Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών
«Προηγμένα Συστήματα Πληροφορικής»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**ΜΕΛΕΤΗ ΤΟΥ ΝΟΜΙΚΟΥ ΠΛΑΙΣΙΟΥ ΚΑΙ ΤΩΝ ΚΑΝΟΝΙΣΜΩΝ ΠΟΥ ΔΙΕΠΟΥΝ ΤΗΝ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΩΝ**
Ονοματεπώνυμο Φοιτητή	**ΓΙΩΡΓΟΣ ΠΑΙΔΑΚΑΚΗΣ**
Πατρώνυμο	**ΒΑΣΙΛΕΙΟΣ**
Αριθμός Μητρώου	**ΜΠΣΠ12054**
Επιβλέπων	**ΧΡΗΣΤΟΣ ΔΟΥΛΗΓΕΡΗΣ, ΚΑΘΗΓΗΤΗΣ**

Ημερομηνία Παράδοσης **Οκτώβριος 2016**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Όνομα Επώνυμο Βαθμίδα	Όνομα Επώνυμο Βαθμίδα	Όνομα Επώνυμο Βαθμίδα

Πίνακας περιεχομένων

Ευχαριστίες

Για τη διεκπεραίωση της παρούσας Πτυχιακής Εργασίας, θα ήθελα να ευχαριστήσω τον επιβλέποντα, Δρ Μάνο Γεωργακάκη για τη συνεργασία και την πολύτιμη συμβολή του στην ολοκλήρωση της.

Επίσης θα ήθελα να ευχαριστήσω την σύζυγο μου Αναστασία για την κατανόησή της, ιδιαίτερα κατά τη διάρκεια των τελευταίων μηνών της προσπάθειάς μου κατά την διάρκεια της εγκυμοσύνης της και τέλος να ευχαριστήσω το καινούριο μέλος της οικογένειας μας , την μικρή Ανδριάνα. Αφιερώνω την εργασία στην οικογένεια μου.

Παιδακάκης Γιώργος

Περίληψη- Abstract

Η χρήση των Πληροφοριακών Συστημάτων συνεχώς αυξάνεται. Οι περισσότεροι πλέον οργανισμοί βασίζουν μεγάλο μέρος της λειτουργίας τους στην χρήση των Πληροφοριακών Συστημάτων. Ωστόσο το μεγάλο πρόβλημα με τα Πληροφοριακά Συστήματα είναι η ασφάλεια τους. Στη παρούσα Μεταπτυχιακή Διατριβή, παρουσιάζονται τα βασικά θέματα που αφορούν τις Πολιτικές Ασφάλειας των Πληροφοριακών Συστημάτων. Σε πρώτη φάση εντάσσονται η έννοια της Πολιτικής Ασφάλειας στον ευρύτερο τομέα της Διαχείρισης της Ασφάλειας των Πληροφοριακών Συστημάτων, η σκοπιμότητα εφαρμογής και ανάπτυξης μιας πολιτικής ασφαλείας καθώς περιγράφονται και τα βασικά χαρακτηριστικά της. Στη συνέχεια δίνεται η μεθοδολογία υλοποίησης της μελέτης και το πεδίο ορισμού αυτής. Ακολουθεί περιγραφή της υφιστάμενης κατάστασης μέσα από συγκριτική ανάλυση θεσμικών πλαισίων τόσο στην Ευρώπη όσο και στις ΗΠΑ αλλά και στην Ελλάδα. Στο καταληκτικό τμήμα θα παρατεθούν τα συμπεράσματα και παρατηρήσεις για την αναγκαιότητα περαιτέρω ανάπτυξης των ζητημάτων ασφάλειας στο διαδίκτυο για την διασφάλιση των δεδομένων.

The use of information systems is increasing. Most organizations now rely much of their operation in the use of Information Systems. But the big problem with the information systems is security. In this Master Thesis, are presented the key issues concerning the Security Policies of Information Systems. Initially part of the concept of security policy in the wider field of Security of Information Systems Management, the importance of implementing and developing a security policy as described and the main characteristics. Then given the implementation methodology of the study and the scope of this definition. A description of the current situation through a comparative analysis of institutional frameworks in both Europe and the US but also in Greece. In the concluding part will be set the findings and observations on the need for further development of the security issues on the Internet to secure data.

ΚΕΦΑΛΑΙΟ 1 ΕΙΣΑΓΩΓΗ

Η ασφάλεια των δεδομένων έχει όλο και μεγαλύτερη σημασία ενώ παρέχει τα απαραίτητα εργαλεία για την ασφαλή επικοινωνία και την προστασία των δεδομένων. Λόγω της ραγδαίας ανάπτυξη του Διαδικτύου τα τελευταία χρόνια, έχει γίνει πιο σημαντικό για το μέσο καταναλωτή να διασφαλίσει ότι οι πληροφορίες που αποτελούν κομμάτι του «εαυτού του» θα είναι ασφαλείς.

Οι πληροφορίες που οι εισβολείς βρίσκουν χρήσιμες εμπεριέχουν υλικά και λογισμικά που χρησιμοποιούνται για τη διαμόρφωση του συστήματος, τον τύπο των συνδέσεων του δικτύου και τις διαδικασίες πρόσβασης και ελέγχου ταυτότητας.

Πληροφορίες που σχετίζονται με την ασφάλεια των πληροφοριών μπορεί να επιτρέψουν σε μη εξουσιοδοτημένα άτομα να έχουν πρόσβαση σε σημαντικά αρχεία και προγράμματα, θέτοντας έτσι σε κίνδυνο την ασφάλεια του συστήματος. Παραδείγματα σημαντικών πληροφοριών είναι οι κωδικοί πρόσβασης, τα αρχεία ελέγχου πρόσβασης, οι πληροφορίες προσωπικού, και οι αλγόριθμοι κρυπτογράφησης.

Εκείνοι που επηρεάζονται, σχετίζονται κατά κύριο λόγο με ιδρύματα τραπεζών, χρηματοοικονομικές και ασφαλιστικές εταιρείες, μεσιτικά γραφεία, συμβούλους, εργολάβους της κυβέρνησης, κυβερνητικές υπηρεσίες, νοσοκομεία και ιατρικά εργαστήρια, φορείς παροχής υπηρεσιών δικτύου, κλωστοϋφαντουργικές επιχειρήσεις, πανεπιστήμια αλλά και το χονδρικό και λιανικό εμπόριο.

Για να αντιμετωπιστεί η κατάσταση, ορισμένες κυβερνήσεις και οργανώσεις έχουν δημιουργήσει νομικές ρυθμίσεις σχετικά με τις πληροφορίες, προκειμένου να εξασφαλίσουν μεγαλύτερη ασφάλεια. Η ασφάλεια πληροφοριών είναι κάτι στο οποίο πρέπει να συμμετέχουν όλα τα ενδιαφερόμενα μέλη. Τα ανώτερα διοικητικά στελέχη, οι επαγγελματίες της ασφάλειας των πληροφοριών, οι επαγγελματίες της πληροφορικής και οι χρήστες, όλοι πρέπει να έχουν ένα ρόλο στην εξασφάλιση των περιουσιακών στοιχείων ενός οργανισμού.

Η παρούσα Μεταπτυχιακή Διατριβή, ολοκληρώνεται μέσα από τέσσερα κεφάλαια, όπου πιο συγκεκριμένα, το πρώτο κεφάλαιο αφορά εισαγωγικά στοιχεία που προετοιμάζει τον αναγνώστη για το θέμα που θα ακολουθήσει. Το δεύτερο κεφάλαιο θα αναπτύξει τη βιβλιογραφική ανασκόπηση κάνοντας αναφορά στη σπουδαιότητα των πνευματικών δικαιωμάτων και του ηλεκτρονικού εμπορίου.

Το τρίτο κεφάλαιο πρόκειται να συγκρίνει το εφαρμοστέο στην Ελλάδα δίκαιο με ΕΚ και δίκαια άλλων κρατών όπως της Αμερικής ή περιοχές της Μεγάλης Βρετανίας και της Ευρώπης γενικότερα. Το τέταρτο και τελευταίο κεφάλαιο θα μελετήσει το νομοθετικό πλαίσιο της Ελλάδας σε σχέση με τις ΗΠΑ και την Ευρώπη εξετάζοντας το διεθνές κανονιστικό πλαίσιο, τα όρια της ιδιωτικότητας καθώς και την έλλειψη ορίων. Τέλος, η Μεταπτυχιακή Διατριβή, θα κλείσει με τα συμπεράσματα. Μέσα από αυτά, αποδεικνύεται οτι παρά το ότι γίνονται προσπάθειες στο ευρωπαϊκό σύνολο, αλλά και στην Ελλάδα, στην Αμερική τα μέτρα σε όλους τους τομείς είναι αρκετά αυστηρά. Αυτό εγείρει την ανάγκη περαιτέρω προσπαθειών δίνοντας βαρύτητα στον ελλαδικό χώρο και στην απόκτηση αυστηρότερων μέτρων σε κάθε επίπεδο που αφορά τα όρια της ιδιωτικότητας και της προστασίας προσωπικών δεδομένων εξασφαλίζοντας ασφάλεια στον κάθε πολίτη ξεχωριστά και στη χώρα ως σύνολο.

ΚΕΦΑΛΑΙΟ 2 ΤΟ ΠΕΔΙΟ ΤΩΝ ΠΝΕΥΜΑΤΙΚΩΝ ΔΙΚΑΙΩΜΑΤΩΝ ΒΙΒΛΙΟΓΡΑΦΙΚΗ ΑΝΑΣΚΟΠΗΣΗ

Στο παρόν Κεφάλαιο, θα αναλυθούν ζητήματα παραβίασης πνευματικών δικαιωμάτων. Πρόκειται για ένα φαινόμενο το οποίο είναι σύνηθες στην Ελλάδα, όπου παρουσιάζονται συχνά φαινόμενα, παραβίασης και μάλιστα σε ευρεία έκταση κάθε είδους πνευματικών δικαιωμάτων, είτε αυτά αφορούν προγράμματα υπολογιστών, είτε τηλεοπτικά προγράμματα, είτε εκδόσεις βιβλίων, είτε εμπορικές και σχεδιαστικές πατέντες (Στογιάννου,1999).

Κάθε χώρα έχει δική της ερμηνεία για το νόμο περί πνευματικής ιδιοκτησίας, αλλά υπάρχουν αρκετές συμφωνίες μεταξύ των κρατών. Οι άδειες ισχύουν σύμφωνα με τη νομοθεσία περί πνευματικής ιδιοκτησίας, η οποία είναι διαφορετική από ότι το δίκαιο των συμβάσεων.

2.1 Πνευματικά δικαιώματα

Όταν δημιουργούμε κάτι, π.χ. μία φωτογραφία, κατέχουμε τα πνευματικά δικαιώματα αυτής, τα οποία είναι δικά μας αποκλειστικά δικαιώματα, καθώς εμείς είμαστε οι πρωτουργοί αυτού του έργου το οποίο και μας ανήκει. Ελέγχουμε ποιος άλλος μπορεί να χρησιμοποιήσει το έργο μας και με ποιον τρόπο. Τα έργα που υπόκεινται σε καθεστώς πνευματικών δικαιωμάτων μερικές φορές αναφέρονται και ως «πνευματική ιδιοκτησία» . Οι άδειες παραχώρησης και χρήσης πνευματικών δικαιωμάτων, χορηγούνται από συγκεκριμένες αρχές οι οποίες έχουν την αρμοδιότητα να χρησιμοποιούν ή να εκμεταλλεύονται κάποιο έργο. Στην περίπτωση μιας δικής μας φωτογραφίας, η χρήση και η διανομή των πηγών ορίζονται από τον κάτοχο των πνευματικών δικαιωμάτων (δηλαδή εμάς).

Ωστόσο, μπορεί κάποιος να αποφασίσει να προσφέρει μια φωτογραφία δωρεάν ή να χρεώσει και αμοιβή με οποιονδήποτε τρόπο ή μέσο. Μπορούμε, επομένως, να εκδώσουμε άδεια για να περιορίσουμε τη χρήση και να διατηρήσουμε τα δικαιώματα της πνευματικής ιδιοκτησίας.

Επειδή όμως κάποιος διατίθεται να πληρώσει χρήματα για να χρησιμοποιήσει ένα έργο, αυτό δεν σημαίνει ότι μπορεί και να αποκτήσει τον πλήρη έλεγχο ή τα δικαιώματα σε ό,τι αγοράζει. Οι άδειες μπορεί να υπαγορεύουν τον αριθμό ή τις χρήσεις, τα όρια χρήσης, ακόμα και το χρονικό διάστημα μέχρι τη λήξη ισχύος της άδειας (Αρχή Προστασίας Προσωπικών Δεδομένων,2003).

Επιπλέον, σύμφωνα με τον όρο «έργο προς ενοικίαση», ο εργοδότης κατέχει τα πνευματικά δικαιώματα ενός έργου και όχι ο συγγραφέας ή ο δημιουργός. Σε πολλές περιπτώσεις, εργοδότης μπορεί να είναι μία εταιρία (όπως ένα δημιουργικό γραφείο) ή ένας πελάτης (με συμβόλαιο). Σε αυτές τις περιπτώσεις, ο δημιουργός διατηρεί τα δικαιώματα του έργου του, συμπεριλαμβανομένου του δικαιώματός του για την απόδοση.

Η χρήση υλικού που υπόκειται σε πνευματικά δικαιώματα είναι ένα νόμιμο δικαίωμα. Παραδείγματα θεμιτής χρήσης μπορεί να είναι (Αρχή Προστασίας Προσωπικών Δεδομένων,2003):

- Για εκπαιδευτικούς σκοπούς, όπως για την διδασκαλία και τις έρευνες φοιτητών.

- Για σχολιασμό και κριτική, ως κομμάτι μίας ειδησεογραφικής έκθεσης ή ενός δημοσιευμένου άρθρου.

Τα έργα που είναι «κοινό κτήμα», δηλαδή τα έργα που έχει παρέλθει η περίοδος προστασίας τους, δεν επισύρουν ουσιαστικά κανένα δικαίωμα πνευματικών δικαιωμάτων στον κάτοχό τους. Μπορεί να χρησιμοποιηθούν, να τροποποιηθούν και να αναδιανεμηθούν. Ο πρωτουργός τους, μπορεί να απωλέσει τα πνευματικά του δικαιώματα και, ως εκ τούτου, να έχει θέσει το έργο του ως κοινό κτήμα.

Τα πνευματικά δικαιώματα ιδιοκτησίας λήγουν μετά το θάνατο του πρωτουργού, συνήθως 50 με 70 χρόνια μετά το θάνατό του για τις περισσότερες χώρες (Copyright Hellenic Data Protection Authority 2003). Η Σύμβαση της Βέρνης (για την προστασία των λογοτεχνικών και καλλιτεχνικών έργων) που θεσπίστηκε το 1886, είναι μία διεθνής συμφωνία που διέπει τα δικαιώματα πνευματικής ιδιοκτησίας. Αναφέρει ότι κάθε κράτος μέλος πρέπει να αναγνωρίζει τα πνευματικά δικαιώματα του έργου από άλλες χώρες, και πρέπει να επεκτείνει τα δικαιώματα που παρέχει στα έργα των πολιτών του και στα έργα ξένων πολιτών. Οι άδειες των δικαιωμάτων ενδέχεται να χαρακτηρίζονται σε κάποια κράτη από ορισμένους περιορισμούς, ορίζοντας στους κατόχους τους τη δυνατότητα να διατηρούν όλα τους τα δικαιώματα σε κάποιες χώρες και σε κάποιες άλλες εν μέρει. (Copyright Hellenic Data Protection Authority 2003).

Δεν θα πρέπει να αποτελεί έκπληξη το γεγονός ότι υφίστανται μία σειρά από άδειες. Κάθε μία προσαρμοσμένη στη χρήση. Προφανώς υπάρχει μία θεμελιώδης διαφορά μεταξύ ας πούμε της ανάπτυξης ενός κώδικα και ενός καταλόγου φωτογραφιών. Πριν αναφερθούμε σε αυτές, ας παραθέσουμε κάποια κοινή ορολογία:

- Αντιγραφή (Copy): Είναι ένα απλό αντίγραφο του πρωτότυπου έργου.
- Τροποποίηση (Modify): Είναι η αλλαγή, τροποποίηση ενός έργου με πνευματικά δικαιώματα με οποιονδήποτε τρόπο πριν από τη χρήση.
- Παράγωγο έργο (Derivative work): Είναι το αποτέλεσμα της τροποποίησης πνευματικών δικαιωμάτων εργασιών για την παραγωγή νέων εργασιών.
- Διανομή (Distribute): Είναι η πράξη της παροχής άδειας ενός έργου σε τρίτο για την διανομή του.
- Αναδιανομή (Redistribute): Είναι η πράξη της διανομής ενός έργου και της άδειάς του μετά την απόκτηση αυτού, κατόπιν αδείας από τον αρχικό ιδιοκτήτη των πνευματικών δικαιωμάτων.
- Παρόμοια διανομή (Share alike): Είναι η άδεια για τη διανομή ενός παράγωγου έργου με την ίδια ή παρόμοια άδεια.
- Αναγνώριση ή αναφορά (Credit or attribution): Είναι η πράξη προσδιορισμού του αρχικού ιδιοκτήτη των πνευματικών δικαιωμάτων.
- Ανακοίνωση Πνευματικών Δικαιωμάτων (Copyright notice): Είναι μία γραπτή φράση ή σύμβολο (©) για την ενημέρωση ότι το έργο είναι πνευματική ιδιοκτησία (όχι απαραίτητα από το νόμο).
- Διατηρούνται όλα τα δικαιώματα (All rights reserved): Μία κοινή δήλωση πνευματικών δικαιωμάτων που διαμηνύει ότι δεν υπάρχουν δικαιώματα χρήσης (και πάλι δεν απαιτείται αναγκαστικά).
- Εγγύηση (warranty): Είναι μία γραπτή εγγύηση που συμπεριλαμβάνεται στην άδεια (ή, συνήθως, δεν συμπεριλαμβάνεται).

2.2 Προστασία προσωπικών δεδομένων

Η προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής αποτελεί θεμελιώδες ανθρώπινο δικαίωμα. Ο νόμος παρέχει ορισμένα δικαιώματα στα φυσικά

πρόσωπα (τα υποκείμενα των δεδομένων) και θέτει συγκεκριμένες υποχρεώσεις σε όσους τηρούν και επεξεργάζονται προσωπικά δεδομένα (τους υπευθύνους επεξεργασίας). Έτσι για παράδειγμα, δεδομένου ότι υπάρχει το νομικό πλαίσιο προστασίας των προσωπικών τους δεδομένων, χιλιάδες άνθρωποι σε ολόκληρο τον κόσμο έχουν την ικανότητα να εκτελούν κάποιες χρηματικές και διαφόρων άλλων ειδών συναλλαγές για αγορά αγαθών και υπηρεσιών. Η μέθοδος της «Ανωνυμίας» όμως χρησιμοποιείται και στην προστασία των αρχείων αλλά και πηγών που βρίσκονται μέσα σε ένα ηλεκτρονικό υπολογιστή.

Τα τελευταία χρόνια έχει αναπτυχθεί ένα νέο είδος επίθεσης, οι ηλεκτρονικές επιθέσεις. Κατά κύριο λόγο, οι εν λόγω επιθέσεις, πραγματοποιούνται από βάνδαλους, ενώ τα κίνητρα των επιθέσεων ποικίλουν. Συχνό είναι επίσης το φαινόμενο, ότι οι επιθέσεις αυτές, στρέφονται εναντίον κυβερνητικών οργανισμών και υπηρεσιών.

"Σε μια τυπική επίθεση σ' έναν δικτυακό τόπο, το αποτέλεσμα μπορεί να είναι αναστρέψιμο. Ο βάνδαλος θα διαγράψει ορισμένες σελίδες ή γραφικά και θα ανεβάσει τις δικές του σελίδες, το περιεχόμενο των οποίων, μπορεί να είναι από χιουμοριστικό έως προπαγανδιστικό. Όταν ο ιδιοκτήτης του δικτυακού τόπου αντιληφθεί ότι έχει υποστεί μια τέτοια επίθεση, θα διορθώσει τις προβληματικές σελίδες από εφεδρικά αρχεία. Το κρίσιμο ζήτημα, σ' αυτή την περίπτωση, είναι ο χρόνος που θα απαιτηθεί για την επιδιόρθωση. Αν οι ζημιές που προκλήθηκαν είναι μεγάλες, ίσως να χρειαστεί ο δικτυακός τόπος να παραμείνει εκτός δικτύου για μεγάλο χρονικό διάστημα" (Weinberger and Spotts 1997).

Η «Ανωνυμία» αποτελεί χαρακτηριστικό της εποχής μας αλλά και της τεχνολογικής επανάστασης, αφού μέσω αυτής πολλοί είναι εκείνοι που δραστηριοποιούνται στο ηλεκτρονικό εμπόριο και την πώληση αγαθών και υπηρεσιών. Εξ΄αιτίας της ανωνυμίας, είναι πολλοί εκείνοι οι χρήστες οι οποίοι έχουν την δυνατότητα, να αποστέλλουν πληροφορίες και αρχεία σε άλλα άτομα, χωρίς να αποκαλύπτονται τα ονόματα τους ή η προέλευσή τους. Με αυτό τον τρόπο, κατορθώνουν να διατηρούν ανέπαφο το τρόπο με τον οποίο σκέφτονται και δρουν.

Μέσω της προστασίας των δεδομένων στο διαδίκτυο, οι χρήστες έχουν επιπλέον τη δυνατότητα, να προστατεύουν τα πνευματικά τους δικαιώματα σε συγκεκριμένα αρχεία και να εξασφαλίζουν με αυτό τον τρόπο, το μείζον θέμα της ασφάλειας στις καθημερινές τους συναλλαγές και κινήσεις στον παγκόσμιο διαδικτυακό χώρο (Weinberger and Spotts, 1997).

2.3 Ηλεκτρονικό εμπόριο

Η σημασία του ηλεκτρονικού εμπορίου αναφέρεται σε συναλλαγές που σχετίζονται με αγαθά και υπηρεσίες και οι οποίες εκτελούνται από απόσταση, χωρίς την ύπαρξη των συναλλασσόμενων στο χώρο της συναλλαγής.

Ως ηλεκτρονικό εμπόριο νοούνται συναλλαγές οι οποίες πραγματοποιούνται είτε από απόσταση, αλλά και με ηλεκτρονικά μέσα (με τη χρήση κλειστών δικτύων), είτε με δράσεις που έχουν την τεχνική υποστήριξη άλλων εφαρμογών όπως για παράδειγμα αυτές που βασίζονται στο ηλεκτρονικό ταχυδρομείο.

Σχετικός όρος με το ηλεκτρονικό εμπόριο, είναι το ηλεκτρονικό «επιχειρείν». Το συγκεκριμένο αποτελεί το συνδυασμό βασικών επιχειρησιακών δράσεων μιας επιχείρησης με τις υποδομές της σε πληροφοριακά συστήματα αλλά και με τις υπηρεσίες που προσφέρει το διαδίκτυο. Το ηλεκτρονικό «επιχειρείν», εστιάζει στην αυτοματοποίηση της επικοινωνίας μεταξύ των εμπορικών επιχειρήσεων, με στόχο την απλοποίηση των διαδικασιών που αναπτύσσονται μεταξύ τους, τη δημιουργία προϊόντων, υπηρεσιών αλλά και την αύξηση της ανταγωνιστικότητας μεταξύ τους (Boyd, and Potter, 2003).

Η IBM (Corporation, 2000) ορίζει την ηλεκτρονική αγορά ως εξής. *' Μια ηλεκτρονική αγορά παρέχει μια ομαδοποίηση προϊόντων και υπηρεσιών δίνοντας τη δυνατότητα στα μέλη της να συναλλάσσονται με τη χρήση διάφορων μηχανισμών, οι οποίοι*

*είναι διαθέσιμοι στην ηλεκτρονική αγορά. Η ηλεκτρονική αγορά υλοποιείται και συντηρείται από κάποιον ιδρυτή. Ο ιδρυτής της αγοράς έχει και την ευθύνη της διαχείρισης και διατήρησής της με σκοπό να είναι ανοιχτή στην επιχειρηματικότητα' (*Berger, 1995*).*

2.4 Απόρρητο Επικοινωνιών

Αποτέλεσμα των παραβιάσεων και των επιθέσεων κατά των πληροφοριακών συστημάτων (εφεξής Π.Σ) ενός οργανισμού, είναι η ρήξη χαρακτηριστικών, όπως η εμπιστευτικότητα (Spears & Barki, 2010).

Η ασφάλεια των Π.Σ αποτελεί κομβικό σημείο για τη σύγχρονη κοινωνία. Ανάμεσα στους τομείς της ασφάλειας Π.Σ συμπεριλαμβάνονται η ψηφιακή εγκληματολογία και η εφαρμοσμένη κρυπτογραφία (Peltier, 2013).

Η ασφάλεια των Π.Σ είναι πολύ σημαντική καθώς στηρίζεται σε τρεις βασικές ιδέες οι οποίες είναι σημαντικές για την ορθή λειτουργία ενός Π.Σ., και είναι οι εξής :

1. Ακεραιότητα (Integrity)
2. Διαθεσιμότητα (Availability)
3. Εμπιστευτικότητα (Confidentiality)

Οι απαιτήσεις ασφάλειας μπορεί να προέρχονται από διαφορετικές πηγές, όπως (Whitman & Mattord, 2011):

1.Οι χρήστες των ΠΣ.

2.Η διοίκηση του οργανισμού που επιθυμεί την απρόσκοπτη χρήση των ΠΣ στις λειτουργίες του οργανισμού.

3. Οι πελάτες του οργανισμού, είναι και συνιστώσα του πληροφοριακού συστήματος.

4. Το νομικό και ρυθμιστικό πλαίσιο όπου λειτουργεί ο οργανισμός.

Η αξιολόγηση της ασφάλειας μπορεί να πραγματοποιηθεί με ποικίλους τρόπους, όπως χρήση προτύπων διαχείρισης σχετικά με την ασφάλεια. Στη συνέχεια δίνονται οι ορισμοί για την ανάλυση κινδύνων (Spears & Barki, 2010):

1. **Απειλή**: Ένα μη επιθυμητό γεγονός που μπορεί να προξενήσει μη διαθεσιμότητα του συστήματος.
2. **Ευπάθεια**: Μια σχεδιαστική ατέλεια σε ένα σύστημα, με δυνατότητα παραβίασης της ασφάλειας του συστήματος.
3. **Κίνδυνος**: Ενδεχόμενο κινδύνου στο να εκμεταλλευτεί μια απειλή ή μια ευπάθεια.
4. **Αντίμετρο**: Μέτρο που εφαρμόζεται για την προστασία του ΠΣ και την αντιμετώπιση των απειλών.

Η πολιτική ασφαλείας αφορά κάθε τεχνική που περιορίζει τις ευπάθειες του πληροφοριακού συστήματος (Whitman & Mattord, 2013):

Για την Ελλάδα η πιο σημαντική δυσκολία για τον σχεδιασμό και την υλοποίηση πολιτικών ασφάλειας στα πληροφοριακά συστήματα, οφείλεται κατά κύριο λόγο στο μεγάλο κόστος αυτών των πολιτικών (Peltier, 2013).

Το απόρρητο στο διαδίκτυο, ή αλλιώς η εξασφάλιση που παρέχει ένας ιστοχώρος, σχετικά με την εξασφάλιση των προσωπικών δεδομένων ενός επισκέπτη του, αποτελεί σύμφωνα με τον Trevor Moor (2005) τη βασική μεταβλητή, η οποία καθιστά το συγκεκριμένο ιστότοπο αξιόπιστο, προκειμένου ο πελάτης να προβεί στην αξιοποίησή του. Η εμπιστοσύνη θεωρείται στην εποχή μας η βάση της στρατηγικής ενός δικτυακού τόπου. Συγκεκριμένα, ο κάθε άνθρωπος συνηθίζει να χρησιμοποιεί εκείνον τον ιστότοπο, που του εξασφαλίζει ότι τα στοιχεία του θα μείνουν απόρρητα και ότι θα λάβει τις σωστές πληροφορίες.

2.5 Διαδικτυακές μορφές εγκλήματος

Τα εγκλήματα στον κυβερνοχώρο, καλύπτουν κάθε αξιόποινη πράξη που ασχολείται με τους υπολογιστές και τα δίκτυα (και ονομάζεται hacking). Επιπλέον, το έγκλημα στον κυβερνοχώρο περιλαμβάνει επίσης τα παραδοσιακά εγκλήματα που πραγματοποιούνται μέσω του Διαδικτύου. Για παράδειγμα εγκλήματα μίσους και απάτης στο Διαδίκτυο, κλοπή ταυτότητας, και κλοπές κωδικών πιστωτικής κάρτας, θεωρούνται εγκλήματα στον κυβερνοχώρο, όταν οι παράνομες δραστηριότητες αυτές διαπράττονται μέσω της χρήσης ενός υπολογιστή και του Διαδικτύου.

Η αυξημένη απώλεια χρημάτων μπορεί να αποδοθεί στην αυξανόμενη προσβασιμότητα του Διαδικτύου, για τους παρόχους υπηρεσιών Διαδικτύου που είχαν αρχίσει να αναπτύσσουν μεγάλες βάσεις πελατών (Marcella & Greenfield, 2002).

Με την ανάπτυξη του διαδικτύου, αυξήθηκαν παράλληλα και τα κρούσματα διαδικτυακών εισβολών. Είναι χαρακτηριστικό, ότι μεταξύ του 1991 και του 1994 το Computer Emergency Response Team και το Carnegie-Mellon University διαπίστωσε, πως το ποσοστό των εισβολών στις Ηνωμένες Πολιτείες αυξήθηκε κατά ένα επιβλητικό ποσοστό 498% σε σχέση με τη προηγούμενη πενταετία (Taylor, Fritsch & Liederbach, 2014). Βρέθηκε επίσης ότι ο αριθμός των οικιών και γραφείων που επηρεάζεται από το έγκλημα πληροφορικής ανέβηκε σε ποσοστό της τάξης του 702% (Taylor, Fritsch & Liederbach, 2014)

Για να βοηθήσει στην καταπολέμηση της έκρηξης των εγκλημάτων πληροφορικής, μια νέα ομάδα διαμορφώθηκε στο FBI - ως Εθνική ομάδα εγκλήματος υπολογιστών. Αυτή η ομάδα εργάστηκε αποκλειστικά σε υποθέσεις που αφορούν εγκλήματα πληροφορικής, καθώς μεταξύ του 1991 και του 1997, ερεύνησε πάνω από 200 μεμονωμένες περιπτώσεις.

Ο επιτιθέμενος με τη χρήση ενός Η/Υ συνδεδεμένου στο Διαδίκτυο, μπορεί να εισβάλλει στα υπολογιστικά συστήματα μιας επιχείρησης ή ενός οργανισμού σε οποιοδήποτε σημείο του κόσμου. Δεν απαιτείται η φυσική μετακίνηση του, καθώς οι ενέργειές του μπορεί να ολοκληρωθούν από την οικία του ή άλλο χώρο, με τη χρήση ενός δικτυωμένου προσωπικού υπολογιστή (Jewkes & Yar, 2013).

Το 2002, μια έρευνα από το Ινστιτούτο Ασφάλειας Υπολογιστών διαπίστωσε ότι πάνω από το 90% των μεγάλων εταιρειών, συμπεριλαμβανομένων και πολλών κυβερνητικών οργανισμών, δήλωσαν ότι έχουν δεχτεί παραβιάσεις ασφάλειας. Αυτά τα δεδομένα και μόνο δείχνουν πόσο συνηθισμένα και αποτελεσματικά είχαν αρχίσει να γίνονται τα εγκλήματα υπολογιστών. Η έρευνα επίσης διαπίστωσε ότι μόνο το 2002, υπήρχε μια απώλεια 455 εκατομμύριων δολαρίων που αποδίδεται στο έγκλημα πληροφορικής (Marcella & Greenfield, 2002).

Φαινομενικά, η εισβολή σε κάποιο υπολογιστικό σύστημα φαντάζει δύσκολη. Όμως, η άποψη ότι απαιτούνται εξειδικευμένες γνώσεις για την εξαπόλυση τέτοιου είδους επιθέσεις, αποτελεί μύθο.

Μέχρι το 2012, μια μεγάλη εταιρεία ασφάλειας υπολογιστών, η Symantec, διαπίστωσε ότι το έγκλημα υπολογιστών σε εταιρείες κοστίζει 114 δισεκατομμύρια αμερικανικά δολάρια ετησίως, μια σημαντική αύξηση από εκείνη των 455 εκατομμυρίων αμερικάνικων δολαρίων δέκα χρόνια πριν. Επιπλέον, 274 δισεκατομμύρια δολάρια σπαταλήθηκαν σε απώλεια χρόνου λόγω παρεμβολών που προκαλούνται από το έγκλημα πληροφορικής (Jewkes, 2013).

Δυστυχώς, επειδή η πλειοψηφία των δικτύων ανήκουν σε ιδιωτικές επιχειρήσεις, η κυβέρνηση έχει ελάχιστο έλεγχο όσον αφορά στην εφαρμογή των πρακτικών ασφάλειας στον κυβερνοχώρο.

Στις ΗΠΑ, είχε προταθεί η ψήφιση ενός νόμου, γνωστού ως ασφάλεια στον κυβερνοχώρο, ο οποίος θα επέτρεπε στο Υπουργείο Εσωτερικής Ασφάλειας να συνεργασθεί με τις οργανώσεις για την ανάπτυξη προτύπων ασφαλείας. Ορισμένες εταιρείες, ωστόσο, απαίτησαν από το Κογκρέσο να δίνει ανταμοιβές και κίνητρα σε αντάλλαγμα για την αύξηση της ασφάλειας. Άλλες εταιρείες δεν θέλουν κυβερνητικά τμήματα να αποκτούν εξουσία επάνω τους (Jewkes, 2013).

Επιπλέον, το Διαδίκτυο προσφέρει μια σειρά από νέες δυνατότητες επικοινωνίας. Το ηλεκτρονικό ταχυδρομείο (e-mail) τα δωμάτια συζητήσεων (chat rooms) και οι ομάδες ειδήσεων (newsgroups) επιτρέπουν σε πολλά άτομα ταυτόχρονα να επικοινωνούν γρήγορα, σε πραγματικό χρόνο, χωρίς μετακίνηση, εύκολα και ανέξοδα. Η επανάσταση αυτή στις επικοινωνίες συνέβαλε στη διάδοση εγκλημάτων, όπως η παιδοφιλία, και η ανεπιθύμητη αλληλογραφία (spamming**)**.

Στις περιπτώσεις αυτές, τα υποψήφια θύματα αναζητούνται μέσω των νέων καναλιών επικοινωνίας, που προσφέρει το Διαδίκτυο. Ένας άλλος νόμος έχει επίσης προταθεί, ο «Secure IT», ο οποίος είναι παρόμοιος με εκείνον για την ασφάλεια στον κυβερνοχώρο νόμου του 2012. Ο νόμος αυτός διαφέρει στο γεγονός ότι δεν δίνει καμία επιπλέον εξουσία επί των πρακτικών ασφάλειας των εταιρειών. Αντί αυτού, οι εταιρείες θα πρέπει να δαπανήσουν χρήματα για τις πρακτικές ασφαλείας που λειτουργούν καλύτερα γι' αυτούς (Jewkes, 2013).

Παράλληλα, το ηλεκτρονικό έγκλημα έχει εισαγάγει νέους νομοθετικούς προβληματισμούς. Πολλές φορές, καθίσταται αδύνατο να προσδιοριστεί ο τόπος τέλεσης του εγκλήματος, διότι κάθε εγκληματίας μπορεί να το διαπράξει από οποιοδήποτε σημείο του κόσμου, αρκεί να έχει στην διάθεση του έναν ηλεκτρονικό υπολογιστή. Επίσης, είναι δύσκολο να προσδιοριστεί και ο ακριβής χρόνος τέλεσης του, καθώς τα θύματα συχνά αντιλαμβάνονται μια ηλεκτρονική επίθεση πολύ αργότερα από το χρόνο κατά τον οποίο αυτή συνέβη. Επίσης συχνά είναι δυνατή η διαγραφή από τον εισβολέα των «ιχνών» του ηλεκτρονικού εγκλήματος κάτι που δυσχεραίνει ή εμποδίζει την ανίχνευσή του (Ζάννη, 2005).

Το έγκλημα αποτελεί αναπόσπαστο κομμάτι οποιασδήποτε οργανωμένης κοινωνίας. Ανεξάρτητα από τον τόπο και το χρόνο, ορισμένοι άνθρωποι παραβαίνουν τους κοινωνικούς κανόνες με αποτέλεσμα να επιβάλλονται σε αυτούς διάφορες κυρώσεις. Το είδος της αντίδρασης της κοινωνίας, όπως και το είδος της ποινής που θα επιβληθεί σε αυτόν που παρέβη έναν κανόνα, εξαρτώνται από την εποχή και τον πολιτισμό.

Πράγματι κανένα εθνικό χαρακτηριστικό, πολιτικό, κοινωνικοοικονομικό ή νομικό σύστημα, τιμωρία ή μεταχείριση δεν απήλλαξαν ποτέ μια χώρα από το έγκλημα. Απεναντίας, παρατηρείται μια συνεχής τάση αύξησής του και ταυτόχρονα η εμφάνιση νέων μορφών και η αποποινικοποίηση υφιστάμενων εγκλημάτων (Taylor, Fritsch & Liederbach, 2014).

2.5.1 Βασικά Στοιχεία Εγκληματικού Φαινομένου

Τρία είναι τα βασικά στοιχεία που συνθέτουν την εικόνα του εγκληματικού φιανομένου (Φαρσεδάκης, 1996): α) Ο κανόνας (ποινικός νόμος) β) η παράβαση (έγκλημα) και γ) η κύρωση (ποινή).

α) Ο κανόνας: Ο κανόνας αποτελεί την έκφραση της κοινωνίας έναντι κάποιας συμπεριφοράς. Αν ο κανόνας προβλέπει και την επιβολή ποινών, τότε πρόκειται για ποινικό νόμο. Οι ποινικοί νόμοι δεν είναι σταθεροί, αλλά αλλάζουν με το πέρασμα του χρόνου. Εξαρτώνται από πολλούς παράγοντες όπως κοινωνικούς, ηθικούς, πολιτιστικούς, οικονομικούς κ.ά.

β) Το έγκλημα: Το έγκλημα είναι κάτι το αναμενόμενο και φυσικό μέσα σε μια κοινωνία. Θα ήταν αδύνατο όλα τα μέλη μια κοινωνίας να συμμορφώνονται με τους ίδιους κανόνες, καθώς είναι αδύνατο να έχουν την ίδια δομή προσωπικότητας, την ίδια κοινωνική και οικονομική κατάσταση και να έχουν κοινωνικοποιηθεί με τον ίδιο τρόπο.

Εκτός όμως από αναπόφευκτο, το έγκλημα στα πλαίσια μιας κοινωνικής οργάνωσης, όσο και αν έχει ταυτιστεί με κάτι αρνητικό, είναι και χρήσιμο, είτε έμμεσα, είτε άμεσα/έμμεσα, υπό την έννοια, ότι αποτελεί προϋπόθεση για κάθε ηθική και νομική αλλαγή, η οποία είναι απαραίτητη για να μην περιέλθει η κοινωνία σε ανομία. Άμεσα, υπό την έννοια, ότι αποτελεί την πρόγευση της μέλλουσας ηθικής. Για παράδειγμα, η ελευθερία σκέψης και έκφρασης που υπάρχει σήμερα δεν θα είχε επιτευχθεί ποτέ, αν κάποιοι δεν παραβίαζαν τους κανόνες που κάποτε την περιόριζαν.

γ) Η κύρωση: Η κύρωση αποτελεί τη συνέπεια της παράβασης του κανόνα και δηλώνει ότι η συγκεκριμένη συμπεριφορά δεν είναι αποδεκτή από την κοινωνία. Ως προς την αιτιολογία της επιβολής της ποινής έχουν κατά καιρούς διατυπωθεί διάφορες θεωρίες. Οι επικρατέστερες είναι η θεωρία *της ανταπόδοσης* και η *θεωρία της κοινωνικής άμυνας*. Στην περίπτωση της ανταπόδοσης, η επιβολή της ποινής σκοπεύει στην επανόρθωση των επιβλαβών για την κοινωνία συνεπειών του εγκλήματος, με την πληρωμή του κακού που έγινε με άλλο ισάξιο. Στην περίπτωση της άμυνας, η ποινή έχει ως σκοπό, να αποτρέψει κάποιον να εγκληματήσει είτε με τον εκφοβισμό, είτε με τη γενικότερη καλλιέργεια της ιδέας της αποστροφής προς την αδικία.

Οι διαστάσεις της εγκληματικότητας στο χώρο του Διαδικτύου είναι πιο δύσκολο να καθοριστούν από ότι στον «κοινό» εγκληματικό χώρο.

- Σε εγκλήματα που διαπράττονται τόσο σε συμβατικό περιβάλλον όσο και σε περιβάλλον ηλεκτρονικών υπολογιστών. Στην κατηγορία αυτή εντάσσουμε πολλές κατηγορίες εγκλημάτων.
- Διασπορά κακόβουλου λογισμικού (ιών).

Από τα παραπάνω, διαφαίνεται ότι το ηλεκτρονικό έγκλημα συμμετέχει ποικιλότροπα στο εγκληματικό φαινόμενο, τα δε επιμέρους συστατικά του είναι δύσκολο να καθοριστούν με σαφήνεια. Στην διατριβή αυτή, δίνεται έμφαση στα εγκλήματα που διαπράττονται με τη χρήση ηλεκτρονικών υπολογιστών και την ύπαρξη δικτύωσης, στα οποία θα αναφερόμαστε με τον γενικό όρο ηλεκτρονικό έγκλημα, αναφέροντας περιληπτικά, βασικά στοιχεία για τις υπόλοιπες περιπτώσεις.

Για να αποκτήσουν πρόσβαση σε ένα δίκτυο ή υπολογιστικό σύστημα, οι κυβερνοεισβολείς (hackers) χρησιμοποιούν εργαλεία που εκμεταλλεύονται τις αδυναμίες ασφάλειας και τα πιθανά κενά ασφάλειας ή ενδεχόμενα ελατώμματα των συστημάτων. Οι password crackers κάνουν χρήση ενός αρχείου με πιθανούς κωδικούς (δηλαδή ένα σύνολο από λέξεις που έχουν επιλεγεί από κάποιους χρήστες με μεγάλη πιθανότητα), που συχνά αναφέρεται και ως «λεξικό» (dictionary), ενώ η σχετική επίθεση ως «επίθεση λεξικού» (dictionary attack).

Οι επιθέσεις αυτές εκμεταλλεύονται τρεις βασικές ευπάθειες των συστημάτων ελέγχου πρόσβασης με κωδικούς. Πρώτον, το γεγονός ότι το μήκος των κωδικών είναι μικρό με αποτέλεσμα ένα πρόγραμμα να είναι εύκολο να δοκιμάσει όλους τους κωδικούς μήκους 8 χαρακτήρων που επιλέγονται από τους διαθέσιμους χαρακτήρες του πληκτρολογίου. Δεύτερον, οι χρήστες συχνά επιλέγουν εύκολους κωδικούς, όπως ημερομηνίες γέννησης, ονόματα και τοπωνύμια, κάτι που καθιστά το έργο των crackers ακόμη πιο εύκολο. Και, τρίτον, τα αρχεία με τους κωδικούς των χρηστών δεν προστατεύονται σωστά, με αποτέλεσμα, να είναι συχνά εύκολη η υποκλοπή τους από τον διακομιστή όπου έχουν αποθηκευτεί (Taylor, Fritsch & Liederbach, 2014).

Spoofers: Πρόκειται για προγράμματα που αλλάζουν τη διεύθυνση IP του Η/Υ του επιτιθέμενου προκειμένου να μην ανιχνεύονται οι επιθέσεις του, ή με σκοπό την ενοχοποίηση κάποιου άλλου χρήστη. Συχνά, ανυποψίαστοι χρήστες του Διαδικτύου κατηγορούνται για ηλεκτρονικά εγκλήματα επειδή κάποιος κακόβουλος χρησιμοποίησε την IP διεύθυνσή τους.

2.5.2 Διαδικτυακή Ηλεκτρονική Τρομοκρατία

Ηλεκτρονική Διαδικτυακή Τρομοκρατία ονομάζεται η δραστηριότητα εκείνη που κατατείνει στην καταστροφή ή τη φθορά συστημάτων, που η λειτουργία τους υποστηρίζεται από υπολογιστές, με σκοπό την αποσταθεροποίηση μιας χώρας ή την άσκηση πίεσης σε μια κυβέρνηση. Κατά μια δεύτερη προσέγγιση, ως ηλεκτρονική τρομοκρατία θα μπορούσε να ορισθεί ότι είναι κάθε ενέργεια που αποσκοπεί στην αποσταθεροποίηση μιας χώρας ή στην άσκηση πίεσης σε μια κυβέρνηση, με την ανάπτυξη δραστηριότητας που περιλαμβάνει όλο το φάσμα των ηλεκτρονικών εγκλημάτων μέσω υπολογιστή, ή σε βάρος υπολογιστικών συστημάτων μέσω του διαδικτύου (Taylor, Fritsch & Liederbach, 2014).

Ένας τρίτος ορισμός της ηλεκτρονικής τρομοκρατίας θα μπορούσε να ορισθεί ως η έξυπνη εκμετάλλευση συστημάτων και ηλεκτρονικών υπολογιστών ή άλλων δικτυακών υποδομών και μέσων, εναντίον φυσικών προσώπων, ή ιδιωτικής περιουσίας για τον εκφοβισμό ή τον εξαναγκασμό κυβερνήσεων ή πληθυσμιακών ομάδων, για την προώθηση πολιτικών ή κοινωνικών στόχων.

Κατά μία τέταρτη εκδοχή, ως ηλεκτρονική τρομοκρατία μπορεί να ορισθεί η προμελετημένη επίθεση εθνικών υποομάδων ή μυστικών πρακτόρων με πολιτικά κίνητρα, εναντίον πληροφοριακών συστημάτων, ηλεκτρονικών υπολογιστών, προγραμμάτων λογισμικού και δεδομένων, που έχει βίαιες επιπτώσεις σε μη στρατιωτικούς στόχους.

Επίθεση εναντίον συστημάτων πληροφορικής μπορεί να εννοηθεί με τρεις τρόπους: φυσική καταστροφή του συστήματος και του περιβάλλοντος χώρου, τακτική επίθεση πρώτου επιπέδου στο λογισμικό του συστήματος και η τακτική επίθεση δευτέρου επιπέδου που είναι και η πλέον επικίνδυνη μέχρι να γίνει αντιληπτή.

1. Η φυσική επίθεση αναφέρεται στην καταστροφή του χώρου λειτουργίας του υπολογιστικού συστήματος με τις συμβατικές μεθόδους (καταστροφή με εμπρησμό του χώρου, θραύση των υποδομών, κλοπή των κυρίων συστημάτων, πρόκληση εκρήξεων, πλημμυρών κ.λ.π.).
2. Η τακτική επίθεση πρώτου επιπέδου περιλαμβάνει την κρυφή αλλοίωση βασικών παραμέτρων του συστήματος, που έχει ως σκοπό την εισαγωγή καθυστερήσεως εκτέλεσης προγραμμάτων και την απρόβλεπτη συμπεριφορά του συστήματος.
3. Η τακτική επίθεση δευτέρου επιπέδου αναφέρεται στην προσχεδιασμένη τροποποίηση των εισερχομένων και εξερχόμενων πληροφοριών ενός συστήματος, με τέτοιο τρόπο που οι χρήστες και διαχειριστές του συστήματος να εξακολουθούν να θεωρούν φυσιολογική λειτουργία και η ανταπόκρισή του, ενώ το σύστημα οδηγείται σταδιακά σε πλήρη σύγχυση, σε

λανθασμένη εκτέλεση προγραμμάτων(κατά τη βούληση του επιτιθέμενου) και τελικά στην πτώση του.

2.5.3 Η ταυτότητα των επιθέσεων και του επιτιθέμενου

Ένας επιτιθέμενος μπορεί να είναι ο μαθητής ενός σχολείου που επιθυμεί την καταστροφή των στοιχείων ελέγχου της προόδου του, τρομοκρατικές ομάδες εναντίον κρατικών υποδομών, φορολογούμενοι επιχειρηματίες σε γραφεία ΔΟΥ, διάδικοι σε γραφεία Πρωτοδικείων κ.λ.π.

Οι επιθέσεις σε πρώτο επίπεδο (τακτική επίθεση πρώτου επιπέδου) φαίνεται να κατευθύνονται σε συνδεδεμένα υπολογιστικά συστήματα με σκοπό την διαγραφή αρχείων, ενώ συχνά γίνεται σκόπιμη εμφύτευση ενός ιού σε ένα δίκτυο, προκειμένου να προκληθεί λειτουργική ανωμαλία τόσο σε αυτό όσο και στην υποδομή των χρηστών, ή επιχειρείται ο «τηλεχειρισμός» υπολογιστή μέσω εμφύτευσης ειδικών προγραμμάτων από τους επιτιθέμενους. Ο επιτιθέμενος μπορεί να είναι δυσαρεστημένος υπάλληλος του χώρου, υπάλληλος ανταγωνιστικού χώρου, ή και κάποιος παράνομος εισβολέας (hacker) που δοκιμάζει τις προστασίες και τις αντοχές του συστήματος. Η επίθεση αυτή αφορά το συγκεκριμένο εργασιακό χώρο ή φορέα και δεν στρέφεται εναντίον της κρατικής εξουσίας, ούτε φαίνεται ικανή να απειλήσει την κρατική οντότητα.

Ο επιτιθέμενος σχεδιάζει τις ενέργειές του με ιδιαίτερη προσοχή και στοχεύει στην πρόκληση σοβαρής ανωμαλίας και εντέλει στην καταστροφή του υπολογιστικού συστήματος. Αν μελετηθεί η ταυτότητα του επιτιθέμενου θα επέλθει η σκέψη ότι αυτός μπορεί να είναι οποιοσδήποτε ευφάνταστος εισβολέας, μέχρι την καλύτερα οργανωμένη τρομοκρατική οργάνωση.

Το διαδίκτυο μπορεί να χρησιμοποιηθεί κατάλληλα από έναν τρομοκράτη, αφού παρουσιάζει μια σειρά πλεονεκτημάτων. Ο τρομοκράτης μπορεί να δρα από απόσταση, να μην διαθέτει οικονομικούς πόρους για επιθέσεις και να αποφεύγει τις αιματηρές επιθέσεις με εκρηκτικά και άλλα ηχηρά μέσα, στην προσπάθεια της επιδίωξης δημοσιότητας. Οι σοβαρές επιθέσεις στο διαδίκτυο ή και η προβολή θεμάτων τρομοκρατίας με έμμεση χρήση του διαδικτύου, γοητεύει κοινό και δημοσιογράφους. Η αξία του Διαδικτύου είναι σημαντικότερη για τους επιδιωκόμενους σκοπούς, αφού και για αυτόν αποτελεί ένα αρκετά ασφαλές εργαλείο. Έχει διαπιστωθεί από διάφορες τρομοκρατικές ομάδες να χρησιμοποιούν μονίμως το διαδίκτυο με καλυμμένο τρόπο για να συντονίζουν τις δραστηριότητές τους και να τακτοποιούν οικονομικές υποθέσεις τους, παρά για να κάνουν καταστροφικές επιθέσεις, τουλάχιστον ενάντια στο ίδιο το διαδίκτυο (Frey, 2003).

Εξετάζοντας από μια άλλη οπτική γωνία και με σχετική αντικειμενικότητα το θέμα της διαδικτυακής τρομοκρατίας, θα διαπιστωθεί ότι υπάρχει διάχυτη μια εικόνα αβεβαιότητας και συνεπακόλουθα μια τάση μεγαλοποίησης και υπερβολής των απειλών και των αποτελεσμάτων που αυτές θα επιφέρουν. Κρίνοντας από τις μέχρι τώρα επιθέσεις κατά του Διαδικτύου, διαπιστώνεται ότι οι περισσότερο καταστροφικές επιθέσεις, έχουν διαπραχθεί από διασπορά ιών και από hackers που περιφέρονται παντού ή διαμαρτύρονται για κάθε είδους ζητήματα και από άτομα που επιδιώκουν να κάνουν κακό σε προηγούμενους εργοδότες τους.

Στην ελληνική πραγματικότητα, ομάδες εργαζομένων σε δημόσιο και ιδιωτικό τομέα, εκμεταλλευόμενες την αλλαγή της χιλιετίας, κατάφεραν να αντικαταστήσουν τον εξοπλισμό πληροφορικής με νεότερες εκδόσεις, διαδίδοντας από το πρώτο εξάμηνο του 1999 ότι θα γίνουν βιβλικές καταστροφές σε υποδομές, σε ενεργειακά συστήματα, στις συγκοινωνίες, στις επικοινωνίες κλπ. Μάλιστα, οι συντάκτες τέτοιων εκθέσεων έφθαναν σε σημείο να κατασκευάζουν τερατώδη ψεύδη για να πείσουν τους αρμόδιους να διαθέσουν τα απαραίτητα κονδύλια και μάλιστα αμέσως, για την αντικατάσταση του εξοπλισμού που αποδεδειγμένα ήταν συμβατός με την αλλαγή της χρονολογίας (τετραψήφιο πεδίο).

2.5.4 Από το συμβατικό στο Ηλεκτρονικό Έγκλημα

Το έγκλημα, ως αναπόσπαστο κομμάτι κάθε κοινωνίας, έχει τη μορφή ενός ζωντανού οργανισμού. Συνεχώς μεταβάλλονται οι μορφές του, τα μέσα διάπραξής του και η νομοθεσία που το διέπει. Στις αρχές του 20ου αιώνα, καινούριοι τρόποι-τεχνικές για τη διάπραξη εγκλημάτων έκαναν την εμφάνισή τους (Goodman & Brenner, 2002).

Ίσως τότε κανείς δεν μπορούσε να φανταστεί τι θα επακολουθούσε. Με την εμφάνιση και την ανάπτυξη της τεχνολογίας των ηλεκτρονικών υπολογιστών, συντελούνται αλλαγές στο εγκληματικό φαινόμενο, που ποτέ πριν δεν είχε γνωρίσει η ανθρωπότητα. Οι εγκληματικές απειλές στηρίζονται πλέον σε πιο περίπλοκη τεχνολογία, καταργώντας τα φυσικά όρια. Βέβαια τόσο το συμβατικό έγκλημα όσο και τα μέσα διάπραξης του συνεχίζουν να υπάρχουν, ωστόσο εμφανίζονται νέες μορφές με χαρακτηριστικότερη αυτή του ηλεκτρονικού εγκλήματος, του εγκλήματος δηλαδή που ένας ηλεκτρονικός υπολογιστής ή παρόμοιες συσκευές ηλεκτρονικής επεξεργασίας δεδομένων, διαδραματίζουν κυρίαρχο ρόλο (Casey, 2011).

Ακόμη όμως και τα πρώτα χρόνια έπειτα από την εμφάνιση των υπολογιστών, το ηλεκτρονικό έγκλημα ήταν σπάνιο, διότι ο αριθμός τους ήταν περιορισμένος. Επιπλέον, οι υπάρχοντες υπολογιστές χρησιμοποιούσαν γλώσσα μηχανής, καθιστώντας αδύνατο για τους επίδοξους εγκληματίες να κατέχουν την απαραίτητη γνώση ή τον εξοπλισμό (Frey, 2003). Ο ηλεκτρονικός υπολογιστής αποτελούσε είδος πολυτελείας και κατ' αυτήν την έννοια το ηλεκτρονικό έγκλημα ήταν έγκλημα για λίγους.

Χρονικά, η ανάπτυξη του ηλεκτρονικού εγκλήματος τοποθετείται στην τελευταία δεκαετία του περασμένου αιώνα, σε μια εποχή που χαρακτηρίστηκε από την αλματώδη εξέλιξη των υπολογιστικών συστημάτων. Σήμερα, το μεγαλύτερο ποσοστό του πληθυσμού στις αναπτυγμένες χώρες, έχει πρόσβαση σε ένα Η/Υ, η δε χρήση του έχει απλοποιηθεί τόσο που ακόμη και ένα μικρό παιδί μπορεί να χειρίζεται έναν προσωπικό υπολογιστή με ιδιαίτερη δεξιότητα (Ζάννη, 2005).

Η μεγάλη επανάσταση στον τομέα του ηλεκτρονικού εγκλήματος, επήλθε μετά την εμφάνιση των δικτύων. Τα δίκτυα, δημιούργησαν νέες διόδους πρόσβασης προς την πληροφορία, καθιστώντας μη αναγκαία την παρουσία του επιτιθέμενου στο χώρο όπου αυτή φυλάσσεται. Η τεράστια πληροφοριακή δεξαμενή που δημιουργήθηκε και συνεχίζει να επεκτείνεται, αποτέλεσμα της διασύνδεσης εκατομμυρίων υπολογιστών ανά τον κόσμο, μετέβαλε ριζικά τον τρόπο ζωής του σύγχρονου ανθρώπου. Σήμερα, οι υπολογιστές χρησιμοποιούνται σε όλες τις εκφάνσεις της καθημερινής μας δραστηριότητας και στους σκληρούς τους δίσκους αποθηκεύονται πληροφορίες για τα προσωπικά μας στοιχεία, τους τραπεζικούς μας λογαριασμούς, τις συνήθειες μας, τις προτιμήσεις μας κ.ά.

Το νέο περιβάλλον, χαρακτηρίζεται από την ευρεία ανάπτυξη του ηλεκτρονικού εμπορίου, την πραγματοποίηση τραπεζικών και συναλλαγματικών πράξεων μέσω του Διαδικτύου, την άμεση επικοινωνία σε όλα τα επίπεδα με νέες διόδους (e-mail, chat, newsgroups κ.λ.π.), αλλά και την εξ αποστάσεως εκπαίδευση, την πραγματοποίηση συναλλαγών με δημόσιες υπηρεσίες, την τηλεδιάσκεψη κ.ά.

Οι ευκαιρίες για εγκληματική δραστηριότητα είναι περισσότερες από ποτέ. Το ηλεκτρονικό έγκλημα είναι ευκολότερο, οι δε δυνατότητες δίωξής του από τις αρμόδιες αρχές είναι περιορισμένες λόγω έλλειψης εμπειρίας στο σχετικό τομέα, ελλιπούς εκπαίδευσης αλλά και ασαφούς νομοθετικού πλαισίου, γεγονός που ενθαρρύνει τους επίδοξους εγκληματίες (Frey, 2003).

2.5.5 Εγκλήματα που τελούνται με την χρήση Η/Υ

Πολλά από τα υπάρχοντα εγκλήματα του κοινού ποινικού δικαίου τελούνται με τη βοήθεια και τη χρήση των ηλεκτρονικών υπολογιστών. Ο υπολογιστής μπορεί να χρησιμοποιηθεί ποικιλότροπα στην τέλεση των εγκλημάτων αυτών, όπως:

- Για την αποθήκευση δεδομένων, που σχετίζονται με πρόσωπα και αντικείμενα που εμπλέκονται σε μια παράνομη δραστηριότητα π.χ. προσωπικά στοιχεία εμπόρων ναρκωτικών.
- Για την εύρεση πληροφοριών, σχετικών με μια παράνομη δραστηριότητα π.χ. πώς κατασκευάζεται μια βόμβα.
- Για τη διάδοση πληροφοριών, π.χ. συκοφαντικών έναντι ενός ή περισσοτέρων προσώπων.
- Για την τέλεση μέρους της εγκληματικής πράξης, π.χ. την αγορά αγαθών με χρήση πιστωτικών καρτών που έχουν κλαπεί με φυσικό τρόπο.
- Για τη διακίνηση παράνομου οπτικοακουστικού υλικού π.χ. παιδική πορνογραφία.

2.5.6 Απάτη στο Διαδίκτυο

Η απάτη στο συμβατικό κόσμο είναι ένα από τα πιο συνηθισμένα εγκλήματα. Η εμφάνιση, όμως, και η ανάπτυξη του Διαδικτύου, μεγιστοποίησε τις δυνατότητες για διάπραξη νέων μορφών απάτης. Η τάση αυτή, αυξήθηκε ακόμη περισσότερο, με την εξάπλωση του ηλεκτρονικού εμπορίου, που είχε ως επακόλουθο την ανάπτυξη οικονομικών συναλλαγών με τη χρήση του Διαδικτύου.

Ακολουθούν, οι κυριότερες μορφές απάτης μέσω του Διαδικτύου (Taylor, Fritsch & Liederbach, 2014) :

1. Απάτη με ηλεκτρονικό ταχυδρομείο e-mail: Η απάτη, με τη χρήση του ηλεκτρονικού ταχυδρομείου, αποτελεί την συχνότερη μορφή επιθέσεως, έναντι των χρηστών του Διαδικτύου. Οι επαγγελματίες του είδους, συνεχώς, βρίσκουν νέους τρόπους για να εξαπατήσουν ανυποψίαστους χρήστες, χρησιμοποιώντας μηνύματα ηλεκτρονικού ταχυδρομείου, που προβάλλουν διάφορες δικαιολογίες, με μοναδικό σκοπό, την απόσπαση χρηματικών ποσών και προσωπικών στοιχείων. Χαρακτηριστικές περιπτώσεις απάτης με e-mail, αποτελούν οι νιγηριανές επιστολές και το ισπανικό λόττο.

Οι απάτες προσωπικών πληροφοριών (phishing) είναι σήμερα το πιο δημοφιλές και κατά συνέπεια η πιο επικίνδυνη μορφή απάτης ηλεκτρονικού ταχυδρομείου. Χρησιμοποιούν τα μηνύματα ηλεκτρονικού ταχυδρομείου που φαίνεται να προέρχονται από μια νόμιμη επιχείρηση ή φορέα, όπως μια τράπεζα ή πανεπιστήμιο, και ζητάνε να "ενημερώσουν" ή να "ελέγξουν" τις προσωπικές πληροφορίες. Οι απατεώνες στη συνέχεια θα χρησιμοποιήσουν αυτές τις πληροφορίες για να διαπράξουν κλοπή ταυτότητας.

Στην πρώτη περίπτωση, το θύμα λαμβάνει ένα e-mail από φερόμενο υπήκοο Αφρικανικής χώρας, ο οποίος ζητάει την βοήθειά του για την μεταφορά μεγάλου χρηματικού ποσού από την χώρα του στο εξωτερικό. Ο αποστολέας προβάλλει διάφορες δικαιολογίες (πόλεμος, θάνατος γονέων, φυσικές καταστροφές κ.λ.π.) και ζητά από το θύμα, το άνοιγμα τραπεζικού λογαριασμού με συνδικαιούχο τον ίδιο, τη γνωστοποίηση των στοιχείων του και την κατάθεση χρηματικού ποσού για έξοδα κίνησης. Σε αντάλλαγμα, προσφέρει μεγάλο μερίδιο του μεταφερόμενου ποσού, όταν ολοκληρωθεί η συναλλαγή. Ένας πολύ κοινός τύπος της απάτης με email είναι τα εκ των προτέρων συστήματα απάτης χρέωσης. Οι δράστες της απάτης εκ των προτέρων (μερικές φορές αναφέρονται ως Νιγηριανές ή απάτες ξένης τράπεζας) είναι συχνά πολύ δημιουργικοί και καινοτόμοι. Αυτή η απάτη επίσης ονομάζεται 4-1-9 απάτη ονομαζόμενη από το τμήμα ποινικού κώδικα της Νιγηρίας που

ασχολείται με συστήματα απάτης. Νιγηριανοί υπήκοοι, που υποτίθεται ότι είναι υπάλληλοι της κυβέρνησης ή τραπεζικά ιδρύματα, θα στείλουν με φαξ ή ηλεκτρονικό ταχυδρομείο επιστολές σε ιδιώτες και επιχειρήσεις στις ΗΠΑ και σε άλλες χώρες.

Τα θύματα, τα οποία καλούνται να παράσχουν κεφάλαια για την κάλυψη των διαφόρων τελών, καθώς επίσης καλούνται για προσωπική χρήση, όπως αριθμοί κοινωνικής ασφάλισης, αριθμοί τραπεζικών λογαριασμών, και άλλα παρόμοια στοιχεία. Μόλις ληφθεί αυτή η πληροφορία, τα θύματα συχνά διαπιστώνουν ότι οι τραπεζικοί λογαριασμοί τους έχουν αδειάσει. Είναι δύσκολο να εντοπιστεί το ποσό που έχει χαθεί σε αυτές τις απάτες αφού πολλά από τα θύματα δεν καταγγέλλουν τις απώλειές τους στις αρχές από αμηχανία (Casey, 2011).

Στη δεύτερη περίπτωση, που είναι παρόμοια με τις Νιγηριανές επιστολές, Αφρικανοί υπήκοοι, κάτοικοι Ισπανίας, αποστέλλουν e-mails σε ανυποψίαστους χρήστες, ζητώντας τους προσωπικά στοιχεία και αριθμούς τραπεζικών λογαριασμών, προκειμένου να τους μεταβιβάσουν τα κέρδη από την υποτιθέμενη νίκη τους στο Ισπανικό ΛΟΤΤΟ. Στη συνέχεια, εφόσον τα θύματα έχουν πεισθεί ότι έχουν κερδίσει, τους ζητούν να τους καταβληθούν χρήματα για διαδικαστικά έξοδα. Με τον τρόπο αυτό, κατορθώνουν να αποσπούν σημαντικά χρηματικά ποσά (Frey, 2003).

Το FBI και η αμερικανική υπηρεσία ταχυδρομείων, μαζί με άλλους εταίρους, έχουν ξεκινήσει μια ιστοσελίδα για να εκπαιδεύσουν το κοινό σχετικά με την ασφάλεια στο Διαδικτύο και να παρέχουν μια κεντρική θέση για τους καταναλωτές όπου μπορούν να υποβάλλουν καταγγελίες. Η ιστοσελίδα προσφέρει ένα διαδραστικό-ηλεκτρονικό τεστ κινδύνου διαδικτυακής απάτης που επιτρέπει στους χρήστες να μετρήσουν online συνήθειες ασφάλειας που σχετίζονται με την κλοπή ταυτότητας, οικονομική απάτη, δημοπρασίες στο Internet, πλαστογραφίας, απάτες λοταρίας, και της ιδιωτικής ζωής του υπολογιστή. Επίσης, παρέχει συμβουλές για την πρόληψη, λεπτομέρειες για τις τρέχουσες απάτες στον κυβερνοχώρο, προειδοποιεί τους καταναλωτές, τις ιστορίες των θυμάτων, και μια ευκαιρία να μοιραστούν τις ιστορίες της απάτης στον κυβερνοχώρο (Frey, 2003).

2. Απάτη με πιστωτικές κάρτες: Η χρήση πιστωτικών καρτών στο Διαδίκτυο, για τη διεκπεραίωση πάσης φύσεως συναλλαγών (π.χ. μέσω του ηλεκτρονικού εμπορίου), έχει δημιουργήσει νέες δυνατότητες για τη διάπραξη εγκλημάτων (Frey, 2003).

Με τη χρήση των σύγχρονων τεχνολογιών δεν απαιτείται, πλέον, ιδιαίτερη δεξιότητα για να αποκτήσει κάποιος τον αριθμό μιας πιστωτικής κάρτας και να πραγματοποιήσει αγορές μέσω του Διαδικτύου. Με την τεχνολογία «websniffer», παρακολουθείται η μετάδοση δεδομένων και ανακτώνται αυτόματα δεκαεξαψήφιοι αριθμοί πιστωτικών καρτών. Επιπλέον, είναι δυνατή η αγορά μέσω του Διαδικτύου, αριθμών πιστωτικών καρτών που έχουν υποκλαπεί. Τέλος, υπάρχουν και εφαρμογές λογισμικού, που δημιουργούν αυτόματα αριθμούς πιστωτικών καρτών, χρησιμοποιώντας διάφορους λογάριθμους (Frey, 2003).

3. Παράνομη υποκλοπή τηλεφωνικών συνδιαλέξεων και ηλεκτρονικής παρακολούθησης: Πρώτη μεταξύ αυτών είναι η απαγόρευση για την παράνομη υποκλοπή τηλεφωνικών συνδιαλέξεων και ηλεκτρονικής παρακολούθησης που καλύπτει (Cook & Sobieski ,2014):

Οποιοδήποτε πρόσωπο που σκόπιμα υποκύπτει σε παρακολουθήσεις, ή προσπαθεί να υποκλέψει, ενσύρματα, από του στόματος, ή μέσω ηλεκτρονικών επικοινωνιών χρησιμοποιώντας ηλεκτρονική, μηχανική, ή άλλη συσκευή εκτός εάν φέρει ειδική άδεια ή καλύπτεται ρητά από τον νόμο ή από κάποια σύμβαση, π.χ.

- Ένα από τα μέρη που συμμετέχουν στη συνομιλία έχει συναινέσει στην υποκλοπή,
- Η παρακολούθηση που γίνεται σε συμμόρφωση με τον νόμο επιτρέπεται (και συνήθως υπό δικαστική επίβλεψη) την επιβολή του νόμου ή ξένες

μυστικές υπηρεσίες συλλογή υποκλοπή,

- Η παρακολούθηση παρουσιάζεται ως μέρος της παροχής ή τη ρύθμιση της επικοινωνίας υπηρεσιών,
- Ορισμένες ραδιοφωνικές εκπομπές

4. Συστήματα πυραμίδας: Είναι σύστημα ιεράρχησης (Jewkes & Yar, 2013).

5. Συστήματα Ponzi: Παίρνουν το όνομά τους από τον Charles Ponzi, ο οποίος έτρεξε ένα τέτοιο σύστημα στην περίοδο 1919-1920. Το σύστημα Ponzi είναι ένα επενδυτικό σχήμα στο οποίο οι αποδόσεις καταβάλλονται στους προηγούμενους επενδυτές από τα χρήματα που καταβάλλονται στο σύστημα από νεότερους επενδυτές.

Τα συστήματα Ponzi είναι παρόμοια με τα συστήματα πυραμίδων, αλλά διαφέρουν στο ότι τα συστήματα Ponzi, εκτελούνται από μια κεντρική επιχείρηση ή πρόσωπο, που μπορεί να κάνει ψευδείς ισχυρισμούς σχετικά με το πώς τα χρήματα επενδύονται.

Τα συστήματα Ponzi δεν συνεπάγονται κατ' ανάγκη μια ιεραρχική δομή, όπως σε μια πυραμίδα. Υπάρχει μόνο ένα άτομο ή εταιρεία για είσπραξη των χρημάτων από τους νέους συμμετέχοντες. (Jewkes & Yar, 2013).

6. Πολυεπίπεδα συστήματα μάρκετινγκ (MLM-Multi level Marketing): Πολυεπίπεδα σχέδια μάρκετινγκ, γνωστά ως δίκτυα εμπορίας, είναι ένας τρόπος πώλησης αγαθών ή υπηρεσιών μέσω των διανομέων. Τα σχέδια MLM συνήθως υπόσχονται να πληρώσουν τις προμήθειες μέσω δύο ή περισσότερων επίπεδων προσλήψεων. Ενώ ορισμένα προγράμματα MLM υποτίθεται ότι είναι νόμιμα, εφόσον προσφέρονται να πληρώσουν τις προμήθειες για την πρόσληψη νέων διανομέων, κατά πάσα πιθανότητα είναι παράνομα. Στις περισσότερες χώρες, απαγορεύεται η πρακτική αυτή. (Jewkes, 2013).

7. Chain Mails: Τα chain mails είναι μια μορφή ανεπιθύμητης αλληλογραφίας. Ένα μήνυμα ηλεκτρονικού ταχυδρομείου αλυσίδας/ chain στέλνεται γενικά σε πολλά άτομα και περιλαμβάνει οδηγίες όπου κάθε άτομο πρέπει να διαβιβάσει την επιστολή σε αρκετούς άλλους. Αυτά τα μηνύματα σπαταλούν πόρους του συστήματος και συχνά αναπτύσσονται σε αρκετά μεγάλο αριθμό ατόμων ως αποστολείς που επισυνάπτουν τις δικές τους προσθήκες.

2.5.7 Κρυπτογραφία

Η Κρυπτογραφία είναι η επιστήμη που ασχολείται με τη μελέτη της ασφαλούς επικοινωνίας και της ανάκτησης πληροφοριών. Διακρίνεται στους παρακάτω κλάδους: (Aaron, 2005).

- Κρυπτογραφία: Ο όρος προέρχεται από τις ελληνικές λέξεις "κρυφό" και "γραφή" και κυριολεκτικά σημαίνει μελέτη της μυστικής γραφής. Σε γενικές γραμμές, είναι ο τομέας που ασχολείται με τη μελέτη, τη χρήση και την ανάπτυξη της αποκρυπτογράφησης και κρυπτογράφησης, τεχνικές που κρύβουν τα περιεχόμενα των μηνυμάτων (ή αποθηκευμένα δεδομένα) και διευκολύνει τον εντοπισμό των κακόβουλων τροποποιήσεων στα μηνύματα.
- Κρυπτανάλυση: Είναι η διαδικασία της προσπάθειας να αποκαλυφθεί το αρχικό κείμενο ή το κλειδί από μη εξουσιοδοτημένα πρόσωπα - επίδοξους επιτιθέμενους.
- Κρυπτογράφηση: Η κρυπτογράφηση αφορά την ίδια την διαδικασία μετασχηματισμού ενός μηνύματος σε μια ακατανόητη μορφή χρησιμοποιώντας έναν αλγόριθμο κρυπτογράφησης, προκειμένου να μην μπορούν να διαβαστεί από τρίτους (άλλα από τους προβλεπόμενους αποδέκτες).
- Αποκρυπτογράφηση: Είναι η διαδικασία ανάκτησης του αρχικού μηνύματος (αναγνώσιμο) από μια ακατανόητη έκδοση που παρήχθη από μια

διαδικασία κρυπτογράφησης. Η αποκρυπτογράφηση γίνεται από εξουσιοδοτημένο άτομο, σε αντίθεση με την κρυπτανάλυση (Aaron, 2005).

Το κρυπτογράφημα αποκρυπτογραφείται για να ανακτήθει το απλό κείμενο. Η κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος λαμβάνει χώρα μέσω ενός αλγορίθμου κρυπτογράφησης και ενός κλειδιού κρυπτογράφησης. Ο κρυπτογραφικός αλγόριθμος (cipher) είναι η μέθοδος (συνήθως μια μαθηματική συνάρτηση) για την μετατροπή των δεδομένων σε μορφή που δεν επιτρέπει σε μη εξουσιοδοτημένους τρίτους να έχουν πρόσβαση στα περιεχόμενα τους. Η δυνατότητα, ωστόσο, για διατήρηση της μυστικότητας των πληροφοριών βασίζεται περισσότερο στο κλειδί, το οποίο είναι ένας αριθμός από διάφορα bits που χρησιμοποιείται ως είσοδος για τη λειτουργία κρυπτογράφησης (Aaron, 2005).

ΚΕΦΑΛΑΙΟ 3 ΣΥΓΚΡΙΣΗ ΕΦΑΡΜΟΣΤΕΟΥ ΔΙΚΑΙΟΥ ΣΤΗΝ ΕΚ ΚΑΙ ΔΙΚΑΙΑ ΑΛΛΩΝ ΧΩΡΩΝ (U.K , U.S.A)

Μέσα από τη παρούσα ενότητα θα γίνει επιχειρηθεί μια συγκριτική παρουσίαση και ανάλυση του εφαρμοστέου δικαίου τόσο στην ΕΕ, όσο στο Ηνωμένο Βασιλείου και τις ΗΠΑ.

3.1 Η.Π.Α

Στην Αμερική υπογράφηκε ο ομοσπονδιακός νόμος Ασφάλειας Πληροφοριών Federal Information Security Modernization Act (FISMA) από τον Πρόεδρο του E-Government Act το 2002. Από τότε τροποποιήθηκε ξανά αρκετές φορές. Άλλοτε εστίασε περισσότερο στη μείωση ή την εξάλειψη των απορριμμάτων χαρτιού και άλλοτε στην τυποποίηση των τεχνολογιών και διαδικασιών, ή την εξασφάλιση των πόρων της κυβέρνησης. Όλοι αυτοί οι νόμοι σχεδιάστηκαν για να δώσουν στην ομοσπονδιακή κυβέρνηση εργαλείο αντιμετώπισης του μεταβαλλόμενου κόσμου της τεχνολογίας.

Οι πρώτοι νόμοι (Government Paper Reduction Act 1980 και 1995 (PRA) και Government Paper Elimination Act του 1998 (GPEA)) είχαν ως στόχο να μετακινήσουν την ομοσπονδιακή κυβέρνηση από μια γραφειοκρατία που βασίζεται στο χαρτί, όπου ανακολουθίες σε όλους τους οργανισμούς οδήγησαν σε σπατάλη χρημάτων και πόρων, σε μια «αποδοτική, αποτελεσματική και οικονομική» κυβέρνηση που μοιράζεται πληροφορίες και πόρους αξιοποιώντας την τεχνολογία και όλα όσα είχε να προσφέρει (Webb, 2003).

Σύντομα ακολούθησαν η Πράξη Ασφάλειας Υπολογιστών του 1987 (CSA Computer Security Act) και η Μεταρρύθμιση και Διαχείριση των τεχνολογιών της πληροφορίας (The Information Technology Management Reform Act). Προκειμένου να συνδράμει στις ομοσπονδιακές υπηρεσίες για να συμμορφώνονται με αυτούς τους νόμους, το Γραφείο Διαχείρισης και Προϋπολογισμού (OMB) κυκλοφόρησε την Εγκύκλιο Α-130. Η Εγκύκλιος Α-130 απαιτεί από τις ομοσπονδιακές υπηρεσίες:

- Να μεριμνήσουν για την ασφάλεια
- Να εξασφαλίσουν τους αρμόδιους υπαλλήλους στους οποίους ανατίθεται η ευθύνη της ασφάλειας
- Να επανεξετάζουν περιοδικά τους ελέγχους ασφαλείας στα πληροφοριακά συστήματα
- Να επιτρέπουν την επεξεργασία του συστήματος πριν από την εργασία, και σε τακτά χρονικά διαστήματα.

Το FISMA (Federal Information Security Modernization Act) εισήχθη στο πλαίσιο του νόμου περί Ηλεκτρονικής Διακυβέρνησης, καθιστώντας τις διατάξεις GISRA (Government Information Security Reform Act) μόνιμες. Ο στόχος της FISMA είναι να «απαιτεί από κάθε ομοσπονδιακή υπηρεσία, έγγραφα και να εφαρμόζει ένα πρόγραμμα ασφάλειας των πληροφοριών σε επίπεδο οργανισμού για να παρέχει ασφάλεια των πληροφοριών που υποστηρίζουν τις δραστηριότητες και τα στοιχεία του οργανισμού, συμπεριλαμβανομένων εκείνων που παρέχονται ή διαχειρίζονται από άλλο οργανισμό, εργολάβο, είτε άλλη πηγή (Enloe, 2002). Στο λευκό οίκο ο πρόεδρος είναι υπεύθυνος για την επίβλεψη του Εκτελεστικού Γραφείου του Προέδρου, το οποίο περιλαμβάνει: το Γραφείο Διαχείρισης και Προϋπολογισμού (OMB), το Εθνικό Συμβούλιο Ασφαλείας, το Γραφείο Εσωτερικής Ασφάλειας και το Γραφείο Επιστημονικής και Τεχνολογικής Πολιτικής. Τα γραφεία αυτά είναι κυρίως υπεύθυνα για την παροχή συμβουλών στον πρόεδρο για τα θέματα που αφορούν τους τομείς της ειδικότητάς τους και ως εκ τούτου έχουν σημαντική επιρροή στις αποφάσεις της πολιτικής και τη σύνταξη των εκτελεστικών διαταγμάτων.

Παρακάτω αναφέρονται οι τομείς που δραστηριοποιούνται τα παραπάνω γραφεία τα οποία ευθύνονται για τη παροχή συμβουλών στα ζητήματα στα οποία το καθένα εξειδικεύεται:

- Γραφείο Διαχείρισης και Προϋπολογισμού (OMB - Office of Management and Budget: Ο OMB απαιτεί να ληφθούν πρωτοβουλίες σε νομοθετικό επίπεδο για τη μείωση γραφειοκρατίας για την "ανάπτυξη και εφαρμογή ομοιόμορφης και συνεπούς πληροφόρησης των πολιτικών διαχείρισης των πόρων ", καθώς και για την παρακολούθηση, την αξιολόγηση και τη μέτρηση της συμμόρφωσης. Το Γραφείο OMB είναι υπεύθυνο για την επίβλεψη C & A και την αναφορά των αποτελεσμάτων στο Κογκρέσο. Το OMB περιλαμβάνεται στο Εκτελεστικό Γραφείο του Προέδρου.
- Το Υπουργείο Εμπορίου: Το υπουργείο Εμπορίου επιβλέπει ένα ευρύ φάσμα θεμάτων που κυμαίνονται από την διεξαγωγή των εμπορικών συναλλαγών, την οικονομία, τις στατιστικές, την απογραφή, τον καιρό, και την τεχνολογική καινοτομία. Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) είναι μια Υπηρεσία Διοίκησης της Τεχνολογίας του Τμήματος Εμπορίου.
- Γραφείο Ηλεκτρονικής Διακυβέρνησης: Το Γραφείο Ηλεκτρονικής Διακυβέρνησης δημιουργήθηκε στο πλαίσιο του E-Government Act του 2002 για την «βελτίωση διακυβέρνησης IT». Το γραφείο είναι μέρος της OMB και είναι αφιερωμένο στην υλοποίηση της ηλεκτρονικής διακυβέρνησης με ατζέντα του Προέδρου της Δημοκρατίας, που περιλαμβάνει τον νόμο για την Ηλεκτρονική Διακυβέρνηση (και το FISMA), το GPEA, τον νόμο clinger-Cohen, και άλλους.
- Ομοσπονδιακό Συμβούλιο CIO: Το Ομοσπονδιακό CIO Συμβούλιο ιδρύθηκε το 1996 από τον Εκτελεστικό Διάταγμα 13011 και γραπτά σε νόμο υπό την E-Government Act του 2002. Όπως απαιτείται από το E-Government Act, κάθε ομοσπονδιακή υπηρεσία πρέπει να έχει έναν Chief Information Officer. Το CIO αποτελείται από διάφορα τμήματα και υπηρεσίες και «χρησιμεύει ως το κύριο φόρουμ μεταξύ των διάφορων φορέων για τη βελτίωση των πρακτικών στο σχεδιασμό, τον εκσυγχρονισμό, τη χρήση και την απόδοση της ομοσπονδιακής κυβέρνησης σε πόρους του Οργανισμού. Ο Αναπληρωτής Διευθυντής Διαχείρισης στην OMB προεδρεύει του Συμβούλιου CIO» (Todd, 2003).
- Κογκρέσο: Η Βουλή των Αντιπροσώπων και της Γερουσίας, μπορεί να δημιουργήσει την ομοσπονδιακή νομοθεσία. Μπορούν να αξιολογούν τους νόμους για την αποτελεσματικότητα.

3.1.1 Οι Πέντε Εντολές

Το Σύστημα Πιστοποίησης Κυβέρνησης είναι οδηγός στις κυβερνητικές εντολές που προέρχεται από τον Christian Enloe και αφορά την αντιμετώπιση στα βήματα που εμπλέκονται στην C & A (Certification and Accreditation), καθώς γράφτηκαν εκείνη την εποχή και χρησιμεύουν ως μια καλή αφετηρία για την κατανόηση των λεγόμενων C & A (Enloe, 2002).

Τα πρωτογενή C & A έγγραφα, μόλις ολοκληρωθούν και κυκλοφορήσουν, αποτελούνται από

- Πρότυπα για την Ασφάλεια Κατηγοριοποίησης των Πληροφοριακών Συστημάτων (FIPS Δημοσίευση 199) Federal Information
- Οδηγίες για την Πιστοποίηση ασφάλειας και τη διαπίστευση Ομοσπονδιακών Πληροφοριακών Συστημάτων (NIST Ειδική Έκδοση 800-37)
- Έλεγχοι ασφαλείας Ομοσπονδιακών Συστημάτων Πληροφοριών (NIST Ειδική Έκδοση 800-53)
- Τεχνικές και διαδικασίες για την επαλήθευση της αποτελεσματικότητας των Έλεγχων ασφαλείας στα Ομοσπονδιακά Πληροφοριακά Συστήματα (NIST Ειδική 800-53A δημοσίευση)
- Οδηγός για Χαρτογράφηση στα είδη πληροφοριών και

Πληροφοριακών Συστημάτων με τους στόχους ασφαλείας και επίπεδα κινδύνου (NIST Ειδική Έκδοση 800-60).

3.2 Ασφάλεια Μ. Βρετανίας

Η βρετανική νομοθεσία ασφάλειας δεδομένων αναθεωρείται πλήρως με απίστευτη ταχύτητα.

Από το 2004, το FSA (Financial Services Authority) έχει εκδώσει μια σειρά από ομιλίες και δημοσιεύσεις για την ευαισθητοποίηση στον τομέα των χρηματοπιστωτικών υπηρεσιών και την ανάγκη των επιχειρήσεων να αναλάβουν δράση για την καταπολέμηση των κινδύνων του οικονομικού εγκλήματος.

Αξίζει να σημειωθεί ότι η θέση του FSA για την ασφάλεια των δεδομένων είναι ένα παράδειγμα «ενδοτικού δικαίου». Το ενδοτικό δίκαιο, το οποίο περιλαμβάνει οδηγίες που εκδίδονται από τις ρυθμιστικές αρχές, είναι μόνο ένα στοιχείο της μεταρρύθμισης του νόμου. Τα άλλα συστατικά αφορούν το λεγόμενο «σκληρό δίκαιο», το οποίο είναι η μαύρη-επιστολή του καταστατικού και των μέσων όπως οι οδηγίες για το ηλεκτρονικό εμπόριο, η «νομολογία» και οι αποφάσεις των δικαστηρίων. Οι ρυθμιστικές αρχές έχουν αναπτύξει ενδοτικό δίκαιο, προκειμένου να προσθέσουν λεπτομέρειες, ή να προχωρήσουν ή να αναπτύξουν μια αυστηρή νομοθεσία. Έτσι, η μεταρρύθμιση του νόμου για την ασφάλεια των δεδομένων προωθείται με τρεις διαφορετικούς τρόπους, γεγονός που καταδεικνύει γιατί το ρυθμιστικό πλαίσιο έχει εξελιχθεί με τόσο γρήγορους ρυθμούς (Carey, 2009).

Ωστόσο μια σειρά σημαντικών εισβολών στο διαδίκτυο τον Απρίλιο του 2006, ανάγκασε την υπηρεσία να εκδόσει οδηγίες σχετικά με τη χρήση της «ενίσχυσης της ιδιωτικότητας τεχνολογιών» (privacy enhancing technologies - PET) από τους υπεύθυνους επεξεργασίας δεδομένων (Kaufman, 2009).

Η ατζέντα της PET είναι ένα σημαντικό συστατικό της μεταρρύθμισης του νόμου και έχει υιοθετηθεί από τον FSA και την κυβέρνηση. Τα PET έχουν περιγραφεί ως τεχνολογία που βοηθά στην προστασία της ιδιωτικής ζωής ή διευκολύνει τη συμμόρφωση ενός οργανισμού προς τις αρχές της προστασίας των δεδομένων.

Η Ευρωπαϊκή Επιτροπή έχει επίσης αγκαλιάσει τη χρήση των PET, όπως αποδεικνύεται από μια σημαντική ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο το Μάιο του 2007. Ως εκ τούτου, οι οργανισμοί ενθαρρύνονται να ενσωματώσουν τα PET στο πλαίσιο του σχεδιασμού των συστημάτων διαχείρισης της ασφάλειας των πληροφοριών, ένα αποτέλεσμα που προωθείται επίσης από το ISO 27001/2, έναν διεθνή κώδικα πρακτικής για τη διαχείριση της ασφάλειας των πληροφοριών.

Το Νοέμβριο του 2007 η τροποποίηση του "*Η προσέγγισή μας για την κρυπτογράφηση",* για παράδειγμα, χρησιμοποιήθηκε για την υποστήριξη υψηλού προφίλ δράσης σε κρυπτογραφήσεις φορητών υπολογιστών ενώ τον Απρίλιο του 2008 η στρατηγική του FSA για την ασφάλεια των δεδομένων ενίσχυσε περαιτέρω την ημερήσια διάταξη PET (Carey, 2009).

3.2.1 Το Γραφείο του Επιτρόπου Πληροφοριών ICO , η ποινική δικαιοσύνη

Το Γραφείο του Επιτρόπου Πληροφοριών έχει αξιοσημείωτη επιτυχία στην προώθηση των τροποποιήσεων του γράμματος του νόμου. Για παράδειγμα, το Μάιο του 2006, το Γραφείο δημοσίευσε μια έκθεση προς το Ευρωπαϊκό Κοινοβούλιο ζητώντας τη θέσπιση ποινών φυλάκισης για τους ανθρώπους και τις οργανώσεις που εμπλέκονται σε

ζητήματα κλοπής δεδομένων. Η εν λόγω έκθεση «Προστασία της ιδιωτικής ζωής – σε τι τιμή;» οδήγησε άμεσα στην Ποινική Δικαιοσύνη και στο νόμο περί μετανάστευσης του 2008, ο οποίος τροποποίησε το νόμο περί προστασίας δεδομένων για να καταστεί δυνατή η εισαγωγή σχετικών ποινών φυλάκισης (Pearson & Charlesworth, 2009).

Οι αρχές της προστασίας των δεδομένων περιλαμβάνουν την αρχή της ασφάλειας, η οποία απαιτεί από τους υπευθύνους επεξεργασίας δεδομένων να λαμβάνουν «τα κατάλληλα τεχνικά και οργανωτικά μέτρα» για να κρατήσουν ασφαλή τα δεδομένα.

Η Ποινική Δικαιοσύνη όρισε πρόστιμο σε ελεγκτές που παρανομούν από σε θέματα ασφαλείας. Όσον αφορά το πιθανό επίπεδο των ποινών, είναι γνωστό ότι η FSA επέβαλε πρόστιμο στην Norwich Union £1.260.000 το Δεκέμβριο του 2007, και δεν υπάρχει κανένας λόγος να πιστεύεται ότι αυτό αντιπροσωπεύει τις ανώτατες επιβληθείσες ποινές, καθώς είναι ενδεχόμενο να επιβληθούν και ακόμη ανώτερες (Pearson & Charlesworth, 2009).

3.2.2 Νομοθεσία περί κοινοποιήσεως της παραβίασης δεδομένων

Ένας άλλος τομέας της νομοθετικής μεταρρύθμισης είναι αυτός της κοινοποίηση της παραβίασης δεδομένων. Αν και είναι σαφές ότι ο νόμος περί προστασίας των δεδομένων δεν περιέχει ρητή ρύθμιση , υπάρχουν μέτρα στο πλαίσιο της πράξης που είναι ενδεικτικά για την ύπαρξη μιας τέτοιας υποχρεώσεως.

Για παράδειγμα, ο νόμος περιλαμβάνει μια σειρά από εγγυήσεις διαφάνειας, όπως το καθεστώς κοινοποίησης και το καθεστώς πρόσβασης στο θέμα, το οποίο μπορεί να περιλαμβάνει πολλές πτυχές των φιλοσοφιών κοινοποίησης των παραβιάσεων σε μεμονωμένες περιπτώσεις (Kaufman, 2009).

Το Μάρτιο του 2008, το Γραφείο του Επιτρόπου Πληροφοριών εξέδωσε οδηγίες σχετικά με την κοινοποίηση των παραβιάσεων (Pearson & Charlesworth, 2009).

Ομοίως, η ΕΕ εξετάζει το ενδεχόμενο θέσπισης ειδικής υποχρέωσης παραβίασης της κοινοποίησης στο πλαίσιο της ασφάλειας των δεδομένων για τον τομέα των ηλεκτρονικών επικοινωνιών. Τον Νοέμβριο του 2007, η Ευρωπαϊκή Επιτροπή πρότεινε τη θέσπιση κανόνων υποβολής εκθέσεων σε μια νέα οδηγία, και η πρόταση αυτή έτυχε ευρείας υποστήριξης κατά τη διάρκεια συζήτησης στο Ευρωπαϊκό Κοινοβούλιο στις αρχές του Σεπτεμβρίου 2008.

3.2.3 Η νέα δυναμική των νόμων περί της ασφάλειας των δεδομένων

Οι εξελίξεις στον τομέα της ασφάλειας δεδομένων, δεν αποτελούν την κορυφή του παγόβουνου, αλλά υπάρχει ελπίδα ότι θα ενθαρρύνουν τους οργανισμούς να λάβουν τους νόμους περί της ασφάλειας των δεδομένων πιο σοβαρά (Kaufman, 2009).

3.2.4 Computer Misuse Act

Ο νόμος για την Κακή Χρήση των Η/Υ το 1990 είναι ένας νόμος που ψηφίστηκε από το Κοινοβούλιο του Ηνωμένου Βασιλείου και ο οποίος εισήχθη εν μέρει ως απάντηση στην απόφαση κατά των Gold & Schifreen (1988) (βλ. παρακάτω). Οι επικριτές του νομοσχεδίου κατήγγειλαν ότι εισήχθη εσπευσμένα και πως δεν προηγήθηκε καλή μελέτη *(Leyden, 2015).* Σύμφωνα με τους επικριτές, η πρόθεση ήταν συχνά δύσκολο να αποδειχθεί και πως το νομοσχέδιο δεν διαφοροποιούσε επαρκώς τους «ερασιτέχνες» hackers, όπως οι Gold και Schifreen, από τους σοβαρούς παραβάτες ηλεκτρονικού εγκλήματος. Ωστόσο, ο νόμος αποτέλεσε μοντέλο από το οποίο αρκετές άλλες χώρες, συμπεριλαμβανομένου του Καναδά και της Δημοκρατίας της Ιρλανδίας, εμπνεύστηκαν στην συνέχεια την σύνταξη των δικών τους νόμων για την ασφάλεια των πληροφοριών, καθώς θεωρήθηκε «ως ένα ισχυρό και ευέλικτο κομμάτι της νομοθεσίας όσον αφορά στην αντιμετώπιση του εγκλήματος στον κυβερνοχώρο» (IISS, 2011).

Οι Robert Schifreen και Stephen Gold, με τη χρήση συμβατικών οικιακών υπολογιστών και μόντεμ στα τέλη του 1984 και στις αρχές του 1985, απέκτησαν μη εξουσιοδοτημένη πρόσβαση στην διαδραστική υπηρεσία απεικόνισης δεδομένων Prestel της British Telecom. Η PESTLE στην εκτεταμένη μορφή δηλώνει P για την Πολιτική (politics), E για την Οικονομική (economy), S για την κοινωνική (social), T για την Τεχνολογική (technological), L για τη νομική (legal) και E (environmental) για την Περιβαλλοντική επισκόπηση. Δίνει μια πανοραμική άποψη για το σύνολο του περιβάλλοντος από πολλές διαφορετικές οπτικές γωνίες που κάποιος θέλει να ελέγξει, πριν να προβεί σε μια συγκεκριμένη ιδέα / σχέδιο.

Ενώ βρισκόταν σε μια εμπορική έκθεση, ο Schifreen παρατήρησε τον κωδικό πρόσβασης ενός μηχανικού της Prestel: το όνομα χρήστη ήταν 22222222 και ο κωδικός πρόσβασης το 1234. Αυτή η πράξη αργότερα οδήγησε σε μεταγενέστερες κατηγορίες ότι η British Telecom δεν είχε λάβει σοβαρά υπόψη το θέμα της ασφάλειας. Έχοντας αυτές τις πληροφορίες, το ζευγάρι εξερεύνησε το σύστημα και απέκτησε ακόμη και πρόσβαση στα προσωπικά μηνύματα του πρίγκιπα Φιλίππου (Fafinski, 2009).

Η εταιρεία Prestel εγκατέστησε οθόνες στους ύποπτους λογαριασμούς και έδωσε τις πληροφορίες που απέκτησε στην αστυνομία. Το ζευγάρι κατηγορήθηκε βάσει του άρθρου 1 του Νόμου περί Παραποίησης και Πλαστογράφησης το 1981 για παράνομη επεξεργασία του κωδικού που είχε υποκλέψει ο Gold.

Παρά το γεγονός ότι τα πρόστιμα που επιβλήθηκαν δεν ήταν υψηλά, οι κατηγορούμενοι επέλεξαν να ασκήσουν έφεση στο ποινικό τμήμα του Εφετείου (MacEwan, 2008).

Το 1988, η Βουλή των Λόρδων εξέδωσε την αθωωτική απόφαση (IISS, 2011). Ο Λόρδος Brandon δήλωσε:

Η έντονη προσπάθεια (*Leyden, 2015)* όλα αυτά τα γεγονότα να τεθούν υπό το καθεστώς και το ρυθμιστικό πλαίσιο, ενός νόμου που δεν είναι σχεδιασμένος με τρόπο που να προσιδιάζει σε αυτά τα γεγονότα, παράγει σοβαρές δυσκολίες τόσο για τους δικαστές, όσο και για τους ενόρκους που δεν θα θέλαμε να δούμε να επαναλαμβάνεται. Αυτό όμως δεν είναι ποινικό αδίκημα. Εάν θεωρείται σκόπιμο να θεωρείται αδίκημα, τότε πρόκειται για ένα θέμα με το οποίο πρέπει να ασχοληθεί ο νομοθέτης και όχι τα δικαστήρια (Fafinski, 2009).

Η απόφαση της Βουλής των Λόρδων για το νόμο οδήγησε πολλούς νομικούς μελετητές να πιστεύουν ότι η πειρατεία δεν ήταν παράνομη όπως έλεγε ο νόμος τότε. Η Επιτροπή για το Αγγλικό Δίκαιο και η ομόλογή της στην Σκωτία, εξέτασαν το θέμα. Η Επιτροπή για το Δίκαιο στην Σκωτία κατέληξε στο συμπέρασμα ότι η εισβολή καλύπτεται

επαρκώς στην Σκωτία στο πλαίσιο του κοινού δικαίου που σχετίζεται με την απάτη, αλλά η Επιτροπή της Αγγλίας θεώρησε ότι ένας νέος νόμος ήταν απαραίτητος.

Από τότε που έγινε η δίκη, οι δύο κατηγορούμενοι έχουν γράψει εκτενώς για θέματα πληροφορικής. Ο Gold, ο οποίος αναφέρεται λεπτομερώς στο σύνολο της υπόθεσης στο *Hacker's Handbook*, έχει κάνει παρουσιάσεις σε συνέδρια, μαζί με τους αστυνομικούς που πραγματοποίησαν τις συλλήψεις στην υπόθεση *(Leyden 2015).*

Με βάση τις συστάσεις της Επιτροπής Αγγλικού Δικαίου, εισήχθη ένα νομοσχέδιο από τον συντηρητικό βουλευτή Michael Colvin. Το νομοσχέδιο που έφερε η κυβέρνηση, τέθηκε σε ισχύ το 1990. Οι ενότητες 1-3 του Νόμου εισήγαγαν τρία ποινικά αδικήματα (Akdeniz, 1995):

1. την μη εξουσιοδοτημένη πρόσβαση σε υλικό υπολογιστή, η οποία τιμωρείται με ποινή φυλάκισης 12 μηνών (ή 6 μήνες στη Σκωτία) και/ή χρηματική ποινή «που δεν υπερβαίνει το επίπεδο 5 της πρότυπης κλίμακας» (από το 2015, απεριόριστο).

2. την μη εξουσιοδοτημένη πρόσβαση με πρόθεση διάπραξης ή διευκόλυνσης διάπραξης νέων αδικημάτων, η οποία τιμωρείται με 12 μήνες/μέγιστο πρόστιμο (ή 6 μήνες στη Σκωτία) με συνοπτική καταδίκη ή/και 5 έτη/πρόστιμο κατ' έγκληση.

3. την μη εξουσιοδοτημένη τροποποίηση υλικού υπολογιστή, η οποία τιμωρείται με 12 μήνες/μέγιστο πρόστιμο (ή 6 μήνες στην Σκωτία) με συνοπτική καταδίκη ή/και 10 έτη/πρόστιμο κατ' έγκληση *(Leyden, 2015).*

Σκοπός ήταν να αποτραπούν οι πιο επικίνδυνοι εγκληματίες από την χρήση ενός υπολογιστή στην διευκόλυνση ή διάπραξη μιας αξιόποινης πράξης ή να παρακωλυθεί ή εμποδιστεί η πρόσβαση σε δεδομένα που είναι αποθηκευμένα σε έναν υπολογιστή. Το βασικό αδίκημα είναι να προσπαθήσει κανείς να επιχειρήσει την πρόσβασή ή να επιτύχει τελικά πρόσβαση σε έναν υπολογιστή ή στα δεδομένα που αποθηκεύει. Επομένως, οι χάκερς που προγραμματίζουν τους υπολογιστές τους να κάνουν αναζητήσεις μέσα από παραλλαγές κωδικών καθίστανται υπόλογοι, ακόμη και εάν όλες οι προσπάθειές τους να συνδεθούν έχουν απορριφθεί από τον υπολογιστή προορισμού. Η μόνη προϋπόθεση για να καθιστούν υπόλογοι είναι να γνωρίζουν οι χάκερς ότι η απόπειρα πρόσβασης είναι μη εξουσιοδοτημένη.

Η χρήση του ονόματος χρήστη άλλου ατόμου και του κωδικού πρόσβασης χωρίς κατάλληλη εξουσιοδότηση για πρόσβαση σε δεδομένα ή άλλες υπηρεσίες, συνιστούν αδίκημα.

Ακόμη και αν η αρχική πρόσβαση επιτρέπεται, μετά την εξερεύνηση, εάν υπάρχει μια ιεραρχία στα προνόμια του συστήματος, αυτή μπορεί να οδηγήσει σε είσοδο σε τμήματα του συστήματος για τα οποία τα απαιτούμενα προνόμια απουσιάζουν κι έτσι το αδίκημα μπορεί να τελεστεί.

Παρά το γεγονός ότι ο νόμος στοχεύει φαινομενικά όσους επιθυμούν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση στα συστήματα πληροφορικής για διάφορους λόγους, οι επιπτώσεις του στις προηγουμένως σχετικά διαδεδομένες ή γνωστές πρακτικές , όπως το «κλείδωμα» του λογισμικού σε συγκεκριμένο χρόνο, έχουν περιγραφεί σε διάφορες δημοσιεύσεις στον κλάδο της πληροφορικής *(Leyden, 2015)*. Το κλείδωμα σύμφωνα με τον χρόνο χρήσης, αποτελεί μία πρακτική για την απενεργοποίηση της λειτουργίας προγραμμάτων, προκειμένου να διασφαλιστεί ότι το λογισμικό, που ενδεχομένως να έχει παραδοθεί υπό τον όρο μιας περαιτέρω πληρωμής, θα «λήξει» και ως εκ τούτου δεν θα είναι πλέον σε λειτουργία **(**MacEwan, 2008).

Το 2004, το All-Party Internet Gro
ένας οργανισμός που ιδρύθηκε το 1998 για να παρέχει ένα φόρουμ συζήτησης μεταξύ των νέων βιομηχανιών των media και του διαδικτύου και κυβερνητικών εκπροσώπων, για το

αμοιβαίο όφελος και των δύο μερών, δημοσίευσε ένα άρθρο ανασκόπησης της νομοθεσίας και επισήμανε τους τομείς για ανάπτυξη **(**MacEwan, 2008). Οι συστάσεις τους οδήγησαν στην σύνταξη του Νομοσχεδίου του 1990 για την Κακή Χρήση των Η/Υ (Τροποποίηση) που επεδίωξε να τροποποιήσει την Κακή Χρήση των Η/Υ ώστε ο νόμος να συμμορφωθεί με τα προβλεπόμενα από την Ευρωπαϊκή Σύμβαση για το έγκλημα στον κυβερνοχώρο (*Naylor, 1994)*. Σύμφωνα με τους όρους της, η μέγιστη ποινή φυλάκισης για παράβαση του νόμου άλλαξε από τους έξι μήνες στα δύο έτη. Επεδίωξε επίσης να ποινικοποιήσει ρητώς τις επιθέσεις άρνησης εξυπηρέτησης και άλλων εγκλημάτων που διευκολύνονται από την άρνηση της εξυπηρέτησης. Το νομοσχέδιο δεν έλαβε τη βασιλική σύμφωνη γνώμη, διότι το Κοινοβούλιο είχε διαλυθεί (Akdeniz, 1996).

Οι Ενότητες 35-38 του Νόμου για την Αστυνομία και την Δικαιοσύνη του 2006, περιέχει τροποποιήσεις στον νόμο περί της Κακής Χρήσης των Η/Υ του 1990.

Η Ενότητα 37 (Κατασκευή, τροποποίηση ή απόκτηση αντικειμένων για χρήση σε αδικήματα κακής χρήσης των υπολογιστών) εισάγει μία νέα ενότητα 3Α στον νόμο του 1990 και έχει λάβει έντονη κριτική από τους επαγγελματίες της πληροφορικής, καθώς πολλά από τα εργαλεία τους μπορούν να χρησιμοποιηθούν και από τους εγκληματίες πέρα από τους νόμιμους σκοπούς τους και συνεπώς εμπίπτουν στην Ενότητα 3Α *(Leyden 2015).*

Μετά το τηλεφωνικό σκάνδαλο με το «hacking» της News International το 2011, βρίσκονται σε εξέλιξη συζητήσεις σχετικά με την τροποποίηση του νόμου για τον προσδιορισμό των «έξυπνων» τηλεφώνων (δηλαδή αυτών με προγράμματα περιήγησης στο Διαδίκτυο και άλλες δυνατότητες συνδεσιμότητας). Η τροποποίηση αυτή μπορεί επίσης να εισαγάγει ένα νέο αδίκημα που αφορά στο άτομο που καθιστά πληροφορίες διαθέσιμες με πρόθεση, δηλαδή που αποκαλύπτει δημοσίως έναν κωδικό πρόσβασης για το τηλέφωνο ή τον υπολογιστή κάποιου έτσι ώστε άλλοι να μπορούν να έχουν πρόσβαση σε αυτό παράνομα (Fafinski, 2009).

3.3 Μεθοδολογία

Η παρούσα μελέτη θα εστιάσει στον εντοπισμό, την επιλογή και την αξιολόγηση κατάλληλων ερευνητικών μελετών αλλά και την καταγραφή και την ανάλυση δεδομένων μελετών. Συγκεκριμένα η μελέτη στηρίχθηκε σε δευτερογενείς έρευνες που έχουν διεξάγει άλλοι μελετητές.

Με τη συστηματική ανασκόπηση ερευνητικής βιβλιογραφίας συνοψίζεται η γνώση η οποία υπάρχει ήδη, αποσαφηνίζεται το θέμα και ο ερευνητής εμβαθύνει σε αυτό, επιβεβαιώνεται η σπουδαιότητα του θέματος, εντοπίζονται κενά στη βιβλιογραφία και αναζητούνται νέες ερευνητικές κατευθύνσεις. Μετά την αξιολόγηση της ποιότητας των ερευνών επιλέγονται οι κατάλληλες και γίνεται η κριτική ανάλυση των ευρημάτων τους (Κυριαζόπουλος & Σαμαντά, 2011).

Για τη συλλογή δεδομένων χρησιμοποιήθηκαν κυρίως ερευνητικά άρθρα αλλά και βιβλία και διατριβές. Αρχικά έγινε ανάγνωση της περίληψης των μελετών έτσι ώστε να διαχωριστούν όσες χρησιμοποιήθηκαν από αυτές που δεν έχουν σχέση με το θέμα.

Κατά την εξέταση των μελετών αποφασίστηκε εάν οι μελέτες πληρούν τα κριτήρια εισόδου – αποκλεισμού. Κάποιες μελέτες απορρίφθηκαν άμεσα από την ανάγνωση των τίτλων και περιλήψεων, ενώ για κάποιες άλλες μελέτες πρώτα εντοπίστηκε και διαβάστηκε το πλήρες κείμενο ώστε να αποφασισθεί η συμπερίληψη τους (Κυριαζόπουλος & Σαμαντά, 2011).

ΚΕΦΑΛΑΙΟ 4 ΣΥΓΚΡΙΤΙΚΗ ΑΝΑΣΚΟΠΗΣΗ ΝΟΜΙΚΟΥ ΠΛΑΙΣΙΟΥ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ ΣΕ ΗΠΑ, ΕΥΡΩΠΗ ΚΑΙ ΕΛΛΑΔΑ

Στη παρούσα ενότητα θα γίνει μια συγκριτική παρουσίαση και ανάλυση του υφιστάμενου νομικού πλαισίου και των κανονισμών που αναφέρονται στην ασφάλεια των πληροφοριών και ευρύτερα της ιδιωτικότητας. Η διερεύνηση θα γίνει με γνώμονα το ελληνικό, το αμερικανικό και το ευρωπαϊκό δίκαιο.

4.1 Διερεύνηση

Μία από τις πιο συνηθισμένες έννοιες της ασφάλειας της πληροφορίας είναι ότι αυτή προτείνεται στον απόρρητο χαρακτήρα κάποιων θεμάτων και υπό αυτήν την έννοια προσβάλλεται η απόρρητη πληροφορία (Solove, 2008). Η «κλασική» προσέγγιση της ιδιωτικότητας παρουσιάζει ταύτιση με την έννοια του απορρήτου. Οι εν λόγω όροι, αν και γίνονται αντιληπτοί και σαν ισοδύναμοι, εκφράζονται ως παρεμφερείς αξιώσεις προστασίας, αλλά στην ουσία δεν ταυτίζονται: Η έννοια του απόρρητου (secrecy) αναφέρεται είτε στη μη προσπελασιμότητα κάποιων δεδομένων επιρροής ενός ατόμου είτε στην υποχρέωση ατόμων ή οργανισμών να προστατεύουν πληροφορίες που τους έχουν ανατεθεί είτε τις γνωρίζουν επί τη βάσει της θέσης και της αρμοδιότητάς τους.

Προκειμένου να είναι απόρρητα τα δεδομένα είναι σκόπιμο να είναι σε μία κατάσταση χαμηλής προσβασιμότητας από πρόσωπα, ομάδες κ.λπ. Το “απόρρητο” αποκλείει τους τρίτους από τη γνώση και την αξιοποίηση των δεδομένων, εφόσον δεν υφίσταται ένας νόμιμος λόγος και η αντίστοιχη διαδικασία που επιτρέπουν την άρση του απορρήτου.

Η εν λόγω άποψη σχετίζεται με κρίσιμες για τα πρόσωπα αποτελέσματα, όπως π.χ. το εύρος και οι προϋποθέσεις για επιπλέον κοινοποίηση των στοιχείων. Το Ανώτατο Δικαστήριο των ΗΠΑ θεώρησε ότι ένα πρόσωπο δεν έχει αναμενόμενη προσδοκία ιδιωτικότητας, αναφορικά με πληροφορίες που αποκάλυψε εθελοντικά σε ένα τρίτο πρόσωπο ή οργανισμό και στη συνέχεια διαβιβάστηκαν από αυτό σε δημόσια αρχή (Solove, 2002;Taipale, 2005). Στο σημείο αυτό εστιάζεται μία κύρια ατέλεια της επίκλησης της ιδιωτικότητας ως πληροφοριακής απομόνωσης: η χρήση της σταματάει να υφίσταται όταν η πληροφορία “διαφεύγει” και παύει να είναι “μυστική”.

Αναφορικά με την ευρωπαϊκή προσέγγιση, ο απόρρητος χαρακτήρας των προσωπικών δεδομένων δεν συνάγεται μόνο από τη φύση τους αλλά προβλέπεται και ρητά στο σχετικό κανονιστικό πλαίσιο. Το άρθρο 16 της Οδηγίας 95/46/ΕΚ για την προστασία προσωπικών δεδομένων περιλαμβάνει μία -ιδιότυπης αρνητικής διατύπωσης – ρύθμιση για το απόρρητο, καθώς ορίζει ότι όποιος επεξεργάζεται στοιχεία για λογαριασμό του υπεύθυνου επεξεργασίας το κάνει μόνο κατ’ εντολή του υπεύθυνου επεξεργασίας. Ο ελληνικός νόμος για την προστασία προσωπικών δεδομένων (ν. 2472/97) στο άρθρο 10 § 1 εμπεριέχει μεν μία ανάλογη διατύπωση αλλά ταυτόχρονα θεωρεί συνολικά την επεξεργασία στοιχείων προσωπικού χαρακτήρα ως απόρρητη.

Το απόρρητο σχετίζεται με την ασφάλεια των δεδομένων χωρίς να ταυτίζεται με αυτή (Γκρίτζαλη, 2004**)**. Η κοινοτική όσο και η ελληνική νομοθεσία για την προστασία προσωπικών δεδομένων απαιτούν τη λήψη «κατάλληλων» μέτρων ασφάλειας, προκειμένου να προστατεύονται τα δεδομένα από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας (άρθρο 10 § 3 του Ν. 2472/97), (άρθρο 10 ν. 2472/97).

Η συνειδητοποίηση των κινδύνων και η ανάγκη ατομικής προστασίας δεν αντιμετωπίζεται με τον ίδιο τρόπο από τις διάφορες έννομες τάξεις. Η κανονιστική αντιμετώπιση, αντικατοπτρίζει τις ποικίλες προσεγγίσεις της πληροφοριακής ιδιωτικότητας που αναφέρθηκαν συνοπτικά και τη θέση αυτής στην εκάστοτε κλίμακα συνταγματικών αξιών.

Ακόμα και αν ο αριθμός των νομοθετημάτων σημειώνει ανοδική πορεία, η προστασία των προσωπικών δεδομένων διατηρείται -μάλλον εξαίρεση στο διεθνές περιβάλλον, ενώ εκτός Ευρώπης, λίγες μόνο χώρες έχουν εισαγάγει δεσμευτικούς κανόνες προστασίας προσωπικών δεδομένων (Simitis, 2008).

Σχετικά με χώρες οι οποίες έχουν πλαίσιο προστασίας των προσωπικών δεδομένων, ταξινομούνται σε δύο κατηγορίες:

α) αυτές που προάγουν μία ολιστική ρύθμιση όλων των τομέων κρατικής και ιδιωτικής δραστηριότητας και

β) αυτές που ρυθμίζουν τομείς και πεδία κρατικής και ιδιωτικής δραστηριότητας επενδύοντας, κυρίως, στη λύση της αυτορρύθμισης (Στρατηλάτη, 2005).

Ο κατάλογος των περιορισμών είναι, όντως, ευρύς. Επικρατεί η άποψη ότι η διαμόρφωση των κανόνων για τη χρήση της προσωπικής πληροφορίας ανταποκρίνεται στο αίτημα της εξασφάλισης ατομικών δικαιωμάτων, υπολογίζοντας την ίδια στιγμή και τα δικαιώματα των άλλων αλλά και τις ανάγκες μιας κοινωνίας, η λειτουργία της οποίας εξαρτάται όλο και περισσότερο από τη διαθεσιμότητα, ροή και επεξεργασία δεδομένων.

Η προστασία της ιδιωτικότητας δεν ταυτίζεται με πλήρη αποκλεισμό των δεδομένων των άλλων ή με δικαιώματα κυριότητας επί των ιδίων δεδομένων. Ως κοινωνική ιδιότητα του προσώπου, η ιδιωτικότητα υπόκειται σε περιορισμούς. Οι εν λόγω περιορισμοί, είναι ανεκτοί μόνο υπό την αίρεση της νομιμότητας και της αναλογικότητας και αφορούν (κυρίως) ένα υπέρτερο δημόσιο συμφέρον είτε τα «δικαιώματα των άλλων».

Σταθμός για την προστασία δεδομένων θεωρείται η κοινοτική Οδηγία 95/46/ΕΚ «*για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών»,* με τη βοήθεια της οποίας επιδιώχθηκε η εναρμόνιση των ευρωπαϊκών νομοθεσιών σε ένα υψηλό επίπεδο προστασίας. Η Οδηγία θεμελιώνεται σε μία από τις περιοριστικά απαριθμούμενες βάσεις επεξεργασίας. Η εισαγωγή ψηφιακών τεχνολογιών στα δίκτυα ηλεκτρονικών επικοινωνιών έχει ειδικές απαιτήσεις αναφορικά με την προστασία δεδομένων προσωπικού χαρακτήρα και την ιδιωτική ζωή των συνδρομητών και χρηστών.

Η Οδηγία αυτή αντικαταστάθηκε από την Οδηγία 2002/58/ΕΚ για την προστασία δεδομένων στον κλάδο των ηλεκτρονικών επικοινωνιών που τελεί και αυτή υπό τροποποίηση, στο πλαίσιο της οποίας έχουν εγερθεί συζητήσεις για ζητήματα όπως π.χ. η φύση των διαδικτυακών διευθύνσεων και η νομική αντιμετώπισή τους.

Οι Οδηγίες αυτές προέκυψαν, ως αναγκαία εργαλεία για την ολοκλήρωση της εσωτερικής αγοράς, όπου υπηρεσίες και άνθρωποι θα ήταν σκόπιμο να κυκλοφορούν ελεύθερα και για τον λόγο αυτό το πεδίο εφαρμογής τους εστιάζει στη ρύθμιση σχέσεων μεταξύ ιδιωτών. Η βαρύτητα που απέδιδε η ΕΕ στο θέμα της προστασίας προσωπικών δεδομένων αποτυπώθηκε περαιτέρω ήδη στη Συνθήκη του Άμστερνταμ (1997) με το άρθρο 286, που εφάρμοσε κανόνες στο εσωτερικό των κοινοτικών οργάνων και οργανισμών, προβλέποντας την δημιουργία ενός “ανεξάρτητου εποπτικού οργάνου” με αντικείμενο τον έλεγχο της ρύθμισης ρυθμίσεων.

Η εν λόγω αξία αναδεικνύεται ως προς τις δραστηριότητες της Ένωσης και των κρατών –μελών στον τομέα της αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις. Η πολιτική της ΕΕ στον τομέα αυτό χαρακτηρίζεται από έλλειψη συνοχής και ολιστικής αντίληψης. Η ανάγκη για την εναρμόνιση των σχετικών ρυθμίσεων θεωρήθηκε αναγκαία έπειτα από την υιοθέτηση του λεγόμενου «Προγράμματος της Χάγης για την ενδυνάμωση της ελευθερίας, ασφάλειας και δικαιοσύνης στην ΕΕ»

4.2 Μελέτη εφαρμογής της υπάρχουσας νομοθεσίας – σχολιασμός αποφάσεων

4.2.1 Το ελληνικό κανονιστικό πλαίσιο

Η Ελλάδα ήταν από τα πρώτα κράτη που μετέφεραν την κοινοτική Οδηγία στο εσωτερικό δίκαιο. Το ελληνικό νομοθετικό πλαίσιο για την διαφύλαξη προσωπικών στοιχείων σχηματίζεται από τη συνταγματική άδεια διαφύλαξης προσωπικών στοιχείων όπως κατοχυρώνεται στο άρθρο 9 Α του Συντάγματος, τον νόμο 2472/97 (ΦΕΚ Α' 50/10.04.1997) για την ατομική διαφύλαξη από την επεξεργασία στοιχείων προσωπικού χαρακτήρα, όπως ισχύει μετά τις τροποποιήσεις που κατά καιρούς εισήχθησαν καθώς και τον νόμο 3471/06 (ΦΕΚ Α' 133/28.06.2006) που – πέραν των τροποποιήσεων που επέφερε στον Ν. 2472/97 – έχει να κάνει με τη διαφύλαξη των προσωπικών στοιχείων και της ιδιωτικής ζωής στον κλάδο των ηλεκτρονικών επικοινωνιών.

4.2.2 Η συνταγματική κατοχύρωση της διαφύλαξης προσωπικών στοιχείων

"Κατά την αναθεώρηση του Συντάγματος το 2001 κρίθηκε επιβεβλημένη η κατοχύρωση ενός νέου, ειδικού δικαιώματος διαφύλαξης των προσωπικών στοιχείων. Το νέο άρθρο 9Α του Συντάγματος που περιλήφθηκε στο Σύνταγμα με την τελευταία αναθεώρηση του 2001 ορίζει ότι «καθένας έχει άδεια διαφύλαξης από τη, κατεργασία και χρήση, με ηλεκτρονικά μέσα, των προσωπικών του στοιχείων, όπως ο νόμος ορίζει. Η διασφάλιση της διαφύλαξης των προσωπικών στοιχείων ανατίθεται από τον αναθεωρητικό νομοθέτη σε ανεξάρτητη αρχή, που σχηματίζεται και λειτουργεί, όπως ο νόμος ορίζει»" (Μήτρου, 2001).

4.2.3 Το νομοθετικό πλαίσιο για την ατομική διαφύλαξη από την κατεργασία προσωπικών στοιχείων

Ο Ν. 2472/97 μετέφερε τις ρυθμίσεις της κοινοτικής Οδηγίας για την διαφύλαξη προσωπικών δεδομένων (95/46/ΕΚ) στην εσωτερική έννομη τάξη. Ο νομοθέτης με το ν. 2472/97 οριοθετεί με διαδικαστικούς κανόνες τη συνταγματικά κατεργασία προσωπικών στοιχείων και έτσι ρυθμίζει τη ροή των προσωπικών στοιχείων στο πλαίσιο του κράτους, της οικονομίας και οργανώνει τις πληροφοριακές σχέσεις μεταξύ των προσώπων (Μήτρου, 2001).

Ο ν. 2472/97 έχει τέσσερις πυλώνες: α) ένα σύστημα ουσιαστικών ρυθμίσεων που θέτει από τη μία τις προϋποθέσεις νομιμότητας της επεξεργασίας προσδιορίζοντας δεσμευτικά το σημείο ισορροπίας μεταξύ των αντιτιθεμένων συμφερόντων και από την άλλη τις βασικές αρχές του νόμου με έμφαση στην αρχή του σκοπού και της αναλογικότητας (άρθρα 4-10), β) στην απονομή δικαιωμάτων στα πρόσωπα προκειμένου να προστατεύσουν τα δικαιώματα και συμφέροντά τους (άρθρα 11-14), γ) στην εισαγωγή και οργάνωση θεσμικού ελέγχου της διαφύλαξης προσωπικών δεδομένων προκειμένου να διασφαλίζεται η υλοποίηση της νομοθεσίας (άρθρα 15-20) και δ) στους κανόνες που προβλέπουν διοικητικές, ποινικές και αστικές κυρώσεις σε περιπτώσεις παράβασης του νόμου (άρθρα 21-23).

Είναι άξιο αναφοράς ότι η Αρχή Προστασίας Προσωπικών Δεδομένων ορίζει το θεμέλιο του ελληνικού συστήματος διαφύλαξης στοιχείων επί του οποίου δομείται το σύστημα ελέγχου και ο μηχανισμός της εφαρμογής, της τήρησης αλλά και της εξέλιξης των νομικών ρυθμίσεων (Μήτρου, 2001). Ο νόμος και η ελεγκτική αρμοδιότητα της Αρχής εμπεριείχε το σύνολο της επεξεργασίας. Διάσπαση στο σύστημα διαφύλαξης επέφερε το άρθρο 8 του ν. 3625/07 που εισήγαγε την εξαίρεση ενός ευρύτατου φάσματος επεξεργασίας προσωπικών στοιχείων, συγκεκριμένα αυτής που πραγματοποιείται από τις δικαστικές –

εισαγγελικές αρχές και τις διωκτικές αρχές για την εξυπηρέτηση των αναγκών της λειτουργίας τους με σκοπό τη βεβαίωση εγκλημάτων, από το πεδίο εφαρμογής του νόμου και κατ' επέκταση από την εποπτεία της Αρχής. Η εξαίρεση αυτή που έχει να κάνει με έναν κλάδο εντασσόμενο στον σκληρό πυρήνα της κρατικής δράσης θέτει μείζονα ζητήματα συνταγματικότητας (Μήτρου, 2001).

Ο «γενικός» νόμος συμπληρώνεται από τον ν. 3471/06 για την διαφύλαξη των προσωπικών στοιχείων και της ιδιωτικής ζωής στον κλάδο των ηλεκτρονικών επικοινωνιών που αντικατέστησε τον προηγούμενο ν. 2774/1999 για την διαφύλαξη προσωπικών δεδομένων στον τηλεπικοινωνιακό τομέα. Ο νόμος αυτός, ενσωματώνοντας την Οδηγία 2002/58/ΕΚ, αποσκοπεί στην εισαγωγή ειδικών ρυθμίσεων που αφορούν τόσο το απόρρητο της επικοινωνίας και την διαφύλαξη προσωπικών δεδομένων της ιδιωτικότητας των χρηστών από πρακτικές όπως π.χ. η εγκατάσταση κατασκοπευτικού λογισμικού (spyware) (Μήτρου, 2001).

4.2.4 Το διεθνές κανονιστικό περιβάλλον

Αναφορικά με την αντίδραση της διεθνούς κοινότητας στους κινδύνους των νέων Τεχνολογιών πληροφορίας και επικοινωνίας (ΤΠΕ) για τα ανθρώπινα δικαιώματα, η απόφαση 2450/19.12.1968 της Γ.Σ. των Ηνωμένων Εθνών ορίζεται στα πρώτα σχετικά κείμενα. Ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ) ήταν ο δεύτερος διεθνής οργανισμός που ασχολήθηκε με την διαφύλαξη προσωπικών δεδομένων, εκδίδοντας τις λεγόμενες «Κατευθυντήριες Αρχές που εκφράζουν την διαφύλαξη της ιδιωτικότητας και τις διασυνοριακές ροές προσωπικών στοιχείων ».

Η πίεση αυτή επιτείνεται από τη θεσμική πραγματικότητα που έχει διαμορφώσει η Ευρώπη: η Οδηγία 95/46/ΕΚ (άρθρο 25) απαιτεί την ύπαρξη «ικανοποιητικού επιπέδου προστασίας» των προσωπικών στοιχείων προκειμένου να είναι σύννομη η διαβίβαση στοιχείων σε μία Τρίτη χώρα. Διαπιστώνεται μία αύξηση των εθνικών νόμων αλλά και η ανάπτυξη περιφερειακών πρωτοβουλιών, όπως αυτή των χωρών του APEC (Asia-Pacific Economic Cooperation) με στόχο, τη θέσπιση προδιαγραφών για τη χρήση προσωπικών στοιχείων (Μήτρου, 2001).

4.3 Τα όρια και οι προκλήσεις της (διαφύλαξης της) ιδιωτικότητας

Η διαφύλαξη προσωπικών δεδομένων (δεν μπορεί παρά να) αποτελεί εγγενές στοιχείο της νέας πληροφοριακής συνταγματικής τάξης. Αποκτά περίγραμμα και περιεχόμενο σταδιακά και σύστοιχα προς την εξελισσόμενη Εποχή της Πληροφορίας.

Τα όρια της ιδιωτικότητας και της διαφύλαξής της προσδιορίζονται από τεχνολογικούς παράγοντες, τις διαφορετικές αντιλήψεις ατόμων και κρατικών φορέων ως προς την ιδιωτικότητα.

Η τεχνολογία τελεί σε μία «διαλεκτική» σχέση προς τις άλλες εξελίξεις: ο νέος ρόλος του κράτους και οι αλλαγές στη διάρθρωση της οικονομίας ενέτειναν τις ανάγκες για επεξεργασία στοιχείων. Οι νέες τεχνολογίες είναι προϊόν της κοινωνίας, η προέλευση και η εξέλιξή τους προσδιορίζονται από αυτή. Από την άλλη πλευρά οι τεχνολογίες επηρεάζουν, ενίοτε δε καθορίζουν την εξέλιξη της κοινωνίας και των θεσμών της (Μήτρου, 2001).

4.4 Η τεχνολογία

Οι τεχνολογικές εξελίξεις έχουν εισαχθεί σχεδόν σε κάθε τομέα της ζωής και φαίνεται πως η ενσωμάτωση της τεχνολογίας στην εκπαίδευση και ειδικά των ηλεκτρονικών πλατφορμών είναι αναπόφευκτη. Με δεδομένη τη σημαντική θέση που έχουν καταλάβει οι τεχνολογικές πλατφόρμες όπως το live@edu και το moodle, τα σχολεία έχουν μεγάλη ευθύνη για την εκπαίδευση ατόμων που θα είναι σε θέση να μπορούν να κάνουν αποτελεσματική χρήση των πλατφορμών αυτών και γενικά των εφαρμογών και παροχών του διαδικτύου. Σήμερα, οι εκπαιδευτικοί θα πρέπει να προβαίνουν στις αναγκαίες κινήσεις για να εξασφαλίσουν ότι η τεχνολογία και ειδικά οι ηλεκτρονικές πλατφόρμες θα ενσωματωθούν επιτυχώς στη διδακτική-μαθησιακή διαδικασία (Buttarelli, 2009). Ο κόσμος εξελίσσεται σε μία «δικτυωμένη κοινωνία, όπου τα προσωπικά δεδομένα συλλέγονται, εμπλουτίζονται, τροποποιούνται, ανταλλάσσονται και επαναχρησιμοποιούνται διαρκώς» (Robinson et all, 2009), (European Commission, 2008). Σήμερα, οι περισσότερες τεχνολογίες που χρησιμοποιούμε διέπονται από κανόνες, πρότυπα. Βασικά, αυτά καθορίζουν τις ελάχιστες απαιτήσεις ορισμένων τεχνολογιών, προκειμένου να επιτευχθεί η διαλειτουργικότητα, η οποία είναι ιδιαίτερα σημαντική ιδίως για τα συστήματα Radio Frequency Identification Radio Frequency Identification (RFID) τα οποία αποτελούν τεχνολογία που επιτρέπει την αυτόματη αναγνώριση αναγνώριση αντικειμένων. Βασίζεται στην αποθήκευση και ασύρματη ανάκτηση δεδομένων μέσω μικροσκοπικών συσκευών , τα ονομαζόμενα RFID tags ή transporders. Για να γίνει κατανοητή η ανάγκη για διαλειτουργικότητα στην τεχνολογία RFID θα θέσουμε το παράδειγμα των προβλημάτων στην εφοδιαστική αλυσίδα των επιχειρήσεων (Μήτρου, 2001).

Η διαχείριση της εφοδιαστικής αλυσίδας αρχίζει σε ένα ορυχείο ή ένα αγρόκτημα και καταλήγει σε ένα εργοστάσιο ανακύκλωσης ή σκουπιδιών.

Στο μεταξύ, το αρχικό υλικό έχει τροποποιηθεί ή υποβληθεί σε επεξεργασία από στάδιο σε στάδιο κλπ. Σε αυτόν τον παγκοσμιοποιημένο κόσμο, το εν λόγω υλικό ή αντικείμενο, πιθανότατα συνδεδεμένο με μια ετικέτα RFID, μπορεί να ταξιδέψει σε όλο τον κόσμο .

Αυτό σημαίνει ότι οι ετικέτες RFID θα πρέπει να διαβάζονται σωστά από όλους και παντού, στο παρόν και στο μέλλον και χωρίς καμία περιορισμένη πρόσβαση ή εφαρμογή, δηλαδή τα συστήματα RFID πρέπει να είναι διαλειτουργικά. Η τεχνολογία RFID είναι γεγονός ότι παρουσιάζει αξιοσημείωτη, αυξανόμενη δημοτικότητα. Κατά συνέπεια, ένας μεγάλος και ποικίλος αριθμός λύσεων RFID χρησιμοποιούνται από όλο και περισσότερες επιχειρήσεις και εταιρείες. Δεν αποτελεί έκπληξη ότι και οι εθνικές κυβερνήσεις έχουν επίσης παρατηρήσει τα οφέλη των συστημάτων RFID σε συνηθισμένα πεδία αρμοδιότητάς τους, π.χ. στον έλεγχο των διαβατηρίων και παρακολούθησης εγγράφων. Ως εκ τούτου, είναι δύσκολο να πούμε ακριβώς πόσα συστήματα RFID έχουν ήδη αναπτυχθεί σε όλο τον κόσμο. Ωστόσο, είναι σαφές ότι τα συστήματα αυτά γίνονται ολοένα και πιο δημοφιλή (Marx, 2006).

4.5 Η εμπορευματοποίηση της προσωπικής πληροφορίας

Σε γενικές γραμμές, η ασφάλεια σημαίνει ότι τα δεδομένα που αποθηκεύονται στη μνήμη μιας ετικέτας θα πρέπει να είναι προσβάσιμα μόνο από εξουσιοδοτημένα μέρη και ότι η πλαστογραφία ή η παραποίηση μιας ετικέτας θα μπορεί να επιτευχθεί μόνο ως αμελητέα πιθανότητα. Από την άλλη πλευρά, η διατήρηση της ιδιωτικότητας μπορεί να οριστεί ως η ικανότητα των ετικετών να παράγουν ασυσχέτιστα μηνύματα ταυτοποίησης (Marx, 2006).

Οι πρόοδοι στην τεχνολογία της πληροφορίας επιτρέπουν την εισαγωγή της καινοτομίας σε όλους τους τομείς. Οι εξελίξεις στον τομέα της πληροφορικής δίνουν στους ερευνητές ισχυρά νέα εργαλεία, δίνοντας ευκαιρίες σε μικρές επιχειρήσεις να μπορέσουν να επεκτείνουν σημαντικά στην έρευνα και στην ανάπτυξη καθώς και στην τόνωση της

καινοτομίας παρέχοντας στους χρήστες περισσότερο από ένα ρόλο, επιτρέποντας στους οργανισμούς να διαχειρίζονται πιο αποδοτικά την υπάρχουσα γνώση των υπαλλήλων τους (Hotaling, 2007-2008), (Gurria, 2008). Η φάση ανάδειξης των κρυμμένων σχέσεων και τάσεων στους μεγάλους αδόμητους όγκους δεδομένων, ονομάζεται εξόρυξη δεδομένων (Data Mining). Στις υλοποιήσεις εξόρυξης δεδομένων χρησιμοποιείται η επιχειρηματική εμπειρία σε συνδυασμό με την ισχυρή αναλυτική τεχνολογία, προκειμένου να διερευνηθούν τα διαθέσιμα επιχειρηματικά δεδομένα και να αναδειχθεί πολύτιμη πληροφορία που απαντά γρήγορα και ξεκάθαρα σύνθετα ερωτήματα προσφέροντας την απαραίτητη γνώση για την επίτευξη των επιχειρηματικών στόχων .Με την χρήση της διαδικασίας της εξόρυξης δεδομένων είναι δυνατόν να επιλυθεί κάθε επιχειρηματικό πρόβλημα που βασίζεται στα ιστορικά δεδομένα.

Ωστόσο αν και η πρόοδος στον τομέα των επικοινωνιών και του διαδικτύου είναι δεδομένη, ωστόσο υφίστανται παράλληλα και ορισμένες παράμετροι που κάνουν έντονο τον προβληματισμό για την διαφύλαξη προσωπικών δεδομένων. Οι παράμετροι αυτές, αφορούν κατά κύριο λόγο τις επιχειρηματικές αλλαγές που συντελούνται στο πεδίο της ψηφιακής οικονομίας και που εμπορευματοποιούν τα προσωπικά δεδομένα, καθιστώντας τα ευάλωτα σε παραβιάσεις. (Karyda et all,2006) .

4.6 Η έλλειψη ορίων και η δικτυακή παγκοσμιοποίηση

Η παγκοσμιοποίηση δεν έχει απλώς μία προφανή τεχνολογική διάσταση αλλά, πολύ περισσότερο, συντελείται ακριβώς πάνω σε τεχνολογική βάση. Η Κοινωνία της Πληροφορίας αποτελεί μια από τις σημαντικότερες προτεραιότητες του ανεπτυγμένου κόσμου δεδομένης της ψηφιοποίησης της πληροφορίας και της διάχυσης της μέσω των ηλεκτρονικών δικτύων και του διαδικτύου (Marx, 2006).

Ο σύγχρονος άνθρωπος αποδεσμευμένος από χωρο-χρονικούς περιορισμούς αναζητά την πληροφορία χωρίς να μετακινείται. Σχηματικά, η μορφολογία της πληροφορίας είναι που έχει μεταλλαχθεί προκειμένου να προσεγγίζει τον ενδιαφερόμενο χρήστη εκμηδενίζοντας τις αποστάσεις και τους χρονικούς περιορισμούς. Ακόλουθα, η πληροφορία αποκτά νεωτεριστικές διαστάσεις καθώς μεταβάλλεται σε εμπορικό προϊόν που αναζητά παραγωγούς, διακινητές και εν τέλει καταναλωτές.

Ως παράγοντας των κοινωνικών αλλαγών, η επιστήμη της πληροφορικής επιταχύνει την εξέλιξη, τόσο των γεγονότων που έχουν ήδη μπει σε τροχιά όσο και αυτών που θα συνέβαιναν μελλοντικά ακόμα και χωρίς την επιρροή της. Συνεπώς, η επιστήμη της πληροφορικής έχει επιτελέσει κυρίως ρόλο καταλυτικό παρά πρωταρχική αιτία των αλλαγών (Laver, 1989).

Αντίστοιχα, οι ραγδαίες εξελίξεις της παγκοσμιοποίησης στην οικονομία και στις Νέες Τεχνολογίες επέβαλαν προσαρμογές στα παγκόσμια οικονομικό-κοινωνικά συστήματα. Οι αναπτυγμένες χώρες προσαρμόστηκαν έγκαιρα, σε αντίθεση με τις αναπτυσσόμενες χώρες όπου οι μεταρρυθμίσεις προκάλεσαν κοινωνικό-οικονομικούς τριγμούς, καθώς αποτέλεσαν απόρροια βίαιου εκσυγχρονισμού. (Laver, 1989). Κάτι τέτοιο θα σήμαινε απαγόρευση ανάρτησης προσωπικών στοιχείων καθώς είναι προφανές ότι δεν διαθέτουν όλα τα κράτη το «ικανοποιητικό επίπεδο προστασίας» των στοιχείων που απαιτεί η κοινοτική Οδηγία για τη διασυνοριακή ροή προσωπικών στοιχείων. Ανάλογα ζητήματα είχαν τεθεί στην πολύκροτη υπόθεση των λεγόμενων passenger name record (PNR-data),(αρχείο στη βάση δεδομένων) όπου το Ευρωπαϊκό Κοινοβούλιο υποστήριξε ότι η πρόσβαση δημόσιων αρχών των ΗΠΑ στα δεδομένα PNR σε αντίθεση με την εναλλακτική λύση της προώθησης στοιχείων (σύστημα push), ορίζεται ως μη ρυθμιζόμενη από την Οδηγία και γι' αυτό μη επιτρεπτή αναφορικά με το ευρωπαϊκό δίκαιο κατεργασία στοιχείων.

Παρακάτω ακολουθούν τα βασικότερα σημεία αναφοράς μέσα από κριτήρια σύγκρισης που αναφέρονται στις παραμέτρους σε σχέση με το ποιες είναι οι παράμετροι

για τη διαφύλαξη των προσωπικών στοιχείων. Αρχικά κάθε περιοχή θα αναλυθεί ξεχωριστά και στη συνέχεια, θα γίνει σύγκριση των τριών περιοχών βάσει των κριτηρίων.

ΝΟΜΟΘΕΣΙΑ ΕΛΛΑΔΑΣ

Ν. 2472/97

Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.
v. 2774/1999

Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα.
Ν.3051/2002

Συνταγματικά κατοχυρωμένες ανεξάρτητες αρχές, τροποποίηση και συμπλήρωση του συστήματος προσλήψεων στο δημόσιο τομέα και συναφείς ρυθμίσεις.
v. 3471/06

Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών
Ν. 3783/2009

Ταυτοποίηση των κατόχων και χρηστών εξοπλισμού και υπηρεσιών κινητής τηλεφωνίας και άλλες διατάξεις
Ν. 3917/2011

Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις.
Ν.4070/2012

Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις.

ΝΟΜΟΘΕΣΙΑ ΕΥΡΩΠΗΣ

Το άρθρο 16 της Οδηγίας 95/46/ΕΚ για την προστασία προσωπικών δεδομένων περιλαμβάνει μία -ιδιότυπης αρνητικής διατύπωσης – ρύθμιση για το απόρρητο, καθώς ορίζει ότι όποιος επεξεργάζεται στοιχεία για λογαριασμό του υπεύθυνου επεξεργασίας το κάνει μόνο κατ' εντολή του υπεύθυνου επεξεργασίας

Οδηγία 95/46/ΕΚ (άρθρο 25)

Την ύπαρξη «ικανοποιητικού επιπέδου προστασίας» των προσωπικών στοιχείων προκειμένου να είναι σύννομη η διαβίβαση στοιχείων σε μία Τρίτη χώρα.
Οδηγία 95/46/ΕΚ

Για την προστασία των φυσικών προσώπων έναντι της επεξεργασία δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών
Οδηγία 2002/58/ΕΚ

Για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών.
Οδηγία 2006/24/ΕΚ

Για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών και για την τροποποίηση της οδηγίας 2002/58/ΕΚ
Οδηγία 2009/136/ΕΚ

Για τροποποίηση της οδηγίας 2002/22/ΕΚ για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών, της οδηγίας 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και του κανονισμού (ΕΚ) αριθ. 2006/2004 για τη συνεργασία μεταξύ των εθνικών αρχών που είναι αρμόδιες για την επιβολή της νομοθεσίας για την προστασία των καταναλωτών

Αποφάσεις

Απόφαση του Δικαστηρίου της Ευρωπαϊκής Ένωσης (Γενικό Δικαστήριο) της 8ης Απριλίου 2014 Απόφαση στις συνεκδικασθείσες υποθέσεις C-293/12 και C-594/12 Digital Rights Ireland και Seitlinger κ.λπ.

Οδηγία 2009/136/ΕΚ και Οδηγία 2009/140/ΕΚ και Κανονισμός αριθ. 1211/2009 Οδηγία 2009/136/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Νοεμβρίου 2009, για τροποποίηση της Οδηγίας 2002/22/ΕΚ, της Οδηγίας 2002/58/ΕΚ και του Κανονισμού (ΕΚ) αριθ. 2006/2004

Οδηγία 2006/24/ΕΚ Οδηγία 2006/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15ης Μαρτίου 2006 για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών

Απόφαση του Δικαστηρίου της Ευρωπαϊκής Ένωσης (τρίτο τμήμα) της 16ης Φεβρουαρίου 2012 Απόφαση στην υπόθεση C-360/10 Belgische Vereniging van Auteurs, Componisten en Uitgevers (SABAM) κατά Netlog NV. Αίτηση για την έκδοση προδικαστικής αποφάσεως: Rechtbank van eerste aanleg te Brussel - Βέλγιο.

Απόφαση ΕΔΑΔ - Υπόθεση Copland κατά Ηνωμένου Βασιλείου Απόφαση του Ευρωπαϊκού Δικαστηρίου Ανθρώπινων Δικαιωμάτων (3-4-2007)

1973 Απόφαση Griswold έναντι Connecticut 381 U.S 479(1965) Να σημειωθεί οτι verbatim στο Αμερικανικό σύνταγμα αναφορά και προστασία δικαιώματος ιδιωτικής ζωής δεν υπάρχει.

381 U.S 479 (1965)

National association for the Advancement of colored people

Η υπόθεση εκτυλίχθηκε κατά τα τέλη της δεκαετίας του 1950
Breard v. city of Alexandria, 341 U.S 622 (1951) Kovacs v Cooper, 336 U.S 77 (1949) και Federal communications commission v Pacifica foundation , 438 U.S 726 (1978) συνταγματική η διάταξη που απαγορεύει δηλώσεις σε μέρη της πόλης που υπάρχουν μόνο κατοικίες , καθώς το σπίτι σε κάθε πολίτη είναι το τελευταίο καταφύγιο των "κουρασμένων", "αδυνάτων" και "ασθενών" Federal communications όπ στο 484
Boyd v United states, 116 U.S. 616 (1886) Katz v United states 389 United states 347 (1967) αντισυνταγματική η χρήση από την ομοσπονδιακή αστυνομία μηχανισμού παρακολούθησης τηλεφωνικής συνομιλίας σε θάλαμο τηλεφώνου.
Ruckelshaus v Monsato Co ., 467 United states 986 (1984)
Reinberg J., Privacy in thw information economy:a fortress or frontier for individual rights; 44 fed Comm . L.J 195 (1992)

Πηγή: Weerakkody, V., & Reddick, C. G. (Eds.). (2012). *Public sector transformation through e-government: experiences from Europe and North America*. Routledge.

ΣΥΓΚΡΙΣΗ ΝΟΜΟΘΕΣΙΑΣ

Στη συνέχεια, στον παρακάτω πίνακα, παρατίθενται τα κυριότερα νομοθετικά ζητήματα των χωρών που εξετάστηκαν. Περιγράφονται εν συντομία τα βασικά σημεία που πρεσβεύει η νομοθεσία του κάθε κράτους εστιάζοντας στα

κυριότερα.

ΚΡΙΤΗΡΙΑ ΣΥΓΚΡΙΣΗΣ	**ΕΛΛΑΔΑ**	**ΑΜΕΡΙΚΗ**	**ΕΥΡΩΠΗ**	**ΣΥΓΚΡΙΣΗ ΤΩΝ ΤΡΙΩΝ ΠΕΡΙΟΧΩΝ**
Επεξεργασία προσωπικών στοιχείων	Η Ελλάδα θεωρεί συνολικά την επεξεργασία στοιχείων προσωπικού χαρακτήρα ως απόρρητη.	Η αμερικανική νομοθεσία δίνει λύσεις στο ζήτημα επεξεργασίας προσωπικών στοιχείων οι οποίες σιγά σιγά βοηθούν να αντιμετωπίζονται κάποια κύρια σημεία του προβλήματος	Γίνονται σημαντικές προσπάθειες, όμως αυτές οι προσπάθειες δεν είναι εξίσου ισχυρές στο σύνολο της Ευρώπης	Δεν υπάρχει διαφορά μεταξύ των 3 εξεταζόμενων περιοχών. Και οι τρεις δίνουν την ίδια βαρύτητα στο ζήτημα των προσωπικών δεδομένων.
Προστασία προσωπικών δεδομένων	Η ελληνική νομοθεσία για την προστασία	Τα μέτρα που λαμβάνονται είναι πιο	Η κάθε χώρα πρέπει τις δράσεις να τις	Η ελληνική νομοθεσία μελετά το ζήτημα αλλά δεν

	προσωπικών δεδομένων απαιτεί τη λήψη «κατάλληλων» μέτρων ασφάλειας	ουσιαστικά και πιο εστιασμένα στο πρόβλημα προστασίας δεδομένων προσωπικών στοιχείων	ενσωματώσει στη δική της νομοθεσία	έχει εφαρμόσει αυστηρά μέτρα και δεν ακολουθεί ακριβώς τις ευρωπαϊκές οδηγίες. Η Αμερική είναι πολύ πιο αυστηρή στο τομέα αυτό και από την Ελλάδα και από την Ευρώπη. Η Ευρώπη ενώ έχει συγκεκριμένη πολιτική επηρεάζεται αυτή η πολιτική από τις πολιτικές κάθε χώρας.
Επιτήρηση σε δημόσιους και ιδιωτικούς χώρους	Συστήματα επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις	Βελτιωμένες προσπάθειες στο τομέα της επιτήρησης σε δημόσιους και ιδιωτικούς χώρους στις νομοθετικές ρυθμίσεις για το μέλλον	Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών και υπηρεσιών επιτήρησης	Παρατηρείται ότι και στις τρεις περιοχές το διαδίκτυο αποτελεί μέσο επιτήρησης χώρων με στόχο την ασφάλεια. Στην Ελλάδα είναι μικρότερη η έκταση αυτών των υπηρεσιών υπάρχει όμως σχετικό νομικό πλαίσιο που καλύπτει το όλο θέμα . Στην Αμερική είναι ακόμα πιο αυστηρή η επιτήρηση και υπάρχει ακόμα πιο αυστηρό νομικό πλαίσιο δεδομένων και των συνθηκών. Στην Ευρώπη υπάρχουν ευρωπαϊκές οδηγίες που καθορίζουν τις διαδικασίες και ανά χώρα αλλάζει ο τρόπος εφαρμογής.

Όπως προκύπτει μέσα από τα στοιχεία των παραπάνω πινάκων, είναι εμφανές, ότι σε σχέση με τις υπό εξέταση χώρες, η Αμερική έχει μια αυστηρή νομοθεσία, περισσότερο από τις υπόλοιπες χώρες. Καλύπτει περισσότερες διαστάσεις των προβλημάτων, λαμβάνοντας μέτρα που επικεντρώνονται στο πρόβλημα.

ΕΠΙΛΟΓΟΣ - ΣΥΜΠΕΡΑΣΜΑΤΑ

Στη παρούσα Διατριβή, μελετήθηκε το θέμα του ηλεκτρονικού εμπορίου και συγκεκριμένα μια από τις πιο σημαντικές του πτυχές. Αυτή των εγκληματικών πράξεων και δράσεων που αναπτύσσονται στο διαδίκτυο. Ουσιαστικά το θέμα που διερευνήθηκε κυρίως ήταν η νομοθεσία και πως αυτή αναπτύσσεται σήμερα σε παγκόσμιο επίπεδο και στην Ελλάδα, πως καλύπτει το συγκεκριμένο ζήτημα, αν είναι επαρκές και γενικά αυτό που προσπάθησε να καλύψει ο συγγραφέας μέσα στη μελέτη του, είναι το αν οι ευρύτερες νομοθετικές ρυθμίσεις είναι ικανές να δώσουν λύση στο μέλλον και να μειωθεί η εγκληματικότητα μέσα από το διαδίκτυο.

Η βασική διαπίστωση είναι ότι όντως γίνονται σημαντικές προσπάθειες, όμως αυτές οι προσπάθειες δεν είναι εξίσου ισχυρές στο σύνολο της Ευρώπης, κυρίως στη χώρα μας, ενώ είναι πιο βελτιωμένες στην Αμερική. Μελετώντας τη Νομοθεσία στην Αμερική θεωρήθηκε ότι τα μέτρα που λαμβάνονται είναι πιο ουσιαστικά και πιο εστιασμένα στο πρόβλημα. Αυτό είναι ένα συμπέρασμα το οποίο εξήχθη από το συγγραφέα δεδομένου ότι στην Αμερική η νομοθεσία καλύπτει περισσότερες διαστάσεις του προβλήματος, είναι πιο αυστηρή και ευρύτερα δίνει λύσεις οι οποίες σιγά σιγά βοηθούν να αντιμετωπίζονται κάποια κύρια σημεία του προβλήματος. Φυσικά από την Αμερική ξεκινάνε κυρίως τα προβλήματα λόγω της συνεχούς ανάπτυξης που υπάρχει εκεί στη τεχνολογία και το διαδίκτυο και είναι φυσικό να δίνονται περισσότερες λύσεις μιας και είναι πιο ξεκάθαρο το πώς λειτουργεί γενικότερα το ίντερνετ. Στην Ευρωπαϊκή ένωση έχουμε δει ότι έχουν γίνει σημαντικές δράσεις. Το πρόβλημα όμως με την Ευρωπαϊκή ένωση είναι ότι η κάθε χώρα πρέπει να ενσωματώσει αυτές τις δράσεις στη δική της νομοθεσία. Αυτό δεν είναι πάντα εφικτό και έχει ως αποτέλεσμα να μην λαμβάνονται πάντα αποτελεσματικά μέτρα. Μια από αυτές τις περιπτώσεις είναι και η Ελλάδα η οποία και εξετάστηκε. Σαφώς υπάρχει ακόμη δρόμος, να διανυθεί σε θεσμικό επίπεδο, προκειμένου να επιτευχθεί ένα ικανοποιητικό θεσμικό πλαίσιο που θα εξασφαλίζει την ασφάλεια των δεδομένων στο διαδίκτυο.

Αυτό σημαίνει ότι πρέπει να γίνουν περεταίρω προσπάθειες ώστε να επέλθει βελτίωση στην ελληνική νομοθεσία και αυτό μπορεί να γίνει αν ακολουθηθεί από τη μία το ευρωπαϊκό πρότυπο και από την άλλη αν υπάρξουν ανεξάρτητοι φορείς πιο εξειδικευμένοι οι οποίοι θα δίνουν λύση στο πρόβλημα. Θεωρείται ότι πρέπει να υπάρξει ακόμα καλύτερη ενημέρωση στο κοινωνικό, το σχολικό, και το οικογενειακό περιβάλλον της χώρας ώστε να υπάρξει συνολική αντιμετώπιση στο πρόβλημα. Όχι μόνο από το κράτος αλλά να αναπτυχθεί μια ευρύτερη κουλτούρα πάνω στο θέμα.

Στο μέλλον θα πρέπει σίγουρα το πρόβλημα αυτό να αντιμετωπιστεί σε παγκόσμιο επίπεδο προκειμένου το διαδίκτυο να αποτελέσει ένα ασφαλές περιβάλλον για όλους.

Βιβλιογραφία

Ξενόγλωσση

- Aaron E. Earle, (2005) “Wireless Security Handbook”, Auerbach Publications Boston, MA, USA
- Barnard, L. & Wesson, J. (2004). A Trust Model for E-commerce in South Africa Usability in Web Applications. Proceedings of the 2004 Annual Research Conference of the South African institute of Computer Scientists and Information Technologists on IT Research in developing countries Held in 2004, Stellenbosch, Western Cape, South Africa, 23-32.
- Berger, A.A., (1995), *“Essentials of Mass Communications Theory”*, Thousand Oaks, CA: Sage
- *Boyd,* G and Potter, J.(*2003)*. *Social Network Fragments: An Interactive Tool for Exploring Digital Social Connections*. Siggraph
- Buttarelli, (2009) Towards a Charter on Digital Data Protection And Freedom of Information, Data Protection Conference “Personal Data – more use, more protection, Brussels.
- Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet. Academic press.
- Cook, J. G., & Sobieski Jr, J. L. (2014). Wiretapping and Electronic Eavesdropping (Omnibus Crime Control and Safe Streets Act of 1968, Title III, 18 USC P 2520). *Civil Rights Actions*, *5*.
- Copyright Hellenic Data Protection Authority (2003), Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.
- Council Framework Decision (2008) "on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters" Available from: http://eur-lex.europa.eu/LexUriServ/ [2015]
- Datz, Todd. “A More Perfect Union.” CIO Magazine. 1 Mar. 2003. URL http://www.cio.com/archive/030103/union.html
- Enloe, Christian. “Government System Certification: A Guide to Government Security Mandates.” December 2002. URL:http://www.giac.org/practical/GSEC/Christian_Enloe_GSEC.pdf
- European Commission, (2008). Early Challenges regarding the “Internet of Things”,Commission staff working document
- Frey D. (2003). An Analysis of Cybercrime: Past, present and future. Ανάκτηση από www.acsu.buffalo.edu/-dijfrey/ICO631final_individual.pdf [2015]
- Goodman M., & Brenner S., (2002). The Emerging Consensus on Criminal Conduct in Cyberspace. UCLA Journal and Technology. Ανάκτηση από http://www.lawtechjurnal.com/articles/ [2015]
- Gurria A., (2008) Closing Remarks to the OECD Ministerial meeting on the Future of the Internet Economy, http://www.oecd.org .
- Hotaling A., (2007-2008), Protecting Personally Identifiable Information on the Internet: Notice and Consent in the Age of Behavioral Targeting. Commlaw Conspectus. Vol. 16 . σελ. 529 επ.
- IISS Global Perspectives – Power in Cyberspace. Q&A with Nigel Inkster, Director, Transnational Threats and Political Risk, IISS. 18 January 2011.
- Jewkes, Y. (Ed.). (2013). Crime online. Routledge.
- Jewkes, Y., & Yar, M. (Eds.). (2013). Handbook of Internet crime. Routledge.
- *John Leyden (13 January 2015). "'80s hacker turned journo, IT crime ace Steve Gold logs off". The Register*. Retrieved 14 January 2015.
- Karyda M , Mitrou/ L. Quirchmayr, (G. 2006), A framework for outsourcing IS/IT security services, Information Management & Computer Security, Vol. 14 Issue 5, σελ. 402-415.
- Kaufman, L. M. (2009). Data security in the world of cloud computing. Security & Privacy, IEEE, 7(4), 61-64.

- Laver, M. (1989), Information technology: agent of change, Cambridge University Press, Cambridge.
- Marcella Jr, A., & Greenfield, R. S. (Eds.). (2002). Cyber forensics: a field manual for collecting, examining, and preserving evidence of computer crimes. CRC Press.
- Marx G., (2006) Soft surveillance: The Growth of Mandatory Volunteerism in Collecting Personal Information, σε T. Monahan, Surveillance and Security: Technological Politics and Power in Everyday Life, London, Routledge , σελ. 37.
- *Naylor, Chris (July 1994). "Locked ". Personal Computer World.*
- Neil MacEwan, "The Computer Misuse Act 1990: lessons from its past and predictions for its future" (2008), Criminal Law Review **955**.
- OECD, (2007). Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy – Preface
- Pearson, S. (2009). Taking account of privacy when designing cloud computing services. In Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing (pp. 44-52). IEEE Computer Society.
- Pearson, S., & Charlesworth, A. (2009). Accountability as a way forward for privacy protection in the cloud. In Cloud computing (pp. 131-144). Springer Berlin Heidelberg.
- Peltier, T. R. (2013). *Information security fundamentals*. CRC Press.
- Robinson N., Craux H., Bottermann M., Valeri L. (2009) (RAND Europe), Review of the European Data Protection Directive, Information Commissioner's Office (UK), σελ. 7.
- Rouvroy A., (2008), Privacy, Data Protection and the Unprecedented Challenges ofAmbient Intelligence, Studies in Ethics, Law and Technology, Vol. 2 Issue 1, http://www.bepress.com/selt/vol2/iss/art3 .
- Simitis, S. (2008) International Transfers of Personal Data, Παρουσίαση σε Workshop on International Transfers of Personal Data, Brussels.
- Solove (2008), Understanding Privacy, Harvard University Press
- Solove D.J., (2002) "Digital dossiers and the dissipation of Fourth Amendment Privacy, Southern California Law Review
- Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS quarterly*, *34*(3), 503-522.
- Stefan Fafinski, Computer Misuse: Response, Regulation and the Law (Cullomption, Willan 2009)
- Taylor, R. W., Fritsch, E. J., & Liederbach, J. (2014). Digital crime and digital terrorism. Prentice Hall Press.
- Tipton, H. F., & Krause, M. (2012). *Information security management handbook*. CRC Press.
- Webb, Cynthia. "No Stellar E-Gov Funding." The Washington Post. Government IT Review. 11 Sept. 2003. URL: http://www.washingtonpost.com/wp-dyn/articles/A60315-2003Sep11.htm
- Weerakkody, V., & Reddick, C. G. (Eds.). (2012). *Public sector transformation through e-government: experiences from Europe and North America*. Routledge.
- Weinberger and Spotts (1997), "Assessing the Use and Impact of Humor on Advertising Effectiveness," Journal of Advertising, vol. 26, no. 3.
- Whitman, M., & Mattord, H. (2011). *Principles of information security*. Cengage Learning.
- Whitman, M., & Mattord, H. (2013). *Management of information security*. Cengage Learning.
- Yaman Akdeniz, Section 3 of the Computer Misuse Act 1990: an Antidote for Computer Viruses! (1996) 3 Web JCLI [2] including reference to the case of Christopher Pile (aka 'the Black Baron') in November 1995

Ελληνόγλωσση

- Βλαχόπουλος, Κ. (2007). Ηλεκτρονικό Έγκλημα. Αθήνα: Νομική Βιβλιοθήκη.
- Γκρίτζαλη Δ., (2004) "Ασφάλεια Πληροφοριακών Συστημάτων και Υποδομών: Εννοιολογική Θεμελίωση" Αθήνα
- Ζάννη Α. (2005). Το διαδικτυακό έγκλημα. Αθήνα: Σάκκουλα.
- Κυριαζόπουλος, Π., & Σαμαντά, Ε. (2011). *Μεθοδολογία έρευνας εκπόνησης διπλωματικών εργασιών*. Αθήνα: Σύγχρονη εκδοτική
- Μήτρου Λ., (2001) Προστασία Προσωπικών Δεδομένων: ένα νέο δικαίωμα; σε Δ. Τσάτσου/Ε. Βενιζέλου/Ξ. Κοντιάδη (επιμ.), Το Νέο Σύνταγμα – Πρακτικά συνεδρίου για το αναθεωρημένο Σύνταγμα 1975/1986/2001, Αθήνα – Κομοτηνή, σελ. 83 επ.
- Στογιάννου Φ.,(1999), Πνευματική Ιδιοκτησία, (Copyright, Πατέντες, Εμπορικά σήματα), Homo Ecumenicus
- Στρατηλάτη Κ. (2005) "Η αυτορρύθμιση στον πολιτισμό της διαδικτυακής επικοινωνίας" Αθήνα –Θεσσαλονίκη
- Taipale K. A., Technology, security and privacy: The fear of Frankenstein, the mythology of privacy and the lessons of king Ludd, Yale Journal of Law and Technology, 7 (2004-2005), σελ. 123 επ.
- Φαρσεδάκης Ι., (1996) Στοιχεία εγκληματικότητας. Αθήνα: Νομική Βιβλιοθήκη.

Νομοθεσία

- Οδηγία 95/46/ΕΚ