ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

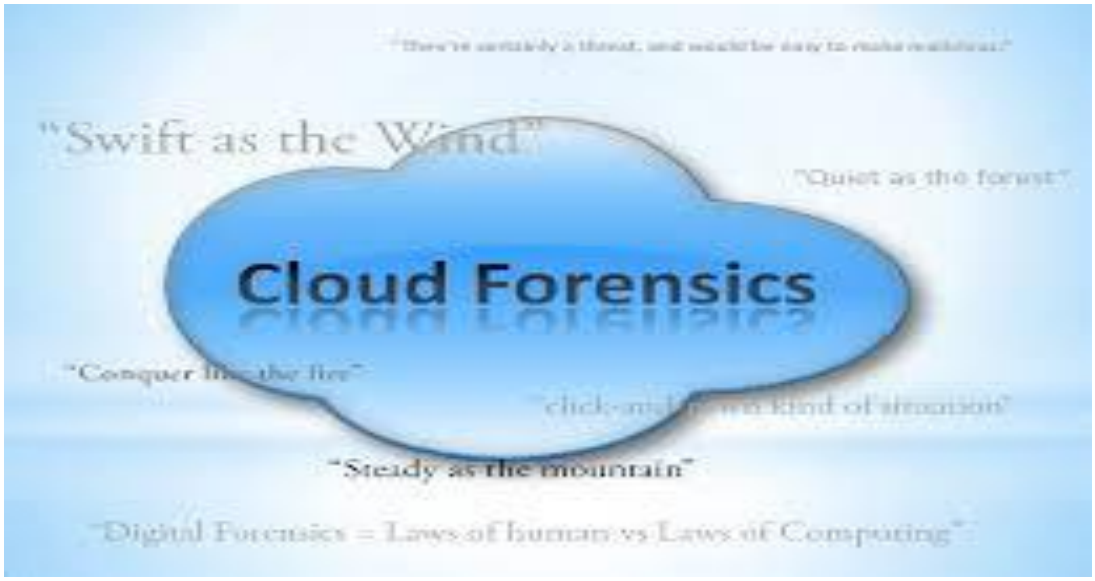
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΣΤΗΝ ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΚΑΝΙΚΗ ΥΠΟΛΟΓΙΣΤΙΚΗ

ΜΠΑΜΠΑΝΗ ΕΛΕΝΗ



Επιβλέπων Καθηγητής: Κ. Λαμπρινουδάκης

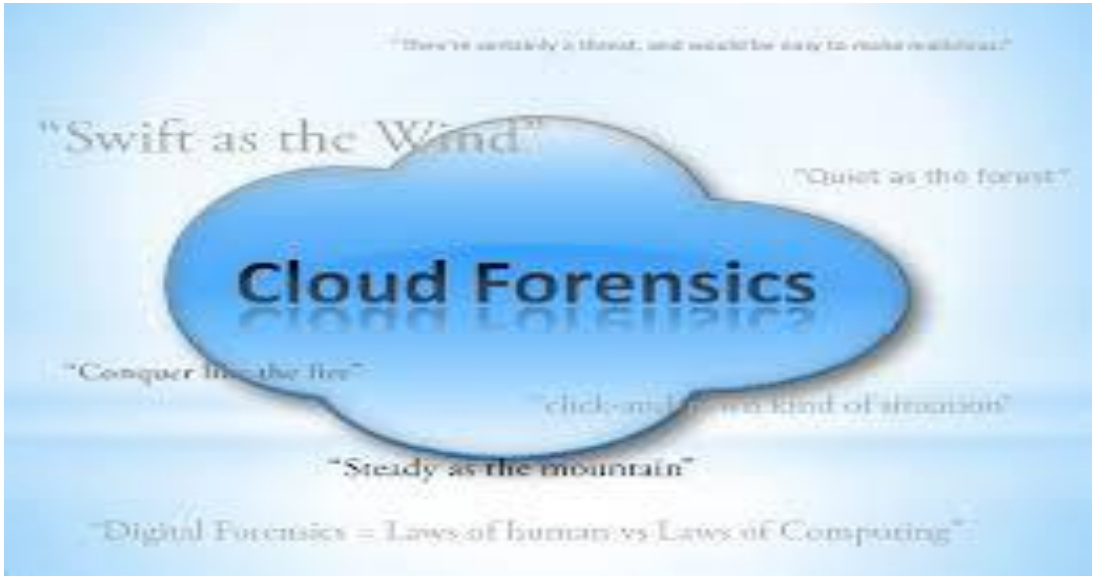
Πειραιάς, Φεβρουάριος 2018

UNIVERSITY OF PIRAEUS
DEPARTMENT OF DIGITAL SYSTEMS

POSTGRADUATE PROGRAMME

DIGITAL SYSTEMS SECURITY

LEGAL ISSUES OF CLOUD FORENSICS



BAMPANI ELENI

Piraeus, February 2018

Ευχαριστίες

Αρχικά, θα ήθελα να ευχαριστήσω την κυρία Λ. Μήτρου για την εμπιστοσύνη που μου έδειξε ώστε να πραγματοποιηθεί την η παρούσα διπλωματική εργασία. Επίσης ένα μεγάλο ευχαριστώ στους γονείς μου για την στήριξη τους όλα αυτά τα χρόνια.

Περίληψη.

Καθώς η τεχνολογία εξελίσσεται παρουσιάζονται ολοένα και περισσότεροι προβληματισμοί και ασάφειες τις οποίες καλούμαστε να καλύψουμε. Άλλοτε αυτές επιλύονται εύκολα και άλλοτε χρειάζεται η δημιουργία εφαρμογών, προγραμμάτων και λογισμικού καθώς και η δημιουργία σχετικού νομοθετικού πλαισίου που θα εξασφαλίζει την λειτουργία των νέων προγραμμάτων. Η παρούσα διπλωματική εργασία έχει ως στόχο να αναδείξει μία νεα τεχνολογία όπως αυτή της ψηφιακής εγκληματολογίας σε ένα υπολογιστικό νέφος. Να εκφράσει προβληματισμούς που γεννούνται αλλά και προτερήματα του.

Στα κεφάλαια που ακολουθούν θα αναλύσουμε το περιβάλλον ενός ψηφιακού υπολογιστικού νέφους **,** θα δούμε έννοιες και ορισμούς, θα απαντήσουμε σε προβληματισμούς και απορίες που δημιουργούνται και θα δούμε τους νόμους που το διέπουν τόσο στην επικράτεια όσο και πως αυτά ορίζονται στον παγκόσμιο ιστό. Ειδικότερα στα επόμενα 5 Κεφάλαια που θα ακολουθήσουν θα έχουμε τη δυνατότητα να παρακολουθήσουμε τις εξελίξεις στο προαναφερόμενο θέμα με την εξής σειρά:

Στο 1^{ο} Κεφάλαιο θα παρουσιάσουμε ένα περιβάλλον «Νέφους» θα δούμε ορισμούς και έννοιες, κανονισμούς, υπηρεσίες, μοντέλα ανάπτυξης και υπηρεσιών.

Στο επόμενο Κεφάλαιο το 2^{ο} , θα αναπτύξουμε τα νομικά θέματα που ισχύουν στα περιβάλλοντα αυτά και ειδικότερα θα δούμε τα νομικά πλαίσια που διέπουν τον τρόπο με τον οποίο επεξεργαζόμαστε τα δεδομένα με σκοπό την διαφύλαξη τους και την διασφάλιση των δεδομένων προσωπικού χαρακτήρα.

Στο 3^{ο} Κεφάλαιο θα δώσουμε ορισμούς και θα αναδείξουμε τεχνικές αναφορικά με την ψηφιακή εγκληματολογία και τους προβληματισμούς

σε αυτό. Θα αναπτυχθεί η τεχνική με την οποία πραγματοποιείται μια πραγματογνωμοσύνη στην Επικράτεια, διάφοροι προβληματισμοί σχετικά με την εφαρμογή του Νόμου και θα αναδείξουμε τον τρόπο με τον οποίο αντιμετωπίζονται τα αδικήματα σε διάφορες χώρες και τι ποινές επιβάλλονται σύμφωνα με το νομικό πλαίσιο κάθε χώρας.
Στο 4^{ο} Κεφάλαιο παρουσιάζουμε τα νομικά θέματα στην εφαρμογή της ψηφιακής ανάλυσης σε περιβάλλοντα όπως το Cloud.
Στο 5^{ο} και τελευταίο Κεφάλαιο θα κλείσουμε την Έκθεση μας καταλήγοντας στο τι πραγματικά συμβαίνει σήμερα και πως το αντιμετωπίζουμε.

Εισαγωγή.

Τον τελευταίο καιρό γίνεται όλο και περισσότερο μεγαλύτερη αναφορά για το **Cloud computing**. Πλέον το **Cloud computing** είναι πιο ώριμο από ποτέ να πραγματοποιήσει αυτό που υπόσχεται, να δώσει δηλαδή υπολογιστικούς πόρους με τη μορφή υπηρεσίας, με την ίδια **λογική** που διέπει και τους άλλους τομείς**.**

Cloud computing σημαίνει μεγάλα κέντρα δεδομένων τα οποία προσφέρουν, οικονομίες κλίμακας, φθηνότερη υπολογιστική ισχύ, ασφαλή διαχείριση, ανθεκτικότητα, αξιοπιστία, βιωσιμότητα, 24/7 υποστήριξη, πρόσβαση από οπουδήποτε, εύκολη και ευκίνητη αποπληρωμή, μεγάλες ταχύτητες, και κυρίως ευελιξία να πληρώνει κανείς μόνο για ότι χρησιμοποιεί.

Ολοένα και περισσότεροι χρήστες ενστερνίζονται την άποψη ότι τόσο οι χρήστες όσο και οι προγραμματιστές έχουν τη δυνατότητα να κάνουν περισσότερα με λιγότερα. Έχουν πρόσβαση σε μεγαλύτερη υπολογιστική ισχύ χωρίς να χρειάζεται να επενδύσουν μεγάλα κεφάλαια σε εξοπλισμό.

Υπηρεσίες πληροφορικής για ιδιώτες και οργανισμούς φιλοξενούνται στο διαδίκτυο και έτσι δεν υπάρχει ανάγκη για τοπικούς server στο χώρο τους. Επιπλέον, επιχειρήσεις και οργανισμοί αποφεύγουν την επένδυση και τη χρήση επιπλέον εξοπλισμού για να καλύψουν εποχιακές ανάγκες.

Με την συνεχή αλλαγή της κυκλοφορίας του δικτύου εξισορροπείται η ζήτηση σε αυτό, χρησιμοποιείται το συνολικό εύρος ζώνης του δικτύου και εκμεταλλεύεται το σύνολο των δυνατοτήτων του Cloud.

Το σύμβολο του σύννεφου χρησιμοποιήθηκε για να υποδηλώσει το σημείο οριοθέτησης μεταξύ των δυνατοτήτων του παρόχου και αυτών των χρηστών. Το **«Υπολογιστικό Νέφος»** επεκτείνει το όριο αυτό όσον αφορά την χρήση των servers, καθώς και την υποδομή του δικτύου. Η βασική ιδέα του **«Υπολογιστικού Νέφους»** χρονολογείται από τη δεκαετία του 1950, όταν μεγάλης κλίμακας κεντρικών υπολογιστών, άρχισαν να διατίθενται σε πανεπιστήμια και επιχειρήσεις, προσβάσιμα μέσω ατομικών τερματικών. Επειδή ήταν δαπανηρή η απόκτηση κεντρικού υπολογιστή, ήταν αναγκαίο να βρεθούν τρόποι να έχουμε τη μέγιστη απόδοση της επένδυσης σε αυτά, επιτρέποντας σε πολλαπλούς χρήστες να μοιράζονται ταυτόχρονα την φυσική πρόσβαση στον κεντρικό υπολογιστή από πολλαπλά τερματικά, καθώς και να μοιράζονται το χρόνο της CPU, εξαλείφοντας τις περιόδους αδράνειας, η οποία έγινε γνωστή στη βιομηχανία των δικτύων ως timesharing. Καθώς οι υπολογιστές έγιναν πιο διαδεδομένοι, οι επιστήμονες και οι τεχνολόγοι ήθελαν να διερευνήσουν τρόπους ώστε να διατίθεται μεγάλης κλίμακας υπολογιστική ισχύ σε περισσότερους χρήστες μέσω του καταμερισμού του χρόνου. Αυτό θα γινόταν με τη χρήση αλγορίθμων, ώστε τόσο η υποδομή όσο και οι εφαρμογές να παρέχουν την αποδοτικότερη χρήση τους, με προτεραιότητα στην πρόσβαση της CPU για την καλύτερη εξυπηρέτηση των τελικών χρηστών. Ο John McCarthy αποφάνθηκε το 1960 ότι "η αξιοποίηση του χρόνου χρήσης υπολογιστικών πόρων μπορεί κάποια μέρα να οργανωθεί ως κοινής

ωφελείας." Σχεδόν όλα τα σύγχρονα χαρακτηριστικά του «Υπολογιστικού Νέφους» (η ελαστική διάταξη, η απευθείας σύνδεση, η ψευδαίσθηση του άπειρου χώρου), σε σύγκριση με τη βιομηχανία ηλεκτρικής ενέργειας και τη χρήση των δημόσιων υπηρεσιών μιας κοινότητας, είχαν διερευνηθεί το 1966 στο βιβλίο του Douglas Parkhill, «The Challenge of the Computer Utility». Άλλοι μελετητές έχουν δείξει ότι οι ρίζες του «Υπολογιστικού Νέφους» πάνε πίσω στη δεκαετία του 1950, όταν ο επιστήμονας Herb Grosch (ο συντάκτης του νόμου Grosch), θεωρούσε ότι ολόκληρος ο κόσμος θα μπορούσε να λειτουργήσει με τερματικά που θα χρησιμοποιούσαν 15 μεγάλα κέντρα δεδομένων. Λόγω της αξίας αυτών των ισχυρών υπολογιστών, πολλές εταιρείες και φορείς θα μπορούσαν να επωφεληθούν από την αποδοτικότητα αυτών των υπολογιστών μέσω του καταμερισμού του χρόνου, όπως η GEISCO της GE, η IBM, η Tymshare (ιδρύθηκε το 1966) κ.ά. Ήδη από το 1970 ένα ήταν κοινό αποδεκτό: η πανταχού παρούσα διαθεσιμότητα των δικτύων υψηλής χωρητικότητας, οι χαμηλού κόστους υπολογιστές και συσκευές αποθήκευσης, καθώς και η ευρεία υιοθέτηση της service oriented αρχιτεκτονικής έχουν οδηγήσει σε τεράστια ανάγκη εξέλιξης του cloud computing. (Tolk A.,2006) Στη συνέχεια η Amazon έπαιξε καθοριστικό ρόλο στην ανάπτυξη του «Υπολογιστικού Νέφους» με τον εκσυγχρονισμό των κέντρων δεδομένων τους, η οποία, όπως και τα περισσότερα δίκτυα υπολογιστών, χρησιμοποιούσαν μόλις το 10% της χωρητικότητάς τους ανά πάσα στιγμή, μόνο και μόνο για να αφήσει χώρο για περιστασιακές αιχμές χρήσης του δικτύου. Αφού διαπίστωσε ότι η νέα αρχιτεκτονική τύπου σύννεφο οδήγησε σε σημαντικές εσωτερικές βελτιώσεις της [9] αποτελεσματικότητας προσθέτοντας νέες λειτουργίες, η Amazon ξεκίνησε μια αναπτυξιακή προσπάθεια για να παρέχει ένα νέο προϊόν, το «Υπολογιστικό Νέφος» σε εξωτερικούς πελάτες. Το αποτέλεσμα αυτής της προσπάθειας ήταν το Amazon Web Service (AWS) με υπολογιστική χρησιμότητα (utility computing) από το 2006. (Galen G.,2009) Στις αρχές του 2008, το Eucalyptus έγινε η πρώτη open-source, AWS API συμβατή πλατφόρμα για την ανάπτυξη των private clouds. Στις αρχές του 2008, η OpenNebula, ενισχύεται με το πρόγραμμα που χρηματοδοτείται από την Ευρωπαϊκή Επιτροπή «RESERVOIR», και έγινε έτσι το πρώτο λογισμικό ανοιχτού κώδικα για την ανάπτυξη των ιδιωτικών και υβριδικών clouds, για την

ομοσπονδία των clouds. Κατά το ίδιο έτος, οι προσπάθειες επικεντρώθηκαν στην παροχή υψηλής ποιότητας υπηρεσιών για cloud-based υποδομές, στο πλαίσιο προγράμματος που χρηματοδοτείται από την Ευρωπαϊκή Επιτροπή με το όνομα «IRMOS», με αποτέλεσμα να δημιουργηθεί ένα περιβάλλον cloud σε πραγματικό χρόνο. Έως τα μέσα του-2008, η εταιρία Gartner είδε μια ευκαιρία για το «Υπολογιστικό Νέφος», να διαμορφώσει τη σχέση μεταξύ των καταναλωτών των υπηρεσιών πληροφορικής, σε εκείνους που χρησιμοποιούν τις υπηρεσίες πληροφορικής και εκείνους που τις πωλούν, αρχίζοντας να στρέφεται στην αξιοποίηση του Cloud Computing. (Kyriazis D., Menychtas A., Kousiouris G. , Oberle K., Voith T., Boniface M., Oliveros E., Cucinotta T., Berger S.,2010) Στις 1 Μαρτίου 2011, η IBM ανακοίνωσε τη χρήση του Smarter Computing framework για την υποστήριξη του Smarter Planet. Το 2012, ο Δρ John Biju και ο Δρ Souheil Khaddaj περιγράφουν το σύννεφο ως μια εικονική και σημασιολογική πηγή πληροφοριών: «Το Υπολογιστικό Νέφος είναι μια καθολική συλλογή των δεδομένων που εκτείνεται πάνω από το διαδίκτυο, με τη μορφή των πόρων (όπως το υλικό πληροφοριών, διάφορες πλατφόρμες, υπηρεσίες κ.λπ.). Διαμορφώνει επιμέρους μονάδων στο εικονικό περιβάλλον ».

Κεφάλαιο 1 :

Επισκόπηση Υπολογιστικού Νέφους (Cloud Computing).

1.1 Ορισμός και Περιγραφή Υπολογιστικού Νέφους (Cloud Computing)

Σύμφωνα με τον NIST, το **Cloud Computing** είναι ένα μοντέλο που επιτρέπει την εύκολη, on-demand (τη στιγμή που ζητείται) πρόσβαση μέσω δικτύου σε ένα "κοινό ταμείο" από παραμετροποιήσιμους υπολογιστικούς πόρους (π.χ. Δίκτυα, servers, αποθηκευτικό χώρο, εφαρμογές και υπηρεσίες) οι οποίοι μπορούν πολύ εύκολα να παρακολουθηθούν και να αποδοθούν με πολύ μικρή παρέμβαση της διαχείρισης ή αλληλεπίδρασης από τον πάροχο των υπηρεσιών**.**

Με τον όρο **Cloud Computing** νοείται η πρόσβαση σε υπολογιστές και στη λειτουργικότητα τους, απομακρυσμένα, μέσω δικτύου. (διαδίκτυο ή τοπικό δίκτυο)

Ένα υπολογιστικό νέφος, παρέχει στον χρήστη υπολογιστική ισχύ, λογισμικό, πρόσβαση σε δεδομένα και υπηρεσίες αποθηκευτικού χώρου, χωρίς να απαιτείται η φυσική τοποθεσία. Εικάζεται ότι του έχει δοθεί το όνομα αυτό από το γεγονός του ότι αν θεαθεί από μακρινή απόσταση φαίνεται σαν ένα νέφος αλλά στην πραγματικότητα ο χρήστης δεν μπορεί ούτε να καταλάβει αλλά ούτε και να προσδιορίσει που ακριβώς βρίσκονται οι υποδομές που χρησιμοποιεί και ο εξοπλισμός που φιλοξενεί τις υπηρεσίες.

1.2 Ιστορική αναδρομή.

Αξίζει λοιπόν να κάνουμε μια αναδρομή στο πώς εξελίχθηκε η ιδέα του **Cloud computing** καθώς η έννοια αυτή κάθε άλλο παρά καινούρια είναι.

Από 1950 έως 1960 τα μεγάλα συστήματα υπολογιστών έγιναν διαθέσιμα σε πανεπιστήμια, σχολεία και οργανισμούς. Οι υποδομές για τα συστήματα αυτά είχαν έκταση ολόκληρων δωματίων και η πρόσβαση γινόταν μέσω "στατικών" τερματικών καθώς δεν υπήρχαν οι δυνατότητες επεξεργασίας δεδομένων παρά μόνο τα μέσα για την επικοινωνία.

Με απώτερο σκοπό την εξοικονόμηση κεφαλαίων και την πιο αποτελεσματική χρήση και εκμετάλλευση των κοστοβόρων υποδομών, αναπτύχθηκε μια πρακτική που επέτρεπε σε πολλούς χρήστες να μοιράζονται, μέσω πολλαπλών τερματικών, την υπολογιστική ισχύ και τον χώρο. Αυτό είχε ως αποτέλεσμα οι περίοδοι αδράνειας των συστημάτων να εξαλειφθούν και η απόδοση της επένδυσης να αυξηθεί. Η πρακτική αυτή ονομάστηκε χρονο-μοιρασμός.

Από το 1960 έως και 1990 λόγω των μεγάλων επενδύσεων που γίνανε για πολύ ισχυρά υπολογιστικά συστήματα, πολλές εταιρείες και οργανισμοί διαφημίζανε τον χρονομοιρασμό ως μια κερδοφόρα επένδυση. Αυτό αποτέλεσε την φυσική εξέλιξη των τερματικών της δεκαετίας του '50 μιας και πλέον μπορούσαν να ζήσουν ξεχωριστά υπολογιστικά περιβάλλοντα σε ένα φυσικό περιβάλλον. Οι κύριες δυνατότητες των εικονικών μηχανημάτων ήταν να τρέχουν δικό τους

λειτουργικό σύστημα, να έχουν δικιά τους μνήμη, CPU, σκληρό δίσκο και συσκευές ανάγνωσης για CD-ROM. Η "Εικονοποίηση" ήταν ο καταλύτης για επαναστατικές εξελίξεις στους τομείς της πληροφορικής και των επικοινωνιών.

Το 1990 έως και το 2000 οι εταιρείες τηλεπικοινωνιών που μέχρι εκείνη την περίοδο προσέφεραν δίκτυα δεδομένων από σημείο σε σημείο, ξεκίνησαν να προσφέρουν εικονικά ιδιωτικά δίκτυα με συγκρίσιμη ποιότητα αλλά και χαμηλότερο κόστος. Ρυθμίζοντας επίσης την κυκλοφορία δεδομένων κατάφεραν να εξισορροπούν τον φόρτο των εξυπηρετητών με αποτέλεσμα το δίκτυο να αξιοποιείται αποδοτικότερα και με τη δυνατότητα της μέγιστης αξιοποίησής του.

Καθώς οι υπολογιστές σιγά-σιγά επικρατούσαν, οι επιστήμονες και οι τεχνολόγοι έψαχναν τρόπους για να καταστήσουν διαθέσιμους, ολοένα και σε μεγαλύτερο κοινό την υπολογιστική ισχύ μεγάλης κλίμακας μέσω χρονο-μοιρασμο, για το λόγο αυτό πειραματίζονταν με αλγορίθμους για την βέλτιστη χρήση της υποδομής της πλατφόρμας και των εφαρμογών.

Από το 2000 μέχρι και σήμερα είναι η πιο επαναστατική περίοδος όσον αφορά τις εξελίξεις στον τομέα του **Cloud computing**.

Το 2004 ιδρύθηκε η εταιρεία **Facebook Ireland Ltd** , η οποία παρείχε τέτοιου είδους υπηρεσίες μέσω του ιστοτόπου **«facebook.com»** όπου κατάφερε και μετέτρεψε την υπηρεσία **Cloud** σε κάτι προσωπικό και δωρεάν.

Το 2007 η **Salesforce.com** ξεκίνησε το «**force.com»** που είναι μια πλατφόρμα ως υπηρεσία (Platform-as-a-service, PaaS), με στόχο να δώσει στους πελάτες της τα απαραίτητα εργαλεία για να κατασκευάσουν, να αποθηκεύσουν και να εκτελέσουν όλες τις εφαρμογές και τις ιστοσελίδες που χρειαζόντουσαν.

Το 2009 η **Google** διέθεσε την υπηρεσία **Google Apps** η οποία επιτρέπει την δημιουργία και τον διαμοιρασμό εγγράφων στο **Cloud**.

Έτσι λοιπόν, καταλήγουμε με βεβαιότητα στο ότι, το **Cloud computing** δεν είναι μια νέα έννοια.

1.3 Βασικά χαρακτηριστικά.

Το μοντέλο του **Cloud** προάγει τη διαθεσιμότητα και απαρτίζεται από πέντε βασικά χαρακτηριστικά, τρία μοντέλα παροχής-παράδοσης της υπηρεσίας και τέσσερα μοντέλα υλοποίησης του.

Τα βασικά χαρακτηριστικά του cloud computing είναι τα εξής:

• **On-demand self-service:** Ένας καταναλωτής μπορεί να δεσμεύσει από μόνος του, όλους τους υπολογιστικούς πόρους που χρειάζεται, όπως χρόνο στον server ή αποθηκευτικό χώρο στο δίκτυο, ανάλογα με τις ανάγκες του, αυτόματα και χωρίς να απαιτείται ανθρώπινη αλληλεπίδραση με το φορέα παροχής κάθε υπηρεσίας.

• **Broad network access (Ευρεία πρόσβαση στο δίκτυο):** Οι δυνατότητες είναι διαθέσιμες μέσω του δικτύου και προσβάσιμες μέσω τυποποιημένων μηχανισμών που προωθούν την χρήση από ετερογενείς πλατφόρμες (π.χ. κινητά τηλέφωνα, φορητούς υπολογιστές).

• **Resource pooling (Κοινή διάθεση των πόρων):** Οι υπολογιστικοί πόροι του παρόχου χρησιμοποιούνται για να εξυπηρετήσουν πολλαπλούς καταναλωτές με τη χρήση μοντέλου πολλαπλών μισθωτών (multi-tenant), με τους διάφορους φυσικούς και εικονικούς πόρους να ανατίθενται δυναμικά, ανάλογα με τη ζήτηση των καταναλωτών.

Υπάρχει μια αίσθηση ανεξαρτησίας από τον τόπο στο γεγονός ότι ο πελάτης δεν έχει γενικά κανέναν έλεγχο ή γνώση σχετικά με την ακριβή τοποθεσία των παρεχόμενων πόρων, αλλά μπορεί να είναι σε θέση να προσδιορίζει την τοποθεσία σε ένα υψηλότερο επίπεδο αφαίρεσης (π.χ. χώρα, κράτος, ή datacenter). Παραδείγματα πόρων αποτελούν οι αποθηκευτικοί χώροι, η επεξεργασία, η μνήμη, το bandwidth του δικτύου, καθώς και οι εικονικές μηχανές.

• **Rapid elasticity (Ταχεία ελαστικότητα):** Οι πόροι μπορούν να δεσμευτούν προς χρήση γρήγορα και ελαστικά, σε ορισμένες περιπτώσεις αυτόματα, έτσι ώστε να εμφανιστούν άμεσα ως μη διαθέσιμοι (scale out) και επίσης να αποδεσμευτούν γρήγορα για να εμφανιστούν ξανά ως διαθέσιμοι (scale in). Για τον καταναλωτή, οι διαθέσιμες δυνατότητες για δέσμευση και χρήση συχνά φαίνεται να είναι απεριόριστες και μπορούν να αγοραστούν ανά πάσα στιγμή και σε οποιαδήποτε ποσότητα.

• **Measured Service (Μετρήσιμα επίπεδα παροχής υπηρεσιών):** Τα συστήματα cloud ελέγχουν και βελτιστοποιούν αυτόματα τη χρήση των πόρων, αξιοποιώντας μια δυνατότητα μέτρησης σε κάποιο επίπεδο αφαίρεσης που είναι κατάλληλο για το είδος της υπηρεσίας (π.χ. αποθήκευση, επεξεργασία, bandwidth, ενεργοί λογαριασμοί χρηστών). Η χρήση των πόρων μπορεί να παρακολουθείται, να ελέγχεται, και να παρουσιάζεται με τη μορφή reports, παρέχοντας διαφάνεια τόσο για τον πάροχο όσο και για τον καταναλωτή της χρησιμοποιούμενης υπηρεσίας.

1.4 Μοντέλα Παροχής Υπηρεσιών cloud computing.

Οι υπηρεσίες του «υπολογιστικού νέφους» διακρίνονται σε τρείς μεγάλες κατηγορίες:

α)Στο λογισμικό ως υπηρεσία IaaS (Infrastructure as a Service):
Στο μοντέλο αυτό οι εφαρμογές φιλοξενούνται σ' ένα απομακρυσμένο κέντρο εφαρμογών ή υπηρεσιών και είναι διαθέσιμες στους πελάτες όποτε αυτοί τις χρειαστούν. Εν προκειμένω, οι χρήστες έχουν τη

δυνατότητα να επεξεργάζονται τη διάταξη, την αποθήκευση, τα δίκτυα και άλλους βασικούς υπολογιστικούς πόρους.

Στο IaaS οι χρήστες μπορούν να αναπτύξουν αυθαίρετο λογισμικό, όπως λειτουργικά συστήματα και εφαρμογές. Μπορεί μεν και πάλι να μην υπάρχει η δυνατότητα ελέγχου της υποδομής του Cloud από τους χρήστες, αλλά οι τελευταίοι μπορούν να αλλάζουν και να παραμετροποιούν το λογισμικό περιορισμένο έλεγχο βασικών παραμέτρων δικτύων (π.χ. firewalls).

Το πλεονέκτημα πού έχει το συγκεκριμένο μοντέλο είναι η λειτουργική αποδοτικότητα και τα μειωμένα κόστη.

Ως μειονέκτημα του ως άνω μοντέλου, και ο λόγος που πολλές επιχειρήσεις το αποφεύγουν είναι το γεγονός πως αντιμετωπίζουν προβλήματα με το συγκεκριμένο τύπο μοντέλου διότι δεν γνωρίζουν πώς αποθηκεύονται τα δεδομένα τους.

β) Στην Πλατφόρμα ως υπηρεσία PaaS (Platform as a Service) : Ο τύπος αυτός βρίσκεται ένα επίπεδο πάνω από τον προηγούμενο. Έτσι λοιπόν εδώ προσφέρονται ολοκληρωμένες υπηρεσίες στους προγραμματιστές δηλαδή, οι χρήστες έχουν τη δυνατότητα να αναπτύξουν δικό τους λογισμικό πάνω στην υποδομή του Cloud με τη χρήση γλωσσών προγραμματισμού, βιβλιοθηκών και εργαλείων που υποστηρίζει ο πάροχος. Σε αντίθεση με το SaaS, εδώ οι χρήστες μπορούν να διαχειρίζονται τις εφαρμογές τους και να παραμετροποιούν το περιβάλλον στο οποίο αυτές βρίσκονται. Το μοντέλο αυτό μειονεκτεί διότι, όλα αυτά που θεωρούνται ως πλεονεκτήματα μπορούν την ίδια στιγμή να προκαλέσουν μεγάλη ζημία εάν βρεθούν στα χέρια κάποιου κακόβουλου ατόμου που σκοπεύει να πλήξει και να επεξεργαστεί τα δεδομένα, καθώς το μοντέλο προσφέρεται για την ανάπτυξη κακόβουλου λογισμικού.

γ) Στην Υποδομή ως υπηρεσία SaaS (Software as a Service):

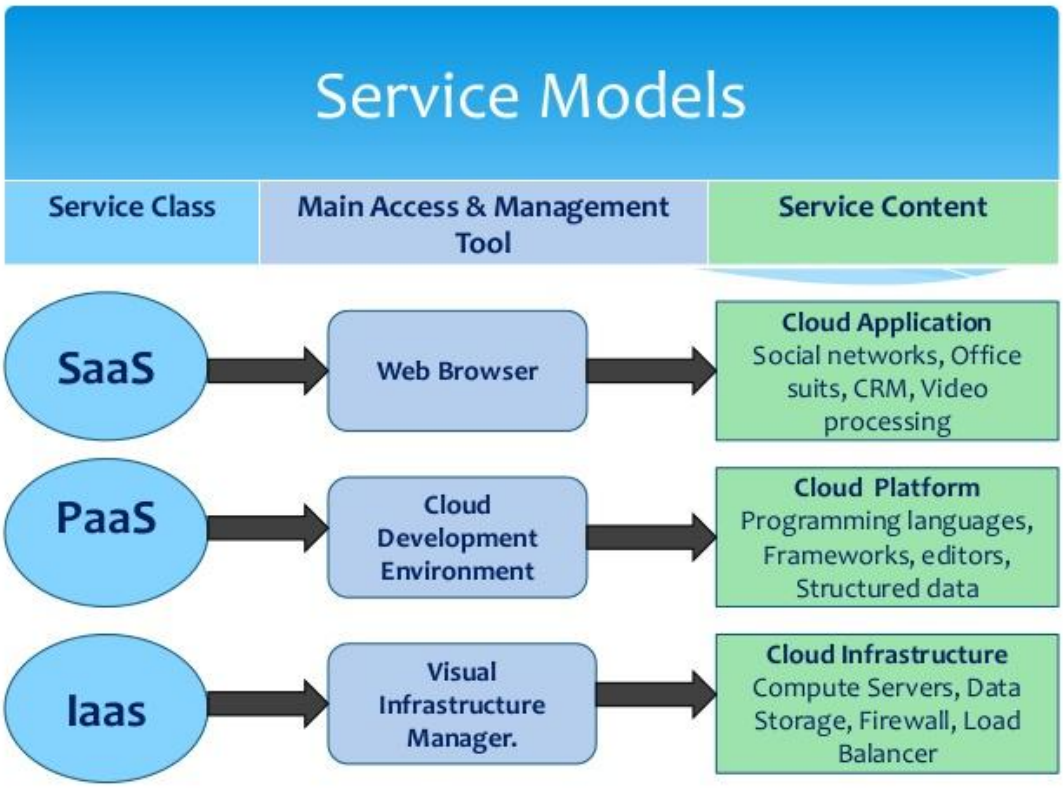
Στη μορφή αυτή οι καταναλωτές, που συνήθως είναι μεγάλες επιχειρήσεις, έχουν τη δυνατότητα να χρησιμοποιούν υπολογιστικούς πόρους όπως η ισχύς επεξεργασίας, της αποθήκευσης και των δικτύων, για να αναπτύξουν και να εκτελέσουν λογισμικό, το οποίο θα περιλαμβάνει λειτουργικά συστήματα και εφαρμογές (π.χ Amazon EC2 and S3, Terremark Enterprise Cloud, Windows Live).

Οι καταναλωτές αυτής της υπηρεσίας δεν διαχειρίζονται και δεν ελέγχουν τη σχετική υποδομή cloud, αλλά έχουν τον έλεγχο των

λειτουργικών συστημάτων, της αποθήκευσης, των αναπτυγμένων εφαρμογών, και ενδεχομένως έχουν περιορισμένο έλεγχο σε επιλεγμένα στοιχεία του δικτύου (π.χ. firewalls υποδοχής). Τέλος οι καταναλωτές έχουν την τελική ευθύνη για την ασφάλεια των πληροφοριών που αποθηκεύουν.

Στο συγκεκριμένο μοντέλο, οι χρήστες έχουν τη δυνατότητα να χρησιμοποιούν εφαρμογές που διατίθενται στο Cloud από τους παρόχους. Οι εφαρμογές αυτές είναι προσβάσιμες μέσα από διεπαφές προγραμμάτων ή με τη βοήθεια διεπαφών web browser. Οι χρήστες δεν έχουν το δικαίωμα να ελέγχουν την υποδομή του Cloud ή να αλλάζουν την παραμετροποίηση των παρεχόμενων εφαρμογών.

Το μοντέλο αυτό διακρίνεται για την ταχύτητα και την ευελιξία του έναντι των άλλων καθώς επίσης και για τις δυνατότητές του, ενώ αντίστοιχα δεν παρουσιάζει αξιόλογα μειονεκτήματα.



1.5 Μοντέλα ανάπτυξης cloud computing

Το «υπολογιστικό νέφος διακρίνεται σε 4 μοντέλα ανάπτυξης:

1. Το δημόσιο νέφος (public cloud)

Στο νέφος αυτό μπορεί κάποιος να μισθώσει υπολογιστική και αποθηκευτική χωρητικότητα σε συστήματα τα οποία βρίσκονται στο Διαδίκτυο και τα διαχειρίζονται οι πάροχοι. Ο πάροχος επιτρέπει στους καταναλωτές να έχουν, υπό τον έλεγχό του, τους πόρους που έχουν ζητηθεί. Το μοντέλο αυτό προσφέρει υπηρεσίες με πληρωμή ανά χρήση, δηλαδή ο εκάστοτε πελάτης που χρησιμοποιεί τις υπηρεσίες χρεώνεται για όσο τις χρησιμοποιεί. Είναι το πιο διαδεδομένο μοντέλο cloud καθώς χαρακτηρίζεται από μειωμένα κόστη. Το βασικότερο μειονέκτημα του είναι η έλλειψη εμπιστοσύνης μεταξύ παρόχου και πελατών, με πολλά προβλήματα σε θέματα ασφαλείας.

2. Το ιδιωτικό νέφος (Private Cloud):

Στην περίπτωση αυτή κάνουμε λόγο για ένα κέντρο δεδομένων, σε αντίθεση με το προηγούμενο μοντέλο, εδώ υπάρχει ο πάροχος υπηρεσιών είναι υπεύθυνος τόσο για την υποδομή όσο και για τη λειτουργία. Με τον τρόπο αυτό ο τύπος του μοντέλου αυτού προσφέρει μεγαλύτερη εμπιστοσύνη μεταξύ των συνεργαζόμενων οντοτήτων. Όλο αυτό συμβαίνει γιατί οι επιχειρήσεις που χρησιμοποιούν υπηρεσίες ιδιωτικού νέφους είναι σε θέση να επιλέξουν οι ίδιες τις πολιτικές που θα εφαρμοσθούν, τόσο σε θέματα που αφορούν την ασφάλεια όσο και την προστασία της ιδιωτικότητας.

Το νέφος αυτό, είναι πιο δαπανηρό σε σχέση με το δημόσιο νέφος.

3.Το νέφος κοινότητας (community cloud)

Το κοινοτικό νέφος χρησιμοποιείται από μια συγκεκριμένη κοινότητα χρηστών οι οποίοι έχουν κοινά ενδιαφέροντα και απαιτήσεις. Έτσι, με τον τρόπο αυτό το μοντέλο, στοχεύει τόσο στη μείωση των ελλείψεων μεμονωμένων τεχνολογιών, όσο και στη μείωση του κόστους διοίκησης. Θεωρείται έμπιστο σε σχέση με το δημόσιο νέφος καθώς επίσης και πιο οικονομικό από το ιδιωτικό νέφος. Ένα επιπλέον πλεονέκτημα του είναι ότι παρέχει την δυνατότητα στους χρήστες του να ελέγχουν τους κοινούς πόρους υποδομής που χρησιμοποιούν. Το μειονέκτημα του είναι η δυσκολία που υπάρχει μεταξύ των χρηστών να συμμορφωθούν και να ακολουθήσουν τους κανονισμούς.

3. Το υβριδικό νέφος(hybrid cloud):

Είναι ένας τύπος cloud που κυμαίνεται μεταξύ του δημόσιου και του ιδιωτικού νέφους. Πιο συγκεκριμένα και όσων αναφορά το κόστος, είναι φθηνότερο από το ιδιωτικό. Επιπλέον τα δεδομένα άλλοτε αποθηκεύονται στο ιδιωτικό νέφος και άλλοτε στο δημόσιο. Δε δημιουργείται πρόβλημα εμπιστοσύνης στην ασφάλεια των δεδομένων προσωπικού χαρακτήρα καθώς γίνεται ένας διαχωρισμός ανάμεσα στα σημαντικά και απόρρητα δεδομένα τα οποία και αποθηκεύονται στο ιδιωτικό νέφος, και σε εκείνα που κρίνονται ως δευτερεύοντα και λιγότερο σημαντικά και αποθηκεύονται στο δημόσιο νέφος. Με τον τρόπο αυτό υπάρχει ασφάλεια στα κρίσιμα δεδομένα αλλά και μείωση του κόστους. Ένα μοντέλο Hybrid Cloud μπορεί να προσφέρει στους χρήστες του τα ακόλουθα:

Επεκτασιμότητα: Ενώ τα private clouds προσφέρουν ένα ορισμένο επίπεδο κλιμάκωσης , ανάλογα με τις ρυθμίσεις τους (είτε φιλοξενούνται εσωτερικά ή εξωτερικά , για παράδειγμα), τα public clouds προσφέρουν επεκτασιμότητα με λιγότερα όρια, διότι οι πόροι αποσπώνται από τη μεγαλύτερη υποδομή cloud.

Εξοικονόμηση κόστους: Τα public clouds είναι πιθανό να προσφέρουν πιο σημαντικές οικονομίες κλίμακας (όπως η κεντρική διαχείριση), και έτσι μεγαλύτερη αποδοτικότητα του κόστους από τα private clouds. Ως εκ τούτου, τα υβριδικά σύννεφα επιτρέπουν στους οργανισμούς να έχουν πρόσβαση σε αυτές τις εξοικονομήσεις για όσες το δυνατόν

περισσότερες επιχειρηματικές λειτουργίες, διατηρώντας παράλληλα ασφαλείς τις όλες τις ευαίσθητες επιχειρήσεις.

Ασφάλεια: Το private cloud ως στοιχείο του hybrid cloud δεν παρέχει μόνο την ασφάλεια , όπου αυτό είναι αναγκαίο για τις ευαίσθητες λειτουργίες, αλλά μπορεί επίσης να εκπληρώσει τις κανονιστικές απαιτήσεις για το χειρισμό και την αποθήκευση όταν μπορεί να εφαρμοστεί.

Ευελιξία: Η διαθεσιμότητα των πόρων μπορεί να παρέχει στους οργανισμούς περισσότερες ευκαιρίες για να εξερευνήσουν διάφορες επιχειρησιακές κατευθύνσεις.

ΣΥΜΠΕΡΑΣΜΑ

Όπως αναλύσαμε και παραπάνω ,το **Cloud computing** είναι μια σχετικά νέα τεχνολογία που μπορεί να αποφέρει μεγάλα οικονομικά οφέλη δεδομένου ότι η διαμόρφωση και η επέκταση των, κατά παραγγελία, πόρων στο διαδίκτυο είναι πιο εύκολες διαδικασίες. Εκτός από οικονομικά οφέλη δύναται να έχει και αρκετά οφέλη σε επίπεδο ασφαλείας καθώς οι επιχειρήσεις μπορούν να αποκτήσουν κορυφαίες τεχνολογίες, με σχετικά χαμηλό κόστος, τις οποίες σε άλλη περίπτωση δεν θα μπορούσαν να αγοράσουν.

Στο κεφάλαιο που ακολουθεί θα μελετηθεί το νομοθετικό πλαίσιο που διέπει το Cloud computing και ο τρόπος αποθήκευσης τους προκειμένου να διασφαλιστεί η ακεραιότητα των προσωπικών δεδομένων.

ΝΟΜΙΚΑ ΘΕΜΑΤΑ ΣΤΟ CLOUD COMPUTING.

Κεφάλαιο 2:

2.1 ΙΔΙΩΤΙΚΟΤΗΤΑ ΚΑΙ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ ΣΤΟ CLOUD

2.1.1 Τι είναι ιδιωτικότητα

Η έννοια της ιδιωτικότητας ποικίλλει ανάλογα με το πολιτισμικό, εθνολογικό, εθιμικό και ηθικό υπόβαθρο. Η αντίληψη για την έννοια της ιδιωτικότητας διαμορφώνεται τόσο από τις δημόσιες προσδοκίες όσο και από το νομικό περιβάλλον της εκάστοτε χώρας του χρήστη, με αποτέλεσμα να μην είναι εφικτός ένας παγκόσμια αποδεκτός ορισμός της ιδιωτικότητας. Η έννοια της ιδιωτικότητας όμως δεν είναι ανεξάρτητη από αυτή των προσωπικών δεδομένων.

2.1.2 Τι είναι προσωπικά δεδομένα.

Με τον όρο προσωπικά δεδομένα νοείται κάθε πληροφορία που αναφέρεται στο πρόσωπο του ατόμου, όπως: το όνομα και το επάγγελμά του, η οικογενειακή του κατάσταση, η ηλικία του, ο τόπος κατοικίας, η φυλετική του προέλευση, τα πολιτικά του φρονήματα, η θρησκεία που πιστεύει, οι φιλοσοφικές του απόψεις, η συνδικαλιστική του δράση, η υγεία του, η ερωτική του ζωή και οι τυχόν ποινικές του διώξεις και καταδίκες.

Δεν θεωρούνται προσωπικά δεδομένα πληροφορίες από τις οποίες δεν δυνάται να ταυτοποιηθεί ένα συγκεκριμένο άτομο.

2.1.3 Ιδιωτικότητα και προσωπικά δεδομένα του Χρήστη στο Cloud.

Προσωπικά δεδομένα και ιδιωτικότητα είναι δύο έννοιες απόλυτα συνυφασμένες μεταξύ τους. Αμφότερες περιγράφουν την δυνατότητα του ατόμου να περιηγείται σε ένα δίκτυο χωρίς να εκθέτει σε άλλους χρήστες στοιχεία από την προσωπική του ζωή. Με σκοπό την προστασία των χρηστών στο διαδίκτυο θα μπορούσαμε να πούμε ότι έχουν γραφτεί εκατοντάδες άρθρα με συμβουλές σωστής χρήσης και ενέργειες για μια ασφαλή πλοήγηση.

Παρατηρούμε ωστόσο πολλές φορές πως δεν είναι δυνατή η ενημέρωση των χρηστών, και πως τα λάθη των χρηστών στο διαδίκτυο διαδέχονται το ένα το άλλο.

Η προστασία των προσωπικών δεδομένων αναφέρεται στα δικαιώματα ή τις υποχρεώσεις που σχετίζονται με τη συλλογή, την επεξεργασία, την κοινολόγηση, την αποθήκευση και την καταστροφή των προσωπικών δεδομένων.

Η ιδιωτικότητα αναφέρεται στα δικαιώματα που σχετίζονται με την διασφάλιση της απόκρυψης πληροφοριών των χρηστών στο δίκτυο.

Ουσιαστικά, όταν μιλάμε για την διασφάλιση του απορρήτου των επικοινωνιών και την προστασία προσωπικών δεδομένων στο cloud εννοούμε την υπευθυνότητα των οργανισμών απέναντι στους τελικούς χρήστες καθώς και το βαθμό διαφάνεια που χαρακτηρίζει την πολιτική των οργανισμών σε σχέση με την διαχείριση των δεδομένων προσωπικού χαρακτήρα.

2.1.4 Προβληματισμοί σχετικά με την ιδιωτικότητα στο cloud.

Από πολλούς ειδικούς, υπάρχουν διαφορά ερωτήματα σχετικά με την προστασία των προσωπικών δεδομένων, όταν αυτά εκτίθενται σε περιβάλλοντα cloud. Οι προβληματισμοί αυτοί πηγάζουν από των

συνδυασμό θεμάτων ασφάλειας των πληροφοριακών συστημάτων και της ιδιωτικότητας.

- Για την Ελληνική Δημοκρατία και με σκοπό στην πρόσβαση στο υποκείμενο των δεδομένων, υπάρχει αναφαίρετο δικαίωμα του χρήστη να γνωρίζει ποιες προσωπικές πληροφορίες κατακρατηθήκαν και σε ορισμένες περιπτώσεις μπορεί να ζητήσει την διακοπή της περαιτέρω επεξεργασίας των δεδομένων του, βάσει του Ν. 2472/97 όπως αυτός τροποποιήθηκε με τον Ν 3471/2006, και αναφέρεται στα προσωπικά δεδομένα.

Αυτό όμως, παρουσιάζει δυσκολίες ως προς την εφαρμογή του σε ένα τέτοιο πολύπλοκο σύστημα όπως είναι το περιβάλλον Cloud, γενάτε λοιπόν η ανησυχία σχετικά με την ικανότητα του εκάστοτε οργανισμού και την δυνατότητα του να παρέχει όλες τις απαραίτητες πληροφορίες στο υποκείμενο της, και στην τελική συμμόρφωση του οργανισμού με τις νομικές του δεσμεύσεις.

Εάν ένας ενδιαφερόμενος εξασκήσει το δικαίωμά του, να ζητήσει δηλαδη από τον Οργανισμό να καταστραφούν τα προσωπικά του στοιχεία, πως μπορεί αυτός να εξασφαλίσει ότι όλες οι πληροφορίες του υποκειμένου σχετικά με αυτόν, θα διαγραφουν και στο Cloud;

Έτσι λοιπόν μας προβληματίζουν τα εξής ερωτήματα :

·Ποιες είναι οι απαιτήσεις συμμόρφωσης αναφορικά με ιδιωτικό απορρήτου σε περιβάλλον cloud;

·Ποιά είναι η ισχύουσα νομοθεσία, οι κανονισμοί;

· Ποιος είναι υπεύθυνος για τη τήρηση και την εφαρμογή των νομικών και άλλων δεσμεύσεων;

·Πώς η υφιστάμενη δομή εξασφαλίζει την τήρηση του απορρήτου; Επηρεάζεται από τη μετάβαση σε περιβάλλον Cloud;

·Πώς ενσωματώνεται στην πολιτική των εταιριών, το γεγονός ότι οι υποδομές cloud είναι αντικείμενα πολλών και κάποιες φορές αντικρουόμενων, εθνικών και υπερεθνικών ρυθμίσεων, δεδομένης μάλιστα και της γεωγραφικής διασποράς τους σε διαφορετικές χώρες;

(Π.Χ) Ποιο δικαστήριο είναι αρμόδιο και ποια νομοθεσία θα πρέπει να εφαρμοστεί στην περίπτωση που τα δεδομένα χρησιμοποιούνται στην Ελλάδα αλλά αποθηκεύονται στις ΗΠΑ;

2.2 Επεξεργασία Προσωπικών Δεδομένων.

Με τον όρο επεξεργασία προσωπικών δεδομένων σύμφωνα με τον νόμο εννοούμε μια σειρά ενεργειών που πραγματοποιείται από δημόσιο ή νομικό πρόσωπο δημοσίου ή ιδιωτικού δικαίου, με ή χωρίς, τη βοήθεια αυτοματοποιημένων μεθόδων που εφαρμόζονται σε προσωπικά δεδομένα. Πιο απλά οι ενέργειες αυτές μπορεί να είναι η συλλογή, η καταχώριση, η διατήρηση, η αποθήκευση, η τροποποίηση, η διαγραφή ή η καταστροφή των δεδομένων προσωπικού χαρακτήρα.

Ο Ν. 2472/1997 στο άρθρο 2 στην παρ δ' θέτει όρια στον τρόπο της επεξεργασίας, κρίνει δηλαδή πότε, είτε σε έντυπη είτε σε ηλεκτρονική μορφή, θεωρείται νόμιμη η επεξεργασία. Στον ίδιο νόμο παρατηρούμε, ότι γίνεται σαφής αναφορά στους αρμόδιους της επεξεργασίας οι οποίοι είναι, ο υπεύθυνος επεξεργασίας και ο εκτελών επεξεργασίας.

2.3 Υπεύθυνος Επεξεργασίας

Σύμφωνα με την νομοθετική οδηγία 95/46 ΕΚ ως υπεύθυνος επεξεργασίας ορίζεται το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή , η υπηρεσία ή οποιοσδήποτε άλλος φορέας, ο οποίος από μόνος ή από κοινού με άλλους καθορίζει τους στόχους και τον τρόπο επεξεργασίας των προσωπικών δεδομένων.

Ο υπεύθυνος επεξεργασίας στην περίπτωση του Cloud computing, δηλαδή ο πελάτης, πρέπει να συμμορφώνεται με τη νομοθεσία για την προστασία προσωπικών δεδομένων και είναι υπεύθυνος για όλες τις νομικές υποχρεώσεις που αναγράφονται στην οδηγία. Πιο αναλυτικά ένας υπεύθυνος επεξεργασίας όταν καλείται να επεξεργαστεί

προσωπικά δεδομένα θα πρέπει να ενημερώσει το υποκείμενο των προσωπικών δεδομένων για την επεξεργασία, να λάβει την συγκατάθεση του και να τηρεί τα μέτρα ασφαλείας κατά την επεξεργασία τους.

2.4 Εκτελών επεξεργασίας

Εκτελών επεξεργασίας θεωρείται (όταν ο πάροχος του cloud παρέχει τα μέσα και την πλατφόρμα, ενεργώντας εξ ονόματος του πελάτη), το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή η υπηρεσία ή οποιοσδήποτε άλλος φορέας επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπεύθυνου επεξεργασίας. Η σχέση μεταξύ του υπεύθυνου επεξεργασίας και του εκτελών είναι συνήθως σχέση σύμβασης έργου.

Οι πάροχοι υπηρεσιών cloud (είτε υπεύθυνοι είτε εκτελούντες) έχουν καθήκον κάθε φορά να διασφαλίζουν το απόρρητο. Σύμφωνα με την νομοθετική οδηγία 95/46/ΕΚ κάθε πρόσωπο που ενεργεί υπό την εποπτεία του υπεύθυνου επεξεργασίας ή του εκτελών συμπεριλαμβανομένου και του ίδιου του εκτελούντα επεξεργασία και έχει πρόσβαση σε δεδομένα προσωπικού χαρακτήρα, μπορεί να τα επεξεργασθεί μόνο κατόπιν εντολής του υπεύθυνου επεξεργασίας, εκτός της περιπτώσεως που υποχρεούται προς τούτο για τα κατά νόμο.

Ένα ακόμη σημείο που πρέπει να προσέχει ο εκτελών επεξεργασίας είναι να λαμβάνει υπ’ όψιν του τον τύπο του cloud (Iaas,Paas,Saas) καθώς επίσης και τα μοντέλα ανάπτυξης(ιδιωτικό, δημόσιο, κοινοτικό, υβριδικό).

2.5 Διασυνοριακή Ροη Δεδομένων

Ένα μεγάλο θέμα που τίθεται σε συστήματα cloud είναι η διασυνοριακή ροή των δεδομένων, δηλαδή η διακίνηση τους. Αυτό το πρόβλημα είναι σύνηθες καθώς σε τέτοια συστήματα πολλές φορές ο πελάτης δεν γνωρίζει που βρίσκεται το νέφος που χρησιμοποιεί.

Για την διασυνοριακή ροή δεδομένων, υπάρχουν δύο περιπτώσεις : Η διακίνηση των δεδομένων εντός της Ε,Ε και η διακίνηση τους εκτός ΕΕ. Σύμφωνα λοιπόν με το νόμο 2472/1997 άρθρο 9 παράγραφος 1 περ α' η διακίνηση των δεδομένων εντός της Ε.Ε με σκοπό την επεξεργασία τους είναι ελεύθερη και δεν προϋποθέτει καμία περεταίρω διαδικασία. Με απλά λόγια η μεταβίβαση των δεδομένων προσωπικού χαρακτήρα μπορεί να γίνει ελεύθερα από και προς οποιοδήποτε κράτος – μέλος της Ε.Ε. Στο σημείο αυτό να τονισθεί ότι αρκετές φορές χρήζει αναγκαία η δικαστική συνδρομή.

Αντίθετα , δηλαδή στην περίπτωση εκείνη που η χώρα διαβίβασης των προσωπικών δεδομένων δεν είναι μέλος της Ε.Ε είναι απαραίτητη η έκδοση άδειας από την Αρχή η οποία επιτρέπει τη μεταβίβαση αυτή. Η εν λόγω άδεια χορηγείται μόνο εάν η χώρα στην οποία θα μεταφερθούν τα προσωπικά δεδομένα είναι σε θέση να παρέχει ένα ικανοποιητικό επίπεδο ασφαλείας στα δεδομένα αυτά. Ο έλεγχος του επιπέδου των χωρών γίνεται από την Αρχή προστασίας προσωπικών δεδομένων.

Σύμφωνα με την ομάδα εργασίας του άρθρου 29 της οδηγίας 95/46/ΕΚ η διαδικασία της επεξεργασίας των προσωπικών δεδομένων στην τεχνολογία cloud computing εγκυμονεί κινδύνους. Αναφέρει λοιπόν, ότι οι κίνδυνοι αυτοί διακρίνονται σε δύο κατηγορίες. Στην πρώτη κατηγορία είναι η έλλειψη διαφάνειας και πιο αναλυτικά η έλλειψη ελέγχου των δεδομένων και η ελλιπής ενημέρωση σχετικά με την ίδια την επεξεργασία.

Έλλειψη ελέγχου: Οι πελάτες υπηρεσιών cloud computing ενδέχεται να χάνουν τον αποκλειστικό έλεγχο των συγκεκριμένων δεδομένων και να μην μπορούν πια να εφαρμόζουν τα τεχνικά και οργανωτικά μέτρα που απαιτούνται για τη διασφάλιση ακεραιότητας, απορρήτου, διαφάνειας, απομόνωσης, δυνατότητας παρέμβασης και φορητότητας των δεδομένων.

2.6 Το πλαίσιο προστασίας των δεδομένων

Το συναφές νομικό πλαίσιο είναι η οδηγία 95/46/ ΕΚ για την προστασία των δεδομένων , η οποία ισχύει σε κάθε περίπτωση στην οποία γίνεται επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τη χρήση υπηρεσιών cloud .
Η οδηγία 2002/58/ ΕΚ για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες (οπως αναθεωρήθηκε με την οδηγία 2009/136/ ΕΚ) ισχύει σε περιπτώσεις επεξεργασίας δεδομένων προσωπικού χαρακτήρα που σχετίζονται με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών σε δημόσια δίκτυα επικοινωνιών (φορείς εκμετάλλευσης τηλεπικοινωνιών) και ,ως εκ τούτου , εφαρμόζεται όταν οι συναφείς υπηρεσίες παρέχονται μέσω υπολογιστικού νέφους.

2.7 Εφαρμοστέο Δίκαιο

Τα κριτήρια βάσει των οποίων προσδιορίζεται το εκάστοτε εφαρμοστέο δίκαιο παρατίθενται στο άρθρο 4 της οδηγίας 95/46/ ΕΚ , το οποίο αναφέρεται στη νομοθεσία που διέπει τους εγκατεστημένους σε ένα ή περισσότερα σημεία εντός του ΕΟΧ υπεύθυνους της επεξεργασίας , καθώς επίσης και στη νομοθεσία που διέπει τους εγκατεστημένους εκτός του ΕΟΧ υπεύθυνους της επεξεργασίας οι οποίοι όμως χρησιμοποιούν για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα μέσα εγκατεστημένα εντός του ΕΟΧ. Η ομάδα εργασίας του άρθρου 29 έχει εξετάσει το ζήτημα αυτό στη γνώμη 8/2010 που έχει εκδώσει για το εφαρμοστέο δίκαιο.
Στην πρώτη περίπτωση , το κριτήριο για την εφαρμογή ή όχι της νομοθεσίας της ΕΕ στον υπεύθυνο της επεξεργασίας είναι η τοποθεσία όπου είναι εγκατεστημένος και οι δραστηριότητες που επιτελεί , σύμφωνα με το άρθρο 4 παράγραφος 1 στοιχείο α της οδηγίας , ενώ κανέναν ρόλο δεν παίζει το μοντέλο παροχής υπηρεσιών cloud. Στην περίπτωση αυτή , εφαρμόζεται το δίκαιο της χώρας στην οποία είναι εγκατεστημένος ο υπεύθυνος της επεξεργασίας που έχει συνάψει σύμβαση για την παροχή υπηρεσιών cloud computing και όχι το δίκαιο της χώρας στην οποία είναι εγκατεστημένοι οι πάροχοι υπηρεσιών cloud computing. Εάν ο υπεύθυνος της επεξεργασίας είναι εγκατεστημένος στο έδαφος περισσότερων του ενός κρατών μελών και

προβαίνει σε επεξεργασία των δεδομένων στο πλαίσιο των δραστηριοτήτων του στις χώρες αυτές, τότε εφαρμόζεται το δίκαιο καθενός εκ των κρατών μελών στο οποίο λαμβάνει χώρα η εν λόγω επεξεργασία. Το άρθρο 4 παράγραφος 1 στοιχείο γ) αναφέρεται στον τρόπο εφαρμογής της νομοθεσίας περί προστασίας των δεδομένων στους υπεύθυνους της επεξεργασίας που δεν είναι μεν εγκατεστημένοι στον ΕΟΧ , αλλά χρησιμοποιούν μέσα , αυτοματοποιημένα ή όχι , ευρισκόμενα στο έδαφος κράτους μέλους , εκτός εάν τα μέσα αυτά χρησιμοποιούνται μόνο με σκοπό τη διέλευση .
Αυτό σημαίνει ότι εάν κάποιος πελάτης υπηρεσιών cloud computing είναι εγκατεστημένος εκτός του ΕΟΧ αλλά έχει προσλάβει πάροχο υπηρεσιών cloud computing εγκατεστημένο εντός του ΕΟΧ , η νομοθεσία περί προστασίας των δεδομένων που διέπει τον πάροχο επεκτείνεται και στον πελάτη.

2.8 Ποιός έχει την ευθύνη για την προστασία του απορρήτου

Υπάρχουν αντικρουόμενες απόψεις σχετικά με το ποιος φορέας είναι υπεύθυνος για την ασφάλεια και το ιδιωτικό απόρρητο. Ορισμένοι νομικοί και κάποιες επιστημονικές εργασίες αποδίδουν την ευθύνη στους παρόχους των υποδομών Cloud- αλλά παρόλο που νομικά είναι δυνατή η μεταβίβαση της αστικής ευθύνης μέσω συμβατικών συμφωνιών, είναι αδύνατη η μεταφορά της απαίτησης για λογοδοσία. Σε τελική ανάλυση, στα μάτια του κοινού και του φυσικού δικαστή, το βάρος για την ασφάλεια των δεδομένων και της ιδιωτικής ζωής εμπίπτει στις υποχρεώσεις της οργάνωσης που συλλέγει αρχικά τα δεδομένα. Τα ιστορικά στοιχεία δείχνουν ότι παραβιάσεις στην ιδιωτικότητα των προσωπικά δεδομένων έχουν ένα συνεχές αποτέλεσμα . Όταν μια οργάνωση χάνει τον έλεγχο των προσωπικών δεδομένων των χρηστών, οι χρήστες υφίσταστε (άμεσα ή έμμεσα) ζημίες, σε μεταγενέστερο χρόνο, ως αποτέλεσμα τις απώλειας. Αν κάτι τέτοιο συμβεί σε περιβάλλον Cloud, τότε οι ευθύνες θα αναζητηθούν από αυτόν που πήρε την απόφαση για την επιλογή του παρόχου του cloud και την μεταφορά των δεδομένων στο Cloud. Είναι ευθύνη του οργανισμού να λαμβάνει όλες της απαραίτητες μέριμνες για την διασφάλιση των δεδομένων των χρηστών. Ο υπεύθυνος για την επιτήρηση της κατάστασης των δεδομένων απαιτείτε να έχει κατάλληλο υπόβαθρο,

που να του επιτρέπει, την σε βάθος κατανόηση της τεχνολογίας που χρησιμοποιείται ως υποδομή για την ανάπτυξη και παροχή υπηρεσιών Cloud αλλά και να αντιλαμβάνεται τις νομικές δεσμεύσεις που αναλαμβάνει ο οργανισμός. Στην πραγματικότητα η αποτελεσματική διαχείριση των προσωπικών δεδομένων απαιτεί την ύπαρξη μια ομάδας νομικών και τεχνικών, με ειδίκευση στις ιδιαιτερότητες των δομών Cloud Computing.

2.9 Προστασία των δεδομένων

Το cloud computing δημιουργεί πολλούς κινδύνους στην προστασία των δεδομένων τόσο για τους πελάτες όσο και για τους παρόχους του cloud. Σε ορισμένες περιπτώσεις, μπορεί να είναι δύσκολο για έναν πελάτη του cloud(στο ρόλο του ως υπεύθυνος διαχείρισης των δεδομένων) να ελέγχει αποτελεσματικά τις πρακτικές διαχείρισης των δεδομένων που εφαρμόζει ο πάροχος του cloud και επομένως να μην είναι σίγουρος ότι τα δεδομένα διαχειρίζονται με τρόπο νόμιμο. Από την άλλη πλευρά, ορισμένοι πάροχοι cloud παρέχουν πληροφορίες σχετικά με τις πρακτικές επεξεργασίας των δεδομένων τους. Κάποιοι εξ' αυτων γνωστοποιούν τον τρόπο (πιστοποίηση) με τον οποίο εξασφαλίζεται η διαφύλαξη των δεδομένων τους, τις δραστηριότητες ασφάλειας και τους ελέγχους των δεδομένων.
Στην πραγματικότητα δεν μπορεί ποτέ ένας πάροχος να είναι 100% σίγουρος για την ασφάλεια των δεδομένων που διαχειρίζεται. Από την άλλη πλευρά ακόμη κι αν υπάρχουν στοιχεία παραβίασης της ασφάλειας αυτα πολλές φορές δεν κοινοποιούνται στον υπεύθυνο διαχείρισης. Ο πελάτης του cloud μπορεί να χάσει τον έλεγχο των δεδομένων του που υφίστανται επεξεργασία από τον πάροχο του cloud. Το πρόβλημα αυτό αυξάνεται σε περίπτωση που υπάρχει πολλαπλή μεταβίβαση δεδομένων (π.χ. μεταξύ συνενωμένων παρόχων cloud). Ο πάροχος του cloud (ο υπεύθυνος διαχείρισης δλδ) μπορεί να λαμβάνει δεδομένα που δεν έχουν νομίμως συλλεχθεί από τους πελάτες τους.

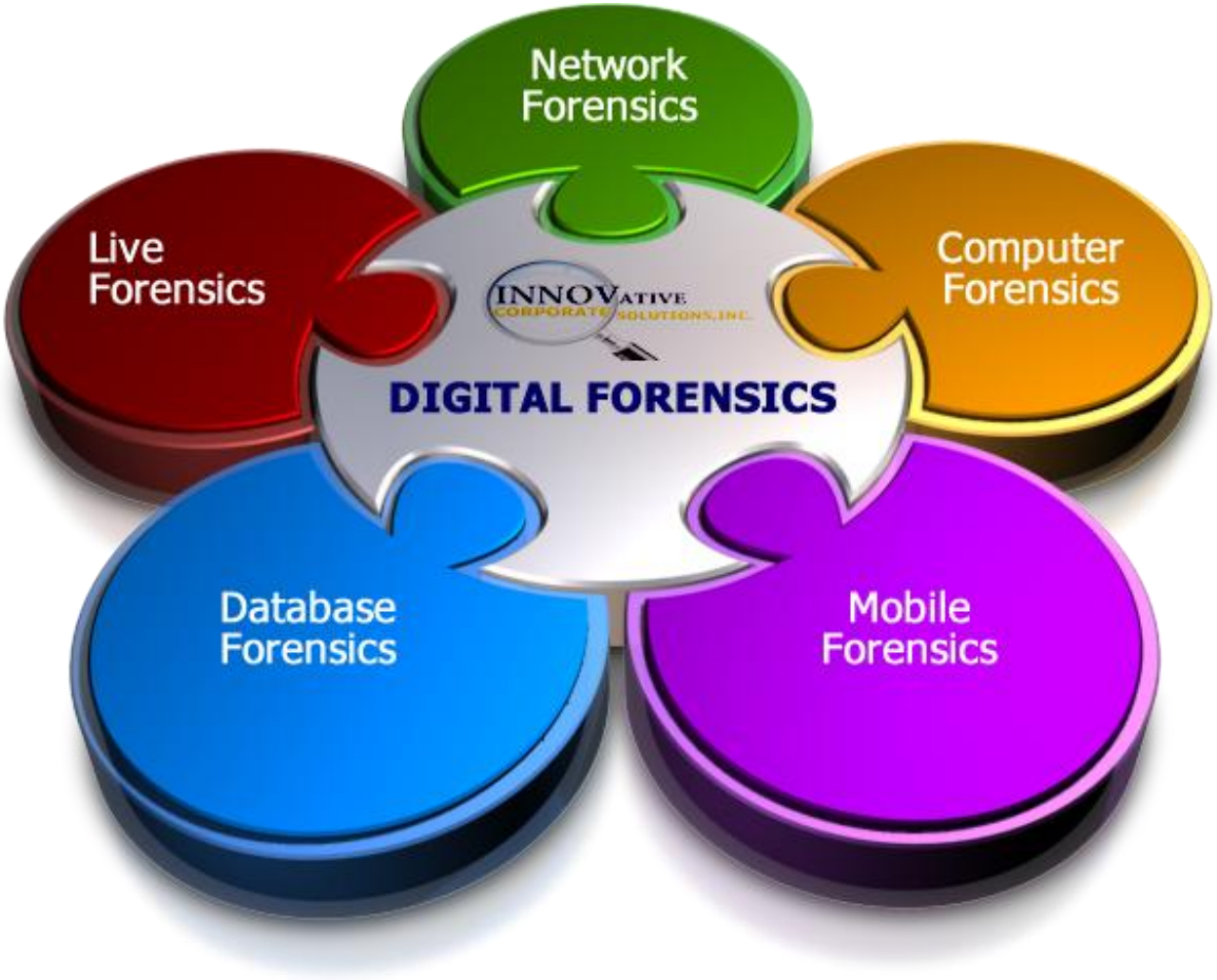
2.10 Νομικά Θέματα

Το cloud computing είναι μια τεχνολογία που χρησιμοποιείται καθημερινά και περισσότερο στον επιχειρησιακό χώρο καθώς παρέχει εύκολη και άμεση λειτουργία στους χρήστες καθώς διαθέτει τους πόρους του και τις λειτουργίες του άμεσα σε αυτους. Επιπλέον, επιλέγεται από τους καταναλωτές του, καθώς είναι οικονομικότερο σε σχέση με άλλες υπηρεσίες. Αυτό που πρέπει όμως να προσέχει ο κάθε πελάτης μιας τέτοιας τεχνολογίας είναι το τι νόμοι ισχύουν στην κάθε περίπτωση και κατά πόσο οι πάροχοι τέτοιων υπηρεσιών συμμορφώνονται σε αυτούς ώστε να μην βρεθούν εκτεθιμένα τα προσωπικά δεδομένα που αποθηκεύει. Το μεγαλύτερο μειονέκτημα μιας τέτοιας τεχνολογίας είναι η προστασία των προσωπικών δεδομένων ή αλλιώς ο έλεγχος της ιδιωτικότητάς τους. Οι κίνδυνοι που εγκυμονούν είναι πολλοί. Οι προβληματισμοί που υπάρχουν από τους χρήστες του cloud computing πηγάζουν από τα θέματα ασφαλείας των συστημάτων και την ιδιωτικότητα.
Ο κάθε χρήστης έχει δικαίωμα να γνωρίζει ποιες προσωπικές πληροφορίες αποθηκεύτηκαν και σε ορισμένες περιπτώσεις, μπορεί να ζητήσει την διακοπή της περαιτέρω επεξεργασίας τους (Νόμος Ν.2472/97 & 3471/2006 για την Ελληνική Δημοκρατία). Σε ένα πολύπλοκο σύστημα όπως το περιβάλλον Cloud, γενάτε η ανησυχία σχετικά με την ικανότητα του οργανισμού για την παροχή όλων των απαραίτητων πληροφοριών στο υποκείμενο της πληροφορίας και τελικά στην συμμόρφωση του οργανισμού με τους νόμους. Εάν ο ενδιαφερόμενος εξασκήσει το δικαίωμα να ζητήσει από τον Οργανισμό να καταστρέψει τα προσωπικά του στοιχεία, πως μπορεί αυτός να εξασφαλίσει ότι όλες οι πληροφορίες του υποκειμένου έχουν διαγραφεί και στο Cloud;

Μια ακόμα ανησυχία των χρηστών αφορά τα πολλαπλά κέντρα δεδομένων, καθώς είναι πολλά και κατανεμημένα σε διάφορες χώρες με αποτέλεσμα να εγείρονται ζητήματα σχετικά με τις διασυνοριακές ροές αλλά και το εφαρμοστέο δίκαιο που τις διέπει. Στην περίπτωση που τα δεδομένα αποθηκεύονται στο Cloud, ενδέχεται να υπάρξει διαβίβαση τους σε διαφορετικές κρατικές οντότητες, χωρίς αυτό να γίνεται εν γνώση του οργανισμού του πελάτη, με αποτέλεσμα τη πιθανή παραβίαση του τοπικού δίκαιου.

Ένα άλλο θέμα που προκύπτει είναι η διατήρηση των προσωπικών δεδομένων, δηλαδή το χρονικό διάστημα που μια υπηρεσία διατηρεί τα δεδομένα και τι γίνεται στην περίπτωση που ένας χρήστης ή μια επιχείρηση δεν κάνει χρήση πλέον των τεχνολογιών αυτών. Τι γίνεται λοιπόν με την οριστική καταστροφή των δεδομένων; Λέγεται ότι για την επίτευξης της μεγίστης διαθεσιμότητας πολλοί πάροχοι του cloud παρέχουν την υπηρεσία replication, η οποία συνιστάται στην αυτόματη αναπαραγωγή/αποθήκευση της πληροφορίας σε πολλαπλά συστήματα και τοποθεσίες. Η υπηρεσία αυτή μετατρέπεται σε πρόκληση όταν ο οργανισμός προσπαθεί να καταστρέψει τα δεδομένα. Δημιουργείται λοιπόν το ερώτημα αν μπορούμε να καταστρέψουμε αποτελεσματικά το σύνολο των δεδομένων όταν αυτά μεταναστεύσουν στο Cloud. Ο πάροχος του cloud πραγματικά καταστρέφει τα δεδομένα η απλά τα κάνει απροσπέλαστα για τον πελάτη του; Δεν υπάρχει σαφής και βέβαιη απάντηση σχετικά με την καταστροφή των δεδομένων αυτων, στις πληοψηφεία τους όμως μπορούμε να πούμε ότι διαχωρίζονται με τετοιο τρόπο ώστε να μην μπορεί να υπάρξει σύνδεση τους με τον κάτοχο που ζήτησε την διαγραφή τους.

Στην συνέχεια θα αναπτύξουμε απόψεις σχετικές με την Ψηφιακή Εγκληματολογία,(Digital Forensics) ορισμούς, έννοιες και νομικά θέματα.



Κεφάλαιο 3 : Ψηφιακή Εγκληματολογία (Digital Forensics)

3.1 Ορισμός Ψηφιακής Εγκληματολογίας

Με τον όρο ψηφιακή εγκληματολογία νοείται η επιστήμη που ασχολείται με την ανάκτηση και τη διερεύνηση υλικού που βρίσκεται αποθηκευμένο σε ψηφιακές συσκευές.

Η ανάλυση των ψηφιακών πειστηρίων, είναι το επιστημονικό κομμάτι της αναγνώρισης, περισυλλογής, εξέτασης και ανάλυσης των ψηφιακών δεδομένων, με κυρίοτερο μέλημα την διασφάλιση της ακεραιότητάς τους.

3.2 Διαδικασίες πραγματογνωμοσύνης

Σειρά διαδικασιών

Η διαδικασία σε όλες τις πραγματογνωμοσύνες, βασίζεται σε ένα μοντέλο **έξι (6)** επιπέδων:

1.Καταγραφη-Αναγνώριση

2.Διατήρηση.

3.Περισυλλογή.

4.Εξέταση.

5.Ανάλυση.

6. Σύνταξη της έκθεσης εργαστηριακής πραγματογνωμοσύνης.

1.Καταγραφή-Αναγνώριση: Κατά τη διαδικασία της αναγνώρισης καθορίζονται οι παραβάσεις του νόμου σύμφωνα με τις οποίες πραγματοποιείται μία εγκληματική δραστηριότητα. Στο επίπεδο αυτό, καταμετρούμε τα hardware (αριθμό ψηφιακών πειστηρίων) και αναγνωρίζουμε το software (όγκος δεδομένων) που χρησιμοποίησε ο ύποπτος για την τέλεση μιας αξιόποινης πράξης και τα οποία θα μας χρησιμεύσουν στην περισυλλογή των αποδεικτικών στοιχείων.

2.Διατήρηση: Διασφαλίζεται η ακεραιότητα των αποδεικτικών στοιχείων.

3.Περισυλλογή: Δημιουργείται ακριβές αντίγραφο των δεδομένων των αποδεικτικών στοιχείων προς διασφάλιση της ακεραιότητας τους και την μετέπειτα διερεύνηση τους. (Επιλέγουμε εκείνη τη μέθοδο που θα μας δώσει το καλύτερο αντίγραφο δεδομένων.)

4.Εξέταση: Στην Ελλάδα η εξέταση γίνεται αποκλειστικά από την Διεύθυνση Εγκληματολογικών ερευνών η οποία έδρεύει στην Αττική, και την υποδιεύθυνσή της η οποία εδρεύει στην Θεσσαλονίκη.

Αμφότερες υπάγονται στο Αρχηγείο της Ελληνικής Αστυνομίας. Στην χώρα μας για την διασφάλιση της ακεραιότητας των αποδεικτικών στοιχείων και της αδιαβλητότητας της διαδικασίας, ο εξεταστής δεν γνωρίζει ούτε τον/τους ύποπτο/ους που πιθανόν να έχουν διαπράξει κάποιο αδίκημα ούτε τον τόπο, ούτε τον τρόπο τέλεσης. Τέλος, όλοι οι πραγματογνωμονες παιρνούν από συγκεκριμενη εκπαίδευση, πιστοποιούνται για τις γνώσεις τους και υποχρεωτικά παραμένουν για μεγάλο χρονικο διάστημα (10 έτη) στην Υπηρεσία αυτή.

5.Ανάλυση: Ο πραγματογνώμονας εξάγει όλα τα δεδομένα που προέκυψαν από την διερεύνηση στα ψηφιακά πειστήρια και ασχολείται με την εύρεση των ζητηθεντων στοιχείων από αυτόν που διεξάγει την έρευνα.

6. Σύνταξη έκθεσης εργαστηριακής πραγματογνωμοσύνης:

Τέλος, ο πραγματογνώμονας εξάγει το σύνολο των αποτελεσμάτων και συντάσσει την σχετική έκθεση ευρημάτων της έρευνας που πραγματοποίησε.

Η τεχνική πτυχή μιας έρευνας ποικίλει ανάλογα με το είδος των ψηφιακών πειστηρίων.

Ειδικότερα, διαφορετικές τεχνικές και προγράμματα ανάλυσης δεδομένων χρησιμοποιούνται για την εξαγωγή των ευρημάτων ανάλογα με το είδος της μονάδας αποθήκευσης, (ηλεκτρονικοί υπολογιστές, κινητά τηλέφωνα, συσκευές τύπου ταμπλετ, κ.λπ)

Συμπερασματικά θα μπορούσαμε να πούμε ότι η ψηφιακή διερεύνηση χωρίζεται σε κλάδους όπως είναι:

1)Η εγκληματολογία υπολογιστών,

2)Η εγκληματολογία δικτύων και

3)Η εγκληματολογία κινητών συσκευών.

Η διαδικασία των τριών κλάδων είναι παρόμοια και περιλαμβάνει:

Α) την κατάσχεση,

Β) την απεικόνιση (απόκτηση),

Γ) την ανάλυση των ψηφιακών μέσων,

Δ)την σύνταξη της έκθεσης εργαστηριακής πραγματογνωμοσύνης.

Παράλληλα με την σύνταξη της έκθεσης Εργαστηριακής πραγματογνωμοσύνης των στοιχείων, όπως αυτά εξάγονται από την εξέτασή τους, οι αρχές επιβολής του νόμου αποδίδουν κατηγορίες στους κατόχους-διαχειριστές. Επιπρόσθετα επιβεβαιώνουν ή προσδιορίζουν την κατοχή-διαχείριση των πηγών (σε περιπτώσεις πνευματικών δικαιωμάτων) και επιβεβαιώνουν τα ευρήματα ή τις αρχικές πληροφορίες.

Μια ψηφιακή έρευνα αποτελείται συνήθως από 3 στάδια:

1. **Την απόκτηση ή απεικόνιση εκθεμάτων,**
2. **Την ανάλυση,**
3. **Την αναφορά.**

Η ιδανική απόκτηση περιλαμβάνει τη λήψη μιας εικόνας της πτητικής μνήμης (RAM) του υπολογιστή και τη δημιουργία ενός ακριβούς διπλού κειμένου των μέσων, συχνά χρησιμοποιώντας μια συσκευή εγγραφής του πρωτοτύπου. Ωστόσο, η αύξηση του μεγέθους των μέσων αποθήκευσης και οι εξελίξεις, όπως το cloud computing, οδήγησαν σε μεγαλύτερη χρήση των «ζωντανών» εξαγορών, με την απόκτηση ενός «λογικού» αντιγράφου των δεδομένων αντί της πλήρους εικόνας της συσκευής φυσικής αποθήκευσης.

Η ψηφιακή εγκληματολογία χρησιμοποιείται τόσο στο ποινικό δίκαιο όσο και στην ιδιωτική έρευνα. Παραδοσιακά όμως, συνδέεται με το ποινικό δίκαιο, κατά το οποίο συλλέγονται όλα τα αποδεικτικά στοιχεία που υποστηρίζουν ή αντιτίθενται σε μια υπόθεση ενώπιον των δικαστηρίων. Όπως συμβαίνει και με άλλους τομείς της εγκληματολογίας, αυτό συχνά αποτελεί μέρος μιας ευρύτερης έρευνας που καλύπτει αρκετούς κλάδους. Σε ορισμένες περιπτώσεις, τα συλλεχθέντα αποδεικτικά στοιχεία χρησιμοποιούνται ως μορφή συλλογής πληροφοριών, που χρησιμοποιείται για σκοπούς άλλους από εκείνους της δικαστικής διαδικασίας (για παράδειγμα, για τον εντοπισμό ή τον τερματισμό άλλων εγκλημάτων). Ειδικότερα να πούμε ότι τα ευρύματα που προκύπτουν από μία έρευνα μπορούν να χρησιμοποιηθούν και για την εξιχνίαση και άλλων εγκλημάτων. Ως αποτέλεσμα, η συλλογή πληροφοριών γίνεται μερικές φορές σε ένα λιγότερο αυστηρό δικαστικό πρότυπο.

Ο κύριος στόχος των ερευνών ψηφιακής εγκληματολογίας είναι η ανάκτηση αντικειμενικών αποδείξεων για μία εγκληματική δραστηριότητα.

Απόδοση
Τα μεταδεδομένα και άλλα αρχεία καταγραφής μπορούν να χρησιμοποιηθούν για την απόδοση ενεργειών σε ένα άτομο. Για παράδειγμα, τα προσωπικά έγγραφα σε μια μονάδα υπολογιστή ενδέχεται να εντοπίσουν τον κάτοχό τους.

Alibis και δηλώσεις
Οι πληροφορίες που παρέχονται από τους συμμετέχοντες μπορούν να ελεγχθούν με ψηφιακά στοιχεία.

Πρόθεση
Εκτός από την εύρεση αντικειμενικών αποδείξεων για την τέλεση μιας αξιόποινης πράξης που διαπράττεται, οι έρευνες μπορούν επίσης να χρησιμοποιηθούν για να αποδείξουν την πρόθεση. Με τον όρο πρόθεση νοούνται όλα τα προπαρασκευαστηκά στάδια για την τέλεση ενός αδικήματος.

Αξιολόγηση της πηγής
Τα αρχεία δεδομένων και τα μεταδεδομένα αρχείων μπορούν να χρησιμοποιηθούν για τον προσδιορισμό της προέλευσης ενός συγκεκριμένου στοιχείου.

Έλεγχος ταυτότητας εγγράφου
Σχετικά με την "Αξιολόγηση της πηγής", τα μεταδεδομένα που σχετίζονται με τα ψηφιακά έγγραφα μπορούν εύκολα να τροποποιηθούν και να αποπροσανατολίσουν τις έρευνες.

Περιορισμοί

Ένας σημαντικός περιορισμός σε μια εγκληματολογική έρευνα είναι η χρήση της κρυπτογράφησης καθώς αυτό διαταράσσει την αρχική εξέταση όπου μπορεί να εντοπιστούν σχετικά αποδεικτικά στοιχεία χρησιμοποιώντας λέξεις-κλειδιά. Οι νόμοι που υποχρεώνουν τα άτομα να αποκαλύψουν κλειδιά κρυπτογράφησης εξακολουθούν να είναι σχετικά νέοι και αμφιλεγόμενοι. Στην πραγματικότητα στην Ελλάδα

δεν υπάρχει νομοθετικό πλαίσιο που να εξασφαλίζει τις αρχές προκειμένου να λάβουν από τον ύποπτο το κλειδί.

3.3 Τεχνικές διερεύνησης στο περιβάλλον του Cloud.

Το υπολογιστικό νέφος, με τη σειρά του, βασίζεται σε ένα ευρύ δίκτυο πρόσβασης, με αποτέλεσμα οι τεχνικές που θα χρησιμοποιηθούν, θα είναι οι βασικές των δικτύων, με ειδικές προσαρμογές για τα περιβάλλοντα του υπολογιστικού νέφους.
Υπό τη μορφή βημάτων και οδηγού, σε κάθε έρευνα που γίνεται στο Cloud, θα πρέπει να αναφέρονται τα κάτωθι:

1. Μελέτη της υπό εξέταση υπόθεσης.

2. Διασαφήνιση του προβλήματος.

3. Εργαλεία που χρησιμοποιήθηκαν.

4. Αναπαράσταση δεδομένων σε πίνακες και γραφήματα.

5. Διαφορές ανάμεσα στη πλήρη απόκτηση και στη πρακτική απόκτησης.

6. Δυσκολίες απόδοσης κατηγοριών, με τα ανευρεθέντα αποδεικτικά στοιχεία στο δικαστήριο.

7. Προτεινόμενες διαδικασίες και απαιτούμενες δεξιότητες.

Καθώς η τεχνολογία εξελίσσεται με γρήγορους ρυθμούς, η νομοθεσία αδυνατεί να την προφτάσει. Και εδώ είναι που γεννάται το ερώτημα αν τελικά ο παγκόσμιος ιστός μπορεί να ελεγχθεί από την άποψη της ποινικής του συμπεριφοράς. Για την αντιμετώπιση του εγκλήματος στο διαδίκτυο απαιτούνται εξειδικευμένες γνώσεις τόσο σε νομικό όσο και τεχνικό επίπεδο κάτι που αποτελεί ένα από τα σημαντικότερα προβλήματα κάθε κράτους καθώς ελάχιστοι νομοθέτες τις διαθέτουν. Όπως παρατηρείται, οι νομοθετικές ρυθμίσεις που αφορούν το ηλεκτρονικό έγκλημα παρουσιάζουν εγγενείς αδυναμίες, τόσο στην Ελλάδα όσο και στις υπόλοιπες χώρες. Αυτό συμβαίνει διότι το Ηλεκτρονικό Έγκλημα αποτελεί εγκληματική δραστηριότητα αρκετά εξειδικευμένη και ανεπτυγμένη τεχνολογικά, με αποτέλεσμα να

παρουσιάζονται προβλήματα στην οριοθέτηση των πράξεων που θα πρέπει να διώκονται ποινικά. Επιπλέον, οι νομοθέτες είναι αναγκασμένοι να ενημερώνονται διαρκώς για τις εξελίξεις στον τομέα της τεχνολογίας των υπολογιστών, προκειμένου να εξοικειωθούν με τον τρόπο διάπραξης αδικημάτων μέσω αυτών. Ειδικότερα, σε ειδική έρευνα που πραγματοποίηθηκε στη Βρετανία, διαπιστώθηκε ότι το έτος 2020 οι κακοποιοί θα γνωρίζουν στην εντέλεια τη λειτουργία των συστημάτων ασφαλείας των τραπεζικών κωδικών και των τεχνικών αναγνώρισης και θα έχουν την τεχνογνωσία να προσπελάσουν οποιοδήποτε ηλεκτρονικό εμπόδιο».

3.4 Το πρόβλημα της Νομοθεσίας

Με τη ραγδαία εξέλιξη της τεχνολογίας στο χώρο των υπολογιστικών συστημάτων αλλά και του διαδικτύου, ακολουθεί μια νέα μορφή εγκλήματος. Το ηλεκτρονικό έγκλημα και η εξέλιξη του είναι ανάλογη με την εξέλιξη της εν λόγω τεχνολογίας και οι διαστάσεις που έχει πλέον λάβει, κάνουν απαραίτητη την ύπαρξη αντίστοιχης νομοθεσίας. Παρ'όλα αυτά, η νομοθεσία που αφόρα στα αδικήματα που διαπράττονται μέσω διαδικτύου θα μπορούσαμε να πούμε ότι είναι ένας ξεχωριστός κλάδος του δικαίου και τα ιδιαίτερα χαρακτηριστικά του το διαφοροποιούν από το συμβατικό έγκλημα. Για την θεσμοθέτηση των νόμων απαιτείται η προσέγγιση κι από τεχνολογικής πλευράς γι' αυτό είναι απαραίτητη η γνώση θεμάτων σχετικά με τους ηλεκτρονικούς υπολογιστές και το διαδίκτυο. Όλοι όσοι συμμετέχουν στη πρόληψη την καταστολή και τη δίωξη εγκλημάτων στον κυβερνοχώρο, δικηγόροι, εισαγγελείς, δικαστές, αστυνομικοί, θα πρέπει να κατέχουν γνώσεις τόσο νομικές όσο και τεχνικές. Η δυσκολία στην θεσμοθέτηση αυτή έγκειται στη διαμόρφωση κατάλληλης ορολογίας και στην άρτια εφαρμογή του Ποινικού Δικαίου. Είναι ευνόητο πως η παγκόσμια έκταση του διαδικτύου συχνα καθίστα αδύνατο τον προσδιορισμό του τόπου του εγκλήματος. Η δικαιοδοσία και η συνεργασία μεταξύ των

κρατών σε διεθνής έρευνες και η διαδικασία έκδοσης όσων έχουν διαπράξει κυβερνοεγκλήματα με διεθνή χαρακτήρα είναι θέματα που θα πρέπει να ληφθούν υπ' όψιν για την πάταξη τέτοιου είδους εγκλημάτων. Επομένως, λόγω των εξελίξεων και της συνεχούς μεταβολής των πραγμάτων, τα αδικήματα στον κυβερνοχώρο διαφέρουν από αυτά του απλού ποινικού δικαίου. Στο διαδίκτυο εμφανίζονται ολοένα και περισσότερο νέοι τρόποι διάπραξης εγκλημάτων. Ειδικότερα εμφανίζονται νέοι τρόποι και τεχνικές διάπραξης γνωστών αδικημάτων. Οι αρχές επιβολής του Νόμου, όλων των δυτικών πολιτισμών προσπαθούν να θεσπίσουν νόμους και κανονισμούς με ενιαία εφαρμογή στα κράτη-μέλη, πράγμα όμως που μέχρι στιγμής δεν έχουν κατορθώσει διότι οι εκάστοτε νόμοι που διέπουν κάθε κράτος, υπερκαλύπτουν τις όποιες αποφάσεις. Δεν υπάρχει ακόμα κάποιος ποινικός κώδικας, με ενιαία εφαρμογή σε όλες τις χώρες, σχετικος με τα εγκλήματα που διαπράττονται στον κυβερνοχώρο πράγμα που δεν μπορεί να πραγματωθεί τόσο γιατί η νομική επιστήμη δεν δύναται να αποτυπώσει και να ποινικοποιήσει τεχνικούς ορούς που χρησιμοποιούνται από την πληροφορική όσο και γιατί η εκάστοτε χώρα προτιμά να λειτουργεί με το δικό της νομοθετικό πλαίσιο. Η ορολογία που χρησιμοποιεί ένας τεχνικός είναι συνήθως νομικά ασαφής, γενική, αόριστη και ελλιπής με αποτέλεσμα να εμποδίζει την ορθή απονομή της δικαιοσύνης. Ωστόσο οι έννοιες που χρησιμοποιεί η πληροφορική αποδίδουν και την εξυπηρετούν. Ακόμη στην περίπτωση που διαπραχτεί κάποιο αδίκημα στον Κυβερνοχώρο για το όποιο δεν υπάρχει νόμος τότε ερευνάται η σχετική νομολογία. Η εκάστοτε νομοθεσία εξαρτάται πλήρως από την τεχνολογία των υπολογιστών και το διαδίκτυο, διότι αυτά καθορίζουν τον ρυθμό εξέλιξης εγκλημάτων στον Κυβερνοχώρο. Το ένα παρακολουθεί και ακολουθεί την πρόοδο του αλλού. Αναμφίβολα η τεχνολογία των ηλεκτρονικών υπολογιστών και του διαδικτύου εξελίσσεται με ραγδαίους ρυθμούς στους οποίους οι αρχές επιβολής του Νόμου πολλές φόρες δεν κατορθώνουν να ανταποκριθούν. Όμως, για το δίκαιο τα πράγματα δεν είναι τόσο εύκολα αφού η θεσμοθέτηση των νόμων απαιτεί τόσο χρόνο που σε καμία περίπτωση δεν αγγίζει εκείνον των εξελίξεων στον Κυβερνοχώρο. Επομένως προκύπτει το συμπέρασμα ότι ακόμα κι αν υφίσταται ειδική νομοθεσία για το έγκλημα στον Κυβερνοχώρο, αυτή θα πρέπει να ενημερώνεται συνεχώς, λαμβάνοντας υπ' όψιν τις όποιες τεχνολογικές εξελίξεις.

3.5 Προβληματισμοί

Βασικό ζήτημα το οποίο θα πρέπει να διευθετηθεί είναι η θεσμοθέτηση σε Παγκόσμιο επίπεδο νομικού πλαισίου για την ρύθμιση των αδικημάτων στον Κυβερνοχώρο. Επιπρόσθετα θα πρέπει να σημειωθεί πως το νομικό πλαίσιο που θα διέπει τον Κυβερνοχώρο να ορίζει ρητά ποιες ενέργειες-πράξεις θα τιμωρούνται και με ποια ποινή. Η οποιαδήποτε προσπάθεια ρύθμισης είναι ιδιαίτερα δύσκολη αφού το διαδίκτυο είναι ένας χώρος αχανής, χωρίς όρια, με απεριόριστες δυνατότητες ανταλλαγής πληροφοριών. Η νομική προσέγγιση του Διαδικτύου βρίσκει υποστηρικτές αλλά και αντιπάλους. **Οι υποστηρικτές** της ρύθμισης του διαδικτύου θεωρούν ότι: Το διαδίκτυο είναι ανοιχτό σε όλους και απαιτείται η ρύθμιση του για τον έλεγχο του παράνομου περιεχομένου του. Θα πρέπει επομένως να γίνει μία προσπάθεια για τον αποτελεσματικό έλεγχό τόσο σε τοπικό, με την έννοια του Κράτους, όσο και σε παγκόσμιο επίπεδο. **Οι πολέμιοι** της ρύθμισης του διαδικτύου θεωρούν ότι: θα χαθεί η ελευθερία του λογού που προσφέρεται σήμερα μέσω αυτού, και πως αυτή είναι απόλυτο και αναφαίρετο δικαίωμα κάθε πολίτη, προστατευόμενο ήδη από συνταγματικές διατάξεις και έτσι οφείλει να παραμείνει.

Το διαδίκτυο είναι διαφορετικό από τα αλλά μέσα επικοινωνίας, με χαρακτηριστικά την ειλικρίνεια, την ελευθερία λόγου, τον πειραματισμό, την ελεύθερη διακίνηση ιδεών και την ανταλλαγή απόψεων. Το διαδίκτυο δε μπορεί να ρυθμιστεί διότι είναι τεράστιο και αχανές και οποιαδήποτε προσπάθεια ελέγχου θα ερχόταν αντιμέτωπη με τη λογοκρισία. Σύμφωνα με την κοινή ομολογία οι γονείς και κηδεμόνες είναι υπεύθυνοι για να προστατευόσουν τα παιδιά τους από τους κινδύνους του παράνομου περιεχομένου του διαδικτύου και όχι τα κράτη με τις νομοθετικές τους ρυθμίσεις.

3.6 Η κοινωνία του Εγκλήματος στον Κυβερνοχώρο.

Αυτό που προβληματίζει ιδιαίτερα την προσπάθεια του νομοθέτη για την εφαρμογή σχετικών ρυθμίσεων για την αντιμετώπιση εγκλημάτων είναι η παγκόσμια διάσταση του διαδικτύου. Η διάσταση αυτή

προβληματίζει γιατί πρόκειται για διαφορετικές χώρες με διαφορετική κουλτούρα, πράγμα που σημαίνει ότι ένα αδίκημα στοιχειωθετείται και αντιμετωπίζεται διαφορετικά από χώρα σε χώρα και ανάλογα με το κοινωνικοπολιτικό καθεστώς, τα ήθη, τα έθιμα και τις παραδόσεις κάθε λαού. Στην περίπτωση αυτή επομένως, εύλογα τίθεται ο προβληματισμός, του πως θα αντιμετωπιστεί ένα έγκλημα που διαπράττεται σε δυο ή περισσότερες χώρες ταυτόχρονα όταν σε αυτές ισχύει διαφορετικό νομοθετικό πλαίσιο ή όταν δεν υπάρχει νομοθετικό πλαίσιο για το συγκεκριμένο αδίκημα;

Έτσι λοιπόν καταλήγουμε στο συμπέρασμα ότι είναι ανάγκη να υπάρξει νομική συνεννόηση μετά των χώρων, με συνεργασία σε παγκόσμιο επίπεδο, που θα βοηθήσει στην αναζήτηση και αποκάλυψη των υπόπτων και γενικότερα στον περιορισμό των διαδικτυακών εγκλημάτων. Περάν όμως από το ποινικό κομμάτι υπάρχει και ο προβληματισμός για την εφαρμογή του δικονομικού τομέα. Αυτό σημαίνει ότι κατά την διερεύνηση των εγκλημάτων στο διαδίκτυο οι αρχές θα έρθουν αντιμέτωπες με θεμελιώδεις αξίες, όπως η προστασία του απορρήτου και της ιδιωτικότητας του άτομου.

3.7 Ζητήματα Δικαιοδοσίας στο Διαδίκτυο.

Με τον όρο δικαιοδοσία νοείται το σύνολο των αρχών που καλούνται να λάβουν αποφάσεις, απο την στιγμή που θα λάβουν γνώση ενός αδικήματος.

Ειδικότερα, με τον όρο αυτό νοείται η απόδοση δικαιοσύνης για μια εγκληματική συμπεριφορά η οποία εντάσσεται στην εδαφική αρμοδιότητα της εκάστοτε χώρας. Επομένως, οι αρχές κάθε χώρας με την συμβολή του εκάστοτε δικαστηρίου θα οδηγήσουν τον ύποπτο, και με την συνδρομή άλλων αρχών, ενώπιον της δικαιοσύνης. Δικαιοδοσία λοιπόν είναι η αρμοδιότητα ενός δικαστηρίου να δικάσει μια συγκεκριμένη υπόθεση αλλά συγχρόνως και η αντίστοιχη αρμοδιότητα των διωκτικών αρχών να διερευνήσουν μια εγκληματική συμπεριφορά. Η ανεύρεση της αρμοδιότητας του δικαστηρίου είναι συνυφασμένη με τον καθορισμό του τόπου τέλεσης του αδικήματος. Για τον καθορισμό

του τόπου τελέσεως του αδικήματος υποστηρίζονται οι εξής τέσσερις θεωρίες:

1. Η θεωρία του τόπου του αποτελέσματος. Ως τόπος τελέσεως ενός αδικήματος θεωρείται ο τόπος όπου εκδηλώθηκε το αποτέλεσμα.

2. Η θεωρία του τόπου ενέργειας. Ως τόπος τέλεσης του αδικήματος θεωρείται ο τόπος όπου έχει τελεστεί η ενέργεια που έτεινε στο άδικο αποτέλεσμα. Εφόσον η ενέργεια έλαβε χώρα σε περισσότερα από ένα κράτη, ως τόπος ενέργειας ορίζεται αυτός στον οποίο ολοκληρώθηκε η ενέργεια.

3. Η μικτή θεωρία. Ως τόπος τέλεσης ενός αδικήματος θεωρείται τόσο ο τόπος ενέργειας όσο και ο τόπος του αποτελέσματος, δίνοντας παράλληλα το δικαίωμα επιλογής του τόπου στον δράστη, σε περίπτωση που αυτός ανευρεθεί.

4. Η θεωρία του βαρύνοντος τόπου. Ως τόπος τέλεσης ενός αδικήματος ορίζεται η εδαφικότητα ενός κράτους, στο οποίο εκδηλώθηκε η κύρια υπόσταση του εγκλήματος. Στον τόπο, δηλαδή στον οποίο υπήρχαν συνέπειες. Στην Θεωρία αυτή εντοπίζονται δυσκολίες στην εφαρμογή της καθώς είναι δύσκολο να καθοριστεί ο τόπος για την τέλεση της διαδικτυακής αδικοπραξίας.

Είναι πολλές φορές δύσκολο να προσδιορίσουμε το γεωγραφικό χώρο, άρα και την κατά τόπον αρμοδιότητα, καθώς επιπτώσεις της πράξης αυτής συχνά εμφανίζονται σε περισσότερες των μία χωρών. Οι Κυβερνοεγκληματίες πολλές φορές γνωρίζουν τις δυσκολίες που υπάρχουν μεταξύ της επικοινωνίας των αρχών των Κρατών, για την εφαρμογή του Ποινικού Κώδικα και των κυρώσεων αυτού και εκμεταλλευόμενοι αυτό παρανομούν διασυνοριακά. Έτσι στο πλήθος των περιπτώσεων, περισσότερα του ενός Κράτη αξιώνουν να λάβουν πλήρη δικαιοδοσία για την επιβολή της Ποινικής τιμωρίας του παραβάτη, πράγμα που συνήθως δεν δύναται να εφαρμοστεί. Ως τόπος τέλεσης λοιπόν ενός αδικήματος θεωρείται ο τόπος εκείνος στον οποίο ο φερόμενος δράστης, παρευρίσκεται με την φυσική του παρουσία την στιγμή που διαπράττεται το αδίκημα, ασχέτως εάν η πράξη αυτή έχει αντίκτυπο και σε άλλες χώρες. Οι αρχές επιβολής του Νόμου, της χώρας

στην οποία ο παραβάτης συλλαμβάνεται, διότι του αναγνωρίζονται και του καταλογίζονται άδικες- παράνομες πράξεις, έχουν την αποκλειστική αρμοδιότητα να αποφασίσουν εάν θα του ασκήσουν Ποινική δίωξη για τα αδικήματα που του καταλογίζονται ή θα τον εκδώσουν στην Χώρα που τον αναζητεί. Έτσι, ένα έγκλημα μπορεί να τελεστεί συνήθως σε μια άλλη χώρα από αυτή στην οποία ανήκει ο δράστης ή επίσης μπορεί κάποιος να διαχέει πληροφορίες στο διαδίκτυο επηρεάζοντας μεμονωμένα άτομα και οργανισμούς που ανήκουν σε διαφορετικές δικαιοδοσίες και σε διαφορετικό νομικό πλαίσιο.

Το ζήτημα της δικαιοδοσίας στο ηλεκτρονικό έγκλημα καθορίζεται αρχικά από τις Εθνικές νομοθεσίες, οι οποίες θέτουν και τους βασικούς κανόνες. Έπειτα από τις διεθνείς συμφωνίες που προσπαθούν να ρυθμιστούν τα όποια θέματα σε διεθνές επίπεδο, από διάφορες διακρατικές συμφωνίες που προκύπτουν ανάλογα με τον αξιόποινο χαρακτήρα και τέλος από τις αποφάσεις των δικαστηρίων. Η δικαιοδοσία είναι δεδομένη όταν ένας δικτυακός τόπος είναι διαδραστικός, όταν υπάρχει δηλαδή άμεση επικοινωνία και ανταλλαγή υλικού μεταξύ του χρηστή και του δικτυακού τόπου. Σε περίπτωση που ένας δικτυακός τόπος είναι παθητικός και απλά παρέχει πληροφορίες τότε δεν υφίσταται δικαιοδοσία.

Το βασικό και κύριο νομοθετικό κείμενο για τον προσδιορισμό της εννοίας της δικαιοδοσίας, είναι **η συνθήκη των Βρυξελλών (1968)** κατά την οποία: *Ένα άτομο που ζει μόνιμα σε κάποιο κράτος – μέλος της Ευρωπαϊκής Ένωσης, μπορεί να εκδοθεί σε αυτό. Σε υποθέσεις παραβίασης συμβατικής υποχρέωσης, ένα άτομο μπορεί να εκδοθεί στον τόπο όπου έλαβε χωρά η υποχρέωση, που τίθεται υπό αμφισβήτηση. Σε αστικά ζητήματα, ένα άτομο μπορεί να εκδοθεί στον τόπο, όπου έλαβε χώρα το αποτέλεσμα. Ένας χρήστης, μπορεί να εκδοθεί μόνο στον τόπο που ζει μόνιμα, μπορεί όμως να επιλέξει την μεταφορά της υπόθεσης στον τόπο μόνιμης κατοικίας του αντιδίκου, εφόσον σε αυτόν υπέστη μεγαλύτερη ζημιά. Σε συμβάσεις που δεν εμπλέκεται μόνο ένας χρήστης, οι αντίδικοι μπορούν να συμφωνήσουν για τον τόπο εκδίκασης της υπόθεσης.*

3.8 Παγκόσμια νομοθεσία στον Κυβερνοχώρο.

ΗΠΑ:

Το 1948 θεσπίστηκε το πρώτο νομοθέτημα σχετικά με το ηλεκτρονικό έγκλημα. Ωστόσο, στο νομοθέτημα αυτό δεν ήταν διακριτός ο προσδιορισμός των ορίων δικαιοδοσίας των δικαστηρίων και αυτό αποτελούσε το σημαντικότερο πρόβλημα. Επίσης, δεν υπήρχε ορολογία σχετική με την τεχνολογία των ηλεκτρονικών υπολογιστών. Τέλος, η νομοθεσία αυτή αφορούσε στην προστασία των κρατικών υπολογιστικών συστημάτων από τη μη εξουσιοδοτημένη πρόσβαση για την αποφυγή διαρροής απόρρητων πληροφοριών που θα μπορούσαν να βλάψουν τις ΗΠΑ. Τα παραπάνω ήταν ο λόγος για την αναθεώρηση του νομού το 1986. Στην αναθεώρησή του, χρησιμοποιείται μια πιο σαφής ορολογία και διαφαίνεται η προσπάθεια αντιμετώπισης περιπτώσεων άρνησης εξυπηρέτησης, ακόμη όμως και ο αναθεωρημένος νόμος κάνει λόγο περί προστασίας των κρατικών υπολογιστικών συστημάτων. Το 1994 γίνεται σημαντική τροποποίηση του νόμου η οποία είχε ως εξης: **Η ισχύς του νομοθετικού πλαισίου επεκτάθηκε και σε ηλεκτρονικούς υπολογιστές που χρησιμοποιούνται στο διαπολιτειακό εμπόριο. Αφαιρέθηκε ο όρος «μη εξουσιοδοτημένη πρόσβαση», κάτι το όποιο σημαίνει ότι οι υπάλληλοι εταιρειών και οι εξουσιοδοτημένοι χρήστες θα μπορούσαν να διωχθούν**. Η πιο σημαντική διάταξη προβλέπει ότι κάθε μεμονωμένος χρήστης που θα εισέρχεται σε έναν προστατευόμενο υπολογιστή θα είναι υπεύθυνος όχι μονό για τις ενέργειές του αλλά και για τις συνέπειες αυτών. Σε περίπτωση που ο χρηστής έχει εξουσιοδότηση για αυτό το σύστημα τότε θα είναι ποινικά υπεύθυνος μονό όταν θα έχει εγκληματικές προθέσεις.

ΑΥΣΤΡΑΛΙΑ:

Στην Αυστραλία θεσμοθετείται ο νομός **Crime Act 1914** που θέτει σα βασικές μορφές ηλεκτρονικού εγκλήματος: α) την παράνομη πρόσβαση σε δεδομένα που βρίσκονται σε κρατικό ηλεκτρονικό υπολογιστή β) την καταστροφή δεδομένων για δεδομένα που βρίσκονται σε κρατικό ηλεκτρονικό υπολογιστή γ) την πρόσβαση σε δεδομένα αποθηκευμένα σε ηλεκτρονικό υπολογιστή χρησιμοποιώντας μέσα κρατικής διευκόλυνσης και δ) την καταστροφή δεδομένων σε ηλεκτρονικό

υπολογιστή χρησιμοποιώντας μέσα κρατικής διευκόλυνσης. Σήμερα ισχύει ο νομός **The Cybercrime Act 2001** και αποτελεί τροποποίηση του **Crime Act 1914**. Ο νομός προβλέπει τρεις βασικές κατηγορίες ηλεκτρονικού εγκλήματος: α) με μη εξουσιοδοτημένη πρόσβαση, μετατροπή και φθορά δεδομένων, με σκοπό τη διάπραξη σοβαρού εγκλήματος, β) με μη εξουσιοδοτημένη τροποποίηση δεδομένων που οδηγεί σε φθορά αυτών, γ) με μη εξουσιοδοτημένη φθορά ηλεκτρονικών επικοινωνιών. Ωστόσο, ο νομός αυτός δημιούργησε τέσσερις νέες μορφές εγκλημάτων: α) μη εξουσιοδοτημένη πρόσβαση ή μετατροπή προστατευόμενων δεδομένων, β) παράνομη καταστροφή δεδομένων αποθηκευμένων σε δίσκους Η/Υ, γ) κατοχή ή έλεγχος δεδομένων, με σκοπό την διάπραξη ηλεκτρονικών αδικημάτων και δ) παραγωγή, προμήθεια ή απόκτηση δεδομένων, με σκοπό τη διάπραξη ηλεκτρονικού εγκλήματος.

ΑΓΓΛΙΑ:

Στην Αγγλία η πρώτη νομοθεσία για το ηλεκτρονικό έγκλημα ψηφίστηκε το 1990 **Computer Misuse Act** και αποτελεί πρότυπο νομοθεσίας και για άλλες χώρες. Η νομοθεσία αυτή διακρίνει τρεις βασικές κατηγορίες εγκλημάτων: α) μη εξουσιοδοτημένη πρόσβαση, σε πληροφορίες που είναι αποθηκευμένες σε ηλεκτρονικό υπολογιστή, β) μη εξουσιοδοτημένη πρόσβαση με σκοπό τη διάπραξη αδικημάτων και γ) μη εξουσιοδοτημένη τροποποίηση πληροφοριών, αποθηκευμένων σε υπολογιστικό σύστημα. Επίσης στη νομοθεσία υπάρχουν και διατάξεις σχετικές με τη νομοθεσία και τον τρόπο απονομής δικαιοσύνης.

ΑΡΓΕΝΤΙΝΗ:

Στην Αργεντινή δεν υπάρχει σχετικό νομοθετικό πλαίσιο που να αναφέρεται στο ηλεκτρονικό έγκλημα. Η ποινική αντιμετώπιση των περιπτώσεων αυτών γίνεται σύμφωνα με τον κοινό Ποινικό Κώδικα. Η δίωξη των ηλεκτρονικών εγκλημάτων γίνεται με διασταλτική ερμηνεία των ισχυουσών διατάξεων.

ΚΙΝΑ:

Στην Κίνα υπάρχει σχετική νομοθεσία για το ηλεκτρονικό έγκλημα. Καθιστά παράνομη οποιαδήποτε δραστηριότητα έχει να κάνει με τη διασπορά ιών ή αλλού κακόβουλου λογισμικού σε συστήματα ηλεκτρονικών υπολογιστών. Παράνομη θεωρείται επίσης και η πώληση συστημάτων προστασίας υπολογιστών χωρίς άδεια. Αξίζει να ειπωθεί πως η νομοθεσία της Κίνας πάνω σε αυτή τη μορφή εγκλήματος καταδικάζει την δημιουργία, την αναπαραγωγή και τη διάδοση υλικού που θα κλονίσει την εθνική ενότητα, όπως επίσης απαγορεύεται η παραποίηση της αλήθειας και η διάδοση οποιασδήποτε φήμης που θα βλάψει τη συνοχή της κοινωνίας.

ΔΙΕΘΝΕΙΣ ΠΡΟΣΠΑΘΕΙΕΣ (Συνεργασία Europol-Interpol).

Η Interpol ήταν η πρώτη που προσέγγισε το θέμα του εγκλήματος στον Κυβερνοχώρο σε διεθνές-διακρατικό επίπεδο. Η επιτροπή κατέληξε σε ένα κείμενο που λειτούργησε ως κοινός παρανομαστής μεταξύ των διαφορετικών νομικών προσεγγίσεων, που εξετάστηκαν στα κράτη – μέλη. Το κείμενο που συνέταξε **απαγόρευε:**

την εισαγωγή,

την τροποποίηση,

τη διαγραφή και

την απόκρυψη των δεδομένων με σκοπό την παράνομη μεταφορά κεφαλαίων, τη διάπραξη πλαστογραφίας και την παρεμπόδιση λειτουργίας ενός υπολογιστή ή δικτυού.

Εκτός των άλλων απαγορεύει και την πρόσβαση σε σύστημα Η/Υ χωρίς άδεια.

Οργανισμός Ηνωμένων Εθνών:

Τα Ηνωμένα Έθνη στο 8ο Συνέδριο για την Πρόληψη του Εγκλήματος και την Μεταχείριση των Παραβατών παρουσίασε ένα ψήφισμα σχετικά με τη νομοθεσία του ηλεκτρονικού εγκλήματος. Το Εγχειρίδιο για την Πρόληψη και τον Έλεγχο του Ηλεκτρονικού Εγκλήματος εκδόθηκε το 1994 και αντιμετωπίζει συνολικά το ζήτημα αυτό. Με αυτό το τρόπο προτείνει λύσεις που θα μπορέσουν να βοηθήσουν στο πρόβλημα της νομοθεσίας. Είναι η πρώτη συστηματική προσπάθεια σε

διεθνές επίπεδο νομοθετικής προσέγγισης του εγκλήματος. Στην Ομάδα των Οκτώ : (G-8)

Την **ομάδα των Οκτώ** συνθέτουν οι **οκτώ ισχυρότερες χώρες** του κόσμου οι οποίες δημιούργησαν το 1997 μια ομάδα για το Έγκλημα Υψηλής Τεχνολογίας. Η ομάδα αυτή με τη συμμέτοχη των υπουργών εσωτερικών και δικαιοσύνης των οκτώ χωρών, κατέληξε σε **«Δέκα Αρχές»** και **«Δέκα Τομείς Δράσης»** με σκοπό τη διασφάλιση της ενιαίας αντιμετώπισης του εγκληματικού φαινόμενου, σε όλες τις χώρες του κόσμου. Επιπρόσθετα ή Ομάδα των Οκτώ ίδρυσε κι ένα δίκτυο συνεχούς λειτουργίας με σκοπό τη συνεργασία μεταξύ των χώρων σε επίπεδο ερευνών για εγκλήματα υψηλής τεχνολογίας.

ΕΛΛΑΔΑ:

Στην Ελλάδα, όπως έχει ήδη αναφερθεί, δεν υπάρχουν ειδικές διατάξεις για τα εγκλήματα στον Κυβερνοχώρο. Οι περισσότερες υποθέσεις που έχουν προκύψει μέχρι σήμερα έχουν διωχθεί με τις διατάξεις του **Ν. 1805/1988** ο όποιος πρόσθεσε τα άρθρα **370Β** (παράνομη πρόσβαση σε Απόρρητα) και **386Α** (Απάτη με υπολογιστή) στον ποινικό κώδικα. Επίσης το άρθρο **370Α** (παραβίαση του απορρήτου των τηλεπικοινωνιών) και το άρθρο **348Α** (Πορνογραφία Ανηλίκων). Τα άρθρα αυτά συνήθως δεν επαρκούν για τη πλήρη περιγραφή του διαπραχθέντος αδικήματος και την ποινική δίωξη του δράστη διότι δεν έχουν προβλέψει πλήρως και σε κάθε έκταση το ύφος και τις περιστάσεις του εγκλήματος. Αδικήματα που σχετίζονται με τη διασπορά κακόβουλου λογισμικού (Crypto locker) και με επιθέσεις άρνησης εξυπηρέτησης τιμωρούνται με το άρθρο **370Γ** (παραβίαση υπολογιστικών συστημάτων) ή της παράνομης πρόσβασης σε προσωπικά δεδομένα κατά παράβαση του **Ν.2472/97** όπως τροποποιήθηκε και ισχύει. Τα όποια κενα της νομοθεσίας για τα εν λόγο εγκλήματα καλύπτονται συνήθως από τη νομοθεσία των συμβατικών εγκλημάτων. Η Ελλάδα έχει υπογράψει την Ευρωπαϊκή Σύμβαση για το Έγκλημα στον Κυβερνοχώρο αλλά δεν έχει τεθεί ακόμα σε ισχύ. Όταν αυτό θα ισχύσει τότε θα πρόκειται για μεγάλο βήμα της ελληνικής νομοθεσίας στον ποινικό και στο δικονομικό τομέα.

3.9 ΕΥΡΩΠΑΪΚΗ ΣΥΜΒΑΣΗ ΓΙΑ ΤΟ ΈΓΚΛΗΜΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Το Συμβούλιο της Ευρώπης έχει ασχοληθεί τόσο με το ηλεκτρονικό έγκλημα όσο και με το έγκλημα στον κυβερνοχώρο. Έχουν εκδοθεί δύο σχετικές με το θέμα συστάσεις και ειδικότερα: **Η Σύσταση No R** (89) 9 σχετική με το έγκλημα που διαπράττεται με ηλεκτρονικό υπολογιστή (Recommendation No R (89) 9 on Computer related crime) και **Η Σύσταση No R** (95) 13 σχετική με τα ποινικά και δικονομικά προβλήματα που συνδέονται με την τεχνολογία των πληροφοριών (Recommendation No R (95) 13 Problems of criminal procedural Law connected with information technology). Η σπουδαιότητα της σύστασης αυτής είναι πολύ μεγάλη, διότι καθιερώνονται για πρώτη φορά σε διεθνές νομικό κείμενο, οι γενικές δικονομικές αρχές που πρέπει να ισχύουν κατά την έρευνα των ηλεκτρονικών εγκλημάτων. Ήδη καταρτίθηκε Διεθνής Σύμβαση (N. 185, Βουδαπέστη, 23.11.2001) με αντικείμενο την καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Στην κατάρτιση της Σύμβασης αυτής έλαβε μέρος και η Ελλάδα. Σκοπός της είναι η προστασία της Κοινωνίας από το έγκλημα στον κυβερνοχώρο με τη θέσπιση της κατάλληλης νομοθεσίας. Κύριο χαρακτηριστικό της Σύμβασης είναι ότι καθιερώνει την υποχρέωση εναρμόνισης των εθνικών νομοθεσιών σε θέματα εγκλημάτων στον κυβερνοχώρο. Η συζήτηση της Σύμβασης άρχισε τον Απρίλιο του 1997 με αρχικό χρονοδιάγραμμα περάτωσης το τέλος του έτους 1999 ,λόγω όμως των ιδιαιτέρων προβλημάτων (η εξέλιξη της τεχνολογίας και η παρουσία νέων μορφών συμπεριφορών που θα μπορούσαν να θεωρηθούν ως αξιόποινες έτρεχαν ταχύτερα από τις εργασίες της Σύμβασης), η προθεσμία περάτωσης παρατάθηκε μέχρι το τέλος του έτους 2000. Η Σύμβαση περατώθηκε και έχει ήδη υπογραφεί από 33 κράτη. Το Συμβούλιο της Ευρώπης συνειδητοποιεί ότι επήλθαν βαθιές αλλαγές στην ψηφιοποίηση, στη σύγκλιση και στη συνεχιζόμενη παγκοσμιοποίηση των ηλεκτρονικών υπολογιστών.

Εκφράζει λοιπόν την ανησυχία του για την ολοένα αυξανόμενη εγκληματικότητα στον κυβερνοχώρο και αναγνωρίζει ότι η αποτελεσματική αντιμετώπιση του εγκλήματος αυτού μπορεί να γίνει

μόνο με μία πιο αναπτυγμένη, γρήγορη και καλά εφαρμοσμένη διεθνή συνεργασία σε ποινικά θέματα. Διακηρύσσει επίσης ότι κατά την κατάρτιση της Σύμβασης αυτής πρέπει να ληφθεί υπ' όψιν ο σεβασμός των ανθρωπίνων δικαιωμάτων, όπως αυτός αναφέρεται στην Σύμβαση του 1950 του Συμβουλίου της Ευρώπης για την προστασία των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών και στο διεθνές σύμφωνο του 1966 των Ηνωμένων Εθνών για τα αστικά και πολιτικά δικαιώματα, τα οποία αμφότερα επιβεβαιώνουν το δικαίωμα όλων να έχουν άποψη χωρίς παρέμβαση.

Σκοποί της Σύμβασης είναι:

α) η εναρμόνιση των εσωτερικών ποινικών νομοθεσιών των κρατών μελών στον τομέα της εγκληματικότητας στον κυβερνοχώρο,

β) η θέσπιση εσωτερικών δικονομικών ποινικών διατάξεων, που είναι απαραίτητες για την έρευνα, δίωξη και εκδίκαση των εγκλημάτων του κυβερνοχώρου, καθώς και των άλλων εγκλημάτων που διαπράττονται με τη χρήση συστημάτων ηλεκτρονικών υπολογιστών, αλλά και για τη συλλογή αποδεικτικών στοιχείων, που βρίσκονται σε ηλεκτρονική μορφή,

γ) η θέσπιση γρήγορων και αποτελεσματικών κανόνων στον τομέα της διεθνούς συνεργασίας. Διευκρινίζεται ότι προς επίτευξη των παραπάνω αντικειμενικών στόχων λήφθηκαν υπόψη οι εμπειρίες από τη Σύσταση No R (89) 9, η οποία ήταν σχετική με το έγκλημα που διαπράττεται με ηλεκτρονικό υπολογιστή (Recommendation No R (89) 9 on Computer related crime), από τη Σύσταση No R (95) 13 για τα ποινικά δικονομικά προβλήματα που συνδέονται με την τεχνολογία των πληροφοριών, καθώς και εμπειρίες από την καθιέρωση σχετικών κανόνων από άλλους Διεθνείς Οργανισμούς, όπως είναι ο Οργανισμός Ηνωμένων Εθνών, ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (OECD) και η ομάδα των οκτώ πλέον αναπτυγμένων κρατών (G8)" .

ΚΕΦΑΛΑΙΟ 4 Το υπολογιστικό νέφος και η Ψηφιακή του Ανάλυση.

4.1 Εφαρμογή των Digital forensics σε Cloud Computing.

Στα προηγούμενα κεφάλαια αναπτύχθηκαν ως ξεχωριστές έννοιες το υπολογιστικό νέφος και η ψηφιακή εγκληματολογία. Εξετάσθηκαν λοιπόν ορισμοί, έννοιες, νομικά θέματα, προβληματισμοί καθώς και η εφαρμογή νομοθετικού πλαισίου που τις διέπει. Στο κεφάλαιο αυτό θα αναπτύξουμε το κείμενό μας με σκοπό την σύνδεση των δύο εννοιών και θα αναλύσουμε την εφαρμογή της ψηφιακής εγκληματολογίας σε περιβάλλοντα του Cloud, καθώς και κάθε κενό που δύναται να υπάρξει σε νομικό-νομοθετικό επίπεδο στο περιβάλλον του cloud.

Μετά από όσα παρατέθηκαν νωρίτερα, συμπεραίνουμε πως η εγκληματολογική ανάλυση δεδομένων που βρίσκεται αποθηκευμένη στο νέφος επηρεάζεται από πολλούς παράγοντες.

Αν θέλαμε να παραθέσουμε ορισμένους από αυτούς θα μπορούσαμε να καταδείξουμε τους εξής:

1) Κοινή χρήση φυσικών εξυπηρετητών: Περισσότεροι του ενός χρήστες χρησιμοποιούν τις ίδιες υπηρεσίες οι οποίες βρίσκονται αποθηκευμένες σε ένα υπολογιστικό νέφος, πιο συγκεκριμένα ένας χρήστης δύναται να χρησιμοποιεί δεδομένα τα οποία έτερος χρήστης ν τα έχει καταχωρήσει ή ακόμη και να τα έχει διαγράψει.

2) Πολυδικαιοδοσία- Πολυεδαφικότητα: Χρήστες εντός και εκτός συγκεκριμένης επικράτειας αποκτά πρόσβαση σε επίπεδο διαχείρισης στα δεδομένα, τα επεξεργάζεται, τα μεταφέρει τα χρησιμοποιεί. Ακόμη δεν μπορεί να προσδιοριστεί το γεωγραφικό σημείο στο οποίο βρίσκεται ο αποθηκευτικός χώρος υπολογιστικού νέφους. Επίσης, το νομοθετικό πλαίσιο που δύναται να εφαρμοστεί

σε όποια επεξεργασία των δεδομένων διαφέρει και εξαρτάται από τον εκάστοτε χρήστη.

3) Στάδια εξέτασης και αλληλουχία αυτών: Ο ερευνητής οφείλει να προστατεύει και να σέβεται τα δεδομένα που επεξεργάζεται και χρησιμοποιεί, σεβόμενος κάθε νομοθετικό πλαίσιο σε σχέση με αυτά. Λόγω της φύσης και της τοποθεσίας του υπολογιστικού νέφους ο ερευνητής αναγκάζεται να απευθυνθεί στον υπεύθυνο επεξεργασίας, πράγμα που ενέχει κινδύνους, καθώς εμπλέκονται και τρίτα πρόσωπα στην έρευνα. Τέλος ο ερευνητής οφείλει να είναι ιδιαίτερα προσεκτικός για την διασφάλιση της αλληλουχίας των ερευνών, καθώς θα πρέπει να διαφυλάξει στο ακέραιο κάθε δεδομένο που θα λάβει για επεξεργασία.

Τέλος, πολλά από τα εμπόδια που παρατέθηκαν στα προηγούμενα κεφάλαια θα μπορούσαν να προσπεραστούν εφόσον στους όρους της συμφωνίας εμπεριέχονταν ρητές διατάξεις για το πώς θα αντιμετωπίζεται η κάθε κατάσταση (λ.χ. ατομικότητα, πρόσβαση σε δεδομένα προσωπικού χαρακτήρα, απόρρητο επικοινωνίας κ.λπ.). Οι επιλογές του πελάτη, προς το παρόν τουλάχιστον, είναι περιορισμένες, αφού είτε θα πρέπει να δεχθεί τους όρους που θέτει ο πάροχος, είτε να απορρίψει τις υπηρεσίες του.

Κεφάλαιο 5 Επίλογος-Συμπεράσματα.

5.1 Επίλογος

Σύμφωνα με όσα αναλύσαμε παραπάνω καταλήγουμε στο συμπέρασμα ότι είναι εξαιρετικά δύσκολο να κατανοήσουμε τι πραγματικά συμβαίνει μέσα σ' ένα υπολογιστικό νέφος. Ίσως τα πράγματα να ήταν ευκολότερα για τους ερευνητές εάν υπήρχαν τόσο οι εφαρμογές όσο και το νομοθετικό πλαίσιο που θα ανέλυαν και θα όριζαν συγκεκριμένες μεθόδους ανάλυσής τους. Μέχρι σήμερα αν και έχουν γίνει αρκετές προσπάθειες για τη δημιουργία αυτοματοποιημένων εφαρμογών για την ανάλυση των δεδομένων του υπολογιστικού νέφους, οι οποίες μάλιστα θα εξασφάλιζαν την ιδιωτικότητα και τη διαφύλαξη των προσωπικών δεδομένων δεν κατόρθωσαν να λειτουργήσουν αποτελεσματικά διότι παρουσίασαν δυσλειτουργίες στον τρόπο συλλογής, επεξεργασίας και αποθήκευσης των υπό διερεύνηση δεδομένων. Καταλήγουμε λοιπόν, ότι λόγω της μη αποδοτικής αξιοποίησης των εφαρμογών αυτών, σήμερα είμαστε αναγκασμένοι να χρησιμοποιούμε χειροκίνητες επισφαλείς και πιο χρονοβόρες τεχνικές οι οποίες ωστόσο φέρουν το επιθυμητό αποτέλεσμα.

Λόγω αναγκαιότητας της ύπαρξης αποδοτικής τεχνικής σχετικά με την ανάλυση των δεδομένων σ ένα υπολογιστικό νέφος είναι παγκοσμίως αποδεκτή η δεύτερη τεχνική, αυτή της ανάλυσης των δεδομένων από έναν ερευνητή παρά τους υπάρχοντες κινδύνους. Στη χώρα μας και με σκοπό τη διασφάλιση μιας έγκυρης πραγματογνωμοσύνης, η οποία θα αποδίδει πραγματικά την υπάρχουσα κατάσταση και θα διασφαλίζει την αλήθεια στο ακέραιο, χρησιμοποιούνται πραγματογνώμονες οι οποίοι δεν έχουν καμία σχέση με την υπόθεση.

Εν κατακλείδι , καταλήγουμε ομόφωνα στο γεγονός ότι πρέπει να δημιουργηθεί ένα νομοθετικό πλαίσιο σε παγκόσμιο επίπεδο, το οποίο θα είναι κοινώς αποδεκτό και εφαρμόσιμο. Πράγμα που θα διευκολύνει κατά πολύ χρήστες ερευνητές και δικαιοσύνη, και θα θεσπίσει σαφείς κανονισμούς μεταξύ των χρηστών παγκοσμίως.

Βιβλιογραφία

- Ruan, K., Carthy, J., Kechadi, T., & Crosbie, M. (2011, January). Cloud forensics. Στο IFIP International Conference on Digital Forensics (pp. 35-46). Springer Berlin Heidelberg.

- Cloud Computing Strategies, Dimitris N. Chorafas, CRC Press (2011)

- Armbrust, M. et al., (2010). A view of cloud computing. Στο Communications of the ACM, 53(4), pp. 50-58 Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime.
- Brian J.S Chee and Curtis Franklin, Sr(2010, σελ.168)

- Cloud Computing Technologies and Strategies.CRC Press Anthony T. Velve, Toby J. Velve, Robert Elsenpeter (2010)

- Simou, S., Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2014, June). Cloud forensics: identifying the major issues and challenges. Στο International Conference on Advanced Information Systems Engineering (pp. 271-284).

- Dhage, S. N., Meshram, B. B. (2012). Intrusion detection system in cloud computing environment. Στο International Journal of Cloud Computing, 1(2-3), 261-282

- Ghemawat, S., Gobioff, H., Leung, S. T. (2003). The Google file system. Στο ACM SIGOPS operating systems review

- Haeberlen, A. (2010). A case for the accountable cloud.

- Kotzanikolaou, P. (2008). Data retention and privacy in electronic• communications. Στο IEEE Security & Privacy.

- Lalas, E., Mitrou, L., Lambrinoudakis, C. (2013, August). Procave: Privacypreserving collection and authenticity validation of online evidence. Στο International Conference on Trust, Privacy and Security in Digital Busines.

- Marangos N., Rizomiliotis P., Mitrou L. (2014). Time synchronization: pivotal element in cloud forensics. Security and Communication Networks.

- Geir M. Koien, Vladimir A. Oleshchuk. Personal Privacy in a Digital World.

- Armbrust, M. et al., (2010). A view of cloud computing.

- Mather T. , Kumaraswamy S., Shahed Latif , Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance (Theory in Practice), O'Reilly Media, Inc. 2009

- Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1'', December 2009.

- Galen G., "What cloud computing really means", InfoWorld, Retrieved 02-06-2009
  Opinion 05/2012 on Cloud Computing, Article 29 Data Protection Working Party, Adopted July 1st 2012

- Cloud Computing - article by "Communications of the ACM" magazine, (2008)

- Cloud Computing – Issues, Research and Implementations, Mladen A. Vouk

  - Μήτρου, Λ., «Η προστασία της Ιδιωτικότητας στην Πληροφορική και στις Επικοινωνίες – Η νομική διάσταση», Τμήμα Μηχανικών & Πληροφοριακών Συστημάτων, Πανεπιστήμιο Αιγαίου.

  - Κάτσικας, Σ, Γκρίτζαλης, Δ., & Γκρίτζαλης, Στ. (2004), «Ασφάλεια πληροφοριακών συστημάτων», Εκδόσεις νέων τεχνολογιών, Αθήνα.

  - Αρχή Προστασία Δεδομένων Προσωπικού Χαρακτήρα, «Ελληνική Νομοθεσία για την Προστασία των Προσωπικών Δεδομένων»

  - Σύμβαση για την Προστασία των Δικαιωμάτων του Ανθρώπου και των Θεμελιωδών Ελευθεριών, όπως τροποποιήθηκε από τα Πρωτόκολλα υπ' αριθ. 11 και 14, Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου.

- Μήτρου, Λ., «Η προστασία της Ιδιωτικότητας στην Πληροφορική και στις Επικοινωνίες – Η νομική διάσταση», Τμήμα Μηχανικών & Πληροφοριακών Συστημάτων, Πανεπιστήμιο Αιγαίου.

- Service Level Agreement in Cloud Computing

http://knoesis.wright.edu/library/download/OOPSLA_cloud_wsla_v3.pdf

- Outsourcing Business to Cloud Computing Services: Opportunities and Challenges http://www.lrr.in.tum.de/~gerndt/home/Teaching/CloudComputing/20111006112649503.pdf

- Towards Trusted Cloud Computing http://static.usenix.org/event/hotcloud09/tech/full_papers/santos.pdf

- Cloud Computing Privacy Concerns on our Doorstep http://old-lipn.univ-paris13.fr/~choppy/IFIP/WINCHESTER-2011/WINCH-DATA/p36CACM-ryan.pdf

- A View Of Cloud Computing http://delivery.acm.org/10.1145/1730000/1721672/p50-armbrust.pdf?ip=46.198.82.106&acc=OPEN&CFID=281253423&CFTOKEN=58883976&__acm__=1361660528_85a95927bcc000b1d7c33e6503875ec0

- The NIST Definition of Cloud Computing, National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

- An Early Performance Analysis of Cloud Computing Services for Scientific Computing http://www.cs.princeton.edu/courses/archive/spring11/cos448/web/docs/week7_optional1.pdf

- http://www.dpa.gr

- https://en.wikipedia.org/wiki/Cloud_computing

- http://www.nist.gov

- http://www.lawnet.gr/pages/eofn/2/cybercrime.asp