δημόσιους διοικητικούς υπαλλήλους.
Η οργάνωση της Γραμματείας, η διαίρεση της σε τμήματα και γραφεία και οι επί μέρους αρμοδιότητες τούτων, ο αριθμός των θέσεων του προσωπικού κατά κλάδους και ειδικότητες και κάθε άλλη αναγκαία λεπτομέρεια καθορίζονται με προεδρικό διάταγμα που εκδίδεται με πρόταση των Υπουργών Εσωτερικών Δημόσιας Διοίκησης & Αποκέντρωσης, Οικονομικών και Δικαιοσύνης, ύστερα από εισήγηση της Αρχής, η οποία διατυπώνεται μέσα σε δύο (2) μήνες από τη συγκρότησή της. Με το αυτό διάταγμα προβλέπεται συγκρότηση, ως υπηρεσιακής μονάδας της Γραμματείας, τμήματος Ελεγκτών, η πρόσληψη και η υπηρεσιακή κατάσταση των υπαλλήλων του οποίου ρυθμίζεται κατά παρέκκλιση από τις εκάστοτε ισχύουσες διατάξεις. Ο προϊστάμενος της Γραμματείας προέρχεται υποχρεωτικά από τον κλάδο ελεγκτών. Ο αριθμός των θέσεων του πάσης φύσεως προσωπικού της Γραμματείας δεν μπορεί να υπερβαίνει τις τριάντα (30).

Η πλήρωση των θέσεων της Γραμματείας γίνεται σύμφωνα με τις εκάστοτε ισχύουσες διατάξεις για την πρόσληψη δημόσιων υπαλλήλων. Ειδικά για τους υπαλλήλους του κλάδου ελεγκτών της Γραμματείας η πρόσληψή τους γίνεται από την Αρχή, με επιλογή ή διαγωνισμό, ύστερα από προκήρυξή της.

4.Τα θέματα υπηρεσιακής κατάστασης του προσωπικού της Γραμματείας κρίνονται από υπηρεσιακό συμβούλιο, που συγκροτείται με απόφαση του Προέδρου της Αρχής και αποτελείται από δύο (2) μέλη της, έναν (1) υπάλληλο που ορίζεται από αυτήν και δύο (2) αιρετούς εκπροσώπους των υπαλλήλων. Κατά τα λοιπά εφαρμόζονται οι εκάστοτε ισχύουσες διατάξεις για τα υπηρεσιακά συμβούλια του προσωπικού των δημόσιων υπηρεσιών και των νομικών προσώπων δημοσίου δικαίου.

5.Οι τακτικοί υπάλληλοι της Γραμματείας της Αρχής υπάγονται ως προς την επικουρική ασφάλισή τους στο Ταμείο Αρωγής Προσωπικού Υπηρεσιών Αρμοδιότητος Υπουργείου Δικαιοσύνης. Όσοι προέρχονται από άλλες υπηρεσίες μπορούν να διατηρήσουν τα ταμεία ασφαλίσεως της προηγούμενης υπηρεσίας τους. Οι υπάλληλοι της Γραμματείας ασφαλίζονται υποχρεωτικώς στο Ταμείο Νομικών, υπό τους αυτούς όρους με τους οποίους ασφαλίζονται και οι λοιποί έμμισθοι ασφαλισμένοι του. Οι διατάξεις της παραγράφου αυτής έχουν εφαρμογή και επί των υπαλλήλων που μετατάσσονται στη Γραμματεία της Αρχής από νομικά πρόσωπα ιδιωτικού δικαίου.

6.Κατά την πρώτη εφαρμογή του παρόντος, η πλήρωση των θέσεων προϊσταμένων υπηρεσιακών μονάδων της Γραμματείας, εκτός του Τμήματος Ελεγκτών, γίνεται ύστερα από προκήρυξη της Αρχής, είτε με μετάταξη υπαλλήλων βαθμού Α' ή αντίστοιχου του Δημοσίου ή νομικών προσώπων δημοσίου δικαίου, είτε με διορισμό. Διορισμός γίνεται μόνο στις θέσεις που δεν θα πληρωθούν με μετάταξη. Η επιλογή των μετατασσομένων ή διοριζομένων γίνεται από την Αρχή. Ο διορισμός των επιλεγομένων από την Αρχή γίνεται με απόφαση του Υπουργού Δικαιοσύνης και η μετάταξη με απόφαση του ίδιου και του οικείου Υπουργού. Για την μετάταξη δεν απαιτείται γνώμη του οικείου υπηρεσιακού συμβουλίου της υπηρεσίας από την οποία μετατάσσεται ο υπάλληλος. Τον προϊστάμενο της Γραμματείας επιλέγει η Αρχή από τους υπαλλήλους του κλάδου ελεγκτών, κατά παρέκκλιση από κάθε άλλη διάταξη.

7.Κατά την πρώτη εφαρμογή του παρόντος οι λοιπές θέσεις της Γραμματείας πληρούνται με τις προϋποθέσεις και την διαδικασία της προηγούμενης παραγράφου. Προτιμούνται υποψήφιοι που έχουν αποδεδειγμένη εμπειρία σε θέματα πληροφορικής. Για τους υπαλλήλους του κλάδου ελεγκτών ισχύουν οι διατάξεις της παρ. 3 του παρόντος άρθρου.

8.Ο χρόνος της προηγούμενης υπηρεσίας των μετατασσομένων από νομικά πρόσωπα δημοσίου δικαίου ή νομικά πρόσωπα ιδιωτικού δικαίου λογίζεται ως χρόνος πραγματικής δημόσιας υπηρεσίας για κάθε συνέπεια.

9.Οι διατάξεις της παρ. 4 του άρθρου 18 εφαρμόζονται και επί των υπαλλήλων της Γραμματείας.

## ΚΕΦΑΛΑΙΟ Ε'
## ΚΥΡΩΣΕΙΣ

### Άρθρο 21
### Διοικητικές κυρώσεις

Η Αρχή επιβάλλει στους υπεύθυνους επεξεργασίας ή στους τυχόν εκπροσώπους τους τις ακόλουθες διοικητικές κυρώσεις, για παράβαση των υποχρεώσεών τους που απορρέουν από τον παρόντα νόμο και από κάθε άλλη ρύθμιση που αφορά την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα:

α)Προειδοποίηση, με αποκλειστική προθεσμία για άρση της παράβασης.

β)Πρόστιμο ποσού από τριακόσιες χιλιάδες (300.000) έως πενήντα εκατομμύρια (50.000.000) δραχμές.

γ)Προσωρινή ανάκληση άδειας.

δ)Οριστική ανάκληση άδειας.

ε)Καταστροφή αρχείου ή διακοπή επεξεργασίας και καταστροφή των σχετικών δεδομένων.

Οι υπό στοιχεία β, γ, δ και ε διοικητικές κυρώσεις της προηγούμενης παραγράφου επιβάλλονται πάντοτε ύστερα από ακρόαση του υπεύθυνου επεξεργασίας ή του εκπροσώπου του. Είναι ανάλογες προς τη βαρύτητα της παράβασης που καταλογίζεται. Οι υπό στοιχεία γ, δ και ε διοικητικές κυρώσεις επιβάλλονται σε περιπτώσεις ιδιαίτερα σοβαρής ή καθ' υποτροπήν παράβασης. Πρόστιμο μπορεί να επιβληθεί σωρευτικά και με τις υπό στοιχεία γ, δ και ε κυρώσεις. Εάν επιβληθεί η κύρωση της καταστροφής αρχείου, για την καταστροφή ευθύνεται ο υπεύθυνος επεξεργασίας αρχείου, στον οποίο μπορεί να επιβληθεί και πρόστιμο για μη συμμόρφωση.

Τα ποσά των προστίμων της παρ. 1 μπορεί να αναπροσαρμόζονται με απόφαση του Υπουργού Δικαιοσύνης, ύστερα από πρόταση της Αρχής.

Οι πράξεις της Αρχής με τις οποίες επιβάλλονται πρόστιμα συνιστούν εκτελεστικό τίτλο και επιδίδονται στον υπεύθυνο επεξεργασίας ή τον τυχόν εκπρόσωπό του. Η είσπραξη των προστίμων γίνεται κατά τις διατάξεις του Κώδικα Εισπράξεως Δημοσίων Εσόδων (ΚΕΔΕ).

**Άρθρο 22**

**Ποινικές κυρώσεις**

Όποιος παραλείπει να γνωστοποιήσει στην Αρχή, κατά το άρθρο 6 του παρόντος νόμου τη σύσταση και λειτουργία αρχείου ή οποιαδήποτε μεταβολή στους όρους και τις προϋποθέσεις χορηγήσεως της άδειας που προβλέπεται από την παρ. 3 του άρθρου 7 του παρόντος νόμου, τιμωρείται με φυλάκιση έως τριών (3) ετών και χρηματική ποινή τουλάχιστον ενός εκατομμυρίου (1.000.000) δραχμών έως πέντε εκατομμυρίων (5.000.000) δραχμών.

Όποιος κατά παράβαση του άρθρου 7 του παρόντος νόμου διατηρεί αρχείο χωρίς άδεια ή κατά παράβαση των όρων και προϋποθέσεων της άδειας της Αρχής, τιμωρείται με φυλάκιση τουλάχιστον ενός (1) έτους και χρηματική ποινή τουλάχιστον ενός εκατομμυρίου (1.000.000) δραχμών έως πέντε εκατομμυρίων (5.000.000) δραχμών.

Όποιος κατά παράβαση του άρθρου 8 του παρόντος νόμου προβαίνει σε διασύνδεση αρχείων χωρίς να την γνωστοποιήσει στην Αρχή, τιμωρείται με φυλάκιση έως τριών

(3) ετών και χρηματική ποινή τουλάχιστον ενός εκατομμυρίου (1.000.000) δραχμών έως πέντε εκατομμυρίων (5.000.000) δραχμών.

Όποιος προβαίνει σε διασύνδεση αρχείων χωρίς την άδεια της Αρχής, όπου αυτή απαιτείται ή κατά παράβαση των όρων της άδειας που του έχει χορηγηθεί, τιμωρείται με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή τουλάχιστον ενός εκατομμυρίου (1.000.000) δραχμών

έως πέντε εκατομμυρίων (5.000.000) δραχμών.

4.Όποιος χωρίς δικαίωμα επεμβαίνει με οποιονδήποτε τρόπο σε αρχείο δεδομένων προσωπικού χαρακτήρα ή λαμβάνει γνώση των δεδομένων αυτών ή τα αφαιρεί, αλλοιώνει, βλάπτει, καταστρέφει, επεξεργάζεται, μεταδίδει, ανακοινώνει, τα καθιστά προσιτά σε μη δικαιούμενα πρόσωπα ή επιτρέπει στα πρόσωπα αυτά να λάβουν γνώση των εν λόγω δεδομένων, ή τα εκμεταλλεύεται με οποιονδήποτε τρόπο, τιμωρείται με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή και αν πρόκειται για ευαίσθητα δεδομένα με φυλάκιση τουλάχιστον ενός (1) τουλάχιστον ενός εκατομμυρίου (1.000.000) δραχμών έως δέκα εκατομμυρίων (10.000.000) δραχμών, αν η πράξη δεν τιμωρείται βαρύτερα από άλλες διατάξεις.

Υπεύθυνος επεξεργασίας που δεν συμμορφώνεται με τις αποφάσεις της Αρχής που εκδίδονται για την ικανοποίηση του δικαιώματος πρόσβασης, σύμφωνα με την παρ. 4 του άρθρου 12, για την ικανοποίηση του δικαιώματος αντίρρησης, σύμφωνα με την παρ. 2 του άρθρου 13, καθώς και με πράξεις επιβολής των διοικητικών κυρώσεων των περιπτώσεων γ', δ' και ε' της παρ. 1 του άρθρου 21 τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών και με χρηματική ποινή τουλάχιστον ενός εκατομμυρίου (1.000.000) δραχμών έως πέντε εκατομμυρίων (5.000.000) δραχμών. Με τις ποινές του προηγούμενου εδαφίου τιμωρείται ο υπεύθυνος επεξεργασίας που διαβιβάζει δεδομένα προσωπικού χαρακτήρα κατά παράβαση του άρθρου 9 καθώς και εκείνος που δεν συμμορφώνεται προς την δικαστική απόφαση του άρθρου 14 του παρόντος νόμου.

Αν ο υπαίτιος των πράξεων των παρ. 1 έως 5 του παρόντος άρθρου είχε σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, ή να βλάψει τρίτον, επιβάλλεται κάθειρξη έως δέκα (10) ετών και χρηματική ποινή τουλάχιστον δύο εκατομμυρίων (2.000.000) δραχμών έως δέκα εκατομμυρίων (10.000.000) δραχμών.

Αν από τις πράξεις των παρ. 1 έως και 5 του παρόντος άρθρου προκλήθηκε κίνδυνος για την ελεύθερη λειτουργία του δημοκρατικού πολιτεύματος ή για την εθνική ασφάλεια, επιβάλλεται κάθειρξη και χρηματική ποινή τουλάχιστον πέντε εκατομμυρίων (5.000.000) δραχμών έως δέκα εκατομμυρίων (10.000.000) δραχμών.

Αν οι πράξεις των παρ. 1 έως 5 του παρόντος άρθρου τελέσθηκαν από αμέλεια, επιβάλλεται φυλάκιση έως τριών (3) ετών και χρηματική ποινή.

Για την εφαρμογή των διατάξεων του παρόντος άρθρου, αν υπεύθυνος επεξεργασίας δεν είναι φυσικό πρόσωπο, ευθύνεται ο εκπρόσωπος του νομικού προσώπου ή ο επικεφαλής της δημόσιας αρχής ή υπηρεσίας ή οργανισμού αν ασκεί και ουσιαστικά τη διοίκηση ή διεύθυνση αυτών.

Για τα εγκλήματα του παρόντος άρθρου ο Πρόεδρος και τα μέλη της Αρχής καθώς και οι προς τούτο ειδικά εντεταλμένοι υπάλληλοι του τμήματος ελεγκτών της Γραμματείας, είναι ειδικοί ανακριτικοί υπάλληλοι και έχουν όλα τα δικαιώματα που προβλέπει σχετικά ο Κώδικας Ποινικής Δικονομίας. Μπορούν να διενεργούν προανάκριση και χωρίς εισαγγελική παραγγελία, όταν πρόκειται για αυτόφωρο κακούργημα ή πλημμέλημα ή υπάρχει κίνδυνος από την αναβολή.

Για τα εγκλήματα της παρ. 5 του παρόντος άρθρου καθώς επίσης και σε κάθε άλλη περίπτωση όπου προηγήθηκε διοικητικός έλεγχος από την Αρχή, ο Πρόεδρος αυτής ανακοινώνει γραπτώς στον αρμόδιο εισαγγελέα οτιδήποτε αποτέλεσε αντικείμενο έρευνας από την Αρχή και διαβιβάζει σε αυτόν όλα τα στοιχεία και τις αποδείξεις.

Η προανάκριση για τα εγκλήματα του παρόντος άρθρου περατώνεται μέσα σε δύο (2) το πολύ μήνες από την άσκηση της ποινικής δίωξης και εφόσον υπάρχουν ενδείξεις για την παραπομπή του κατηγορουμένου σε δίκη, η δικάσιμος ορίζεται σε ημέρα που δεν απέχει περισσότερο από τρεις (3) μήνες από το πέρας της προανάκρισης ή αν η παραπομπή έγινε με βούλευμα δύο (2) μήνες από τότε που αυτό έγινε αμετάκλητο. Σε περίπτωση εισαγωγής της υπόθεσης με απευθείας κλήση του κατηγορουμένου στο ακροατήριο δεν επιτρέπεται η προσφυγή κατά του κλητήριου θεσπίσματος.

Δεν επιτρέπεται αναβολή της δίκης για τα εγκλήματα του παρόντος άρθρου παρά μόνον μία φορά για εξαιρετικά σοβαρό λόγο. Στην περίπτωση αυτή ορίζεται ρητή δικάσιμος, που δεν απέχει περισσότερο από δύο (2) μήνες και η υπόθεση εκδικάζεται κατ' εξαίρεση πρώτη.

Τα κακουργήματα που προβλέπονται από τον παρόντα νόμο υπάγονται στην αρμοδιότητα του δικαστηρίου των εφετών.

**Άρθρο 23**

**Αστική ευθύνη**

Φυσικό πρόσωπο ή νομικό πρόσωπο ιδιωτικού δικαίου, που κατά παράβαση του παρόντος νόμου, προκαλεί περιουσιακή βλάβη, υποχρεούται σε πλήρη αποζημίωση. Αν προκάλεσε ηθική βλάβη, υποχρεούται σε χρηματική ικανοποίηση. Η ευθύνη υπάρχει και όταν ο υπόχρεος όφειλε να γνωρίζει την πιθανότητα να επέλθει βλάβη σε άλλον.

Η κατά το άρθρο 932 ΑΚ χρηματική ικανοποίηση λόγω ηθικής βλάβης για παράβαση του παρόντος νόμου ορίζεται κατ' ελάχιστο στο ποσό των δύο εκατομμυρίων (2.000.000) δραχμών, εκτός αν ζητήθηκε από τον ενάγοντα μικρότερο ποσό ή η παράβαση οφείλεται σε αμέλεια. Η χρηματική αυτή ικανοποίηση επιδικάζεται ανεξαρτήτως από την αιτούμενη αποζημίωση για περιουσιακή βλάβη.

Οι απαιτήσεις του παρόντος άρθρου εκδικάζονται κατά τα άρθρα 664 - 676 του Κώδικα Πολιτικής Δικονομίας, ανεξάρτητα από την τυχόν έκδοση ή μη απόφασης της Αρχής ή την τυχόν άσκηση ποινικής δίωξης, καθώς και από την αναστολή ή αναβολή της για οποιοδήποτε λόγο. Η απόφαση του δικαστηρίου εκδίδεται μέσα σε δύο (2) μήνες από την πρώτη συζήτηση στο ακροατήριο.

## ΚΕΦΑΛΑΙΟ ΣΤ'
## ΤΕΛΙΚΕΣ - ΜΕΤΑΒΑΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

**Άρθρο 24**

**Υποχρεώσεις υπεύθυνου επεξεργασίας**

Οι υπεύθυνοι επεξεργασίας αρχείων τα οποία λειτουργούν κατά την έναρξη ισχύος του παρόντος νόμου, υποχρεούνται να υποβάλλουν την κατά το άρθρο 6 γνωστοποίηση λειτουργίας στην Αρχή μέσα σε έξι (6) μήνες από την έναρξη λειτουργίας της Αρχής.

Την ίδια υποχρέωση έχουν και οι υπεύθυνοι επεξεργασίας αρχείων με ευαίσθητα δεδομένα, τα οποία λειτουργούν κατά την έναρξη ισχύος του παρόντος νόμου, προκειμένου να εκδοθεί η κατά την παρ. 3 του άρθρου 7 άδεια.

Για αρχεία που λειτουργούν και επεξεργασίες που εκτελούνται κατά την έναρξη ισχύος του παρόντος νόμου οι υπεύθυνοι επεξεργασίας οφείλουν να προβούν στην κατά την παρ. 1 του άρθρου 11 ενημέρωση των υποκειμένων μέσα σε έξι (6) μήνες από την έναρξη λειτουργίας της Αρχής. Η ενημέρωση, εφόσον αφορά μεγάλο αριθμό υποκειμένων μπορεί να γίνει και δια του τύπου. Στην περίπτωση αυτή τις λεπτομέρειες καθορίζει η Αρχή. Οι διατάξεις της παρ. 4 του άρθρου 11 έχουν εφαρμογή και εν προκειμένω.

Για τα εξ ολοκλήρου μη αυτοματοποιημένα αρχεία οι προθεσμίες των προηγουμένων παραγράφων είναι ενός (1) χρόνου.

Οι διατάξεις των άρθρων 11, 12, 13, και 19 παρ. 1 του παρόντος νόμου δεν εφαρμόζονται στο ποινικό μητρώο και στα υπηρεσιακά αρχεία που τηρούνται από τις αρμόδιες δικαστικές αρχές για την εξυπηρέτηση των αναγκών της λειτουργίας της ποινικής δικαιοσύνης και στο πλαίσιο της λειτουργίας της.

**Άρθρο 25**

**Έναρξη λειτουργίας της Αρχής**

Μέσα σε εξήντα (60) μέρες από την έναρξη ισχύος του παρόντος νόμου, διορίζεται ο Πρόεδρος της Αρχής και ο αναπληρωτής του. Μέσα στην ίδια προθεσμία ο Υπουργός Δικαιοσύνης υποβάλει στον Πρόεδρο της Βουλής πρόταση για τον διορισμό των τεσσάρων τακτικών μελών της Αρχής και των ισάριθμων αναπληρωτών τους.

Ο χρόνος της έναρξης λειτουργίας της Αρχής ορίζεται με απόφαση του Υπουργού Δικαιοσύνης που εκδίδεται το αργότερο μέσα σε τέσσερις (4) μήνες μετά τη συγκρότηση της Αρχής. Από τον διορισμό των μελών της και έως την κατά τις παρ. 6 και 7 του άρθρου 20 του παρόντος νόμου πλήρωση των θέσεων της Γραμματείας της, η Αρχή εξυπηρετείται από προσωπικό το οποίο αποσπάται προσωρινά σε αυτήν, με απόφασή της, κατά παρέκκλιση από κάθε άλλη διάταξη.

Έως ότου η Αρχή λειτουργήσει σύμφωνα με την προηγούμενη παράγραφο, η εκκαθάριση των δαπανών της γίνεται από τη Διεύθυνση Οικονομικού της Κεντρικής

Υπηρεσίας του Υπουργείου Δικαιοσύνης, σε βάρος του προϋπολογισμού του Υπουργείου Δικαιοσύνης.

Η κατά την παρ. 2 του παρόντος άρθρου απόφαση του Υπουργού Δικαιοσύνης για τον χρόνο έναρξης λειτουργίας της Αρχής δημοσιεύεται στην Εφημερίδα της Κυβερνήσεως και σε τέσσερις (4) τουλάχιστον ημερήσιες πολιτικές εφημερίδες ευρείας κυκλοφορίας που εκδίδονται στην Αθήνα και την Θεσσαλονίκη και σε δύο (2) τουλάχιστον ημερήσιες οικονομικές εφημερίδες.

**Άρθρο 26**

**Έναρξη ισχύος**

Η ισχύς των διατάξεων των άρθρων 15, 16, 17, 18 και 20 του παρόντος νόμου αρχίζει από τη δημοσίευσή του στην Εφημερίδα της Κυβερνήσεως.

Η ισχύς των λοιπών διατάξεων αρχίζει από την κατά το προηγούμενο άρθρο έναρξη λειτουργίας της Αρχής.

# ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Cyberlaw & E-Commerce- D. Baumer and L. C. Poindexter-Έκδοση Mc Graw Hill 2000 International Edition.

[2] Πληροφορική και Δίκαιο, Αποστόλη Γέροντα, Εκδόσεις Αντ. .Ν. Σακκούλα, 1991

[3] www.privacyfoundation.org

[4] www.dpa.gr

[5] Λ. Μήτρου -Ασφάλεια Πληροφοριών

[6] Abbott,S., *"The Debate for Secure E-Commerce"*, Performance Computing, February 1999.

[7] Adam, N., Dogramaci, O., Gangopadhyay, A., Yesha, Y., *"Electronic Commerce, Technical, Business, and Legal Issues"*, Prentice Hall Inc., ISBN 0-13-949082-5, 1999.

[8] Aslam, T., *"Protocols for E-Commerce"*, Dr. Dobb' s Journal, 1998.

[9] Bellovin S., *"Security Problems in the TCP/IP Protocol Suite"*, Computer Communications Review, pp. 32-48, 1989.

[10] Bhimani, A., *"Securing the Commercial Internet"*, Communications of the ACM, No. 6, 1996.

[11] Abbott, S., *"The Debate for Secure E-Commerce"*, Performance Computing, February 1999.

[12] Dekker, M., *"Security of the Internet"*, Published in The Froehlich/Kent Encyclopedia Vol. 15, pp. 231-255, 1997.

[13] Howard, J., *"An Analysis of Security Incidents on the Internet"*, available at http://www.cert.org/research/JHThesis/Start.html, 1989-1995.

[14] Kalakota, K., Whinston, A., *"Frontiers of Electronic Commerce"*, Addison-WesleyPublishing Company Inc., ISBN 0-201-84520-2, 1996.

[15] Kosiur, D., *"Understanding Electronic Commerce"*, Microsoft Press, ISBN 1-57231-560-1, 1997.

[16] Lacoste, G., *"SEMPER: A Security Framework for the Global Electronic Market Place"*, IBM France, 1997.

[17] Lauckner, K., Lintner, M., *"Computers Inside and Out"*, Fifth Edition, Pippin Publishing Ltd., Ann Arbor, MI, 1996.

[18] Lucent Technologies, Bell Labs Innovations, *"Overview of Firewall Technologies"*, 1998.

[19] Menezes, A., Van Oorschot, P., *"Handbook of Applied Cryptography"*, CRC Press LLC, ISBN 0-8493-8523-7, 1997.

[20] Oppliger, R., *"Internet Security: Firewalls and Bey"*, Communications of the ACM, Vol. 40, No. 5, 1999. Ranum, M., *"Thinking About Firewalls"*,available at http://citeseer.nj.nec.com/ranum94thinking.html

*[21] "RSA Laboratories' Frequently Asked Questions About Today' s Cryptography"*, v4.0, RSA Data Security Inc., 1998.

[22] Treese, W., Stewart, L., *"Designing Systems for Internet Commerce"*, Addison-Wesley Publishing Company Inc., ISBN 0-201-57167-6, 1998.

[23] 3Com Corporation, Technical Papers, *"Internet Firewalls and Security – A Technology Overview". "Cryptography Policy: The Guidelines and the Issues"*, available at http://www.oecd.org/dsti/sti/it/secur/prod/ecrypto.htm, 1997.

*[24] "Guidelines for the Security of Information Systems"*, available at http://www.oecd.org/dsti/sti/it/secur/prod/e_secur.htm

*[25] "Computer Incident Advisory Capability (CIAC)"*, available at http://www.ciac.org/ciac/

*[26] "Forum of Incident Response and Security Teams (FIRST)"*, available at http:// www.first.org

[27] Chung, A., Ephraim, A., Hechmann, P., Laseter, T., Long, B., Oliver, K., Schwarting, D., Von Der Decken, T., *The e-Marketplace Revolution: Creating and Capturing the Value in B2B e-Commerce*, Booz Allen and Hamilton Inc., 2001, Datamonitor,

[28] Business-to-Business *Electronic Commerce: Exploiting Market Opportunities in the Extranet Age*, 1997.

[29] European Commission, *European Initiative in Electronic Commerce*, COM (97) 157, 1997.

[30] Forrester Research Report, *Sizing Intercomoany Commerce*, 1997. Available at http://www.forrester.com

[31] Holsapple, C., Singh M., *Electronic Commerce: from a Definitional Taxonomy Toward a Knowledge-Management View, Journal of Organizational Computing and Electronic Commerce*, 10(3), pp. 149-170, 2000.

[32] Mougayar, W., *Opening Digital Markets, Advanced Strategies for Internet-driven Commerce, Cybermanagement Publications*, pp. 201-211, 1997.

[33] Πομπόρτσης Α., Τσούλφας Α., *Εισαγωγή στο Ηλεκτρονικό Εμπόριο*, Εκδόσεις Τζιόλα, 2002.

[34] Porter M.E., Millar V.E., *How Information Gives Toy Competitive Advantage*, Harvard Business Review, p.151, 1985.

[35] Rappa, M., *Business Models of the Web, Managing the Digital Enterprise*, 2001.Available at http://digitalenterprise.org /models/models.html

[36] Spiller, P., Lohse, G., *A Classification of Internet Retail Stores, International Journal of Electronic Commerce*, Vol. 2, No. 2, pp. 29, 1997.

[37] The Report on Electronic Commerce, Vol. 5, No. 4, 1998.

[38] Timmers, P., *Business Models for Electronic Markets,* In: Gadient, Y., Schmid, Beat,

[39] F., Selz, D., EM – *Electronic Commerce in Europe.*

[40] EM – *Electronic Markets*, Vol. 8, No. 2, 1998.