Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή στα Πληροφοριακά και Επικοινωνιακά Συστήματα

Ζητήματα Ασφάλειας και Προστασίας της Ιδιωτικότητας σε Πληροφοριακά Συστήματα στη Δημόσια Διοίκηση και σε περιβάλλοντα Κρίσιμων Υποδομών (Critical Infrastructure) που αξιοποιούν τεχνολογίες Νέφους (Cloud).

ΠΑΤΤΑΚΟΥ ΑΡΓΥΡΗ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΣΤΕΦΑΝΟΣ ΓΚΡΙΤΖΑΛΗΣ

ΙΟΥΝΙΟΣ 2014

Ανοικτό Πανεπιστήμιο Κύπρου
Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Ζητήματα Ασφάλειας και Προστασίας της Ιδιωτικότητας σε Πληροφοριακά Συστήματα στη Δημόσια Διοίκηση και σε περιβάλλοντα Κρίσιμων Υποδομών (Critical Infrastructure) που αξιοποιούν τεχνολογίες Νέφους (Cloud).

ΠΑΤΤΑΚΟΥ ΑΡΓΥΡΗ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΣΤΕΦΑΝΟΣ ΓΚΡΙΤΖΑΛΗΣ

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στα Πληροφοριακά Συστήματα

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

ΙΟΥΝΙΟΣ 2014

Περίληψη

Στις μέρες μας, η τεχνολογία της Νεφοϋπολογιστικής παρουσιάζει παγκοσμίως μία ραγδαία ανάπτυξη και ένα ιδιαίτερο ενδιαφέρον, ενώ όλο και περισσότερα φυσικά πρόσωπα, Ιδιωτικοί ή Δημόσιοι Οργανισμοί υιοθετούν τεχνολογίες Νέφους για την παροχή υπηρεσιών, την ανάπτυξη εφαρμογών ή απλά ως μέσο αποθήκευσης Δεδομένων. Η βασική ιδέα της Νεφοϋπολογιστικής είναι ο διαμοιρασμός πόρων, λογισμικού και πληροφοριών μεταξύ πολλών χρηστών, ενώ τείνει να μεταστρέψει το παραδοσιακό IT μοντέλο σε μοντέλο παροχής Υπηρεσιών. Οι τεχνολογίες Νέφους παρέχουν τη δυνατότητα στους χρήστες να αποθηκεύουν τα Δεδομένα τους σε απομακρυσμένα Data Center ενώ μπορούν να έχουν πρόσβαση σε αυτά ανά πάσα στιγμή και από οποιοδήποτε υπολογιστή. Η Νεφοϋπολογιστική ευελπιστεί να καλύψει τις ανάγκες των χρηστών στο πεδίο της επιστημονικής έρευνας, στο ηλεκτρονικό εμπόριο, στη διοικητική μεταρρύθμιση και σε πλήθος άλλων πεδίων εφαρμογής.

Στην παρούσα εργασία, εκτός από την παρουσίαση των βασικών εννοιών και χαρακτηριστικών της Νεφοϋπολογιστικής, θα ασχοληθούμε με τα ζητήματα της Ασφάλειας και της Ιδιωτικότητας που ανακύπτουν έπειτα από την υιοθέτηση της Νεφοϋπολογιστικής σε Πληροφοριακά Συστήματα της Δημόσιας Διοίκησης και των Κρίσιμων Υποδομών ενός Κράτους. Μέσα στο πλαίσιο αυτό θα μελετηθούν τα βραχυπρόθεσμα και μακροπρόθεσμα ζητήματα που ενδεχομένως θα κληθούν να αντιμετωπίσουν οι υπεύθυνοι ενός Δημόσιου Οργανισμού ή η γενική Κυβέρνηση στην προσπάθεια τους να παρέχουν Υπηρεσίες, είτε προς τους πολίτες είτε μεταξύ των Δημόσιων Οργανισμών, κάνοντας εκτεταμένη χρήση της Cloud Computing τεχνολογίας.

Ωστόσο, η ραγδαία ανάπτυξη της τεχνολογίας αυτής αλλά και η έκταση του πεδίου εφαρμογής της δε θα μπορούσε να μη διέπεται από ένα αυστηρά καθορισμένο νομικό πλαίσιο. Η Ευρωπαϊκή Ένωση έχει εκδώσει από το 1995 μία πλήρη οδηγία, με σκοπό να ενσωματωθεί στη Νομοθεσία που διέπει το κάθε κράτος-μέλος της. Από την άλλη πλευρά, οι Ηνωμένες Πολιτείες της Αμερικής, παρά το γεγονός ότι θεωρούνται πρωτοπόροι στην υιοθέτηση τεχνολογιών Νέφους, δεν διαθέτουν ένα ολοκληρωμένο Νομικό Πλαίσιο που να διέπει τη λειτουργία των Παρόχων και τη χρήση της αναπτυσσόμενης αυτής τεχνολογίας. Το Νομικό πλαίσιο καθώς και το πλαίσιο που καθορίζει τις σχέσεις μεταξύ Παρόχων-χρηστών θα μελετηθεί ακολούθως.

Στη συνέχεια της εργασίας πρόκειται να παρουσιαστούν διαφορετικές περιπτώσεις εφαρμογής της Νεφοϋπολογιστικής σε Δημόσιους Οργανισμούς παγκοσμίως, όπως για παράδειγμα στην Ελλάδα, σε άλλες Ευρωπαϊκές χώρες, στην Ιαπωνία, στην Ινδία αλλά και στις Ηνωμένες Πολιτείες της Αμερικής. Ωστόσο, ιδιαίτερη έμφαση πρόκειται να δοθεί στο σχεδιασμό και την τήρηση μίας σωστής στρατηγικής για τη μετάβαση των Δημόσιων Υπηρεσιών στο Νέφος. Στο σημείο αυτό, θα γίνει ιδιαίτερη μνεία τόσο στην επιλογή των Υπηρεσιών που πρόκειται να μεταφερθούν στο Νέφος όσο και στο μοντέλο του Νέφους που θα επιλεχθεί, προκειμένου να υποστηριχθούν σωστά οι Υπηρεσίες που θα μεταβούν.

Παρά το γεγονός ότι η Νεφοϋπολογιστική αποτελεί μία ιδιαίτερα δελεαστική λύση με ευρύ πεδίο εφαρμογής, πολλοί είναι οι ερευνητές εκείνοι που εγείρουν σημαντικά ζητήματα αναφορικά με την Ασφάλεια και την Ιδιωτικότητα των Πληροφοριών στις

Υποδομές Νέφους ενώ παράλληλα ανησυχίες εκφράζονται και για την μετάβαση των Κρίσιμων Υποδομών ενός Κράτους στο Νέφος. Τα ζητήματα αυτά θα παρουσιαστούν στη συνέχεια.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου κ. Στέφανο Γκρίτζαλη για τη διαρκή καθοδήγηση και συμπαράσταση που μου προσέφερε σε όλη τη διάρκεια εκπόνησης της εργασίας αυτής.

Περιεχόμενα

Κεφάλαιο 1ο

Ανάλυση Θεμελιωδών Εννοιών

Η Νεφοϋπολογιστική ή αλλιώς Cloud Computing αποτελεί μία νέα τεχνολογία η οποία αναπτύσσεται με ραγδαίους ρυθμούς παγκοσμίως, ενώ παράλληλα βρίσκει εφαρμογή σε ολοένα και περισσότερους τομείς. Την τελευταία δεκαετία επιδεικνύεται ιδιαίτερο ενδιαφέρον για την εφαρμογή της Νεφοϋπολογιστικής στη Δημόσια Διοίκηση, με σκοπό την παροχή ποιοτικότερων και αποτελεσματικότερων υπηρεσιών είτε προς τους πολίτες είτε μεταξύ των Δημόσιων Φορέων ή ακόμη και για την ενίσχυση της διαλειτουργικότητας των κυβερνήσεων διαφορετικών Κρατών. Στο Κεφάλαιο αυτό παρουσιάζονται τα βασικά χαρακτηριστικά, τα διαθέσιμα μοντέλα υπηρεσιών και εφαρμογών που παρέχονται σήμερα και τα σημαντικότερα οφέλη της τεχνολογίας της Νεφοϋπολογιστικής. Ακολουθεί μία σύντομη περιγραφή των θεμελιωδών εννοιών που σχετίζονται με την Ασφάλειας και την προστασία της Ιδιωτικότητας σε περιβάλλον Νέφους.

1.1 Εισαγωγή στην έννοια της Υπολογιστικής Νέφους (Cloud Computing)

Η «Υπολογιστική Νέφους» ή αλλιώς «Cloud Computing» συνιστά μία νέα τεχνολογία, με σκοπό να διευκολύνει την αποθήκευση, την επεξεργασία και τη χρήση των δεδομένων σε απομακρυσμένους υπολογιστές μέσω διαδικτύου. Πρόκειται αναμφίβολα για μία ταχέως αναπτυσσόμενη τεχνολογία, η οποία αναμένεται να προσφέρει πολλαπλά οφέλη στην παγκόσμια οικονομία, προσφέροντας φθηνότερη υπολογιστική ισχύ και ευκολότερη πρόσβαση στα δεδομένα και τις εφαρμογές. Εξαιτίας αυτού του παγκόσμιου ενδιαφέροντος, πολλοί ορισμοί δόθηκαν κατά καιρούς αναφορικά με τις έννοιες που αναφέρονται στην Cloud Computing τεχνολογία. Το National Institute of Standards and Technology (NIST) έχει ορίσει με μεγάλη σαφήνεια και ακρίβεια όλες αυτές τις έννοιες που σχετίζονται με τη Νεφοϋπολογιστική, έτσι ώστε να δημιουργήσει ένα κοινό πρότυπο επικοινωνίας.

Βασικές έννοιες κατά NIST [01]:

- *Cloud Customer (Χρήστης Υπηρεσιών Νέφους):* Αποτελεί οποιοδήποτε φυσικό πρόσωπο ή οργανισμός, ο οποίος χρησιμοποιεί Cloud Υπηρεσίες διαμέσου κάποιου Παρόχου.

- *Cloud Provider (Πάροχος Υπηρεσιών Νέφους):* Αποτελεί οποιοδήποτε φυσικό πρόσωπο ή οργανισμό ή οντότητα που είναι υπεύθυνη για τη διαθεσιμότητα των παρεχόμενων Υπηρεσιών στους χρήστες.

- *Cloud Access (Πρόσβαση):* Η επικοινωνία ή η πρόσβαση στις παρεχόμενες Cloud Υπηρεσίες.

Ορισμός «Cloud Computing» κατά NIST [01]:

Ως Cloud Computing ορίζεται το μοντέλο εκείνο που επιτρέπει την ευέλικτη, on-demand δικτυακή πρόσβαση σε ένα κοινόχρηστο σύνολο παραμετροποιήσιμων υπολογιστικών πόρων (π.χ. δίκτυα, servers, αποθηκευτικοί χώροι, εφαρμογές και υπηρεσίες) και το οποίο μπορεί να τροφοδοτηθεί γρήγορα και να διατεθεί με ελάχιστες απαιτήσεις διαχείρισης ή αλληλεπίδραση με τον Πάροχο της υπηρεσίας. Αυτό το Cloud μοντέλο προωθεί την διαθεσιμότητα και αποτελείται από πέντε βασικά χαρακτηριστικά, τρία μοντέλα παροχής υπηρεσιών, και τέσσερα μοντέλα ανάπτυξης.

1.1.1 Βασικά χαρακτηριστικά Νέφους

Η μετάβαση ενός οργανισμού, από την παραδοσιακή IT μορφή στο Νέφος, αποτελεί ένα ιδιαίτερα σημαντικό βήμα για την επέκταση των τεχνολογικών ικανοτήτων και δυνατοτήτων του οργανισμού, χωρίς να απαιτείται επιπλέον επένδυση σε υλικοτεχνική Υποδομή, σε εκπαίδευση προσωπικού ή στην αγορά νέου λογισμικού. Η Νεφοϋπολογιστική παρέχει συνδρομητικές υπηρεσίες, σε πραγματικό χρόνο μέσω Διαδικτύου, επεκτείνοντας σημαντικά τις IT δυνατότητες. Ακολούθως περιγράφονται τα πέντε πιο σημαντικά χαρακτηριστικά του Νέφους, όπως περιγράφονται από το NIST [01]:

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

- *Ευρεία πρόσβαση στο δίκτυο – άμεση ανταπόκριση:* Οι δυνατότητες είναι διαθέσιμες μέσω του δικτύου και προσβάσιμες μέσω τυποποιημένων μηχανισμών και πλατφόρμες (π.χ. κινητά τηλέφωνα, φορητούς υπολογιστές και PDAs). Με τις υπηρεσίες Cloud, ακόμα και οι μη αναμενόμενες αιχμές κίνησης μπορούν να γίνουν πια διαχειρίσιμες με ικανοποιητικό τρόπο.

- *Κοινή διάθεση των πόρων (Resource Polling):* Οι υπολογιστικοί πόροι του Παρόχου χρησιμοποιούνται για να εξυπηρετήσουν πολλαπλούς καταναλωτές με τη χρήση του μοντέλου πολλαπλών μισθώσεων (multi-tenant), με τους διάφορους φυσικούς και εικονικούς πόρους να ανατίθενται δυναμικά και εκ νέου 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 data center). Παραδείγματα πόρων αποτελούν οι αποθηκευτικοί χώροι, η επεξεργασία, η μνήμη, το bandwidth του δικτύου, καθώς και οι εικονικές μηχανές.

- *Ταχεία ελαστικότητα (Rapid Elasticity):* 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.

- *Μετρήσιμα επίπεδα παροχής υπηρεσιών (Measured Service):* 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.

1.1.2 Μοντέλα ανάπτυξης Νέφους

Τα βασικά κριτήρια τα οποία καθορίζουν την κατηγοριοποίηση των μοντέλων της Νεφοϋπολογιστικής είναι τόσο το σημείο από το οποίο παρέχονται οι Cloud Υπηρεσίες όσο και το επίπεδο της πρόσβασης σε αυτές. Σύμφωνα με τα δύο αυτά κριτήρια τα μοντέλα εφαρμογών διαχωρίζονται ως εξής:

- *Private Cloud:* Η Cloud υποδομή λειτουργεί αποκλειστικά και μόνο για έναν. Η διαχείρισή της μπορεί να γίνεται από τον ίδιο τον οργανισμό ή από τρίτους και μπορεί να βρίσκεται εντός ή εκτός των εγκαταστάσεων του οργανισμού.

- *Community Cloud:* Η Cloud υποδομή μοιράζεται μεταξύ πολλών οργανισμών και υποστηρίζει μια συγκεκριμένη κοινότητα που έχει κοινές ανησυχίες (π.χ. αποστολή, απαιτήσεις ασφαλείας, πολιτική και θέματα συμμόρφωσης). Η διαχείρισή της μπορεί να γίνεται από τον ίδιο τον οργανισμό ή από τρίτους και μπορεί να βρίσκεται εντός ή εκτός των εγκαταστάσεων του οργανισμού.

- *Public Cloud:* Η Cloud υποδομή διατίθεται στο ευρύ κοινό ή σε μια μεγάλη ομάδα εταιρειών και ανήκει σε έναν οργανισμό που πουλά υπηρεσίες Cloud (Πάροχος Υπηρεσιών Νέφους).

- *Hybrid Cloud:* Η Cloud υποδομή είναι μια σύνθεση από δύο ή περισσότερα Cloud (private, Community or public) τα οποία παραμένουν μοναδικές οντότητες, αλλά συνδέονται μεταξύ τους με τυποποιημένη ή αποκλειστική τεχνολογία που επιτρέπει τη φορητότητα δεδομένων και εφαρμογών (π.χ. εξισορρόπηση φόρτου εργασίας μεταξύ των Cloud).

1.1.3 Μοντέλα Παροχής Υπηρεσιών

Η κατηγοριοποίηση βασίζεται στην υπηρεσία για την οποία αναπτύχθηκε να παρέχει η Cloud τεχνολογία.

- *Λογισμικό ως Υπηρεσία (Cloud Software as a Service - SaaS):* Η δυνατότητα που παρέχεται στον καταναλωτή είναι να χρησιμοποιεί τις εφαρμογές του Παρόχου που τρέχουν σε μια Cloud υποδομή. Οι εφαρμογές είναι προσβάσιμες από διάφορες Client συσκευές, όπως ένα πρόγραμμα περιήγησης στο Web (π.χ. Web-based email). Ο καταναλωτής δεν έχει τη διαχείριση ή τον έλεγχο της χρησιμοποιούμενης Cloud υποδομής συμπεριλαμβανομένων των δικτύων, των server, των λειτουργικών συστημάτων, των αποθηκευτικών μονάδων, ή ακόμα και μεμονωμένων δυνατοτήτων της εφαρμογής, εκτός από την πιθανή εξαίρεση κάποιων περιορισμένων user-specific ρυθμίσεων παραμετροποίησης των εφαρμογών.

  Ως χαρακτηριστικά παραδείγματα SaaS Υπηρεσιών αναφέρονται:

1. E-mail and Office Productivity: Περιλαμβάνει εφαρμογές γραφείου, όπως επεξεργασία κειμένου, λογιστικά φύλλα, παρουσιάσεις και εφαρμογές ηλεκτρονικού ταχυδρομείου.

2. Διαχείριση Ανθρώπινου Δυναμικού: Περιλαμβάνει εφαρμογές διαχείρισης ανθρώπινων πόρων εντός επιχείρησης.

3. Οικονομική Διαχείριση: Περιλαμβάνει εφαρμογές διαχείρισης οικονομικών διαδικασιών, όπως διαχείριση εξόδων, τιμολόγηση και φορολογική διαχείριση.

4. Collaboration: Περιλαμβάνει εργαλεία που επιτρέπουν τη συνεργασία των χρηστών μεταξύ ομάδων εργασίας της ίδια επιχείρησης ή ακόμα και μεταξύ ομάδων εργασίας διαφορετικών επιχειρήσεων.

- *Cloud Platform as a Service (PaaS):* Η δυνατότητα που παρέχεται στον καταναλωτή να αναπτύσσει πάνω στην Cloud Υποδομή εφαρμογές που έχει δημιουργήσει ή εφαρμογές που έχει αποκτήσει, οι οποίες έχουν δημιουργηθεί με χρήση γλωσσών προγραμματισμού και εργαλείων που υποστηρίζονται από τον Πάροχο. Ο καταναλωτής δεν διαχειρίζεται ούτε ελέγχει τη σχετική Cloud Υποδομή (που συμπεριλαμβάνει τα δίκτυα, τους server, τα λειτουργικά συστήματα ή τα αποθηκευτικά μέσα), αλλά έχει τον έλεγχο των εφαρμογών που έχουν αναπτυχθεί, και ενδεχομένως, των παραμετροποιήσεων του περιβάλλοντος φιλοξενίας των εφαρμογών.

  Ως χαρακτηριστικά παραδείγματα PaaS Υπηρεσιών αναφέρονται:

  1. Business Intelligence: Πλατφόρμες για την ανάπτυξη εφαρμογών, όπως συστήματα αναφορών (reports) και ανάλυσης δεδομένων.

  2. Βάσεις Δεδομένων: Υπηρεσίες επέκτασης των σχεσιακών βάσεων δεδομένων.

  3. Ανάπτυξη και Testing εφαρμογών: Πλατφόρμες για την ανάπτυξη και δοκιμή των υπό ανάπτυξη εφαρμογών.

  4. Integration: Πλατφόρμα για τη δημιουργία Integration εφαρμογών σε Cloud στο πλαίσιο μίας επιχείρησης.

  5. Ανάπτυξη Εφαρμογών: Πλατφόρμες κατάλληλες για ανάπτυξη εφαρμογών γενικού σκοπού. Οι υπηρεσίες αυτές παρέχουν βάσεις δεδομένων και περιβάλλον εκτέλεσης Web εφαρμογών.

- *Cloud Infrastructure as a Service (IaaS):* Η δυνατότητα που παρέχεται στον καταναλωτή να μπορεί να δεσμεύσει επεξεργαστική ισχύ, αποθηκευτικά μέσα, δίκτυα, και άλλους υπολογιστικούς πόρους, έτσι ώστε να αναπτύξει και να εκτελέσει αυθαίρετο λογισμικό, όπως λειτουργικά συστήματα και

εφαρμογές. Ο καταναλωτής δεν έχει τη διαχείριση ή τον έλεγχο της χρησιμοποιούμενης Cloud Υποδομής, αλλά έχει τον έλεγχο των Λειτουργικών Συστημάτων, των αποθηκευτικών μέσων, των εφαρμογών που έχουν αναπτυχθεί και πιθανόν κάποιον περιορισμένο έλεγχο επιλεγμένου εξοπλισμού δικτύωσης (π.χ. Firewalls). Επίσης, διαθέτει απομακρυσμένες εικονικές μηχανές, οι οποίες συμπεριφέρονται ακριβώς όπως οι φυσικές ισοδύναμές τους.

Ως χαρακτηριστικά παραδείγματα IaaS Υπηρεσιών αναφέρονται:

1. Backup και Recovery: Υπηρεσίες για την δημιουργία αντιγράφων ασφαλείας και ανάκτησης αρχείων.

2. Compute: Παροχή υπολογιστικών πόρων για την εκτέλεση Cloud συστημάτων και τα οποία μπορούν να παραμετροποιηθούν δυναμικά ανάλογα με τις ανάγκες του χρήστη.

3. Υπηρεσίες Διαχείρισης: Υπηρεσίες που διαχειρίζονται πλατφόρμες της Cloud Υποδομής. Τα εργαλεία αυτά παρέχουν συχνά τα χαρακτηριστικά που οι Cloud Πάροχοι Υπηρεσιών δεν παρέχουν ή ειδικεύονται στη διαχείριση ορισμένων τεχνολογικών εφαρμογών.

4. Αποθήκευση: Παρέχεται τεράστια επεκτάσιμη χωρητικότητα αποθήκευσης που μπορεί να χρησιμοποιηθεί για εφαρμογές, δημιουργία αντιγράφων ασφαλείας, αρχειοθέτησης και αποθήκευσης αρχείων.

1.1.4 Οφέλη από τη χρήση Υπηρεσιών Νέφους [05]

Η λύση των Cloud Υπηρεσιών, όπως διαμορφώνεται σήμερα, μπορεί να προσφέρει σημαντικό πλεονέκτημα, έναντι των παραδοσιακών μορφών IT σε οργανισμούς κάθε μεγέθους. Ο κάθε Δημόσιος ή Ιδιωτικός οργανισμός οφείλει να εξετάσει προσεκτικά τα οφέλη που προκύπτουν από την υιοθέτηση της νέας τεχνολογίας, πριν την απόφαση για μετάβαση των συστημάτων και των υπηρεσιών της. Μερικά από τα οφέλη που θα πρέπει να αξιολογηθούν αναφέρονται ακολούθως.

- *Σημαντική Μείωση του κόστους*: Από τη χρήση Cloud υπηρεσιών και συστημάτων προκύπτει σημαντική εξοικονόμηση πόρων σε σχέση με τις παραδοσιακές IT Υπηρεσίες. Για παράδειγμα, μία επιχείρηση μεσαίου ή μεγάλου μεγέθους απαλλάσσεται από την απαίτηση διατήρησης ενός data center με ακριβό εξοπλισμό και λογισμικό, καθώς μπορεί εύκολα να νοικιάζει υπολογιστικούς πόρους ανά πάσα στιγμή και μόνο για τη διάρκεια κατά την οποία αυτοί απαιτούνται. Επίσης, αποφεύγεται η περίπτωση αγοράς πλεονάζοντος εξοπλισμού και λογισμικού καθώς στο Νέφος οι επιχειρήσεις πληρώνουν ακριβώς για αυτά που χρησιμοποιούν, ενώ ανά περίοδο συνδρομής μπορούν τα μεγέθη αυτά να τα αυξομειώνουν ανάλογα με τις εκάστοτε ανάγκες τους [03].

- *Ευελιξία:* Αφορά κυρίως την κατ΄ απαίτηση δέσμευση και αποδέσμευση υπολογιστικών πόρων με αποτέλεσμα την αποτελεσματική προσαρμογή των πληροφοριακών συστημάτων, ανάλογα με τις εκάστοτε ανάγκες του κάθε χρήστη.

- *Εύκολη πρόσβαση σε δεδομένα και εφαρμογές:* Τα δεδομένα και οι εφαρμογές φυλάσσονται σε data center του Παρόχου ενώ επιτρέπεται η πρόσβαση σε αυτά ανά πάσα στιγμή και από οποιαδήποτε υπολογιστική μηχανή με πρόσβαση στο Διαδίκτυο.

- *Ασφάλεια και Αξιοπιστία:* Αυξάνεται η ικανότητα ανάκαμψης ενός Πληροφοριακού Συστήματος σε περίπτωση καταστροφής. Είναι φυσικό οι Πάροχοι Cloud Υπηρεσιών να παρέχουν καλύτερες πολιτικές ασφάλειας από ένα μικρομεσαίο οργανισμό γιατί αφενός μεν χρησιμοποιούν ειδικούς εμπειρογνώμονες και αφετέρου ακολουθούν πιστοποιημένες διαδικασίες ασφαλείας. Επίσης, για το λόγο ότι εξειδικεύονται στο αντικείμενο αυτό, είναι πολύ ευκολότερο να χτίσουν συστήματα υψηλής αξιοπιστίας ώστε να προστατεύουν και να υποστηρίζουν τα συστήματα χιλιάδων αντίστοιχων επιχειρήσεων [03].

- *Υπηρεσίες Υποστήριξης:* Οι περισσότεροι αξιόπιστοι Πάροχοι διαθέτουν μεγάλη αποθηκευτική ικανότητα και υπολογιστική ισχύ καθώς και 24ωρη υποστήριξη των χρηστών.

Ως επιπλέον πλεονεκτήματα από τη χρήση Cloud υποδομών αναφέρονται:

- Εύκολη υλοποίηση Πληροφοριακών Συστημάτων καθώς δεν απαιτείται η αγορά του ανάλογου hardware, software ή Πνευματικών Δικαιωμάτων.
- Pay as you go: Ο χρήστης ή ο Οργανισμός υποχρεούται να καταβάλει αντίτιμο μόνο για όποιες Υπηρεσίες χρησιμοποίησε, ενώ δικαιούται να αναπροσαρμόζει τις ανάγκες και τις επιλογές του ανά πάσα στιγμή.
- Εύκολος διαμοιρασμός αρχείων και προώθηση της συνεργασίας μεταξύ διαφορετικών ομάδων εργασίας εντός ή εκτός του οργανισμού.
- Δυνατότητα πρόσβασης στο πλέον ενημερωμένο λογισμικό.
- Μείωση της απαιτούμενης IT υποδομής εντός του οργανισμού σε σχέση με τα παραδοσιακά IT τμήματα, με αποτέλεσμα τη μείωση του κόστους προμήθειας και συντήρησής του.

Από τα προαναφερόμενα, μπορεί εύκολα να αντιληφθεί κανείς ότι η Νεφοϋπολογιστική παρέχει τεράστιες δυνατότητες σε κάθε αυτόνομο χρήστη, σε μία επιχείρηση ή σε ένα Δημόσιο Οργανισμό. Τα πλεονεκτήματα που περιγράφησαν αποτελούν ένα μικρό δείγμα καθώς τα οφέλη πληθαίνουν όσο επεκτείνονται οι δυνατότητες της τεχνολογίας αυτής και ανάλογα με το πεδίο που αυτή εφαρμόζεται. Ωστόσο, θα πρέπει να αναφερθεί ότι κατά καιρούς πολλά ζητήματα έχουν τεθεί από μελετητές παγκοσμίως σχετικά με την ασφάλεια των πληροφοριών που διατηρούνται στις υποδομές Νέφους. Πολλά από αυτά τα ζητήματα έχουν πλέον εξαλειφθεί, ωστόσο κάποια είναι ακόμα υπαρκτά. Οι απαιτήσεις για ασφάλεια και προστασία της Ιδιωτικότητας σε μία Υποδομή Νέφους, καθώς και οι σχετικές έννοιες περιγράφονται στη ακόλουθη ενότητα.

1.2 Ασφάλεια και Προστασία της Ιδιωτικότητας σε περιβάλλον Νέφους

1.2.1 Δεδομένα που χρήζουν προστασίας

Κατά καιρούς πολλοί ορισμοί έχουν αποδοθεί αναφορικά με την έννοια των «Δεδομένων» και της «Πληροφορίας». Ενδεικτικά, ορίζονται:

- *Δεδομένα (Data)* είναι ένα σύνολο κατανοητών συμβόλων που έχουν καταγραφεί [12].

- *Πληροφορία (Information)* είναι τα Δεδομένα μαζί με την έννοια που τους αποδίδεται [12].

Στην ελληνική Νομοθεσία ενσωματώθηκαν, υπό την εποπτεία της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, ο Νόμος 2472/1997 που αφορά την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και ο Νόμος 3471/2006 που αφορά την προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών.

Σύμφωνα με την ανεξάρτητη «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα» και με την κείμενη Νομοθεσία, ως Προσωπικά Δεδομένα νοείται «*κάθε πληροφορία που αναφέρεται και περιγράφει ένα άτομο όπως: στοιχεία αναγνώρισης (ονοματεπώνυμο, ηλικία, κατοικία, επάγγελμα, οικογενειακή κατάσταση κλπ.), φυσικά χαρακτηριστικά, εκπαίδευση, εργασία (προϋπηρεσία, εργασιακή συμπεριφορά κλπ), οικονομική κατάσταση (έσοδα, περιουσιακά στοιχεία, οικονομική συμπεριφορά), ενδιαφέροντα, δραστηριότητες, και συνήθειες*.» [13] [15] .

Επίσης, ορίζονται ως Ευαίσθητα Προσωπικά Δεδομένα «*τα προσωπικά δεδομένα ενός ατόμου που αναφέρονται στη φυλετική ή εθνική του προέλευση, στα πολιτικά του φρονήματα, στις θρησκευτικές ή φιλοσοφικές του πεποιθήσεις, στη συμμετοχή του σε συνδικαλιστική οργάνωση, στην υγεία του, στην κοινωνική του πρόνοια, στην ερωτική του ζωή, τις ποινικές διώξεις και καταδίκες του, καθώς και στη συμμετοχή του σε συναφείς με τα ανωτέρω ενώσεις προσώπων*». Τα ευαίσθητα δεδομένα προστατεύονται από τον Νόμο με αυστηρότερες ρυθμίσεις από ότι τα απλά προσωπικά δεδομένα [13] [15].

1.2.2 Ασφάλεια των Δεδομένων στο Νέφος

Η ασφάλεια πληροφοριών (Information Security) και πληροφοριακών συστημάτων (IT Security), αποτελεί ένα από τα πιο σύνθετα θέματα για κάθε φυσικό πρόσωπο, επιχείρηση και οργανισμό. Αποτελεί ένα πολυδιάστατο ζήτημα το οποίο αγγίζει κάθε επιχειρησιακό επίπεδο ή διαδικασία. Το Wikipedia [08] αναφέρει ότι «Ασφάλεια των Δικτύων των Υπολογιστών θεωρείται η δυνατότητα ενός δικτύου ή συστήματος πληροφοριών να αντισταθεί, σε δεδομένο επίπεδο αξιοπιστίας, σε τυχαία συμβάντα ή κακόβουλες ενέργειες που θέτουν σε κίνδυνο τη διάθεση, την επαλήθευση

ταυτότητας, την ακεραιότητα και την τήρηση του απορρήτου των δεδομένων που έχουν αποθηκευτεί ή μεταδοθεί καθώς και τις συναφείς υπηρεσίες που παρέχονται είτε είναι προσβάσιμες μέσω των δικτύων και συστημάτων αυτών.»

Αναφορικά με το μοντέλο Cloud Computing, εξαιτίας της κατανεμημένης αρχιτεκτονικής του, απαιτεί αυξημένη κίνηση δεδομένων και πληροφοριών μέσω δικτύων. Η αυξημένη έκθεση των δεδομένων μεταξύ των διαδικτυακών υποδομών ελλοχεύει κινδύνους σχετικά με την Ασφάλεια των Πληροφοριών.

Το NIST (National Institute of Standards and Technology) [01] έχει δώσει σαφής ορισμούς αναφορικά με τις έννοιες της Ασφάλειας και της Ιδιωτικότητας σε Cloud περιβάλλον. Συγκεκριμένα ορίζεται ως:

1. *Security (Ασφάλεια της Πληροφορίας):* Η ασφάλεια της Πληροφορίας αναφέρεται στην προστασία της Πληροφορίας και των Πληροφοριακών Συστημάτων από μη εξουσιοδοτημένη πρόσβαση, χρήση, αποκάλυψη, τροποποίηση ή καταστροφή προκειμένου να διασφαλίσει στο χρήστη:

    1) Ακεραιότητα (Integrity): Προστασία από καταχρηστική τροποποίηση πληροφοριών ή καταστροφή. Περιλαμβάνει τη διασφάλιση της Πληροφορίας, τη μη αποποίηση και την αυθεντικοποίηση του χρήστη.
    2) Εμπιστευτικότητα (Confidentiality): Διατήρηση των περιορισμών πρόσβασης και αποκάλυψης των πληροφοριών , περιλαμβάνοντας την έννοια της προστασίας της Ιδιωτικότητας και της Ιδιωτικότητας της πληροφορίας.
    3) Διαθεσιμότητα (Availability): Εξασφάλιση της έγκαιρης και αξιόπιστης πρόσβασης και χρήσης των πληροφοριών.

2. *Privacy (Ιδιωτικότητα της Πληροφορίας):* Αναφέρεται στην εξασφαλισμένη, σωστή και συνεπή συλλογή, επεξεργασία, χρήση και διάθεση των πληροφοριών σε όλο τον κύκλο της ζωής τους.

1.2.2.1 Ακεραιότητα (Integrity)

Στην επιστήμη της Πληροφορικής, με τον όρο «Ακεραιότητα» αναφερόμαστε σε όλες τις ιδιότητες που θα πρέπει να διαθέτει ένα σύστημα προκειμένου να προστατευτεί από εσκεμμένη ή μη εξουσιοδοτημένη πρόσβαση, με σκοπό την καταστροφή ή τροποποίηση των αγαθών του συστήματος. Η έννοια της Ακεραιότητας περιλαμβάνει την Ακεραιότητα των Δεδομένων (data integrity), την Ακεραιότητα του Υλικού (Hardware Integrity) και την ακεραιότητα του Λογισμικού (Software Integrity).

Τις περισσότερες φορές η έννοια της Ακεραιότητας των Δεδομένων σχετίζεται άμεσα με την απαίτηση για έλεγχο Πρόσβασης (Access Control) στα Δεδομένα. Με την αποτροπή της μη εξουσιοδοτημένης πρόσβασης, ένας οργανισμός μπορεί να επιτύχει μεγαλύτερη εμπιστευτικότητα (Confidentiality) των Δεδομένων αλλά και γενικότερη Ακεραιότητα του Συστήματος. Τέτοιοι μηχανισμοί ελέγχου μπορούν να προσδώσουν μεγαλύτερη διαφάνεια και καλύτερο έλεγχο στο ποιος και τι μπορεί να

αλλάξει στα Δεδομένα και τις πληροφορίες του συστήματος. Ο έλεγχος Πρόσβασης εξασφαλίζεται με μηχανισμούς Εξουσιοδότησης (Authorization), όπου μέσα από αυτούς καθορίζεται το επίπεδο της πρόσβασης του κάθε πιστοποιημένου χρήστη στους πόρους του συστήματος.

Το Cloud μοντέλο παρουσιάζει μία σειρά από απειλές και πλήθος ενδεχόμενων εξελιγμένων επιθέσεων, εναντίον των εμπιστευτικών Πληροφοριών που διατηρούνται μέσα σε αυτό. Σε αυτό συμβάλλει καθοριστικά η αυξημένη κίνηση εντός της Cloud υποδομής, η διασπορά των δεδομένων σε διαφορετικά κέντρα επεξεργασίας αλλά και το πλήθος των σημείων πρόσβασης στο Cloud περιβάλλον. Ο Πάροχος Cloud Υπηρεσιών οφείλει να παρέχει στους πιστοποιημένους χρήστες ένα αξιόπιστο περιβάλλον αναφορικά με την ακεραιότητα και την ακρίβεια των δεδομένων που διατηρεί. Μία κοινή πρακτική διασφάλισης της απαίτησης για Ακεραιότητα των Δεδομένων είναι ο καθορισμός του Service Level Agreements (SLA) συμβολαίου μεταξύ του Παρόχου και του Χρήστη, μέσα στο οποίο καθορίζεται μεταξύ άλλων η αρχιτεκτονική και ορισμένα standards της Cloud Υποδομής που προσφέρεται.

1.2.2.2 Εμπιστευτικότητα & Ιδιωτικότητα (Confidentiality & Privacy)

Οι όροι «Εμπιστευτικότητα» και «Ιδιωτικότητα» αναφέρονται στο βαθμό στον οποίο μη εξουσιοδοτημένες οντότητες αποκλείονται από την πρόσβαση στα Δεδομένα και τις Πληροφορίες. Πιο συγκεκριμένα, η έννοια της Εμπιστευτικότητας αναφέρεται στις εξουσιοδοτημένες εκείνες οντότητες ή συσκευές που έχουν τη δυνατότητα πρόσβασης σε προστατευμένα Δεδομένα. Από την άλλη πλευρά, η έννοια της Ιδιωτικότητας αναφέρεται στην επιθυμία του ατόμου να ελέγχει πλήρως την αποκάλυψη των προσωπικών του πληροφοριών.

Στο περιβάλλον της Νεφοϋπολογιστικής, η έννοια της Ιδιωτικότητας (Privacy) περιλαμβάνει δύο βασικές απαιτήσεις, τις οποίες ο Πάροχος οφείλει να διασφαλίσει. Η πρώτη αναφέρεται στην διασφάλιση της εμπιστευτικότητας των Πληροφοριών κατά τη διάρκεια της μετάδοσης, πρόσβασης ή αποθήκευσής τους από τον πιστοποιημένο χρήστη μέσω του Διαδικτύου. Η δεύτερη αναφέρεται στη διασφάλιση της εμπιστευτικότητας των δεδομένων του χρήστη από τον ίδιο των Πάροχο [09].

Είναι γεγονός ότι τα δεδομένα που διατηρούνται στο σύννεφο διατρέχουν αυξημένο κίνδυνο από πιθανές επιθέσεις, εξαιτίας των αυξημένων σημείων πρόσβασης (access point) στην Cloud υποδομή. Αυτό οφείλεται κυρίως στο μεγάλο πλήθος οντοτήτων, συσκευών και εφαρμογών που συμμετέχουν στο περιβάλλον του Νέφους. Συνεπώς, η εναπόθεση των δεδομένων στο σύννεφο εγείρει αρκετά ζητήματα αναφορικά με την Ιδιωτικότητα των Δεδομένων.

Τα περισσότερα ερωτηματικά αφορούν την αρχιτεκτονική των πολλαπλών-μισθώσεων (multi-tenancy), στην οποία βασίζονται οι Cloud υποδομές. Ο όρος «multi-tenancy» στη Νεφοϋπολογιστική αναφέρεται στο διαμοιρασμό των πόρων της υποδομής μεταξύ των χρηστών. Για παράδειγμα, σε μία multi-tenancy αρχιτεκτονική, μία μοναδική εφαρμογή λογισμικού διαμοιράζεται με τέτοιο τρόπο ώστε κάθε χρήστης να εργάζεται σε ένα εικονικό στιγμιότυπο της. Εξαιτίας του εικονικού διαχωρισμού των πόρων (hardware, software, network resources)

μεταξύ πολλαπλών χρηστών και μίας μοναδικής υποδομής, τα προστατευόμενα δεδομένα μπορεί να αποκαλυφθούν.

Ως κοινή τακτική για τη διασφάλιση της Εμπιστευτικότητας των Δεδομένων αναφέρεται η αυθεντικοποίηση των χρηστών κατά την πρόσβαση τους στην Cloud υποδομή. Η έλλειψη ισχυρών κανόνων αυθεντικοποίησης μπορεί να οδηγήσει στη μη εξουσιοδοτημένη πρόσβαση στους λογαριασμούς των χρηστών, με αποτέλεσμα την παραβίαση της Ιδιωτικότητας τους.

1.2.2.3 Διαθεσιμότητα (Availability)

Η Διαθεσιμότητα αναφέρεται στην ικανότητα του συστήματος να είναι προσβάσιμο από κάθε εξουσιοδοτημένη οντότητα ανά πάσα στιγμή. Η έννοια της Διαθεσιμότητας περιλαμβάνει και την ικανότητα του συστήματος να παρέχει πρόσβαση στους χρήστες ακόμα και όταν αυτό υπολειτουργεί. Το σύστημα θα πρέπει να συνεχίζει τις δραστηριότητες του ακόμα και στην περίπτωση της παραβίασης της ασφάλειάς του. Η Διαθεσιμότητα αναφέρεται στη γενικότερη υποδομή του συστήματος, δηλαδή τόσο στα Δεδομένα όσο και στο Hardware και Software [10].

Στο περιβάλλον της Νεφοϋπολογιστικής, ο Πάροχος οφείλει να εγγυάται τη διαθεσιμότητα των Πληροφοριών και των Πληροφοριακών διαδικασιών στους χρήστες κατ΄ απαίτηση τους. Με τη σύναψη του SLA (Service Level Agreement) συμβολαίου μεταξύ Παρόχου και χρήστη, εκτός από του όρους και τις προϋποθέσεις χρήσης των Cloud Υπηρεσιών, θα πρέπει να περιλαμβάνεται και το ποσοστό του χρόνου Διαθεσιμότητας των προσφερόμενων Υπηρεσιών. Ο χρήστης θα πρέπει να επιδιώκει τη μέγιστη Διαθεσιμότητα στο σύνολο των Υπηρεσιών με ελαχιστοποίηση ή εξάλειψη του χρόνου αδράνειας [11].

Κεφάλαιο 2ο

Η Νεφοϋπολογιστική στη Δημόσια Διοίκηση: Ζητήματα Ασφάλειας και Προστασίας της Ιδιωτικότητας

Στο Κεφάλαιο αυτό θα επικεντρωθούμε στην υιοθέτηση της τεχνολογίας της Νεφοϋπολογιστικής στη Δημόσια Διοίκηση. Εδώ, πρόκειται να μελετηθούν και να κατηγοριοποιηθούν οι βασικοί βραχυπρόθεσμοι και μακροπρόθεσμοι Κίνδυνοι που πιθανόν θα κληθούν να αντιμετωπίσουν οι υπεύθυνοι ενός Δημόσιου Οργανισμού ή της γενικής Κυβέρνησης, πριν και μετά από την εφαρμογή της Νεφοϋπολογιστικής στις Δημόσιες Υποδομές ενός Κράτους. Ταυτόχρονα, θα μελετηθούν η έννοια της Ηλεκτρονικής Διακυβέρνησης, τα βασικά χαρακτηριστικά της, τα μοντέλα υπηρεσιών και τα οφέλη που προκύπτουν από την εφαρμογή της, ενώ θα γίνει ιδιαίτερη αναφορά στη συμβολή της Νεφοϋπολογιστικής για μία αποτελεσματικότερη Ηλεκτρονική Διακυβέρνηση.

2.1 Η έννοια της Ηλεκτρονικής Διακυβέρνησης

Στη σύγχρονη κοινωνία, ο τομέας της τεχνολογίας των επικοινωνιών και των δικτύων των υπολογιστών έχει επιτελέσει τεράστια πρόοδο με άμεσα και εμφανή αποτελέσματα στον γενικότερη λειτουργία της Δημόσιας Διοίκησης. Η ενσωμάτωση των νέων και διαρκώς αναπτυσσόμενων τεχνολογιών, προάγει ένα νέο μοντέλο διακυβέρνησης στο Δημόσιο Τομέα, όπου οι πολίτες εμπλέκονται δυναμικά στη διαμόρφωση των δημόσιων πολιτικών και στη διαφανή εφαρμογή τους. Το μοντέλο αυτό της Ηλεκτρονικής Διακυβέρνησης (e-Government) συμβάλλει καθοριστικά στην ομαλή μετάβαση από την άκαμπτη γραφειοκρατική οργάνωση των Δημόσιων φορέων στην αποτελεσματική και αποδοτική Δημόσια Διοίκηση, με τη χρήση λιγότερων πόρων.

Ανατρέχοντας στη διεθνή βιβλιογραφία, πολλοί είναι εκείνοι που προσπάθησαν να προσεγγίσουν και να αποδώσουν την έννοια της Ηλεκτρονικής Διακυβέρνησης. Ωστόσο, οι περισσότεροι από αυτούς δεν κατάφεραν να αποσπάσουν ευρεία αποδοχή. Σήμερα, είναι γενικά αποδεκτός ο ορισμός που αποδόθηκε από την Ευρωπαϊκή Ένωση, όπου ως Ηλεκτρονική Διακυβέρνηση ορίζεται «*η χρήση των τεχνολογιών των πληροφοριών και των επικοινωνιών (ΤΠΕ) στις δημόσιες διοικήσεις, σε συνδυασμό με οργανωτικές αλλαγές και νέες δεξιότητες του προσωπικού. Σκοπός είναι η βελτίωση των δημόσιων υπηρεσιών, καθώς και η ενίσχυση των δημοκρατικών διαδικασιών και των διαδικασιών στήριξης των δημόσιων πολιτικών*» [17]. Στην ίδια ανακοίνωση της Ευρωπαϊκής επιτροπής [17], αναφέρεται ότι «*Η ηλεκτρονική διακυβέρνηση μπορεί να μειώσει τις δαπάνες τόσο των επιχειρήσεων όσο και των κυβερνήσεων και να διευκολύνει τις συναλλαγές μεταξύ των δημόσιων υπηρεσιών και των πολιτών. Επιπλέον, συμβάλλει στο μεγαλύτερο άνοιγμα και στη διαφάνεια του δημόσιου τομέα, καθώς και σε κυβερνητικές λειτουργίες λιγότερο περίπλοκες και πιο συνεπείς έναντι των πολιτών*».

Διεθνής εμπειρογνώμονες έχουν καθορίσει τα θέματα στα οποία θα πρέπει να δοθεί προτεραιότητα, ώστε να αρθούν τα εμπόδια για τη γενίκευση της Ηλεκτρονικής Διακυβέρνησης. Τα θέματα που αναφέρονται ως απαραίτητη προϋπόθεση είναι:

- *Η πρόσβαση σε όλους:* Αναφέρεται στον κίνδυνο δημιουργίας «ψηφιακού χάσματος», λόγω του διαφορετικού επιπέδου εκπαίδευσης και κατάρτισης των πολιτών στις αναγκαίες γνώσεις πληροφορικής καθώς και στην άνιση πρόσβαση στις πληροφορίες και στις τεχνολογίες των πληροφοριών.

- *Η εμπιστοσύνη των χρηστών:* Αναφέρεται στην παροχή εγγυήσεων προς τους χρήστες για ασφαλή πρόσβαση στις παρεχόμενες υπηρεσίες. Η έννοια της ασφαλούς πρόσβασης περιλαμβάνει την εμπιστευτικότητα των προσωπικών δεδομένων και την ασφάλεια των ψηφιακών συναλλαγών.

- *Οι Δημόσιες συμβάσεις:* Αναφέρεται στη δυνατότητα της Ηλεκτρονικής Διακυβέρνησης να βελτιώσει την αποτελεσματικότητα, την ποιότητα και τη σχέση κόστους/ απόδοσης των δημόσιων συμβάσεων.

- *Οι πανευρωπαϊκές υπηρεσίες:* Αναφέρεται στη δυνατότητα παροχής πανευρωπαϊκών Υπηρεσιών. Ωστόσο, είναι σημαντικό να ληφθεί μέριμνα ώστε οι Υπηρεσίες αυτές να λαμβάνουν υπόψη τις διαφοροποιήσεις στις

ανάγκες των πολιτών στα διαφορετικά κράτη-μέλη. Χαρακτηριστικό παράδειγμα πανευρωπαϊκών υπηρεσιών αποτελεί η ευρωπαϊκή πύλη για την κινητικότητα στον τομέα της απασχόλησης (EURES).

- *Η Διαλειτουργικότητα:* Αναφέρεται στον τρόπο διασύνδεσης των συστημάτων, των πληροφοριών και των μεθόδων εργασίας. Κατά την Ευρωπαϊκή Επιτροπή «η διαλειτουργικότητα δεν νοείται μόνον ως σύνδεση δικτύων ηλεκτρονικών υπολογιστών. Αφορά επίσης οργανωτικά θέματα, όπως π.χ. την ανάγκη να εξασφαλίζεται η συνεργασία με οργανισμούς-εταίρους, οι οποίοι έχουν διαφορετικό τρόπο εσωτερικής οργάνωσης και λειτουργίας.»[17]

Τα αποτελέσματα από την υιοθέτηση e-Government υπηρεσιών είναι ιδιαίτερα ενθαρρυντικά, γεγονός που στρέφει τις κυβερνήσεις στη διαρκή προσπάθεια ανάληψης νέων πρωτοβουλιών. Από την υιοθέτηση τέτοιων υπηρεσιών προκύπτουν σημαντικά πλεονεκτήματα, όπως:

- Παροχή Υπηρεσιών υψηλού επιπέδου από τους δημόσιους φορείς προς του πολίτες
- Ενδυνάμωση της Δημοκρατίας
- Αποτελεσματικότερη διαχείριση του συνόλου των διαδικασιών της Δημόσιας Διοίκησης
- Μείωση της διαφθοράς με περισσότερη διαφάνεια στις σχέσεις μεταξύ πολίτη και Δημόσιας Διοίκησης
- Εξάλειψη της γραφειοκρατίας με παράλληλη μείωση του κόστους των παρεχόμενων υπηρεσιών
- Μείωση του διοικητικού φόρτου και των χρόνων διεκπεραίωσης.
- Παροχή αξιόπιστων ελεγκτικών μηχανισμών και αύξηση εσόδων.

Η ελληνική κυβέρνηση βρίσκεται στη φάση της υλοποίηση της στρατηγικής για την Ηλεκτρονική Διακυβέρνηση, στο πλαίσιο του νέου στρατηγικού προγράμματος της Ευρωπαϊκής Ένωσης για την «Κοινωνία της Πληροφορίας». Σήμερα, η ελληνική Δημόσια Διοίκηση έχει καταφέρει να αναπτύξει και να ενσωματώσει σημαντικές πρωτοβουλίες Ηλεκτρονικής Διακυβέρνησης, προάγοντας σημαντικά τη διαλειτουργικότητα μεταξύ των δημόσιων φορέων αλλά και την ενεργή συμμετοχή των πολιτών στις διαδικασίες της Δημόσιας Διοίκησης.

2.2 Μοντέλα Ηλεκτρονικής Διακυβέρνησης

Είναι γεγονός ότι τα τελευταία χρόνια έχουν υλοποιηθεί πλήθος υπηρεσιών Ηλεκτρονικής Διακυβέρνησης τόσο στην Ελλάδα αλλά πολύ περισσότερο στα προηγμένα κράτη στην Υφήλιο. Στην Ελλάδα, μέχρι πριν από λίγα χρόνια, ελάχιστα βήματα είχαν πραγματοποιηθεί προς την κατεύθυνση της Ηλεκτρονικής Διακυβέρνησης. Αυτά περιορίζονταν κυρίως στην παροχή Φορολογικών μηχανισμών προς τους πολίτες. Την τελευταία δεκαετία όμως, παρέχονται νέες ηλεκτρονικές δυνατότητες, που ενισχύουν και διευκολύνουν όχι μόνο τη σχέση κράτους-πολίτη αλλά και τη σχέση μεταξύ των δημόσιων φορέων.

Η Ηλεκτρονική Διακυβέρνηση διασπάται σε τρείς διαφορετικές μορφές όπου κάθε μία από αυτές προσδιορίζεται σύμφωνα με τις εμπλεκόμενες οντότητες και τη μεταξύ τους σχέση αλληλεπίδρασης. Πιο συγκεκριμένα, οι περισσότεροι μελετητές αναφέρονται στις κατηγορίες: Κυβέρνηση προς Κυβέρνηση (Government to Government – G2G), Κυβέρνηση προς πολίτες (Government to Citizen - G2C) και Κυβέρνηση προς Επιχειρήσεις (Government to Business - G2B). Αναλυτικότερα:

- *Υπηρεσίες τύπου Κυβέρνηση προς Κυβέρνηση (G2G):* Ο τύπος αυτός αναφέρεται σε υπηρεσίες κατά τις οποίες αναπτύσσεται αλληλεπίδραση μεταξύ διαφορετικών δημόσιων φορέων. Ο κύριος στόχος που επιτυγχάνεται εδώ είναι η ψηφιακή ανταλλαγή πληροφοριών και δεδομένων μεταξύ διαφορετικών κυβερνητικών οργανισμών σε κάθε επίπεδο διοίκησης (στενός Δημόσιος Τομέας, ευρύτερος Δημόσιος Τομέας και Τοπική Αυτοδιοίκηση).

  Οι Ηλεκτρονικές Υπηρεσίες αυτού του τύπου μπορούν να μειώσουν σημαντικά το διοικητικό φόρτο, τη γραφειοκρατία καθώς και να διευκολύνουν το σύνολο των διαδικασιών της Δημόσιας Διοίκησης. Στην Ελλάδα, χαρακτηριστικό παράδειγμα G2G Υπηρεσιών είναι το έργο «ΣΥΖΕΥΞΙΣ» υπό την αιγίδα του Υπουργείου Διοικητικής Μεταρρύθμισης & Ηλεκτρονικής Διακυβέρνησης, το οποίο έχει σκοπό την ανάπτυξη και τον εκσυγχρονισμό της τηλεπικοινωνιακής υποδομής του Δημόσιου Τομέα. Ακόμα ένα χαρακτηριστικό παράδειγμα είναι η Κυβερνητική Διαδικτυακή Πύλη Δημόσιας Διοίκησης «Ερμής», η οποία αναμένεται να συμβάλλει στην άμεση πληροφόρηση των πολιτών και των επιχειρήσεων καθώς και στην ασφαλή διεκπεραίωση υπηρεσιών Ηλεκτρονικής Διακυβέρνησης (παροχή «έξυπνων καρτών» και ψηφιακών πιστοποιητικών).

- *Υπηρεσίες τύπου Κυβέρνηση προς Πολίτες (G2C):* Οι υπηρεσίες αυτές απευθύνονται προς τους πολίτες και έχουν σκοπό τη ταχύτερη και αποτελεσματικότερη διεκπεραίωση των σχετικών αιτημάτων των πολιτών από τους Δημόσιους φορείς. Σημαντικό χαρακτηριστικό αυτών των Υπηρεσιών είναι η άμεση πληροφόρηση των πολιτών (με τη χρήση τεχνολογικών εργαλείων) χωρίς να απαιτείται η επικοινωνία τους με τους εμπλεκόμενους Δημόσιους φορείς. Ιδιαίτερα σημαντικές θεωρούνται οι Υπηρεσίες που δίνουν τη δυνατότητα στους πολίτες να συμμετάσχουν στη διαδικασία διαμόρφωσης (Open Government) και ελέγχου (Πρόγραμμα «ΔΙΑΥΓΕΙΑ») των διοικητικών διαδικασιών, καθώς με τον τρόπο αυτό ενισχύεται η διαφάνεια και ο θεσμός της Δημοκρατίας.

Χαρακτηριστικά παραδείγματα G2C υπηρεσιών είναι το σύστημα TAXISNet με σκοπό την παροχή φορολογικών υπηρεσιών προς τους πολίτες και τις επιχειρήσεις καθώς και η Ηλεκτρονική πλατφόρμα εξυπηρέτησης των ασφαλισμένων του ΙΚΑ (www.ika.gr) ή του συνόλου των πολιτών μέσω των Κέντρων Εξυπηρέτησης Πολιτών (ΚΕΠ - www.kep.gov.gr).

- *Υπηρεσίες τύπου Κυβέρνηση προς Επιχειρήσεις (G2B):* Οι υπηρεσίες αυτές απευθύνονται σε ιδιωτικές επιχειρήσεις και στις συναλλαγές τους με τους Δημόσιους φορείς. Αφορούν κυρίως υπηρεσίες ηλεκτρονικών προμηθειών (e-Procurement) και εφαρμογές υποβολής φορολογικών υποχρεώσεων μέσω συστήματος TAXIS.

2.3 Η Νεφοϋπολογιστική στη Δημόσια Διοίκηση [24]

Είναι γενικά παραδεκτό ότι ένα αποτελεσματικό σύστημα Δημόσιας Διοίκησης, που αξιοποιεί Τεχνολογίες της Πληροφορίας και των Επικοινωνιών (ΤΠΕ), θα πρέπει να χαρακτηρίζεται από αξιοπιστία και ταυτόχρονα να παρέχει υψηλού επιπέδου υπηρεσίες με χαμηλό κόστος. Για την επίτευξη αυτών των στόχων, οι κυβερνήσεις θα πρέπει να εστιάσουν σε δύο βασικούς τομείς. Ο πρώτος τομέας, όπου θα πρέπει να δοθεί ιδιαίτερη έμφαση, είναι η υλικοτεχνική υποδομή των υπολογιστικών συστημάτων που θα χρησιμοποιηθούν, με απώτερο σκοπό την παροχή μεγάλης υπολογιστικής ισχύος με το μικρότερο δυνατό κόστος. Ο δεύτερος τομέας αφορά την εκπαίδευση των τελικών χρηστών και την ανάπτυξη των βασικών ικανοτήτων τους σε θέματα υπολογιστών και Internet. Αναπτύσσοντας τους δύο αυτούς τομείς καθίσταται δυνατή η παροχή σύγχρονων Ηλεκτρονικών Υπηρεσιών στη Δημόσια Διοίκηση.

Τα τελευταία χρόνια, οι τεχνολογίες της Νεφοϋπολογιστικής επιδιώκουν να παρέχουν αξιόπιστες ηλεκτρονικές υπηρεσίες όχι μόνο στον Ιδιωτικό Τομέα αλλά και στη Δημόσια Διοίκηση. Σήμερα, η Νεφοϋπολογιστική αποτελεί ένα σημαντικό εργαλείο στο χέρια των Κυβερνήσεων, καθώς διεθνής εμπειρογνώμονες καταγράφουν ήδη σημαντικά οφέλη στα κράτη εκείνα που υιοθέτησαν Cloud υπηρεσίες είτε προς τους πολίτες είτε μεταξύ των δημόσιων οργανισμών. Το εύρος των υπηρεσιών που μπορεί να υποστηρίξει μία Cloud υποδομή είναι τεράστιο. Πολλές κυβερνήσεις κατάφεραν να γεφυρώσουν το επικοινωνιακό χάσμα μεταξύ κράτους-πολίτη παρέχοντας στους τελευταίους πληθώρα Cloud υπηρεσιών. Η χρησιμότητα τους έγινε ιδιαίτερα εμφανής κυρίως στους πολίτες που διέμεναν σε απομακρυσμένα σημεία της χώρας με χαρακτηριστική δυσκολία πρόσβασης στους Δημόσιους φορείς. Οι Cloud υποδομές μπορούν επίσης να χρησιμοποιηθούν για την αύξηση της διαλειτουργικότητας μεταξύ των δημόσιων οργανισμών ενός κράτους ή ακόμα και για τη συνεργασία των Κυβερνήσεων μεταξύ διαφορετικών κρατών, ενώ ταυτόχρονα μπορεί να υποστηριχθεί η παρακολούθηση της αποτελεσματικότητας των συστημάτων διακυβέρνησης. Επίσης, αξίζει να σημειωθεί η συμβολή της Νεφοϋπολογιστικής στην ουσιαστική μείωση του κόστους εγκατάστασης και συντήρησης IT υποδομών στους Δημόσιους οργανισμούς καθώς χρησιμοποιείται σχεδόν αποκλειστικά η υποδομή του Cloud Παρόχου.

Σε παγκόσμιο επίπεδο, η Ηλεκτρονική Διακυβέρνηση μπορεί να επωφεληθεί από τις Cloud αρχιτεκτονικές με τη μείωση του κόστους και την αύξηση της αποτελεσματικής αξιοποίησης των πόρων. Οι επιχειρήσεις κάθε μεγέθους έχουν ήδη αρχίσει να αποκομίζουν τα οφέλη της Νεφοϋπολογιστικής με τη χρήση του «pay as you use» μοντέλου, το οποίο παρέχει τεράστιες δυνατότητες και άμεση διαθεσιμότητα. Όσον αφορά το Δημόσιο Τομέα, όπου απαιτείται τεράστια υλικοτεχνική υποδομή, είναι ιδιαίτερα σημαντική η χρήση Cloud υποδομών σε μακροπρόθεσμη βάση. Ωστόσο, μία σειρά από προκλήσεις και ενδεχόμενους κινδύνους, κυρίως σε ζητήματα ασφάλειας και Ιδιωτικότητας, έχουν περιορίσει τη χάραξη συγκεκριμένων πολιτικών για μία γενικευμένη χρήση της Νεφοϋπολογιστικής στη Δημόσια Διοίκηση. Η κάθε κυβέρνηση οφείλει την καταγραφή και την αξιολόγηση τέτοιων ζητημάτων, πριν την μετάβαση σε Cloud υποδομές. Μία σειρά από ζητήματα ασφάλειας που έχουν καταγραφεί μέχρι σήμερα αναλύονται στην ακόλουθη ενότητα.

2.4 Κίνδυνοι και Ζητήματα Ασφάλειας κατά τη μετάβαση της Δημόσιας Διοίκησης σε περιβάλλον Νέφους

Στην επιστήμη της Πληροφορικής, με τον όρο «Κίνδυνος» εννοούμε την πιθανότητα μία ενδεχόμενη απειλή να εκμεταλλευτεί μία αδυναμία-ευπάθεια του συστήματος με επιπτώσεις στο οργανισμό. Οι ενδεχόμενοι κίνδυνοι σε ένα οργανισμό δε μπορούν να εξαλειφθούν πλήρως. Μπορούν όμως να περιοριστούν σε αποδεκτά για τον οργανισμό επίπεδα. Αποδεκτοί κίνδυνοι είναι εκείνοι που, έπειτα από μία κατάλληλη εκτίμηση τους, ο οργανισμός αποφασίζει ότι το κόστος από την αντιμετώπιση τους αντισταθμίζεται από τα οφέλη που θα προκύψουν [25].

Όπως αναλύθηκε και προηγουμένως, το μοντέλο του Cloud Computing παρέχει τη δυνατότητα σε οργανισμούς με περιορισμένους πόρους να δημιουργήσουν τη δική τους IT υποδομή, μισθώνοντας την υποδομή ή τις εφαρμογές από ένα Cloud Πάροχο. Από το Cloud Computing μοντέλο, προκύπτουν σημαντικά ζητήματα ασφάλειας, με βασικότερη αιτία την απώλεια της διακυβέρνησης των Δεδομένων του οργανισμού, από τη στιγμή που αυτά μεταφέρονται στην Cloud υποδομή. Το European Network & Information Systems Agency (ENISA), έπειτα από μία αξιόλογη προσπάθεια καταγραφής των ζητημάτων Ασφάλειας σε Cloud περιβάλλον, κατέληξε στη διάκριση των Κινδύνων σε τρείς κατηγορίες: Διαχείρισης, Τεχνικά και Νομικά ζητήματα [27]. Πιο συγκεκριμένα, τα ζητήματα διαχείρισης αφορούν Κινδύνους οι οποίοι πιθανόν να επιφέρουν επιπτώσεις στη λειτουργία του οργανισμού και στην πρόσβαση στα Δεδομένα του, ενώ τα τεχνικά ζητήματα περιλαμβάνουν κυρίως προβλήματα κατά την επικοινωνία του οργανισμού με τον Cloud Πάροχο. Τέλος, τα νομικά ζητήματα αφορούν Κινδύνους οι οποίοι προέρχονται από την ανταλλαγή και φύλαξη των δεδομένων σε data centers διαφορετικών κρατών και τα οποία υπόκεινται σε διαφορετική νομοθεσία σχετικά με την ανταλλαγή, τη διαχείριση και την προστασία των προσωπικών δεδομένων.

Σήμερα, κάποια από τα ζητήματα αυτά έχουν παρακαμφθεί με αποτέλεσμα η τεχνολογία της Νεφοϋπολογιστικής να κατακτά σταδιακά την εμπιστοσύνη όλο και περισσότερων φυσικών προσώπων ή οργανισμών. Με την παράκαμψη των σοβαρών ζητημάτων ασφαλείας, πολλές κυβερνήσεις παγκοσμίως (κυρίως προηγμένων κρατών) δείχνουν εμπιστοσύνη και υιοθετούν Cloud υπηρεσίες στη Δημόσια Διοίκηση. Ωστόσο, αρκετά ζητήματα είναι ακόμη υπαρκτά και θα πρέπει να αξιολογηθούν από τις κυβερνήσεις προτού αποφασίσουν τη μεταφορά των δεδομένων τους σε Cloud περιβάλλον. Αυτά κυρίως αφορούν τόσο την απώλεια του ελέγχου των Δεδομένων όσο και την άμεση εξάρτηση της λειτουργίας ενός κράτους από τον Πάροχο των Cloud υπηρεσιών. Αμέσως μετά περιγράφονται ανά κατηγορία τα σημαντικότερα ζητήματα Ασφάλειας και οι ενδεχόμενοι Κίνδυνοι που οφείλουν πρωτίστως να εξετάσουν οι Κυβερνήσεις.

2.4.1 Διοικητικά – Διαχειριστικά ζητήματα

2.4.1.1 Περιορισμένη φορητότητα των δεδομένων ή εφαρμογών σε άλλο Πάροχο Νέφους

Το πρόβλημα της φορητότητας αναφέρεται στην περιορισμένη δυνατότητα ενός κράτους να μεταβιβάσει τα δεδομένα ή τις εφαρμογές, που διαχειρίζεται μέσω δημόσιων οργανισμών, από ένα Πάροχο Cloud υπηρεσιών σε έναν άλλο ή ακόμη και να επιστρέψει στην παραδοσιακή IT υποδομή. Βασικότερη αιτία του ζητήματος αυτού αποτελεί η έλλειψη τυποποιημένων τεχνολογικών λύσεων για τη διαδικασία μεταφοράς και αποθήκευσης των δεδομένων στο Νέφος. Ο κάθε Πάροχος δύναται να χρησιμοποιεί εφαρμογές και να διαχειρίζεται δεδομένα σύμφωνα με τα δικά του πρότυπα, με αποτέλεσμα να μη μπορεί να εγγυηθεί την φορητότητα τους σε άλλο Πάροχο. Φυσικά, η έλλειψη συγκεκριμένων προτύπων αποδεικνύεται ιδιαίτερα ωφέλιμη για τον Πάροχο αφού δεσμεύει έμμεσα ή άμεσα τον χρήστη και τον αποτρέπει να μεταφερθεί σε άλλο Πάροχο.

Αυτή η εξάρτηση από ένα συγκεκριμένο Πάροχο μπορεί να οδηγήσει σε καταστροφικές επιπτώσεις στη συνολική λειτουργία της Δημόσιας Διοίκησης, σε περίπτωση που ο Πάροχος δεν συμμορφώνεται πλήρως με τις προσυμφωνημένες απαιτήσεις. Αξίζει να σημειωθεί ότι στην περίπτωση της αναγκαίας μετάβασης σε άλλο Πάροχο, το κόστος μεταφοράς των δεδομένων και των εφαρμογών είναι ιδιαίτερα υψηλό. Για το λόγο αυτό, κρίνεται ιδιαίτερα σημαντική η επιλογή ενός αξιόπιστου Παρόχου καθώς και η σαφήνεια και η διαφάνεια στους όρους χρήσης του Νέφους.

2.4.1.2 Απώλεια ελέγχου των δεδομένων

Η μετάβαση των Πληροφοριακών Συστημάτων της Δημόσιας Διοίκησης στο Νέφος σημαίνει υποχρεωτική ανάθεση του ελέγχου των δεδομένων από το Κράτος στον Πάροχο. Το γεγονός αυτό εγείρει πλήθος σημαντικών ζητημάτων σχετικά με την ασφάλεια των δεδομένων που αποθηκεύονται στο Νέφος.

Το κυριότερο ζήτημα που τίθεται είναι ότι το κράτος δεν είναι σε θέση να γνωρίζει με σαφήνεια το που ακριβώς αποθηκεύονται τα δεδομένα και αν αυτά επεξεργάζονται χωρίς την έγκριση κάποιου Δημόσιου φορέα ή πιστοποιημένου χρήστη. Να σημειωθεί ότι ο Πάροχος έχει το δικαίωμα να αποθηκεύει τα δεδομένα του χρήστη σε data centers σε διαφορετικά γεωγραφικά σημεία, όπου η νομοθεσία για την προστασία των δεδομένων και της Ιδιωτικότητας πιθανόν να διαφέρει από εκείνη του χρήστη. Έτσι, υπάρχει η πιθανότητα διαφορετικής επεξεργασίας των δεδομένων του χρήστη, χωρίς προηγούμενη ενημέρωση του. Η Κυβέρνηση μίας, για παράδειγμα, Ευρωπαϊκής χώρας θα πρέπει να λάβει σοβαρά υπόψη τους πιθανούς Κινδύνους από τη μετάβαση σε μία πλατφόρμα, όπου τα δεδομένα αποθηκεύονται σε data centers εκτός Ευρωπαϊκής Ένωσης και υπόκεινται σε διαφορετική νομοθεσία [26]. Να σημειωθεί ότι υπάρχουν και αρκετές περιπτώσεις Παρόχων, οι οποίοι είναι σε θέση να εφαρμόζουν τεχνικές Εξόρυξης Δεδομένων (Data Mining) με αποτέλεσμα να καθίσταται δυνατή η ανάλυση των δεδομένων του χρήστη χωρίς την προηγούμενη συγκατάθεσή του.

Αναφορικά με τη διαχείριση των δεδομένων από τον Πάροχο, σημαντικό είναι το ζήτημα που ανακύπτει αναφορικά με τη διαγραφή των δεδομένων του χρήστη. Θεωρείται αδύνατη η διαγραφή όλων των ηλεκτρονικών αντιγράφων ενός συγκεκριμένου υλικού, για το λόγο ότι είναι αδύνατον να βρεθούν όλα τα αντίγραφα. Οι Πάροχοι συνήθως αποθηκεύουν τα δεδομένα και τα αντίγραφά τους σε διαφορετικά data centers για λόγους ασφάλειας και ανάκαμψης σε περίπτωση καταστροφής, με αποτέλεσμα να μην είναι πάντα εύκολος ο πλήρης εντοπισμός τους. Ωστόσο, ενώ θα πρέπει να ορίζεται σαφώς στους όρους χρήσης του Νέφους, η οριστική διαγραφή των δεδομένων από το Νέφος, ο χρήστης θα πρέπει να γνωρίζει ότι δεν υπάρχουν ουσιαστικές εγγυήσεις [26].

Αναφορικά με τον τομέα της Δημόσιας Διοίκησης, είναι γνωστό ότι οι Δημόσιοι Οργανισμοί διαχειρίζονται τεράστιο πλήθος δεδομένων (και ευαίσθητων προσωπικών δεδομένων) και πολλές φορές μέσα από περιβάλλοντα κρίσιμων Υποδομών (critical Infrastructure). Η απώλεια του ελέγχου και της διακυβέρνησης των Δεδομένων σε τέτοια περιβάλλοντα μπορεί να επιφέρει σημαντικές επιπτώσεις τόσο στη χάραξη της στρατηγικής μίας Κυβέρνησης όσο και στην εκπλήρωση των στόχων και των υποχρεώσεων της Δημόσιας Διοίκησης. Ο Πάροχος δύναται να εκμεταλλευτεί την αδυναμία του ελέγχου με αποτέλεσμα τη μη συμμόρφωση του με τις απαιτήσεις Ασφάλειας και Ιδιωτικότητας των Δεδομένων. Σε αυτή την περίπτωση, η Δημόσια Διοίκηση αντί να παρέχει σύγχρονες υπηρεσίες Νέφους, θα παρέχει υπηρεσίες μειωμένης αξιοπιστίας, απόδοσης και ποιότητας. Ως εκ τούτου, η σωστή επιλογή του Παρόχου και η σαφής διάκριση των ρόλων και των αρμοδιοτήτων του κάθε μέρους κρίνεται ιδιαίτερα κρίσιμη για μία Κυβέρνηση.

2.4.1.3 Αδυναμία συμμόρφωσης του Παρόχου με τις απαιτήσεις της Κυβέρνησης

Ένα σημαντικό ζήτημα το οποίο θα πρέπει να εξεταστεί από μία Κυβέρνηση, η οποία στοχεύει στη μετάβαση των συστημάτων των Δημόσιων οργανισμών στο Νέφος, είναι η δυνατότητα συμμόρφωση του Cloud Παρόχου με πιστοποιήσεις ή άλλες κανονιστικές απαιτήσεις που τυχόν διαθέτει. Τα περισσότερα προηγμένα κράτη έχουν επενδύσει σε διαδικασίες ή υπηρεσίες στη Δημόσια Διοίκηση, για τις οποίες έχουν λάβει αναγνωρισμένες πιστοποιήσεις από διεθνής ή άλλους οργανισμούς. Ο Πάροχος θα πρέπει να είναι σε θέση να υποστηρίξει τις διαδικασίες αυτές χωρίς να θέσει σε κίνδυνο τις πιστοποιήσεις αυτές. Εξαιτίας όμως της έλλειψης τεχνολογικών προτύπων και λύσεων, θεωρείται ιδιαίτερα δύσκολη η πλήρης συμμόρφωση του Παρόχου για την εξασφάλιση των πιστοποιήσεων των Δημόσιων οργανισμών. Μάλιστα, σε κάποιες περιπτώσεις, ο Πάροχος μπορεί να μην είναι σε θέση να υποστηρίξει συγκεκριμένες υπηρεσίες με αποτέλεσμα να τίθενται σε κίνδυνο ολόκληρες διαδικασίες. Για παράδειγμα, ένας Πάροχος Νέφους Δημόσιας Υποδομής, πιθανόν να μη μπορεί να υποστηρίξει συναλλαγές με χρήση πιστωτικών καρτών, με αποτέλεσμα να μην επιτρέπονται οι οικονομικές συναλλαγές μεταξύ πολίτη και Δημόσιου Οργανισμού.

Για την αποφυγή τέτοιων ζητημάτων, ο Πάροχος οφείλει να παρέχει επαρκής και ακριβής αποδείξεις για τη δυνατότητα συμμόρφωσής του με τις σχετικές απαιτήσεις του Δημόσιου φορέα, ενώ ταυτόχρονα θα πρέπει να επιτρέπει τον έλεγχο συμμόρφωσης (audit) από τον φορέα.

2.4.1.4 Αναστολή ή Περιορισμός της λειτουργίας του Παρόχου

Καθώς η Νεφοϋπολογιστική είναι μία σχετικά νέα τεχνολογία στην IT αγορά, δεν αποκλείεται κάποιος Πάροχος να αναστείλει τη λειτουργία του ή να περιορίσει το εύρος των υπηρεσιών του εξαιτίας οικονομικών ή άλλων στρατηγικών προβλημάτων. Το σύνολο των υπηρεσιών ενός Δημόσιου οργανισμού, που υποστηρίζονται από τον Πάροχο του Νέφους, απειλούνται με παύση της λειτουργίας ή με υποβάθμιση της ποιότητάς τους. Να σημειωθεί ότι σε περιβάλλον Δημόσιας Διοίκησης, μία ενδεχόμενη αναστολή της λειτουργίας των Πληροφοριακών Συστημάτων μπορεί να αποδειχτεί καταστροφική αφενός γιατί υποστηρίζονται περιβάλλοντα κρίσιμων Υποδομών για τα οποία είναι απαγορευτική η αναστολή της λειτουργίας τους και αφετέρου γιατί μέσω του ίδιου Cloud Παρόχου ενδέχεται να συνδέεται και να εξυπηρετείται το σύνολο των Δημόσιων οργανισμών ενός κράτους. Στην περίπτωση αυτή, μία ενδεχόμενη αναστολή της λειτουργίας του Παρόχου θα σήμαινε την κατάρρευση των συστημάτων σε ολόκληρο το Δημόσιο Τομέα.

Εκτός από την αναστολή ή τον περιορισμό της λειτουργίας ενός Παρόχου, η Κυβέρνηση θα πρέπει να εξετάσει και την περίπτωση μίας ενδεχόμενης εξαγοράς του Παρόχου. Ο νέος Πάροχος ενδέχεται να επιβάλει νέα στρατηγική στη χρήση και στις παρεχόμενες υπηρεσίες, με αποτέλεσμα να διακυβεύονται οι καθορισμένες απαιτήσεις ασφάλειας. Άλλη περίπτωση είναι ο Πάροχος να αναθέτει κάποιες εξειδικευμένες εργασίες σε τρίτους, με αποτέλεσμα η ασφάλεια του Παρόχου να εξαρτάται άμεσα από το επίπεδο ασφάλειας του κάθε συνδεδεμένου τρίτου Παρόχου. Για παράδειγμα, μία διακοπή στη λειτουργία ενός συνεργαζόμενου τρίτου Παρόχου μπορεί να επιφέρει τη μη διαθεσιμότητα των υπηρεσιών, απώλεια της εμπιστευτικότητας και της ακεραιότητας των δεδομένων, σοβαρές οικονομικές επιπτώσεις κτλ [27].

Εν ολίγης, μία οποιαδήποτε αλλαγή της κατάστασης του Παρόχου μπορεί να προκαλέσει ιδιαίτερα σοβαρές συνέπειες στη λειτουργία του Κράτους και της Δημόσιας Διοίκησης. Για το λόγο αυτό, είναι ιδιαίτερα κρίσιμη τόσο η σωστή επιλογή του Παρόχου όσο και η ακριβής και πλήρης καταγραφή των όρων λειτουργίας του Παρόχου.

2.4.2 Τεχνικά Ζητήματα

2.4.2.1 Εξάντληση των πόρων

Όπως αναφέρθηκε σε προηγούμενο κεφάλαιο, ένα από τα βασικά χαρακτηριστικά των Cloud συστημάτων είναι η κατ΄ απαίτηση ζήτηση και χρέωση των υπηρεσιών. Από τεχνικής άποψης, η ικανοποίηση αυτής της απαίτησης προϋποθέτει τη σωστή κατανομή των πόρων του Νέφους ανά πάσα στιγμή, προκειμένου να εξυπηρετηθούν ταυτόχρονα όλοι οι χρήστες που ζητούν την εκτέλεση των υπηρεσιών σε μία δεδομένη στιγμή. Ωστόσο, η κατανομή των πόρων του συστήματος βασίζεται κυρίως σε στατιστικές προβλέψεις. Ο Πάροχος οφείλει να προβλέπει τις περιόδους αυξημένης ζήτησης (π.χ. ημερομηνίες λήξης της υποβολής των Φορολογικών δηλώσεων) και να φροντίζει για την ενίσχυση της ικανότητας του συστήματος σε αυτές τις περιόδους.

Στο Δημόσιο Τομέα, μία λανθασμένη μοντελοποίηση των χρησιμοποιούμενων πόρων μπορεί να οδηγήσει σε σοβαρές επιπτώσεις στη διαθεσιμότητα των υπηρεσιών, στην ασφάλεια των δεδομένων αλλά και σε οικονομικές επιπτώσεις.

2.4.2.2 Αδυναμία απομόνωσης των χρηστών του Νέφους

Ο κίνδυνος της αποτυχίας απομόνωσης των χρηστών αναφέρεται σε δύο χαρακτηριστικά της τεχνολογίας της Νεφοϋπολογιστικής. Το ένα αναφέρεται στην ιδιότητα του διαμοιρασμού των πόρων και το άλλο στη δυνατότητα των πολλαπλών μισθώσεων. Και τα δύο αυτά χαρακτηριστικά αναφέρονται στη δυνατότητα διαμοιρασμού της υπολογιστικής ισχύος, των αποθηκευτικών χώρων και του δικτύου μεταξύ πολλαπλών χρηστών. Η αποτυχία απομόνωσης αναφέρεται στη αδυναμία του Παρόχου να διαχωρίσει τους πόρους της υποδομής (δίσκους, μνήμη, δίκτυο κτλ) μεταξύ των χρηστών, με αποτέλεσμα τη σύγχυση των δεδομένων, των εφαρμογών και των υπηρεσιών.

Αν και σε περιβάλλον Ιδιωτικού Νέφους (Private Cloud) ελαχιστοποιείται αυτός ο κίνδυνος, στο Δημόσιο Νέφος (Public Cloud) αυξάνονται οι πιθανότητες μίας τέτοιας απειλής. Στην περίπτωση ενός Δημόσιου οργανισμού, ο οποίος διαχειρίζεται πλήθος ευαίσθητων δεδομένων, οι σημαντικότερες επιπτώσεις αφορούν τη διαρροή ή απώλεια των δεδομένων αυτών αλλά και την έλλειψη εμπιστοσύνης των πολιτών έναντι των παρεχόμενων υπηρεσιών της Δημόσιας Διοίκησης.

2.4.2.3 Κακόβουλες επιθέσεις από το εσωτερικό του Παρόχου

Ο κίνδυνος αυτός αναφέρεται στην πιθανότητα παραβίασης της ασφάλειας των δεδομένων από το εσωτερικό του Παρόχου, δηλαδή τους ίδιους τους εργαζόμενους. Αυτή η απειλή προέρχεται εξαιτίας της αρχιτεκτονικής του Νέφους, η οποία απαιτεί τη δημιουργία θέσεων εργασίας με αυξημένα δικαιώματα, ρόλους και αρμοδιότητες. Οι θέσεις αυτές αποδεικνύονται ιδιαίτερα υψηλού κινδύνου για την παραβίαση της ασφάλειας των δεδομένων. Χαρακτηριστικά παραδείγματα αποτελούν οι διαχειριστές των συστημάτων καθώς και οι διαχειριστές της ασφάλειας του που ασχολούνται με την ανίχνευση εισβολών στο σύστημα και την αντιμετώπιση των περιστατικών ασφαλείας.

Όπως αναφέρθηκε και προηγουμένως, σε περιβάλλον Δημόσιας Διοίκησης όπου τηρείται πλήθος σημαντικών εφαρμογών και ευαίσθητων δεδομένων, μία παραβίαση της ασφάλειας των δεδομένων και των υπηρεσιών μπορεί να αποδειχτεί καταστροφική για το σύνολο του Δημόσιου τομέα αλλά και των πολιτών. Τέτοιου είδους επιθέσεις συνήθως οφείλονται στην ασάφεια των ρόλων και των αρμοδιοτήτων που δίνονται στους εργαζόμενους από τον Πάροχο αλλά και στην απουσία του ελέγχου των εργαζομένων στις κρίσιμες θέσεις.

2.4.3 Νομικά Ζητήματα

2.4.3.1 Η μεταφορά των Δεδομένων σε κράτη με διαφορετική Νομοθεσία

Όλοι οι Cloud Πάροχοι έχουν τη δυνατότητα να αποθηκεύουν τα δεδομένα των πελατών τους σε data centers διαφορετικών κρατών. Ωστόσο, κάποια από αυτά τα κράτη μπορούν να χαρακτηριστούν ως υψηλού κινδύνου. Ως τέτοια μπορούν να θεωρηθούν τα κράτη που παρουσιάζουν ελλιπή θεσμικό πλαίσιο για την προστασία της Ιδιωτικότητας των δεδομένων, τα κράτη με αυταρχικό καθεστώς ή εκείνα που παραβιάζουν τις διεθνής συμφωνίες. Η φύλαξη των δεδομένων σε τέτοια κράτη μπορεί να σημαίνει την παραβίαση των κανόνων ασφάλειας από τις τοπικές αρχές ή τις Κυβερνήσεις, με αποτέλεσμα τη διακύβευση της Ιδιωτικότητας, της Διαθεσιμότητας και της Ακεραιότητάς τους.

Εκτός από τα κράτη υψηλού ρίσκου, όπως προαναφέρθηκε, θα πρέπει να λαμβάνεται υπόψη το γεγονός ότι δεν υπάρχει ενιαίο νομοθετικό πλαίσιο σε όλα τα κράτη για τη διαχείριση των δεδομένων, ακόμη και σήμερα που η Νεφοϋπολογιστική θεωρείται η υπηρεσία του μέλλοντος παγκοσμίως. Συνεπώς, στην περίπτωση της μετάβασης των συστημάτων της Δημόσιας Διοίκησης σε περιβάλλον Cloud, η επιλογή του Παρόχου θα πρέπει να εξεταστεί προσεκτικά, έτσι ώστε οι πλατφόρμες του Παρόχου να βρίσκονται αποκλειστικά σε κράτη με παρόμοιο νομοθετικό πλαίσιο σχετικά με την επεξεργασία των δεδομένων.

2.4.3.2 Η ελλιπής προστασία των προσωπικών Δεδομένων

Η ελλιπής προστασία των προσωπικών δεδομένων από τον Πάροχο μπορεί να θέσει σε σοβαρό κίνδυνο τον πελάτη του Νέφους. Στην περίπτωση όπου τα δεδομένα αυτά προέρχονται από εφαρμογές Δημόσιων οργανισμών, κάθε παραβίαση των προσωπικών Δεδομένων μπορεί να θεωρηθεί ιδιαίτερα σοβαρή και επικίνδυνη. Για το λόγο ότι ο πελάτης του Νέφους δε μπορεί να ελέγξει αποτελεσματικά την επεξεργασία των δεδομένων στην οποία προβαίνει ο Πάροχος, δε μπορεί να ελέγξει και το αν η επεξεργασία αυτή γίνεται σύμφωνα με την κείμενη νομοθεσία. Ωστόσο, για οποιαδήποτε μη νόμιμη επεξεργασία των προσωπικών Δεδομένων ευθύνεται ο πελάτης, ακόμη και όταν αυτή έχει ανατεθεί σε Cloud Πάροχο [27]. Φυσικά, κάθε κράτος οφείλει να λειτουργεί σύμφωνα με την κείμενη Νομοθεσία και να αποφεύγει με κάθε τρόπο την οποιαδήποτε παράβαση των Νόμων. Συνεπώς, μία γενικευμένη μετάβαση της Δημόσιας Διοίκησης στο Νέφος απαιτεί την σωστή επιλογή του Παρόχου και την σαφή διατύπωση του πλαισίου μέσα στο οποίο λειτουργεί ο Πάροχος, προς αποφυγή τέτοιων φαινομένων.

Ωστόσο, το ζήτημα αυτό λαμβάνει όλο και μεγαλύτερες διαστάσεις εξαιτίας της δυνατότητας των Παρόχων να μεταφέρουν τα δεδομένα των πελατών σε άλλα κράτη, τα οποία ενδεχομένως υπόκεινται σε διαφορετική νομοθεσία αναφορικά με την επεξεργασία των προσωπικών δεδομένων. Σε αυτή την περίπτωση, κατά τη σύναψη του συμβολαίου (Service Level Agreement-SLA) μεταξύ Δημόσιου οργανισμού και Παρόχου θα πρέπει να συμπεριληφθεί και η σαφής υποχρέωση του Παρόχου να παρέχει επαρκής πληροφορίες και πιστοποιήσεις Ασφάλειας για τα δεδομένα που πρόκειται να επεξεργαστούν σε άλλο κράτος.

2.5 Προτάσεις για την αντιμετώπιση των Κινδύνων και την ενίσχυση της Ασφάλειας

Η κάθε κυβέρνηση, που στοχεύει σε μία γενικευμένη μετάβαση των Δημόσιων υπηρεσιών της σε περιβάλλον Νέφους, οφείλει να αξιολογεί προσεκτικά τα χαρακτηριστικά του Νέφους που πρόκειται να αξιοποιήσει. Η σωστή αξιολόγηση, πριν την τελική επιλογή του Παρόχου, μπορεί να περιορίσει σημαντικά τους ενδεχόμενους Κινδύνους κατά τη μετάβαση στην Cloud υποδομή. Ωστόσο, η διαδικασία της αξιολόγησης θα πρέπει να πραγματοποιείται με τη συνεργασία όλων των Δημόσιων οργανισμών, που πρόκειται να εμπλακούν στη διαδικασία μετάβασης των υπηρεσιών τους στην νέα υποδομή.

Σύμφωνα με το Council of European Professional Informatics Societies (CEPIS) [26], η εκάστοτε Κυβέρνηση θα πρέπει να αξιολογεί τα ακόλουθα σημεία, πριν τη μετάβαση των Δημόσιων Υπηρεσιών στην Cloud υποδομή. Αναλυτικότερα:

- Για την ενίσχυση της εμπιστοσύνης μεταξύ της Κυβέρνησης και του Παρόχου απαιτείται ο σαφής και ακριβής προσδιορισμός των νομικών ζητημάτων συμμόρφωσης του Παρόχου στη σύμβαση μεταξύ των δύο μερών. Με αυτό τον τρόπο επιτρέπεται η διαφάνεια όσον αφορά την επεξεργασία και την αποθήκευση των δεδομένων, όπως για παράδειγμα η φυσική τοποθεσία αποθήκευσης τους.

- Η φυσική τοποθεσία των data centers του νέφους θα πρέπει να αποτελεί κρίσιμο ζήτημα για μία Κυβέρνηση, καθώς το γεωγραφικό σημείο των μονάδων αποθήκευσης καθορίζει και τη Νομοθεσία στην οποία υπόκεινται τα δεδομένα. Συνεπώς, επηρεάζεται άμεσα το επίπεδο ασφάλειας και προστασίας της Ιδιωτικότητας των δεδομένων. Για παράδειγμα, για μία Ευρωπαϊκή κυβέρνηση δεν προτείνεται η αξιοποίηση ενός Cloud Παρόχου με πλατφόρμες τοποθετημένες σε μη Ευρωπαϊκά κράτη. Σε τέτοια περίπτωση, κρίνεται σκόπιμη η άμεση ενημέρωση της Κυβέρνησης για την ακριβή τοποθεσία αποθήκευσης των δεδομένων αλλά και η πιστοποίηση της ασφάλειας των δεδομένων αυτών. Οι όροι επεξεργασίας, αποθήκευσης, διαγραφής και μεταφοράς των δεδομένων επιβάλλεται να αναγράφονται στο συμβόλαιο συμφωνίας των δύο μερών.

- Ιδιαίτερο βάρος απαιτεί η διασφάλιση της γραμμής επικοινωνίας μεταξύ των Δημόσιων οργανισμών και του Παρόχου, προκειμένου να επιτευχθεί η ασφαλής μετάδοση των δεδομένων αλλά και να αποφευχθούν ενδεχόμενες επιθέσεις τύπου Denial-of-Service. Οι μετρήσεις ασφάλειας της γραμμής επικοινωνίας θα πρέπει να είναι υποχρεωτικές και να γίνονται με διαφανή τεχνολογικά πρότυπα.

- Ο Cloud Πάροχος, κατά τη σύναψη του συμβολαίου, θα πρέπει να εγγυάται ρητά, εκτός από την εμπιστευτικότητα και την ακεραιότητα, την πλήρη διαγραφή των δεδομένων, όταν αυτή ζητηθεί. Ωστόσο, η Κυβέρνηση θα πρέπει να γνωρίζει ότι ουσιαστικές εγγυήσεις για τη διαγραφή των δεδομένων δεν υπάρχουν.

- Η Κυβέρνηση θα πρέπει να διατηρεί τοπικά back up αρχεία των κρίσιμών

δεδομένων προκειμένου να αποφευχθούν περιστατικά μη διαθεσιμότητας των δεδομένων. Στο πλαίσιο αυτό επιβάλλεται η ανάπτυξη και η τακτική χρήση ειδικού λογισμικού για την μεταφορά των δεδομένων σε τοπικές μηχανές.

- Ο Cloud Provider οφείλει να παρέχει στην Κυβέρνηση επαρκή καταγραφή και έλεγχο των διαδικασιών ανά πάσα στιγμή.

- Πριν τη μετάβαση στο Νέφος, σημαντικά ζητήματα που αφορούν την οποιαδήποτε αλλαγή της κατάστασης και της λειτουργίας του Παρόχου θα πρέπει να καθορίζονται με σαφήνεια και ακρίβεια στο συμβόλαιο συμφωνίας μεταξύ Κυβέρνησης και Παρόχου. Οι ενδεχόμενες αλλαγές αφορούν την αναστολή ή τον περιορισμό της λειτουργίας του Παρόχου ή ακόμα και την εξαγορά του από άλλο Πάροχο.

- Ιδιαίτερο βάρος οφείλει να δώσει η Κυβέρνηση στην εκπαίδευση των τελικών χρηστών και κυρίως εκείνων που διατηρούν το δικαίωμα μεταφοράς δεδομένων στο Νέφος. Ως χρήστες αναφέρονται τόσο οι Δημόσιοι λειτουργοί όσο και οι πολίτες. Η εκπαίδευση θα πρέπει να είναι προσανατολισμένη τόσο στην ορθή χρήση των υπηρεσιών όσο και στην εκμάθηση ατομικών κανόνων προστασίας στο Νέφος.

- Η Κυβέρνηση οφείλει την προώθηση της έρευνας σε ζητήματα ασφάλειας και προστασίας της Ιδιωτικότητας αλλά και της πιστοποίησης των εφαρμογών σε περιβάλλον Νέφους.

Συμπερασματικά, η μετάβαση ενός Δημόσιου Οργανισμού ή του συνόλου τη Δημόσιας Διοίκησης στο Νέφος αποτελεί μία ιδιαίτερα δύσκολη υπόθεση. Απαιτεί τη χάραξη και την τήρηση μίας ολοκληρωμένης πολιτικής από την πλευρά της Κυβέρνησης ώστε να διασφαλιστεί η λειτουργία και η συνέχεια των Δημόσιων Υπηρεσιών και των Κρίσιμων Υποδομών ενός κράτους.

Κεφάλαιο 3ο

Νομικό Πλαίσιο

Η επέκταση του πεδίου εφαρμογής της Νεφοϋπολογιστικής στον τομέα της έρευνας, της Δημόσιας Διοίκησης, στο ηλεκτρονικό εμπόριο κτλ δημιούργησε την ανάγκη θέσπισης ενός ολοκληρωμένου Νομικού πλαισίου, το οποίο θα διέπει τη λειτουργία και τη χρήση των Υποδομών Νέφους. Η θέσπιση των κανόνων αυτών στοχεύουν στην ασφαλή και απρόσκοπτη λειτουργία των Υποδομών Νέφους, ενώ παράλληλα καθορίζει με σαφήνεια τις υποχρεώσεις και τα δικαιώματα τόσο των χρηστών όσο και των Παρόχων υπηρεσιών Νέφους (Cloud Provider). Ωστόσο, παρά το γεγονός ότι αναγνωρίζεται παγκοσμίως η ανάγκη για ασφάλεια και προστασία των δεδομένων που φυλάσσονται στις Υποδομές αυτές, το Νομικό πλαίσιο κάποιων κρατών δεν διαφυλάσσει πλήρως το δικαίωμα του χρήστη για προστασία της Ιδιωτικότητας των πληροφοριών του. Χαρακτηριστικό παράδειγμα αποτελούν οι Ηνωμένες Πολιτείες της Αμερικής, οι οποίες δε διέπονται από ένα ολοκληρωμένο και σταθερό Νομικό Πλαίσιο αλλά αντιθέτως δίνει τη δυνατότητα επέμβασης στη λειτουργία των Παρόχων και την επιβολή αποκάλυψης των πληροφοριών των χρηστών, υπό συγκεκριμένες προϋποθέσεις. Αντιθέτως, η Ευρωπαϊκή Ένωση υιοθετεί ένα πιο αυστηρό πλαίσιο, το οποίο έχουν ενσωματώσει στη Νομοθεσία τους όλα τα κράτη-μέλη. Στο Κεφάλαιο αυτό παρουσιάζονται τα βασικά σημεία του Νομικού Πλαισίου για την προστασία των δεδομένων, που διέπει τόσο τα κράτη-μέλη της Ευρωπαϊκής Ένωσης όσο και τις Η.Π.Α. Ιδιαίτερη αναφορά γίνεται στην ενσωμάτωση των Ευρωπαϊκών οδηγιών στο ελληνικό Νομικό πλαίσιο, καθώς και στη σύμβαση που καθορίζει την ασφάλεια των Δεδομένων των Ευρωπαίων πολιτών, τα οποία φυλάσσονται σε κέντρα δεδομένων εντός της Αμερικανικής επικράτειας.

3.1 Ευρωπαϊκή Νομοθεσία

3.1.1 Το Ευρωπαϊκό νομικό πλαίσιο προστασίας δεδομένων

Είναι γεγονός ότι η εποχή που διανύουμε είναι άμεσα συνυφασμένη με το Διαδίκτυο και τη διακίνηση των πληροφοριών. Οι νέες τεχνολογίες ευνοούν την άμεση και ταχεία διακίνηση των δεδομένων. Ωστόσο, η διακίνηση και η κάθε είδους διαχείριση προσωπικών ή ευαίσθητων δεδομένων απαιτεί συγκεκριμένους κανόνες προστασίας και ασφάλειας. Για το λόγο αυτό, η Ευρωπαϊκή Ένωση έχει δημιουργήσει ένα ολοκληρωμένο νομικό πλαίσιο, με σκοπό την προστασία των φυσικών προσώπων από την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την ελεύθερη κυκλοφορία των δεδομένων αυτών. Η θέσπιση των Νόμων αυτών αποσκοπεί τόσο στην προστασία των θεμελιωδών δικαιωμάτων και της ιδιωτικής ζωής του ατόμου όσο και στην τεχνική και επιστημονική συνεργασία μεταξύ των κρατών-μελών, στην ολοένα αναπτυσσόμενη κοινωνία της Πληροφορικής και των Επικοινωνιών.

Το πιο πρόσφατο και συναφές Ευρωπαϊκό νομοθετικό πλαίσιο αποτελείται από:

- Την 95/46/ΕΚ οδηγία για την προστασία των δεδομένων, η οποία ισχύει σε κάθε περίπτωση όπου υφίσταται επεξεργασία δεδομένων προσωπικού χαρακτήρα

- Την 2002/58/ΕΚ οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες (όπως αναθεωρήθηκε με την 2009/136/ΕΚ οδηγία) και η οποία 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). Ως εκ τούτου, εφαρμόζεται και όταν οι συναφείς υπηρεσίες παρέχονται μέσω Υπολογιστικού Νέφους.

- Την 2006/24/ΕΚ οδηγία, για τη διατήρηση των δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών και για την τροποποίηση της οδηγίας 2002/58/ΕΚ.

Με βάση τις οδηγίες αυτές, τα κράτη-μέλη της Ευρωπαϊκής Ένωσης υποχρεούνται να θεσπίσουν και να εφαρμόσουν νομοθεσία σχετική με την προστασία των δεδομένων προσωπικού χαρακτήρα. Επιπλέον επιβάλλεται και η δημιουργία της σχετικής εποπτικής αρχής, η οποία οφείλει να διασφαλίζει την εφαρμογή της νομοθεσίας.

Ακολουθεί μία συνοπτική περιγραφή των βασικών άρθρων των οδηγιών 95/46/ΕΚ και 2002/58/ΕΚ (όπως αναθεωρήθηκε από την 2009/136/ΕΚ).

3.1.2 Η οδηγία 95/46/ΕΚ

Όπως προαναφέρθηκε, το 1995 θεσπίστηκε από την Ευρωπαϊκή Ένωση η οδηγία 95/46/ΕΚ ως ένα γενικό πλαίσιο προστασίας των δεδομένων προσωπικού χαρακτήρα. Με την οδηγία αυτή, η Ευρωπαϊκή Ένωση απέκτησε ένα από τα πιο συνεκτικά και

αναλυτικά νομοθετικά κείμενα που επηρέασαν και επηρεάζουν παγκοσμίως τη διεθνή κανονιστική παραγωγή σε θέματα προστασίας προσωπικών δεδομένων [31].

Σύμφωνα με την οδηγία και το Άρθρο 1 αυτής, πρωταρχικός σκοπός της είναι τα κράτη-μέλη να εξασφαλίζουν την προστασία των θεμελιωδών ελευθεριών και δικαιωμάτων των φυσικών προσώπων και της ιδιωτικής ζωής, έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα. Επίσης, επιδιώκεται η εξασφάλιση της προστασίας των δεδομένων αυτών έτσι ώστε να αίρεται κάθε περιορισμός στην ελεύθερη διακίνηση των δεδομένων αυτών, μεταξύ των κρατών-μελών.

Η οδηγία παρέχει τις κατευθυντήριες γραμμές σχετικά με την ποιότητα των δεδομένων που συλλέγονται. Στο Άρθρο 6 ορίζεται ότι τα κράτη- μέλη θα πρέπει να προβλέπουν με τη σχετική νομοθεσία τους τα χαρακτηριστικά των δεδομένων που συλλέγονται προς επεξεργασία. Πιο συγκεκριμένα, ορίζεται ότι τα δεδομένα θα πρέπει να συλλέγονται μόνο για καθορισμένους, σαφής και νόμιμους σκοπούς, ενώ η μετέπειτα επεξεργασία τους να είναι συναφής με το σκοπό της συλλογής τους. Ένα βασικό στοιχείο που εισάγεται στο άρθρο αυτό είναι ότι τα δεδομένα που συλλέγονται και επεξεργάζονται θα πρέπει να είναι ακριβή και έγκυρα και ταυτόχρονα να διατηρούνται σε μορφή που επιτρέπει τον προσδιορισμό της ταυτότητας του ατόμου, στο οποίο αναφέρονται, μόνο κατά τη διάρκεια της περιόδου που απαιτείται για την επίτευξη του στόχου της συλλογής. Ως αποκλειστικά υπεύθυνος για την τήρηση των κανόνων αυτών θεωρείται αποκλειστικά ο υπεύθυνος της επεξεργασίας των δεδομένων.

Εκτός από την ποιότητα των δεδομένων, η οδηγία αναφέρει και τις βασικές αρχές, στα πλαίσια των οποίων θα πρέπει να λαμβάνει χώρα η επεξεργασία των δεδομένων προσωπικού χαρακτήρα. Χαρακτηριστικά, ορίζεται σαφώς ότι δύναται επεξεργασία των δεδομένων μόνο με τη ρητή συγκατάθεση του προσώπου ή για περιπτώσεις εκπλήρωσης δημόσιου συμφέροντος. Επίσης, δύναται επεξεργασία των δεδομένων όταν κρίνεται απαραίτητη για τη διαφύλαξη του ζωτικού συμφέροντος του προσώπου στο οποίο αναφέρονται τα δεδομένα. Στο Άρθρο 7 της οδηγίας αναφέρονται όλες οι περιπτώσεις κατά τις οποίες είναι δυνατή η επεξεργασία των δεδομένων προσωπικού χαρακτήρα.

Ιδιαίτερη βαρύτητα κατέχει το Άρθρο 8 κατά το οποίο εισάγεται η έννοια των «Ευαίσθητων προσωπικών Δεδομένων» ρυθμίζοντας τις ειδικές κατηγορίες των δεδομένων εκείνων για τις οποίες απαγορεύεται ρητά η συλλογή και η επεξεργασία τους. Οι ειδικές αυτές κατηγορίες αναφέρονται στα δεδομένα που προσδιορίζουν τη φυλετική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές πεποιθήσεις, την υγεία και τη σεξουαλική ζωή κτλ. Ωστόσο, καθορίζονται και οι εξαιρέσεις από την εφαρμογή του Άρθρου 8, με χαρακτηριστικό παράδειγμα την περίπτωση όπου το πρόσωπο στο οποίο αναφέρονται τα δεδομένα δίνει τη ρητή συγκατάθεση του. Ταυτόχρονα, η οδηγία δίνει στα κράτη-μέλη τη δυνατότητα να θεσπίσουν και άλλες παρεκκλίσεις, εκτός από τις προβλεπόμενες, για περιπτώσεις εκπλήρωσης δημόσιου συμφέροντος, με τη θέσπιση ειδικών νομοθετικών διατάξεων.

Στα άρθρα που ακολουθούν, αναγνωρίζονται τα θεμελιώδη δικαιώματα του προσώπου αναφορικά με το δικαίωμα της ενημέρωσης, παρακολούθησης και αντίταξης στην επεξεργασία των προσωπικών του δεδομένων. Πιο συγκεκριμένα,

στα Άρθρα 10 – 11 - 12 καθορίζεται ρητά ότι τα κράτη- μέλη οφείλουν να διασφαλίσουν ότι το πρόσωπο, του οποίου τα δεδομένα επεξεργάζονται, δύναται να γνωρίζει ανά πάσα στιγμή την ταυτότητα του υπεύθυνου επεξεργασίας, το σκοπό της συλλογής των προσωπικών του δεδομένων αλλά και σχετικές πληροφορίες αναφορικά με το δικαίωμα του στην πρόσβαση και διόρθωση των δεδομένων επεξεργασίας αλλά και τους αποδέκτες των δεδομένων αυτών. Τα Άρθρα 14-15 αναγνωρίζουν το δικαίωμα του ατόμου να αντιτάσσεται ανά πάσα στιγμή στην συλλογή και την επεξεργασία των προσωπικών του δεδομένων. Στα Άρθρα 22-23-24 η οδηγία επιβάλει στα κράτη μέλη τη θέσπιση ειδικής νομοθεσίας για καταλογισμό ευθυνών και επιβολής κυρώσεων στις περιπτώσεις μη συμμόρφωσης με τις εθνικές διατάξεις της παρούσας οδηγίας. Ταυτόχρονα, αναγνωρίζεται το δικαίωμα του κάθε ατόμου να χρησιμοποιεί ένδικα μέσα στις περιπτώσεις παραβίασης των προσωπικών του δεδομένων, χωρίς την προηγούμενη συγκατάθεσή του.

Στην οδηγία και συγκεκριμένα στο Άρθρο 25, αναπτύσσονται ιδιαίτερα σημαντικές διατάξεις με τις οποίες προβλέπεται η δυνατότητα μεταβίβασης των προσωπικών δεδομένων από ένα κράτος – μέλος σε τρίτη χώρα, με την προϋπόθεση ότι η εν λόγω τρίτη χώρα εξασφαλίζει ικανοποιητικό επίπεδο προστασίας. Η επάρκεια της προστασίας που παρέχεται από τρίτη χώρα σταθμίζεται λαμβανομένων υπόψη όλων των περιστάσεων που επηρεάζουν μια διαβίβαση ή κατηγορία διαβιβάσεων δεδομένων. Ειδικότερα, εξετάζονται η φύση των δεδομένων, οι σκοποί και η διάρκειά της ή των προβλεπομένων επεξεργασιών, η χώρα προέλευσης και τελικού προορισμού, οι γενικοί ή τομεακοί κανόνες δικαίου, οι επαγγελματικοί κανόνες και τα μέτρα ασφαλείας που ισχύουν στην εν λόγω τρίτη χώρα.

Εξαιτίας των διατάξεων αυτών, προέκυψε η ανάγκη δημιουργίας ενός συγκεκριμένου θεσμικού πλαισίου το οποίο αφορά τη μεταβίβαση των δεδομένων από τα κράτη - μέλη της Ευρωπαϊκής Ένωσης στις Η.Π.Α. Το αιτιολογικό βασίζεται στο γεγονός ότι οι Η.Π.Α. αποτελούν το σημαντικότερο πολιτικό και οικονομικό εταίρο της Ε.Ε., ο οποίος όμως δε διαθέτει ικανοποιητικό και συμβατό με την Ε.Ε., νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων των ατόμων. Έτσι, για τη διαβίβαση των προσωπικών δεδομένων στις Η.Π.Α. εφαρμόστηκε, μεταξύ των δύο μερών, η συμφωνία που βασίζεται «στις Αρχές του ασφαλούς λιμένα» (Safe Harbor). Η συμφωνία αυτή περιγράφεται σε ακόλουθη ενότητα.

Τέλος, η οδηγία δημιουργεί την υποχρέωση (Άρθρο 28) στα κράτη-μέλη να δημιουργήσουν ανεξάρτητη εποπτική Αρχή με σκοπό τον έλεγχο της εφαρμογής των εθνικών διατάξεων που έχουν θεσπισθεί από τα κράτη μέλη, κατ' εφαρμογή της παρούσας οδηγίας. Επίσης, με το Άρθρο 29 προβλέπεται η δημιουργία ανεξάρτητης ομάδας εργασίας, η οποία έχει αποστολή να εξετάζει και να παρέχει τη γνώμη της για οποιοδήποτε θέμα σχετικό με την εφαρμογή των εθνικών διατάξεων που έχουν θεσπισθεί κατ' εφαρμογή της παρούσας οδηγίας, ώστε να συμβάλλει στην ομοιόμορφη εφαρμογή τους.

Όλα τα κράτη- μέλη όφειλαν τη συμμόρφωσής τους με την παρούσα οδηγία, θέτοντας σε ισχύ τις αναγκαίες νομοθετικές, κανονιστικές και διοικητικές διατάξεις εντός τριών ετών από την έκδοση της οδηγίας.

3.1.3 Η οδηγία 2002/58/ΕΚ (όπως αναθεωρήθηκε με την 2009/136/ΕΚ)

Η οδηγία 2002/58/ΕΚ προέκυψε έπειτα από τη ραγδαία ανάπτυξη των τεχνολογιών στο περιβάλλον των τηλεπικοινωνιών. Ο τομέας αυτός κρίθηκε ιδιαίτερα επικίνδυνος για επιθέσεις εναντίον των προσωπικών δεδομένων και της ιδιωτικής ζωής του ατόμου, με αποτέλεσμα την ανάγκη για εξειδίκευση της οδηγίας 95/46/ΕΚ στο περιβάλλον των τηλεπικοινωνιών. Ωστόσο, οι συνεχόμενες και ραγδαίες τεχνολογικές εξελίξεις οδήγησαν στην αναθεώρηση της οδηγίας, με σκοπό την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες, ανεξάρτητα από τη χρησιμοποιούμενη τεχνολογία. Έτσι, ο όρος «επικοινωνία» αναφέρεται σε κάθε πληροφορία που διαβιβάζεται μέσω μίας διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών. Συνεπώς, μπορεί να θεωρηθεί ότι η 2002/58 οδηγία, μετά την αναθεώρηση της από τη 2009/136/ΕΚ, καλύπτει και την προστασία των δεδομένων σε περιβάλλον Νεφοϋπολογιστικής.

Η οδηγία αυτή, όπως ορίζεται στο Άρθρο 3, εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών σε δημόσια δίκτυα επικοινωνιών, περιλαμβανομένων των δημόσιων δικτύων επικοινωνιών που υποστηρίζουν συσκευές συλλογής δεδομένων και ταυτοποίησης.

Ιδιαίτερη βαρύτητα δίνεται αναφορικά με την ασφάλεια της επεξεργασίας των δεδομένων τόσο από τον Πάροχο όσο και από οποιοδήποτε ενδεχόμενο κακόβουλο χρήστη. Πιο συγκεκριμένα, στο Άρθρο 4 ορίζεται ότι οι αρμόδιες εθνικές αρχές πρέπει να είναι σε θέση να ελέγχουν τα μέτρα που λαμβάνονται από Παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών και να εκδίδουν συστάσεις σχετικά με βέλτιστες πρακτικές, όσον αφορά το επίπεδο ασφάλειας το οποίο πρέπει να επιτυγχάνεται με αυτά τα μέτρα.

Ως ελάχιστες απαιτήσεις ασφάλειας, τις οποίες οφείλει να εξυπηρετεί ο Πάροχος είναι:

- Η εξασφάλιση ότι η πρόσβαση σε προσωπικά δεδομένα μπορεί να γίνει μόνον από εξουσιοδοτημένο προσωπικό και για αυστηρά νομίμως εγκεκριμένους σκοπούς.

- Η προστασία των αποθηκευμένων ή των μεταδιδόμενων δεδομένων προσωπικού χαρακτήρα από τυχαία ή παράνομη καταστροφή, απώλεια ή αλλοίωση, καθώς και από παράνομη αποθήκευση, επεξεργασία, πρόσβαση ή αποκάλυψη.

- Η διασφάλιση της εφαρμογής της πολιτικής ασφάλειας σε σχέση με την επεξεργασία προσωπικών δεδομένων.

Σύμφωνα με την οδηγία, τα κράτη μέλη οφείλουν τη θέσπιση νομοθεσίας έτσι ώστε να επιβάλλεται στους Παρόχους η λήψη των κατάλληλων τεχνικών ή οργανωτικών μέτρων ώστε να κατοχυρώνεται ένα αποδεκτό επίπεδο ασφάλειας. Ακόμη και σε περίπτωση παραβίασης των προσωπικών δεδομένων, ο Πάροχος υποχρεούται να γνωστοποιήσει το γεγονός τόσο στην αρμόδια εθνική αρχή όσο και στο ίδιο το πρόσωπο του οποίου τα δεδομένα παραβιάστηκαν. Στο ίδιο άρθρο καθορίζεται και η

μορφή αποθήκευσης των δεδομένα, δηλαδή σε μορφή μη κατανοητή για μη εξουσιοδοτημένα πρόσωπα.

Οι Πάροχοι τηρούν αρχείο παραβιάσεων δεδομένων προσωπικού χαρακτήρα που περιλαμβάνει την περιγραφή των σχετικών περιστατικών, τα αποτελέσματά τους και τα ένδικα μέσα που έχουν ληφθεί, σε επίπεδο που να επιτρέπει στις αρμόδιες εθνικές αρχές να διαπιστώνουν τη συμμόρφωση με τις διατάξεις της παραγράφου περί γνωστοποίησης των παραβιάσεων. Το αρχείο περιλαμβάνει μόνον τις πληροφορίες που απαιτούνται προς το σκοπό αυτό.

Στο Άρθρο 5 της οδηγίας εισάγεται η έννοια του απορρήτου των επικοινωνιών με το οποίο απαγορεύεται η ακρόαση, υποκλοπή, αποθήκευση ή άλλο είδος παρακολούθησης και επιτήρησης των επικοινωνιών και των συναφών δεδομένων κίνησης, χωρίς τη συγκατάθεση των ενδιαφερομένων χρηστών, εκτός αν υπάρχει σχετική νόμιμη άδεια. Ωστόσο δεν εμποδίζεται η τεχνική αποθήκευσης, η οποία είναι αναγκαία για τη διαβίβαση της επικοινωνίας, με την επιφύλαξη της αρχής του απορρήτου.

Στο Άρθρο 6 της οδηγίας αναφέρονται οι κατευθυντήριες γραμμές οι οποίες θα πρέπει να υιοθετήσουν τα κράτη-μέλη σχετικά με την αποθήκευση και επεξεργασία των δεδομένων κίνησης, δηλαδή των δεδομένων που επεξεργάζονται οι Πάροχοι για τους σκοπούς της διαβίβασης μιας επικοινωνίας σε δίκτυο ηλεκτρονικών επικοινωνιών ή της χρέωσής της. Πιο συγκεκριμένα, τα δεδομένα που αφορούν συνδρομητές ή χρήστες θα πρέπει να απαλείφονται ή να καθίστανται ανώνυμα όταν δεν είναι απαραίτητα για το σκοπό της επικοινωνίας. Από την άλλη μεριά, τα δεδομένα που είναι απαραίτητα για τη χρέωση συνδρομητών μπορούν να υποβάλλονται σε επεξεργασία, μόνο έως το τέλος της χρονικής περιόδου εντός της οποίας δύναται να αμφισβητείται νομίμως ο λογαριασμός ή να επιδιώκεται η πληρωμή. Τέλος, ορίζεται ότι τα κράτη-μέλη θα πρέπει να επιβάλλουν στους Παρόχους την ενημέρωση των χρηστών για τον τύπο των δεδομένων που θέτουν σε επεξεργασία, ενώ η επεξεργασία αυτή μπορεί να λάβει χώρα μόνο από πρόσωπα τα οποία ενεργούν υπό την εποπτεία του Παρόχου. Να σημειωθεί ότι οι ίδιες διατάξεις που περιγράφονται στο Άρθρο αυτό, ισχύουν κατά βάση και για τα δεδομένα θέσης, τα οποία περιγράφονται αναλυτικά στο Άρθρο 9.

Σύμφωνα με την παρούσα οδηγία, τα κράτη – μέλη οφείλουν να μεριμνούν για την εφαρμογή των διατάξεων χωρίς όμως να επιβάλλουν καμία υποχρεωτική απαίτηση σχετικά με ειδικά τεχνικά χαρακτηριστικά στις τερματικές συσκευές ή στον άλλο εξοπλισμό ηλεκτρονικών επικοινωνιών, η οποία θα μπορούσε να παρακωλύσει τη διάθεση εξοπλισμού στην αγορά και την ελεύθερη κυκλοφορία του εξοπλισμού αυτού στα κράτη μέλη ή μεταξύ των κρατών μελών. Ωστόσο, μπορούν να θεσπιστούν μέτρα που να εξασφαλίζουν ότι ο τερματικός εξοπλισμός είναι κατασκευασμένος κατά τρόπο συμβατό με το δικαίωμα των χρηστών να προστατεύουν και να ελέγχουν τη χρησιμοποίηση των προσωπικών τους δεδομένων.

3.2 Η Ελληνική Νομοθεσία

3.2.1 Το Ελληνικό νομικό πλαίσιο προστασίας των δεδομένων – Συνταγματική κατοχύρωση

Ο σεβασμός και η προστασία της ιδιωτικής ζωής θα πρέπει να αποτελεί πρωταρχικό σκοπό κάθε δημοκρατικής κοινωνίας. Ωστόσο, η ραγδαία εξέλιξη των τεχνολογιών και η υιοθέτησή τους τόσο στον Ιδιωτικό όσο και στο Δημόσιο Τομέα έχουν ως συνέπεια την αυξημένη ζήτηση προσωπικών δεδομένων. Η Ελλάδα, στο πλαίσιο των τεχνολογικών αυτών εξελίξεων αλλά και ως κράτος-μέλος της Ευρωπαϊκής Ένωσης, υποχρεώθηκε στη θέσπιση ενός ολοκληρωμένου Νομικού πλαισίου για την προστασία της Ιδιωτικότητας των Ελλήνων πολιτών, σύμφωνα πάντα με τις οδηγίες τις Ε.Ε. που αναφέρθηκαν στην προηγούμενη ενότητα. Πιο συγκεκριμένα, το Νομικό πλαίσιο στην Ελλάδα καθορίζεται από:

- Το Σύνταγμα της Ελλάδος (αναθεώρηση 2001, ‘Άρθρο 9Α)
- Το Ν. 2472/1997 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα
- Το Ν. 3471/2006 για την προστασία των δεδομένων προσωπικού χαρακτήρα και της Ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών
- Το Ν. 3917/2011 για τη διατήρηση των 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.

Με το Νομοθετικό πλαίσιο αυτό, η Ελλάδα συμμορφώνεται πλήρως με τις οδηγίες της Ευρωπαϊκής Ένωσης για την προστασία των δεδομένων προσωπικού χαρακτήρα. Με το ψήφισμα της 6ης Απριλίου 2001 της Ζ’ Αναθεωρητικής Βουλής των Ελλήνων, η προστασία των προσωπικών δεδομένων κατοχυρώνεται ρητά και ενσωματώνεται στο «Σύνταγμα της Ελλάδος» με το Άρθρο 9Α του Συντάγματος. Πιο συγκεκριμένα, ορίζεται ότι « *Καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως ο νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή που συγκροτείται και λειτουργεί, όπως ο νόμος ορίζει.* » [33].

Ακολουθεί μία συνοπτική περιγραφή των Νόμων 2472/1997 και 3471/2006.

3.2.2 Ο Νόμος 2472/1997

Η Κοινοτική οδηγία 95/46 για την προστασία των ατόμων απέναντι στην επεξεργασία προσωπικών δεδομένων ενσωματώθηκε στην ελληνική Νομοθεσία με το

Ν. 2472/1997 με σκοπό την προστασία των ατόμου από την επεξεργασία των δεδομένων προσωπικού χαρακτήρα. Ο Νόμος αποτελείται από έξι (6) Κεφάλαια και είκοσι έξι (26) άρθρα, τα βασικότερα των οποίων περιγράφονται ακολούθως.

ΚΕΦΑΛΑΙΟ Α΄: Πεδίο Εφαρμογής και Ορισμοί

Το πρώτο Κεφάλαιο περιλαμβάνει τα Άρθρα 1-3 στα οποία ορίζεται το αντικείμενο του Νόμου καθώς και το πεδίο εφαρμογής του. Πιο συγκεκριμένα, ως αντικείμενο ορίζεται η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα προς προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής. Ως πεδίο εφαρμογής του Νόμου αναφέρεται στην εν όλο ή εν μέρει αυτοματοποιημένη επεξεργασία καθώς και στη μη αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε αρχείο. Ωστόσο, ο νομοθέτης ορίζει ότι ο Νόμος εφαρμόζεται στην περίπτωση που η επεξεργασία των δεδομένων προσωπικού χαρακτήρα εκτελείται από υπεύθυνο επεξεργασίας εγκατεστημένο είτε στην Ελληνική επικράτεια είτε σε κάποια Τρίτη χώρα εκτός Ευρωπαϊκής Ένωσης αλλά για την επεξεργασία των δεδομένων χρησιμοποιεί μέσα, αυτοματοποιημένα ή μη, ευρισκόμενα εντός της Ελληνικής Επικράτειας.

ΚΕΦΑΛΑΙΟ Β΄: Επεξεργασίας δεδομένων προσωπικού χαρακτήρα

Το δεύτερο Κεφάλαιο περιλαμβάνει τα Άρθρα 4-10 και αναφέρεται στις προϋποθέσεις που θα πρέπει να πληρούνται προκειμένου ο υπεύθυνος επεξεργασίας να προβεί σε νόμιμη επεξεργασία προσωπικών δεδομένων. Η νομιμότητας της επεξεργασίας αναφέρεται σε δύο κατευθύνσεις: στην ποιότητα των δεδομένων που συλλέγονται και στις προϋποθέσεις επεξεργασίας των δεδομένων αυτών.

Αναφορικά με την ποιότητα των δεδομένων, ο Νομοθέτης ορίζει πως η συλλογή τους θα πρέπει να βασίζεται σε καθορισμένους, νόμιμους, σαφής και ακριβής σκοπούς, ενώ και τα ίδια θα πρέπει να είναι συναφή με το σκοπό της επεξεργασίας τους, ακριβή και ενημερωμένα. Ταυτόχρονα, επιβάλλεται η διατήρησή τους σε μορφή που να επιτρέπει τον προσδιορισμό της ταυτότητας των υποκειμένων τους μόνο κατά τη διάρκεια που απαιτείται για την επεξεργασία και την εκπλήρωση του σκοπού αυτής. Σημειώνεται ότι αποκλειστικά υπεύθυνος για την ποιότητα των δεδομένων που συλλέγονται και επεξεργάζονται είναι ο υπεύθυνος επεξεργασίας.

Εκτός από την ποιότητα των δεδομένων ο νομοθέτης προβλέπει και τις προϋποθέσεις για νόμιμη επεξεργασία των δεδομένων. Αναφέρεται ρητά ότι η επεξεργασία των δεδομένων επιτρέπεται μόνο με τη συγκατάθεση του υποκειμένου των δεδομένων, εκτός αν συντρέχουν συγκεκριμένες προϋποθέσεις όπως η διασφάλιση ζωτικού συμφέροντος του υποκειμένου, η εκτέλεση έργου δημοσίου συμφέροντος κτλ χωρίς φυσικά να θίγονται τα δικαιώματα και η ελευθερία των προσώπων στα οποία αναφέρονται τα δεδομένα.

Με το Άρθρο 7 εισάγεται η έννοια των «Ευαίσθητων προσωπικών δεδομένων» και

καθορίζονται οι προϋποθέσεις επεξεργασίας τους. Κατά βάση, πέραν των συγκεκριμένων εξαιρέσεων που ορίζει ο Νόμος, απαγορεύεται ρητά η συλλογή και επεξεργασία ευαίσθητων δεδομένων. Ωστόσο, η Αρχή Προστασίας Δεδομένων διατηρεί το δικαίωμα χορήγησης αδειών επεξεργασίας ύστερα από σχετική αίτηση του υπεύθυνου επεξεργασίας. Η άδεια παραχωρείται για συγκεκριμένους σκοπούς και εκδίδεται για ορισμένο χρόνο. Ωστόσο, η εποπτεύουσα Αρχή μπορεί να επιβάλει συγκεκριμένους όρους και προϋποθέσεις για την αποτελεσματικότερη προστασία της ιδιωτικής ζωής του ατόμου. Σε κάθε περίπτωση, πέραν των περιπτώσεων που ορίζει ο Νόμος, ο υπεύθυνος επεξεργασίας οφείλει να γνωστοποιεί στην εποπτεύουσα Αρχή την έναρξη της λειτουργίας επεξεργασίας προσωπικών ή ευαίσθητων δεδομένων.

Ο νομοθέτης συνεχίζει με τον καθορισμό των προϋποθέσεων για τη διασύνδεση δύο ή περισσότερων αρχείων τα οποία εξυπηρετούν διαφορετικούς σκοπούς. Πιο συγκεκριμένα, ο/οι υπεύθυνος/οι επεξεργασίας υποβάλλουν από κοινού δήλωση με την οποία γνωστοποιείται η διασύνδεση των αρχείων στην εποπτεύουσα Αρχή. Στην περίπτωση που ένα από τα αρχεία που πρόκειται να διασυνδεθούν περιέχει ευαίσθητα δεδομένα, η διασύνδεση επιτρέπεται μόνο με προηγούμενη άδεια της εποπτεύουσας Αρχής. Η άδεια περιλαμβάνει κατ΄ ελάχιστον το σκοπό, τη διάρκεια και τους όρους επεξεργασίας, καθώς και το είδος των δεδομένων που αφορά η διασύνδεση.

Στη συνέχεια του Νόμου και συγκεκριμένα στο Άρθρο 9, καθορίζεται η μεταβίβαση των δεδομένων προσωπικού χαρακτήρα εκτός της Ελληνικής επικράτειας. Ορίζεται ότι η διακίνηση των προσωπικών δεδομένων πραγματοποιείται ελεύθερα σε χώρες της Ευρωπαϊκής Ένωσης, ενώ δύναται η μεταβίβαση και σε τρίτες χώρες υπό προϋποθέσεις και έπειτα από άδεια της εποπτεύουσας Αρχής, εάν κρίνει ότι η εν λόγω χώρα εξασφαλίζει ικανοποιητικό επίπεδο προστασίας. Δεν απαιτείται άδεια της Αρχής εφόσον η Ευρωπαϊκή Επιτροπή έχει αποφανθεί για ικανοποιητικό επίπεδο προστασίας της χώρας αυτής. Πάντως, σε κάθε περίπτωση ο υπεύθυνος επεξεργασίας θα πρέπει να λαμβάνει τα κατάλληλα οργανωτικά και τεχνικά μέτρα ώστε να διασφαλίζεται το απόρρητο και η ασφάλεια της επεξεργασίας των δεδομένων.

ΚΕΦΑΛΑΙΟ Γ΄: Δικαιώματα του υποκειμένου των δεδομένων

Στο τρίτο Κεφάλαιο και συγκεκριμένα στα Άρθρα 11-14, αναγνωρίζονται και κατοχυρώνονται τα δικαιώματα του υποκειμένου για την προστασία των προσωπικών του δεδομένων. Ορίζεται σαφώς:

- Το δικαίωμα του υποκειμένου για ενημέρωση σχετικά με την ταυτότητα του υπεύθυνου επεξεργασίας, του σκοπού της επεξεργασίας, τους αποδέκτες των δεδομένων και των αποτελεσμάτων.

- Το δικαίωμα πρόσβασης του υποκειμένου ανά πάσα στιγμή στα δεδομένα που επεξεργάζονται

- Το δικαίωμα να προβάλλει οποτεδήποτε αντιρρήσεις για την επεξεργασία των δεδομένων που το αφορούν.

- Το δικαίωμα του υποκειμένου να χρησιμοποιεί τα ένδικα μέσα με σκοπό την

αναστολή ή τη μη εφαρμογή της επεξεργασίας των δεδομένων που το αφορούν, εφόσον η επεξεργασία αυτή παραβιάζει την Ιδιωτική του ζωή.

ΚΕΦΑΛΑΙΟ Δ΄: Αρχή Προστασίας Δεδομένων Προσωπικού χαρακτήρα

Το τέταρτο Κεφάλαιο περιλαμβάνει τα Άρθρα 15-20 και αναφέρεται στη σύσταση της ανεξάρτητης Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Πιο συγκεκριμένα, ο νομοθέτης ορίζει στο Άρθρο 15 τη σύσταση της Αρχής με αποστολή την εποπτεία της εφαρμογής του παρόντος νόμου και άλλων ρυθμίσεων που αφορούν την προστασία του ατόμου και της Ιδιωτικής του ζωής. Η Αρχή αποτελεί ανεξάρτητη δημόσια αρχή και υπάγεται στον Υπουργό Δικαιοσύνης. Στα υπόλοιπα άρθρα ορίζονται ρητά οι όροι σύστασης της Αρχής, οι υποχρεώσεις και τα δικαιώματα των μελών καθώς και οι αρμοδιότητες και οι λειτουργίες της Αρχής.

ΚΕΦΑΛΑΙΟ Ε΄-ΣΤ΄: Κυρώσεις και Μεταβατικές Διατάξεις

Στο πέμπτο Κεφάλαιο ορίζονται οι ποινές που επιβάλλει η Αρχή στους υπεύθυνους επεξεργασίας, για τυχόν παράβαση των υποχρεώσεων τους που απορρέουν από αυτό τον Νόμο. Το έκτο Κεφάλαιο ορίζει τις απαραίτητες μεταβατικές διατάξεις προς εφαρμογή του Νόμου.

3.2.3 Ο Νόμος 3471/2006

Η Κοινοτική οδηγία 2002/58 ενσωματώθηκε στην ελληνική Νομοθεσία με το Ν. 3471/2006 με σκοπό την προστασία των θεμελιωδών δικαιωμάτων των ατόμων και της ιδιωτικής ζωής και τη θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τη διασφάλιση του απορρήτου των επικοινωνιών στον τομέα των ηλεκτρονικών επικοινωνιών. Όπως ορίζεται στο Νόμο, με τον όρο «Ηλεκτρονικές επικοινωνίες» νοούνται «*οι υπηρεσίες που παρέχονται συνήθως έναντι αμοιβής και των οποίων η παροχή συνίσταται, εν όλο ή εν μέρει, στη μεταφορά σημάτων σε δίκτυα ηλεκτρονικών επικοινωνιών, συμπεριλαμβανομένων των υπηρεσιών τηλεπικοινωνιών και των υπηρεσιών μετάδοσης σε δίκτυα που χρησιμοποιούνται για ραδιοτηλεοπτικές μεταδόσεις*». Συνεπώς, ο Νόμος εφαρμόζεται για την προστασία των Δεδομένων προσωπικού χαρακτήρα σε περιβάλλον Νεφοϋπολογιστικής.

Ιδιαίτερα σημαντικό είναι το Άρθρο 5 του Νόμου με το οποίο ο Νομοθέτης ορίζει ρητά του κανόνες επεξεργασίας των δεδομένων που διαβιβάζονται μέσω ηλεκτρονικών επικοινωνιών, ανεξάρτητα από τα τεχνικά μέσα που χρησιμοποιείται. Ως βασική αρχή ορίζεται ότι η επεξεργασία των δεδομένων προσωπικού χαρακτήρα, περιλαμβανομένων των δεδομένων κίνησης και θέσης, πρέπει να περιορίζεται στο απολύτως αναγκαίο μέτρο για την εξυπηρέτηση των σκοπών της. Ωστόσο, η επεξεργασία δύναται να λάβει χώρα μόνο με την έγγραφη ή με ηλεκτρονικά μέσα συγκατάθεση του υποκειμένου των δεδομένων ή όταν η επεξεργασίας είναι αναγκαία

για την εκτέλεση σύμβασης στην οποία ο χρήστης είναι συμβαλλόμενο μέρος.

Ιδιαίτερη μνεία γίνεται στο Άρθρο 6 για τα δεδομένα κίνησης και θέσης που υποβάλλονται σε επεξεργασία ενώ συνδέονται με συγκεκριμένους χρήστες. Εδώ, ο Νομοθέτης ορίζει ότι τα δεδομένα αυτά αποθηκεύονται μόνο κατά τη διάρκεια της επικοινωνίας και καταστρέφονται ή καθίστανται ανώνυμα μετά το πέρας αυτής. Η επεξεργασίας επιτρέπεται μόνο για σκοπούς χρέωσης του χρήστη και όχι για διάστημα μεγαλύτερο των δώδεκα (12) μηνών, εκτός εάν τίθεται θέμα αμφισβήτησης ή μη εξόφλησης της χρέωσης. Σε κάθε περίπτωση, η επεξεργασίας των δεδομένων αυτών καθίσταται δυνατή μόνο εφόσον αυτά καθίστανται ανώνυμα ή με τη ρητή συγκατάθεση του χρήστη, πάντα στην απαιτούμενη έκταση και διάρκεια για την παροχή μίας υπηρεσίας. Κατ` εξαίρεση επιτρέπεται, χωρίς προηγουμένη συγκατάθεση του χρήστη, η επεξεργασία δεδομένων θέσης από τους φορείς παροχής δημόσιου δικτύου ή διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών, προκειμένου να παρέχουν στις αρμόδιες για την αντιμετώπιση καταστάσεων έκτακτης ανάγκης αρχές, όπως στις διωκτικές αρχές, στις υπηρεσίες πρώτων βοηθειών και πυρόσβεσης, τις απαραίτητες πληροφορίες για τον εντοπισμό του καλούντος και μονό για το συγκεκριμένο αυτό σκοπό.

Στο Άρθρο 12 του Νόμου αυτού, ο νομοθέτης ορίζει τις υποχρεώσεις και τους κανόνες που επιβάλλονται στο Παρόχους ηλεκτρονικών επικοινωνών προκειμένου να διασφαλίζουν ικανοποιητικό επίπεδο ασφάλειας των δεδομένων προσωπικού χαρακτήρα κατά τη διάρκεια της επεξεργασίας τους. Πιο συγκεκριμένα, ως βασική υποχρέωση του Παρόχου αποτελεί η λήψη όλων των ενδεδειγμένων τεχνικών και οργανωτικών μέτρων προκειμένου να προστατεύεται η ασφάλεια των παρεχόμενων υπηρεσιών του. Στην περίπτωση που υφίσταται ιδιαίτερος κίνδυνος παραβίασης της ασφάλειας, ο Πάροχος οφείλει να ενημερώσει άμεσα τους χρήστες ή συνδρομητές του. Όπως ο νομοθέτης ορίζει, ο Πάροχος οφείλει κατ΄ ελάχιστον:

- Να εξασφαλίζεται ότι πρόσβαση σε δεδομένα προσωπικού χαρακτήρα μπορεί να έχει μόνο εξουσιοδοτημένο προσωπικό και μόνο για νόμιμα εγκεκριμένους σκοπούς

- Να προστατεύει τα αποθηκευμένα ή διαβιβασθέντα δεδομένα προσωπικού χαρακτήρα από τυχαία ή παράνομη καταστροφή, απώλεια ή αλλοίωση και από μη εξουσιοδοτημένη ή παράνομη επεξεργασία

- Να διασφαλίζει την εφαρμογή της πολιτικής ασφάλειας σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Σε περίπτωση παραβίασης των προσωπικών δεδομένων, ο Πάροχος των ηλεκτρονικών επικοινωνιών οφείλει την άμεση γνωστοποίηση της παραβίασης στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) και στην Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ). Στην περίπτωση που η παραβίαση αυτή επιφέρει επιπτώσεις στη ιδιωτική ζωή του ατόμου, ο Πάροχος οφείλει τη γνωστοποίηση της παραβίασης και στο θιγόμενο άτομο. Οι Πάροχοι οφείλουν να τηρούν αρχείο παραβιάσεων όπου περιλαμβάνεται η περιγραφή των σχετικών περιστατικών.

3.3 Η Νομοθεσία των Η.Π.Α.

3.3.1 Το Νομικό πλαίσιο περί προστασίας των δεδομένων και της Ιδιωτικής ζωής των Η.Π.Α.

Από τη Διακήρυξη Ανθρωπίνων δικαιωμάτων (1791) των Η.Π.Α. μέχρι και τις πρόσφατες αποκαλύψεις του Edward Snowden για παρακολούθηση των τηλεφωνικών επικοινωνιών Αμερικανών ή Ευρωπαίων πολιτών, υπήρξε πάντα μία διαμάχη ανάμεσα στην Ιδιωτική ζωή του ατόμου και την ασφάλεια. Παρά το γεγονός ότι πολλά κράτη παγκοσμίως έχουν θεσπίσει ένα ολοκληρωμένο νομοθετικό πλαίσιο για το απόρρητο των πληροφοριών, είναι αξιοσημείωτο το γεγονός ότι οι Η.Π.Α. δεν έχουν υιοθετήσει ένα σφαιρικό νομικό πλαίσιο για την προστασία των δεδομένων και της Ιδιωτικότητας του ατόμου. Το νομοθετικό πλαίσιο των Η.Π.Α. περιορίζεται σε συγκεκριμένους τομείς όπως αυτούς της Υγείας (Health Insurance Portability and Accountability Act (HIPAA)), των Ηλεκτρονικών Επικοινωνιών (Electronic Communications Privacy Act (ECPA)), της Παιδείας και της Πρόνοιας. Παρά τους επιμέρους αυτούς κανονισμούς δεν υπάρχει ολοκληρωμένη νομοθεσία για την απόκτηση, την αποθήκευση ή τη χρήση των προσωπικών δεδομένων.

Σε αντίθεση με την Ευρωπαϊκή Ένωση, η οποία διαθέτει μία ενιαία νομοθεσία για την προστασία των δεδομένων και της Ιδιωτικής ζωής, οι Η.Π.Α. ακολουθούν μία διαφορετική προσέγγιση στη νομοθεσία της, την «τομεακή» προσέγγιση. Σύμφωνα με αυτή την προσέγγιση, η προστασία των δεδομένων και της Ιδιωτικότητας βασίζεται περισσότερο στο συνδυασμό της νομοθεσίας, των κανονιστικών ρυθμίσεων και της αυτο-ρύθμισης των εμπλεκόμενων εταιριών και φυσικών προσώπων, παρά στην Κυβερνητική παρέμβαση. Κατά κύριο λόγο, η πολιτική των Η.Π.Α. στον τομέα της προστασίας των δεδομένων προσανατολίζεται στην Ιδιωτική πρωτοβουλία. Αυτό σημαίνει ότι οι εταιρίες οφείλουν να αναπτύσσουν και να εφαρμόζουν τις δικές τους πολιτικές και τη δική τους τεχνολογία για την προστασία των προσωπικών δεδομένων που διαχειρίζονται , ενώ τα υποκείμενα των δεδομένων θα πρέπει να λαμβάνουν τα κατάλληλα μέτρα για την πρόληψη της διάδοσης των δεδομένων τους. Παρακάτω ακολουθεί μία συνοπτική περιγραφή των βασικότερων Νόμων και ρυθμίσεων περί προστασίας των προσωπικών δεδομένων και των ηλεκτρονικών επικοινωνιών, που θεσπίστηκαν στις Η.Π.Α.

3.3.1.1 Η 4η τροποποίηση του Συντάγματος (1791)

Με την τροποποίηση αυτή του Συντάγματος αναγνωρίζεται για πρώτη φορά το δικαίωμα του ατόμου στην ιδιωτική ζωή, ενώ ορίζεται «η σοβαρή αιτία» ως προαπαιτούμενο για την έκδοση εντάλματος για έρευνες και κατασχέσεις. Πιο συγκεκριμένα αναφέρεται:
« *Το δικαίωμα των πολιτών στην ατομική ασφάλεια, στην ασφάλεια των οικιών τους, των εγγράφων τους και των αντικειμένων τους έναντι παράλογων ερευνών και κατασχέσεων, δεν θα παραβιαστεί και δεν θα εκδοθούν Εντάλματα, εκτός λόγω σοβαρής αιτίας, συνοδευόμενα από Όρκο (ένορκη καταγγελία) ή επιβεβαίωση (αποδείξεις), και ειδική περιγραφή του τόπου που θα ερευνηθεί και των ατόμων ή των αντικειμένων που θα συλληφθούν* » [37].

3.3.1.2 Ο Νόμος περί προστασίας της Ιδιωτικής ζωής (Privacy Act -1974)

Με το Νόμο αυτό καθιερώθηκε στις Η.Π.Α. ένας κώδικας χρηστής διαχείρισης των Πληροφοριών και αφορά τη συλλογή, την αποθήκευση και την επεξεργασία των προσωπικών δεδομένων που διατηρούνται στα συστήματα των Ομοσπονδιακών υπηρεσιών. Ο Νόμος αυτός στόχευε τόσο στην προστασία των προσωπικών δεδομένων που διατηρούσαν οι Ομοσπονδιακές υπηρεσίες όσο και στην παραχώρηση συγκεκριμένων δικαιωμάτων στα υποκείμενα των δεδομένων που περιλαμβάνονται σε αυτές τις Βάσεις Δεδομένων. Έτσι, καθιερώνονται δύο βασικές αρχές. Η πρώτη αφορά τη ρητή απαγόρευση της αποκάλυψης των προσωπικών δεδομένων από ένα σύστημα εγγραφών, χωρίς την προηγούμενη γραπτή συγκατάθεση του υποκείμενου των δεδομένων. Η δεύτερη αφορά το δικαίωμα του ατόμου να έχει πρόσβαση σε πληροφορίες που το αφορούν καθώς και το δικαίωμα του να τις αμφισβητεί.

Ωστόσο, ο ίδιος ο Νόμος εισάγει και μερικές εξαιρέσεις όπου επιτρέπεται η επεξεργασία των προσωπικών δεδομένων που τηρούνται στα αρχεία των Ομοσπονδιακών υπηρεσιών. Οι εξαιρέσεις αυτές εξυπηρετούν σκοπούς στατιστικούς, ερευνητικούς, διοικητικούς ή επιβολής των νόμων. Να σημειωθεί ότι ο Νόμος αυτός εφαρμόζεται μόνο για τα αρχεία δεδομένων που τηρούνται στις Ομοσπονδιακές υπηρεσίες και όχι σε οποιοδήποτε άλλο μη Κυβερνητικό οργανισμό. Επιπλέον, ο Privacy Act δεν παρέχει καμία προστασία σε μη Αμερικανούς πολίτες.

Εκτός από το Νόμο Privacy of Act, το Κογκρέσο ενέκρινε το 1987 το Νόμο «Computer Security Act» ο οποίος επίσης αφορά την προστασία προσωπικών δεδομένων στα συστήματα των Ομοσπονδιακών υπηρεσιών αλλά εισάγει και την έννοια των ευαίσθητων προσωπικών δεδομένων. Με το Νόμο αυτό θεσπίζονται πρότυπα για την ασφάλεια των υπολογιστικών συστημάτων των Ομοσπονδιακών γραφείων, ενώ επιβάλλεται και ο εντοπισμός όλων των κυβερνητικών συστημάτων που διατηρούν ευαίσθητα προσωπικά δεδομένα, με σκοπό την ανάπτυξη σχεδίων ασφαλείας για τα συστήματα αυτά.

3.3.1.3 Ο Νόμος περί απορρήτου των Ηλεκτρονικών Επικοινωνιών (Electronic Communications Privacy Act -1986)

Ο Νόμος περί απορρήτου των Ηλεκτρονικών επικοινωνιών ψηφίστηκε από το Κογκρέσο το 1986, με σκοπό να επεκτείνει τους περιορισμούς για τις τηλεφωνικές υποκλοπές σε κάθε είδους ηλεκτρονική επικοινωνία, ανεξάρτητα από την τεχνολογία που χρησιμοποιείται. Ο ECPA αποσκοπούσε στην προστασία των δικαιωμάτων στις ψηφιακές και ηλεκτρονικές επικοινωνίες, μέσα σε ένα συνεχώς εξελισσόμενο τεχνολογικό κόσμο. Βασική αρχή του ECPA αποτελεί η «*απαγόρευση της εκ προθέσεως, της απόπειρας ή της υποκλοπής, της χρήσης, της αποκάλυψης, ή της επέμβασης κάθε άλλου προσώπου στο να υποκλαπούν ή να γίνει προσπάθεια να υποκλαπεί, οποιαδήποτε ενσύρματη, προφορική ή και ηλεκτρονική επικοινωνία*» [34].

Ο Νόμος εισάγει και συγκεκριμένες εξαιρέσεις, οι οποίες δεν εμπίπτουν στην ισχύ του Νόμου αυτού. Πιο συγκεκριμένα, εξαιρέσεις υφίστανται:

- Για τους Παρόχους Ηλεκτρονικών υπηρεσιών "*κατά τη συνήθη πορεία της εργασίας τους, ενώ συμμετέχουν σε οποιαδήποτε δραστηριότητα η οποία είναι απαραίτητη περιστασιακά για την παράδοση της υπηρεσίας τους*" [34].

- Για "*πρόσωπα που είναι εξουσιοδοτημένα από το νόμο να υποκλέψουν ενσύρματες, από στόματος, ή ηλεκτρονικές επικοινωνίες ή να διεξάγουν ηλεκτρονική επιτήρηση, όπως ορίζεται στο άρθρο 101 του (FISA) του 1978 "* [34].

Ωστόσο, ο Νόμος αυτός δέχτηκε πολλές κριτικές, κυρίως λόγω της αποτυχίας του να προστατέψει τα προσωπικά δεδομένα των χρηστών, αφού δεν καλύπτει πλέον τις σύγχρονες τεχνολογικές εξελίξεις με τις οποίες οι χρήστες διαμοιράζονται, αποθηκεύουν και επεξεργάζονται τις πληροφορίες τους. Χαρακτηριστικό παράδειγμα αυτού είναι ότι οι πληροφορίες που αποθηκεύονται σε απομακρυσμένο διακομιστή προστατεύονται μόνο για 180 ημέρες. Να σημειωθεί ότι ο περιορισμός αυτός ισχύει μέχρι και σήμερα, με αποτέλεσμα πολλά σύγχρονα τεχνολογικά περιβάλλοντα, όπως αυτό της Νεφοϋπολογιστικής, να μην καλύπτονται από τις διατάξεις του Νόμου αυτού.

3.3.1.4 Ο Νόμος FISA του 1978 όπως τροποποιήθηκε το 2008 (Foreign Intelligence Surveillance Act of 1978 Amendments of 2008 -FISAA) και η εφαρμογή του στο περιβάλλον της Νεφοϋπολογιστικής

Το 1978 εγκρίνεται από το Κογκρέσο ο Νόμος FISA με τον οποίο καθιερώνονται για πρώτη φορά διαδικασίες για την παραχώρηση δικαστικής άδειας για την παρακολούθηση ξένων "Υπηρεσιών Πληροφοριών". Για το λόγο αυτό θεσμοθετήθηκε η δημιουργία ενός ειδικού δικαστηρίου (Foreign Intelligence Surveillance Court -FISC) με σκοπό να εγκρίνει τις υποκλοπές σε πράκτορες ξένων κρατών. Ουσιαστικά, ο FISA νομιμοποιεί τα κυβερνητικά προγράμματα ηλεκτρονικών υποκλοπών σε «ξένες δυνάμεις». Ωστόσο, η πράξη αυτή μπορεί να περιλαμβάνει και Αμερικανούς πολίτες, έπειτα από απόφαση ενός ειδικού μυστικού δικαστηρίου.

Ο Νόμος FISA τροποποιήθηκε το 2008 (FISAA) υπό τη σκιά της τρομοκρατικής επίθεσης της 11^{ης} Σεπτεμβρίου του 2001. Με τις τροποποιήσεις αυτές εισάγονται νέες διαδικασίες για την πρόσβαση σε προσωπικά δεδομένα ατόμων που βρίσκονται εκτός των Η.Π.Α. Να σημειωθεί ότι οι τροποποιήσεις αυτές αφορούν ακόμη και τους Αμερικανούς πολίτες για όσο διαμένουν εκτός των Η.Π.Α. Πιο συγκεκριμένα, οι τροποποιήσεις που εισάγονται αφορούν [42]:

- Διαδικασίες στόχευσης μη Αμερικανών πολιτών που διαμένουν στο εξωτερικό, χωρίς την προηγούμενη έκδοση ατομικής δικαστικής απόφασης

- Διαδικασίες για την έκδοση ατομικών δικαστικών αποφάσεων για την παρακολούθηση Αμερικανών πολιτών που διαμένουν στο εξωτερικό, έτσι ώστε να επιτραπεί η ηλεκτρονική επιτήρησή τους και η απόκτηση των αποθηκευμένων επικοινωνιών τους.

Η βασική διαφορά που εισάγεται στο Νόμο FISAA με τις παραπάνω τροποποιήσεις

του 2008 έγκειται στη δυνατότητα παρακολούθησης οποιουδήποτε Αμερικανού ή μη πολίτη (και όχι απαραίτητα ύποπτου για τρομοκρατικές ενέργειες), εντός ή εκτός των ΗΠΑ, χωρίς την προηγούμενη έκδοση εντάλματος. Χαρακτηριστικό παράδειγμα τέτοιας περίπτωσης αποτελεί ο ορισμός μιας νέας μορφής ηλεκτρονικής επιτήρησης και αφορά τις επικοινωνίες εκείνες όπου το ένα άκρο πρόσβασης βρίσκεται εντός ΗΠΑ. Να σημειωθεί ότι πριν την ψήφιση των τροποποιήσεων αυτών απαιτούνταν η έκδοση του σχετικού εντάλματος, εφόσον επρόκειτο για Αμερικανούς πολίτες εντός ΗΠΑ. Μετά την ψήφιση τους, η παρακολούθηση επιτράπηκε και χωρίς την έκδοση εντάλματος.

Οι τροποποιήσεις του Νόμου FISA, ουσιαστικά παρέχουν τη δυνατότητα μαζικής παρακολούθησης ατόμων εκτός των ΗΠΑ, με εφαρμογή και στο περιβάλλον της Νεφοϋπολογιστικής. Αυτό σημαίνει ότι οι αμερικανικές εταιρείες με παρουσία στην ΕΕ μπορεί να υποχρεωθούν κάτω από μια μυστική διαταγή παρακολούθησης –που εκδίδεται από ένα μυστικό δικαστήριο– να παραδώσουν δεδομένα σχετικά με Ευρωπαίους πολίτες. Αυτό που διαφοροποιεί τον νόμο FISA από τη συνήθη παρακολούθηση συνομιλιών και email υπόπτων από μυστικές υπηρεσίες διαφόρων χωρών, είναι το γεγονός πως συνδέει τα δεδομένα που έχουν αποθηκευτεί στο Νέφος με την επικοινωνία "πολιτικών οργανώσεων του εξωτερικού" και όχι μόνο ύποπτων τρομοκρατών. Ουσιαστικά νομιμοποιείται η παρακολούθηση δημοσιογράφων, ακτιβιστών, πολιτικών κτλ, ενώ μπορεί να υποχρεώσει ακόμη και τους Παρόχους Cloud υπηρεσιών να υποκλέπτουν τα δεδομένα των Ευρωπαίων χρηστών [43].

3.3.1.5 Ο Νόμος USA Patriot Act-2001

Ο Νόμος USA Patriot Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act) εγκρίθηκε από το Κογκρέσο έξι εβδομάδες μετά την τρομοκρατική επίθεση της 11ης Σεπτεμβρίου 2001, με σκοπό την ενδυνάμωση της Αμερικής με την παροχή των κατάλληλων εργαλείων για την παρεμπόδιση της τρομοκρατίας.

Με το Νόμο αυτό, ενισχύονται οι διαδικασίες παρακολούθησης των Υπηρεσιών επιβολής των Νόμων και των Υπηρεσιών Εθνικής Ασφάλειας, οι οποίες αποκτούν αυξημένες εξουσίες παρακολούθησης και διαμοιρασμού των ηλεκτρονικών, ενσύρματων και προφορικών πληροφοριών υποκλοπής, με σκοπό την πρόληψη ενδεχόμενων τρομοκρατικών επιθέσεων.

Η βασική αρχή που προωθήθηκε μέσα από τον USA PATRIOT αφορά τη δυνατότητα των δικαστηρίων να εκδίδουν μυστικά εντάλματα παρακολούθησης ανά πάσα στιγμή, χωρίς να προσδιορίζεται το πότε και για ποιό λόγο θα πραγματοποιηθεί η υποκλοπή. Με τις διατάξεις αυτές, αποδυναμώνεται ουσιαστικά η ισχύς του FISA, καθώς δεν απαιτούνται αποδείξεις για το εάν ο στόχος είναι μη πολίτης των ΗΠΑ ή αν είναι πράκτορας ξένης χώρας. Η συλλογή των προσωπικών δεδομένων μπορεί να πραγματοποιείται ανά πάσα στιγμή και για οποιοδήποτε «ΣΗΜΑΝΤΙΚΟ» σκοπό. Ταυτόχρονα, ο USA PATRIOT ενισχύει σημαντικά την πρόσβαση και την ανταλλαγή πληροφοριών, ενώ επιτρέπει την κατάσχεση όχι μόνο αρχείων αλλά και υλικών αντικειμένων. Επιπλέον, οι αρχές μπορούν πλέον να υποχρεώνουν τους Παρόχους των επικοινωνιών στην παράδοση των αρχείων των πελατών τους, ενώ

διαμέσου του ψηφιακού συστήματος παρακολούθησης DCS-1000(Digital Collection System) του FBI, επιτρέπεται η συλλογή δεδομένων που ρέουν μέσα από μία Υπηρεσία Παροχής Internet (ISP).

Η ισχύς του Νόμου ανανεώθηκε κατά τα έτη 2006, 2010 και 2011 ενώ συνεχίζει να επηρεάζει την ασφάλεια και την Ιδιωτικότητα των δεδομένων εκατομμυρίων πολιτών, εντός και εκτός ΗΠΑ, μέχρι και σήμερα.

3.3.2 Οι αρχές «Ασφαλούς Λιμένα» για την προστασία της Ιδιωτικής ζωής (International Safe Harbor Privacy Principles)

Όπως αναφέρθηκε προηγουμένως, η Ευρωπαϊκή Ένωση έχει εγκρίνει ένα ιδιαίτερα αυστηρό και ολοκληρωμένο σύστημα περί προστασίας των προσωπικών δεδομένων των Ευρωπαίων πολιτών και το οποίο, τις περισσότερες φορές, δεν είναι συμβατό με το Νομοθετικό πλαίσιο άλλων κρατών εκτός Ε.Ε.. Χαρακτηριστικό παράδειγμα αποτελεί η απαγόρευση που εισάγει η Ευρωπαϊκή οδηγία 95/46/ΕC, σύμφωνα με την οποία απαγορεύεται η διαβίβαση προσωπικών δεδομένων από τις εταιρείες που δραστηριοποιούνται εντός της Ευρωπαϊκής Ένωσης σε χώρες εκτός της Ευρωπαϊκής οικονομικής περιοχής, εκτός αν υπάρχει πιστοποίηση για την παροχή ισότιμης προστασίας και ασφάλειας των δεδομένων αυτών [43] [44].

Από την άλλη πλευρά, η πολιτική των Η.Π.Α. για την προστασία των προσωπικών δεδομένων ακολουθεί μία διαφορετική προσέγγιση, η οποία βασίζεται στο συνδυασμό της Νομοθεσίας και της αυτό-ρύθμισης. Καθώς όμως, οι Η.Π.Α. διατηρούν ισχυρές οικονομικές σχέσεις με την Ευρωπαϊκή Ένωση, το Υπουργείο Εμπορίου της Αμερικής σε συνεργασία με την Ευρωπαϊκή Επιτροπή ανέπτυξε ένα ρυθμιστικό πλαίσιο, προκειμένου να γεφυρωθούν οι διαφορές μεταξύ των διαφορετικών αυτών προσεγγίσεων και να ενισχυθεί το διεθνές εμπόριο. Το πλαίσιο αυτό εγκρίθηκε από την Ευρωπαϊκή επιτροπή το 2001 και θεωρείται ιδιαίτερα σημαντικό για τις Αμερικανικές επιχειρήσεις καθώς διασφαλίζεται η οικονομική τους δραστηριότητα στην Ευρωπαϊκή οικονομική ζώνη.

Το πλαίσιο αυτό αναφέρεται ως «Ασφαλής Λιμένας» ή «Safe Harbor» και απευθύνεται αποκλειστικά σε επιχειρήσεις των ΗΠΑ, οι οποίες επιθυμούν να λαμβάνουν και να διατηρούν προσωπικά δεδομένα από την Ευρωπαϊκή Ένωση. Η πιστοποίηση συμμόρφωσης των επιχειρήσεων σύμφωνα με τις αρχές του «Ασφαλούς Λιμένα» είναι προαιρετική και ισχύει κατά την ημερομηνία δήλωσης συμμόρφωσης του ενδιαφερόμενου στο Υπουργείο Εμπορίου των ΗΠΑ [45]. Οι εν λόγω επιχειρήσεις οφείλουν να δηλώνουν εγγράφως και σε ετήσια βάση τη συμμόρφωσή τους, ενώ το Υπουργείο Εμπορίου οφείλει να δημοσιοποιεί και να ανανεώνει τακτικά τη λίστα με τους αυτό-πιστοποιημένους φορείς.

Για την πιστοποίηση μίας επιχείρησης ή ενός οργανισμού απαιτείται η συμμόρφωση με τις παρακάτω αρχές [45]:

- Κοινοποίηση: Ένας οργανισμός οφείλει να ενημερώνει τα πρόσωπα σχετικά με τους σκοπούς για τους οποίους συλλέγει και χρησιμοποιεί πληροφορίες που τα αφορούν, τον τρόπο επικοινωνίας με τον οργανισμό για τυχόν αιτήσεις πληροφοριών ή παράπονα, τους τρίτους στους οποίους γνωστοποιεί

τις πληροφορίες, καθώς και τις επιλογές και τα μέσα που προσφέρει ο οργανισμός στα πρόσωπα για τον περιορισμό της χρήσης και της γνωστοποίησης των πληροφοριών.

- Επιλογή: Ένας οργανισμός πρέπει να παρέχει στα πρόσωπα την ευκαιρία να επιλέγουν εάν οι πληροφορίες προσωπικού χαρακτήρα που τα αφορούν πρόκειται να γνωστοποιηθούν σε ένα τρίτο μέρος ή να χρησιμοποιηθούν για ένα σκοπό ο οποίος δεν συνάδει με το σκοπό για τον οποίο συνελέγησαν αρχικά ή για τον οποίο εγκρίθηκαν.

- Περαιτέρω Διαβίβαση: Για να γνωστοποιούν πληροφορίες σε τρίτο μέρος, οι οργανισμοί πρέπει να εφαρμόζουν τις αρχές της κοινοποίησης και της επιλογής. Όποτε ένας οργανισμός επιθυμεί να διαβιβάσει πληροφορίες σε ένα τρίτο μέρος μπορεί να το πράξει αφού εξακριβώσει πρώτα ότι τηρεί τις αρχές του ασφαλούς λιμένα ή υπόκεινται σε κάποιο μηχανισμό που εξασφαλίζει την επάρκεια της προστασίας της ιδιωτικής ζωής, στο ίδιο επίπεδο με εκείνο που επιβάλλουν οι αρχές του ασφαλούς λιμένα.

- Ασφάλεια: Οι οργανισμοί που δημιουργούν, διατηρούν, χρησιμοποιούν ή μεταδίδουν πληροφορίες προσωπικού χαρακτήρα οφείλουν να λαμβάνουν εύλογες προφυλάξεις για την προστασία των πληροφοριών αυτών από τυχόν απώλεια, κατάχρηση και μη εγκεκριμένη πρόσβαση, γνωστοποίηση, αλλαγή και καταστροφή.

- Ακεραιότητα των Δεδομένων: οι πληροφορίες προσωπικού χαρακτήρα πρέπει να παρουσιάζουν συνάφεια με τους σκοπούς για τους οποίους πρόκειται να χρησιμοποιηθούν. Ένας οργανισμός δεν μπορεί να επεξεργαστεί πληροφορίες προσωπικού χαρακτήρα κατά τρόπο που να αντιβαίνει στους σκοπούς για τους οποίους συνελέγησαν ή για τους οποίους εγκρίθηκαν από το πρόσωπο μεταγενέστερα.

- Πρόσβαση: Τα πρόσωπα πρέπει να έχουν πρόσβαση στις πληροφορίες προσωπικού χαρακτήρα που τα αφορούν και να έχουν τη δυνατότητα να διορθώνουν, να τροποποιούν και να εξαλείφουν τις πληροφορίες αυτές όποτε είναι ανακριβείς.

- Εφαρμογή: Για να υπάρξει αποτελεσματική προστασία της ιδιωτικής ζωής πρέπει να υφίστανται μηχανισμοί που να εξασφαλίζουν τη συμμόρφωση με τις αρχές, μέσα προσφυγής για τα πρόσωπα περί των οποίων πρόκειται και τα οποία θίγονται από τη μη συμμόρφωση με τις αρχές καθώς και συνέπειες για τον οργανισμό σε περίπτωση μη τήρησης των αρχών.

Να σημειωθεί ότι το πλαίσιο αυτό αφορά και δύναται να εφαρμοστεί είτε σε Ιδιωτικές επιχειρήσεις των ΗΠΑ είτε σε Δημόσιους φορείς.

Κεφάλαιο 4^{ο}

Περιπτώσεις Εφαρμογής στη Δημόσια Διοίκηση

Την τελευταία δεκαετία, παρατηρείται παγκοσμίως μία συστηματική προσπάθεια υιοθέτησης των σύγχρονων τεχνολογιών Νέφους στη Δημόσια Διοίκηση. Οι Κυβερνήσεις έχουν ήδη αντιληφθεί τα σημαντικά οφέλη που μπορούν να αποκομίσουν από τη μεταστροφή του παραδοσιακού IT μοντέλου στην αγορά υπηρεσιών Πληροφορικής, με αποτέλεσμα η Νεφοϋπολογιστική να βρίσκει εφαρμογή σε ολοένα περισσότερες εκφάνσεις της Δημόσιας Διοίκησης. Όλο και περισσότεροι Δημόσιοι Φορείς προτιμούν πλέον την παροχή υπηρεσιών προς τους πολίτες κάνοντας χρήση σύγχρονων υποδομών Νέφους, ενισχύοντας έτσι την αποδοτικότητα και την ποιότητα των παρεχόμενων υπηρεσιών. Παράλληλα, διαπιστώνεται ότι πολλές Κυβερνήσεις διατηρούν συγκεκριμένο και ολοκληρωμένο σχέδιο για την καθολική μετάβαση των Δημόσιων υπηρεσιών στο Νέφος, με απώτερο σκοπό την ενίσχυση της διαλειτουργικότητας μεταξύ των Φορέων. Στο Κεφάλαιο αυτό θα μελετηθούν περιπτώσεις όπου Δημόσιοι Οργανισμοί έχουν εφαρμόσει τεχνολογίες Νέφους για την παροχή υπηρεσιών είτε προς τους πολίτες είτε για την υποστήριξη των εσωτερικών λειτουργιών τους.

4.1 Εφαρμογές της Νεφοϋπολογιστικής στη Δημόσια Διοίκηση των Η.Π.Α

Από πολύ νωρίς, η Ομοσπονδιακή Κυβέρνηση των Ηνωμένων Πολιτειών κατέβαλε σημαντικές προσπάθειες για τη μεταστροφή των παραδοσιακών IT μοντέλων στις νέες Cloud τεχνολογίες, σε κάθε έκφανση της Δημόσιας Διοίκησης [47]. Η μεταστροφή αυτή σκόπευε στην αναβάθμιση των παρεχόμενων υπηρεσιών προς τους πολίτες, στη διευκόλυνση των εσωτερικών διαδικασιών μεταξύ των Δημόσιων οργανισμών αλλά και στη συνεργασία μεταξύ των τοπικών κυβερνήσεων. Σήμερα, πολλές από αυτές τις προσπάθειες έχουν ήδη υλοποιηθεί και εφαρμοστεί από πολλούς κυβερνητικούς οργανισμούς, με θεαματικά αποτελέσματα αναφορικά με την αναβάθμιση των παρεχόμενων υπηρεσιών και την εξοικονόμηση οικονομικών πόρων. Χαρακτηριστικά παραδείγματα οργανισμών που υλοποίησαν εφαρμογές σε περιβάλλον Νεφοϋπολογιστικής αποτελούν:

- Η Ομοσπονδιακή Υπηρεσία Διαχείρισης Γενικών Υπηρεσιών – GSA (General Services Administration)
- Η Εθνική Υπηρεσία Αεροναυτικής και Διαστήματος (NASA)
- Defence Information Systems Agency (DISA) – Department of Defence (DoD) κ.α.

Η ιδέα και η καθοδήγηση της οργανωμένης μετάβασης της Δημόσιας Διοίκησης στο Νέφος ανήκει στον πρώτο επικεφαλή CIO (Chief Information Officer) των ΗΠΑ υπό την προεδρεία του Barak Obama, Vivek Kundra. Οι περιπτώσεις αυτές μελετώνται ακολούθως.

4.1.1 General Services Administration(GSA)[1]

Όπως αναφέρθηκε προηγουμένως, με την υιοθέτηση τεχνολογιών Νέφους, η Ομοσπονδιακή Κυβέρνηση των Η.Π.Α. στοχεύει στον εκσυγχρονισμό των IT υπηρεσιών και την παροχή κοινών Υπηρεσιών και λύσεων στη Δημόσια Διοίκηση. Για την εκπλήρωση αυτού του σκοπού, το 2009 ιδρύεται η Ομοσπονδιακή Πρωτοβουλία για την προώθηση του Cloud Computing (Federal Cloud Computing Initiative). Στην πρωτοβουλία αυτή συμμετέχει και η GSA με αρμοδιότητες που επικεντρώνονται στην υλοποίηση έργων που αφορούν το σχεδιασμό, την ανάπτυξη και την εφαρμογή τεχνολογικών λύσεων Νέφους στην Ομοσπονδιακή Κυβέρνηση.

Το όραμα του CIO της GSA είναι η παροχή IaaS (Infrastructure as a Service) υπηρεσιών σε όλους τους Ομοσπονδιακούς οργανισμούς, διαμέσου πιστοποιημένων προμηθευτών. Έπειτα από τη συνεργασία του CIO Vivek Kundra με την GSA αποφασίστηκε η δημιουργία ενός «Υπολογιστικού Νέφους Βιτρίνα», με σκοπό να

[1] Η GSA είναι μία ανεξάρτητη Αρχή της Ομοσπονδιακής Κυβέρνησης των Η.Π.Α., η οποία ιδρύθηκε το 1949 με σκοπό την υποστήριξη των βασικών λειτουργιών των Ομοσπονδιακών οργανισμών καθώς και των ομοσπονδιακών υπαλλήλων.

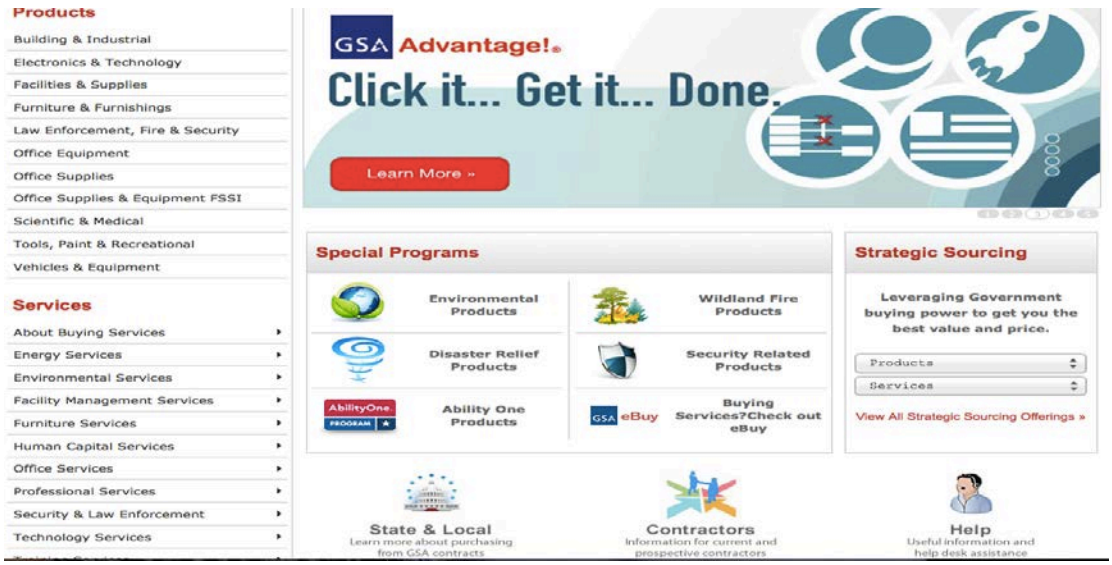
διευκολύνει τους Ομοσπονδιακούς οργανισμούς στην εύκολη επιλογή της βέλτιστης λύσης Νέφους [47]. Η υλοποίηση του Υπολογιστικού Νέφους «βιτρίνα» αντανακλά τις βέλτιστες πρακτικές με τις οποίες μπορεί να μειωθεί αισθητά το κόστος εξαγοράς και συντήρησης IT εξοπλισμού ενώ εξασφαλίζεται η παροχή κοινού επιπέδου υπηρεσιών από όλους τους Ομοσπονδιακούς οργανισμούς.

Η λύση

Το Σεπτέμβριο του 2009, λειτούργησε για πρώτη φορά το portal "Apps.gov" με σκοπό να διευκολύνει τους Ομοσπονδιακούς οργανισμούς στην επιλογή, υλοποίηση και διαχείριση της βέλτιστης λύσης Νέφους. Το portal συγκέντρωνε πλήθος τεχνολογικών λύσεων από πιστοποιημένους Ιδιωτικούς φορείς, ενώ παρέχονταν η δυνατότητα δοκιμαστικής εγκατάστασης πριν την τελική επιλογή της τεχνολογικής λύσης από τον Ομοσπονδιακό οργανισμό. Ωστόσο, το Portal δέχτηκε αρκετές επικρίσεις καθώς θεωρήθηκε ότι δεν εξυπηρετούσε ικανοποιητικά τις ανάγκες των Ομοσπονδιακών οργανισμών, με αποτέλεσμα την διακοπή της λειτουργίας του [47].

Σήμερα, η λειτουργία του αντικαταστάθηκε από το GSA Advantage Online Shopping [2], το οποίο λειτουργεί ως online κατάστημα της Ομοσπονδιακής κυβέρνησης. Μέσω αυτού, δίνεται στις τοπικές κυβερνήσεις και οργανισμούς πρόσβαση σε εκατομμύρια εμπορικές εφαρμογές και υπηρεσίες από φορείς, με τους οποίους η GSA έχει συνάψει ειδικές συμβάσεις. Όλοι οι κρατικοί φορείς μπορούν ανά πάσα στιγμή να περιηγηθούν και να αγοράσουν προϊόντα και υπηρεσίες, ενώ η πληρωμή τους μπορεί να πραγματοποιηθεί αποκλειστικά με πιστωτική κάρτα, η οποία εκδόθηκε από Κρατικό οργανισμό ή οργανισμό Τοπικής Αυτοδιοίκησης. Σημειώνεται ότι δικαίωμα αγοράς από το ηλεκτρονικό κατάστημα έχουν αποκλειστικά και μόνο οι κρατικοί φορείς των Η.Π.Α., ενώ οι ίδιοι οι φορείς υποχρεούνται να διασφαλίζουν ότι η κάθε προμήθεια προορίζεται για την εκπλήρωση των σκοπών του οργανισμού και μόνο [49].

[2] GSA Advantage Online Shopping: https://www.gsaadvantage.gov/advantage/main/start_page.do



Πηγή: GSA Advantage Online Shopping

Αναφορικά με τις Cloud Computing υπηρεσίες, το GSA Advantage παρέχει πλήρη ενημέρωση μέσω του portal Cloud.cio.gov[3]. Το portal αποτελεί πηγή πληροφοριών αναφορικά με τις υπηρεσίες Νέφους που παρέχονται από τους Ομοσπονδιακούς οργανισμούς, ενώ ταυτόχρονα παρέχεται όλη η απαραίτητη πληροφόρηση για την ενδεχόμενη μελλοντική επιλογή, εφαρμογή και διαχείριση εφαρμογών Νέφους από τους κρατικούς φορείς.

Πηγή: cloud.cio.gov[3]

[3] Cloud.cio.gov: http://cloud.cio.gov/

4.1.2 Εθνική Υπηρεσία Αεροναυτικής και Διαστήματος (NASA)

Είναι φυσικό ότι η Εθνική Υπηρεσία Αεροναυτικής και Διαστήματος (NASA) των Η.Π.Α. διατηρεί και διαχειρίζεται τεράστιο όγκο δεδομένων, τα οποία συχνά χρήζουν ιδιαίτερης προστασίας. Ταυτόχρονα, η εκπλήρωση του σκοπού λειτουργίας της NASA προϋποθέτει τη διαρκή επένδυση σε προηγμένες τεχνολογικές λύσεις, οι οποίες διευκολύνουν τους σκοπούς του Οργανισμού. Υπό τους όρους αυτούς αλλά και σύμφωνα με τη διαπιστωμένη ανάγκη για μείωση των δαπανών και αύξηση της διαλειτουργικότητας, είτε στο εσωτερικό του οργανισμού είτε με εξωτερικούς φορείς, οι ομάδες εργασίας της NASA απαίτησαν μία ευέλικτη λύση για την αυστηρή διαχείριση των Δεδομένων του οργανισμού.

Η λύση και τα αποτελέσματά της

Η λύση που επικράτησε και που τελικά υλοποιήθηκε είναι η πλατφόρμα NEBULA. Η NEBULA είναι μια open-source πλατφόρμα Νέφους, η οποία αναπτύχθηκε για να παρέχει μία βελτιωμένη εναλλακτική λύση αντί της κατασκευής νέων δαπανηρών data centers. Η λύση αυτή παρέχει στους ερευνητές και στους επιστήμονες της NASA ένα εύκολο τρόπο διαμοιρασμού μεγάλων και σύνθετων συνόλων δεδομένων τόσο με τους συνεργαζόμενους εξωτερικούς φορείς όσο και με το ευρύ κοινό με ενδιαφέρον για τις αεροδιαστημικές προσπάθειες [51].

Η NEBULA βασίζεται στην Cloud πλατφόρμα "Ευκάλυπτος". Εκτός από τη δυνατότητα να προσφέρει SaaS (Software as a Service) εφαρμογές, μπορεί να λειτουργεί και ως IaaS (Infrastructure as a Service) υλοποίηση, μέσω της οποίας παρέχονται κλιμακωτές υπολογιστικές δυνατότητες, όπως εικονικές μηχανές και αποθηκευτικοί χώροι, για τα επιστημονικά δεδομένα και τις Web εφαρμογές. Ταυτόχρονα παρέχεται και PaaS (Platform as a Service) υλοποίηση, διευκολύνοντας τους προγραμματιστές της NASA στη δημιουργία νέων ασφαλών και συμβατών Web εφαρμογών. Σημειώνεται ότι παρέχονται όλα τα απαραίτητα εργαλεία, όπως βιβλιοθήκες κώδικα και Web Tools, για τη δημιουργία νέων εφαρμογών. Αναφορικά με την πρόσβαση σε πληροφορίες για το ευρύ κοινό, η πλατφόρμα NEBULA παρέχει δυνατότητα πρόσβασης σε online βιβλιοθήκες, blogs κτλ.

Τα αποτελέσματα από τη χρήση της Cloud πλατφόρμας αποδείχτηκαν θεαματικά με σημαντικότερα από αυτά [52]:

- Τη μείωση του κόστους αγοράς και συντήρησης εξοπλισμού
- Τη σημαντική εξοικονόμηση ενέργειας και περιβαλλοντική βιωσιμότητα
- Τη δυνατότητα παροχής υπηρεσιών Νέφους και σε άλλους Ομοσπονδιακούς οργανισμούς
- Τη σημαντική προώθηση της συνεργασίας και της έρευνας

4.1.3 Defence Information Systems Agency (DISA) – Department of Defence (DoD)

Ο DISA λειτουργεί ως ένας υποστηρικτικός οργανισμός του Υπουργείου Άμυνας των Η.Π.Α.. Ο οργανισμός οφείλει να διευκολύνει την ανταλλαγή πληροφοριών μεταξύ των συμβαλλόμενων μερών (στρατιωτικοί και πολιτικοί υπάλληλοι, πολιτική ηγεσία και εξωτερικοί συνεργάτες), παρέχοντας προσιτές υποδομές πληροφόρησης σε παγκόσμιο επίπεδο, για την άμεση στήριξη τους σε όλο το φάσμα των στρατιωτικών επιχειρήσεων [53]. Για την επίτευξη του σκοπού αυτού αναπτύσσει ολοκληρωμένες τεχνολογικές λύσεις, οι οποίες διατίθενται στα συμβαλλόμενα μέρη, για αποκλειστική εξυπηρέτηση των κυβερνητικών σκοπών. Πλήθος αυτών των τεχνολογικών λύσεων αναπτύσσονται και εφαρμόζονται σε περιβάλλον Νεφοϋπολογιστικής, όπως οι υπηρεσίες "forge.mil" [48], οι οποίες εξετάζονται ακολούθως.

Forge.mil [53]

Το «Forge.mil» είναι ένα σύνολο υπηρεσιών που προορίζονται για την υποστήριξη των ομάδων τεχνολογίας του Υπουργείου Άμυνας των Η.Π.Α. Επί του παρόντος, οι υπηρεσίες αυτές παρέχουν τη δυνατότητα της «από κοινού» ανάπτυξης και διαχείρισης λογισμικού ανοικτού κώδικα μεταξύ των ομάδων τεχνολογίας του Υπουργείου Άμυνας, ενώ αναμένεται να προστεθούν και νέες δυνατότητες οι οποίες θα επιτρέπουν τη συνεργασία μεταξύ όλων των ενδιαφερόμενων μερών, συμπεριλαμβανομένων των προγραμματιστών, των tester και των τελικών χρηστών, καθ' όλη τη διάρκεια του κύκλου ζωής των εργασιών.

Πιο συγκεκριμένα, προς το παρόν παρέχονται οι κάτωθι υπηρεσίες:

- Η Forge.mil κοινότητα: Ιστότοπος διαχείρισης γνώσης με σκοπό το εύκολο και γρήγορο διαμοιρασμό των πληροφοριών μεταξύ των μελών της κοινότητας, κάνοντας χρήση εργαλείων κοινωνικής συνεργασίας, όπως blogs, wikis και δημοσκοπήσεων.

- Software Forge: επιτρέπει την από κοινού ανάπτυξη και διανομή λογισμικού ανοικτού κώδικα.

- Project Forge: παρέχει τα ίδια εργαλεία διαχείρισης του κύκλου ζωής των εργασιών που παρέχονται από το Software Forge για τις εφαρμογές του Υπουργείου Άμυνας, εκτός από εκείνες που δεν αναπτύσσονται από τις ομάδες εργασίας του Υπουργείου ή περιέχουν άλλους περιορισμούς πρόσβασης.

Η εφαρμογή των υπηρεσιών του Forge.mil έχει ήδη επιφέρει σημαντική βελτίωση στη ταχύτητα ανάπτυξης και παράδοσης αξιόπιστων εφαρμογών και συστημάτων για την υποστήριξη των στρατιωτικών επιχειρήσεων. Τα κυριότερα οφέλη που προκύπτουν συνοψίζονται στη δυνατότητα εύκολου και γρήγορου διαμοιρασμού της γνώσης και των εφαρμογών μεταξύ των συμβαλλόμενων μερών καθ' όλη τη διάρκεια του κύκλου ανάπτυξης των εφαρμογών, στην ταχύτερη και αποτελεσματικότερη ανάπτυξη και έλεγχο των τεχνολογικών λύσεων, στην αποτελεσματικότερη προστασία του συνόλου των λειτουργικών συστημάτων από ενδεχόμενες κακόβουλες επιθέσεις, στην τμηματική ανάπτυξη των μεγάλων έργων ώστε κάθε τμήμα να λειτουργεί ως ανεξάρτητη συνιστώσα του τελικού προϊόντος και τέλος στη βελτίωση

της αξιοπιστίας των συστημάτων με την καθιέρωση κοινών κριτηρίων δοκιμής και αξιολόγησης.

4.2 Εφαρμογές της Νεφοϋπολογιστικής στη Δημόσια Διοίκηση Ευρωπαϊκών χωρών.

Όπως αναφέρθηκε στην προηγούμενη ενότητα, οι Η.Π.Α. πρωτοπορούν αναφορικά με την υλοποίηση και υιοθέτηση Cloud υπηρεσιών σε όλο το φάσμα της Δημόσιας Διοίκησης. Ωστόσο, σημαντικές πρωτοβουλίες έχουν ληφθεί και από τα περισσότερα Ευρωπαϊκά κράτη, τα οποία ήδη απολαμβάνουν σημαντικά οφέλη από την υιοθέτηση πρωτοποριακών υπηρεσιών σε περιβάλλον Νεφοϋπολογιστικής.

Ακολούθως εξετάζονται τρία χαρακτηριστικά παραδείγματα Cloud εφαρμογών Ευρωπαϊκών χωρών:

- Ηνωμένο Βασίλειο: G-Cloud (Cloud Store)
- Γερμανία: Germany's Administration Services Directory (DVDV)
- Ελλάδα: Κυβερνητικό Νέφος

Πολλοί μελετητές προβλέπουν ακόμη και μελλοντικές διακρατικές προσπάθειες, με απώτερο σκοπό τη δημιουργία μίας κοινής Cloud based IT υποδομής, με εφαρμογή σε όλα τα κράτη-μέλη τη Ευρωπαϊκής Ένωσης.

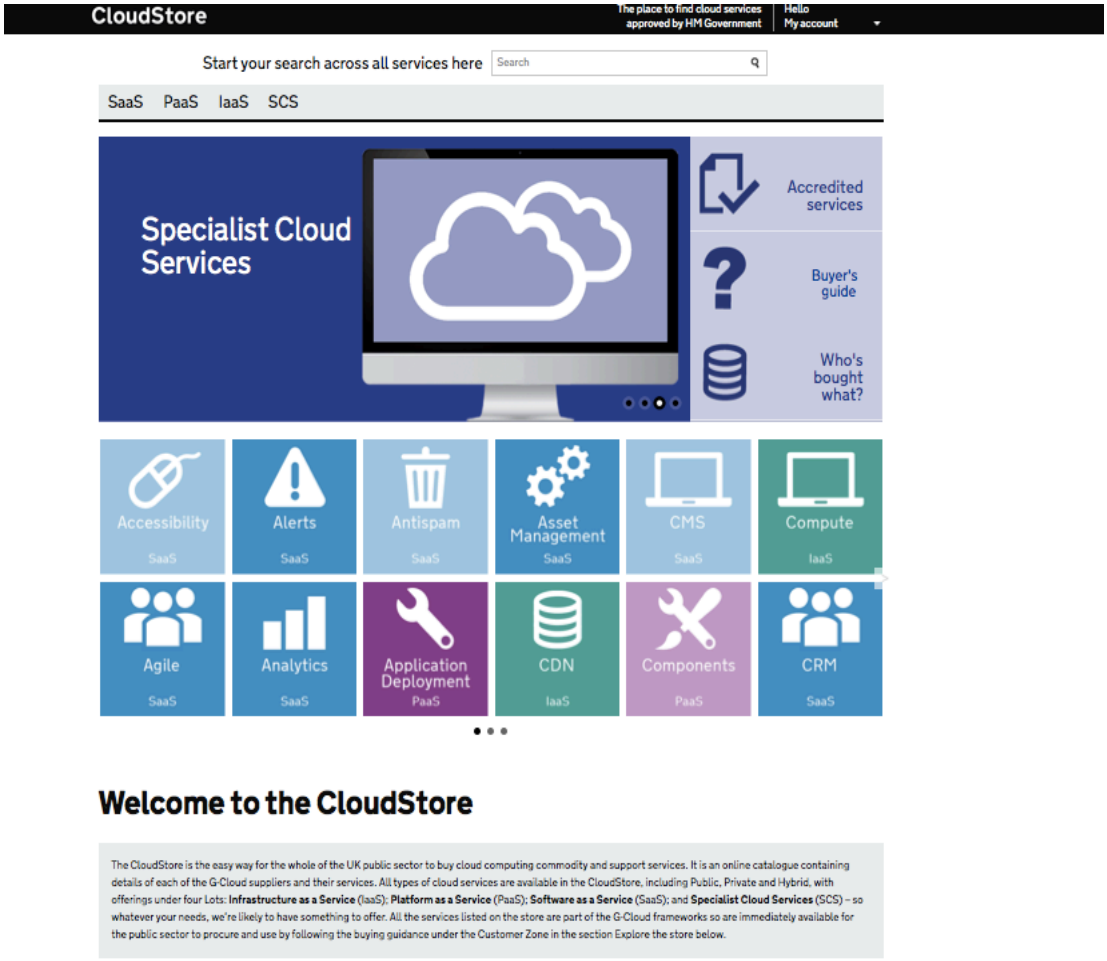
4.2.1 Ηνωμένο Βασίλειο: G- Cloud (Cloud Store) [54]

Τα τελευταία χρόνια, η κυβέρνηση του Ηνωμένου Βασιλείου προσανατολίζεται στην υιοθέτηση Cloud τεχνολογιών σε όλο το φάσμα του Δημόσιου Τομέα. Στο πλαίσιο της προσπάθειας αυτής εντάσσεται η πρωτοβουλία «G-Cloud», η οποία προωθήθηκε με σκοπό να απλοποιηθεί ο τρόπος με τον οποίο οι Δημόσιοι οργανισμοί αγοράζουν και παρέχουν υπηρεσίες. Έτσι προωθείται το μοντέλο pay-as-you-go με σκοπό την ικανοποίηση των διαρκώς μεταβαλλόμενων αναγκών των χρηστών. Με το G-Cloud επιχειρείται η αλλαγή της αντίληψης που επικρατούσε μέχρι σήμερα για τις παραδοσιακές μορφές IT, παρέχοντας στο χρήστη όλα τα απαραίτητα εργαλεία για την υιοθέτηση των νέων τεχνολογιών.

Μία από τις εφαρμογές του G-Cloud αποτελεί η δημιουργία ενός κυβερνητικού Ηλεκτρονικού καταστήματος για αγορές ηλεκτρονικών υπηρεσιών και προϊόντων Νέφους, αποκλειστικά από τους Δημόσιους οργανισμούς. Το portal «Cloud Store», όπως ονομάζεται, επιδιώκει να διευκολύνει τους Δημόσιους οργανισμούς του Ηνωμένου Βασίλειου στην επιλογή και προμήθεια Cloud υπηρεσιών και προϊόντων. Ουσιαστικά, πρόκειται για έναν online κατάλογο που περιέχει τους διαθέσιμους προμηθευτές Cloud υπηρεσιών καθώς και τις υπηρεσίες που αυτοί παρέχουν αναλυτικά. Στο Cloud Store διατίθενται υπηρεσίες για κάθε περιβάλλον Νέφους (Δημόσιο, Ιδιωτικό ή Υβριδικό).

Η βασική ιδέα του portal είναι αντίστοιχη με εκείνη του «GSA Advantage online shopping» των Η.Π.Α., όπου αναφέρθηκε σε προηγούμενη μελέτη περίπτωσης. Για την ώρα, ο κάθε Δημόσιος οργανισμός δύναται να επιλέξει μεταξύ 1.200

προμηθευτών περίπου και περισσότερων από 13.000 IaaS (Infrastructure as a Service), SaaS (Software as a Service) ή PaaS (Platform as a Service) υπηρεσιών, ανάλογα με τις ανάγκες που επιθυμεί να καλύψει ή τις υπηρεσίες που επιδιώκει να παρέχει. Το κόστος των παρεχόμενων υπηρεσιών αναφέρεται ρητά και καθορίζεται έπειτα από τη διαπραγμάτευση και σύναψη σύμβασης μεταξύ της Κυβέρνησης και του Ιδιώτη προμηθευτή. Να σημειωθεί ότι τα προϊόντα και οι υπηρεσίες παρέχονται για αγορά αποκλειστικά σε Δημόσιους φορείς ενώ το κόστος αγοράς δεν είναι διαπραγματεύσιμο από τον επίδοξο Δημόσιο φορέα-αγοραστή.



Πηγή:
http://govstore.service.gov.uk/cloudstore/

Σύμφωνα με την κυβέρνηση του Ηνωμένου Βασίλειου, από την εφαρμογή του G-Cloud αναμένεται εξοικονόμηση πόρων της τάξης των £200.000.000 έως το 2015. Εκτός από τη μείωση του κόστους, σημαντικά είναι τα οφέλη που προκύπτουν και αναφέρονται στη μείωση της γραφειοκρατίας, στην αύξηση της διαφάνειας στο σύστημα προμηθειών καθώς και στην καλύτερη κατανόηση και εξοικείωση με τις

τεχνολογίες Νέφους [52].

4.2.2 Γερμανία: Germany' s Administration Services Directory (Deutsche Verwaltungsdiensteverzeichnis - DVDV)

Οι τεχνολογίες Νέφους αποτελούν βασικό πυλώνα για την υλοποίηση της στρατηγικής της Γερμανικής Ομοσπονδιακής Κυβέρνησης για τις Τεχνολογίες της Πληροφορίας και των Επικοινωνιών (ΤΠΕ) έως το 2015. Η στρατηγική αυτή αποσκοπεί στο να διευκολύνει την υιοθέτηση υπηρεσιών Νέφους τόσο στις μικρές και μεσαίες επιχειρήσεις όσο και στο σύνολο των Δημόσιων οργανισμών της χώρας. Ωστόσο, η Γερμανική κυβέρνηση οφείλει να εξετάσει και να αντιμετωπίσει ένα σύνολο προκλήσεων (ασφάλεια δεδομένων, διασφάλιση της ποιότητας των υπηρεσιών κτλ), οι περισσότερες από τις οποίες προκύπτουν εξαιτίας της απαιτούμενης προσαρμογής των υφιστάμενων δομών Πληροφορικής με τις ειδικές απαιτήσεις της Νεφοϋπολογιστικής [56].

Χαρακτηριστικό παράδειγμα χρήσης τεχνολογιών Νέφους στη Δημόσια Διοίκηση της Γερμανίας αποτελεί η ενσωμάτωση του συστήματος «Germany's Administration Services Directory (DVDV)» (Deutsche Verwaltungsdiensteverzeichnis, DVDV) στο Κυβερνητικό Νέφος. Το DVDV αποτελεί μία e-government υπηρεσία, η οποία χρησιμοποιεί λογισμικό ανοικτού κώδικα, και επιτρέπει την ανταλλαγή ηλεκτρονικών δεδομένων μεταξύ των Δημόσιων οργανισμών της χώρας. Η ηλεκτρονική ανταλλαγή αφορά δεδομένα που διαχειρίζονται οι Δημόσιοι οργανισμοί, συμπεριλαμβανομένων των φορολογικών δεδομένων, των δεδομένων δικαστικών υποθέσεων, δεδομένα κυκλοφορίας οχημάτων και αδειοδότησης επιχειρήσεων. Στη παρούσα φάση, το DVDV καταφέρνει να υποστηρίξει περισσότερους από 5.200 κρατικούς οργανισμούς ενώ χρησιμοποιείται από χιλιάδες δημόσιους υπάλληλους [55].

Το DVDV αποτελεί ένα από τα μεγαλύτερα έργα Ηλεκτρονικής Διακυβέρνησης παγκοσμίως, ενώ το κόστος υλοποίησης του ανέρχεται στα 500.000 Ευρώ περίπου. Ωστόσο, σύμφωνα με έκθεση της Ευρωπαϊκής Επιτροπής, αναμένεται η εξοικονόμηση 1.000.000 Ευρώ ανά μήνα εφαρμογής του. Χαρακτηριστικά αναφέρεται ότι για το έτος 2010 το κόστος ανά ηλεκτρονική συναλλαγή ανήλθε στα 0,38 Ευρώ από 2,70 Ευρώ που απαιτούνταν νωρίτερα. Η Γερμανική κυβέρνηση προχωράει στην υλοποίηση της νέας γενιάς του DVDV συστήματος και το οποίο αναμένεται να τεθεί σε εφαρμογή το 2015.

4.2.3 Το Κυβερνητικό Νέφος της Ελλάδας

Είναι γεγονός ότι παρά την ταχύτατη ανάπτυξη των τεχνολογιών Νέφους παγκοσμίως, η Ελλάδα δεν έχει εφαρμόσει μία ολοκληρωμένη στρατηγική για τον εκσυγχρονισμό των Δημόσιων υπηρεσιών της. Ωστόσο, τα τελευταία χρόνια και καθώς γίνονται αντιληπτά τα σημαντικά οφέλη που ήδη αποκομίζουν άλλα προηγμένα κράτη από την εφαρμογή τέτοιων τεχνολογιών στη Δημόσια Διοίκηση, έχουν αρχίσει να λαμβάνονται και να υλοποιούνται σημαντικές πρωτοβουλίες και στην Ελληνική Δημόσια Διοίκηση. Η πολιτική ηγεσία φαίνεται να έχει πειστεί ότι η

Νεφοϋπολογιστική μπορεί να αποτελέσει εφαλτήριο ανάπτυξης, προόδου, διαφάνειας και εκσυγχρονισμού του Δημόσιου Τομέα.

Στο πλαίσιο αυτό, το 2009 συστάθηκε «η ομάδα Ηλεκτρονικής Διακυβέρνησης», η οποία λειτουργεί έως και σήμερα στο γραφείο του Πρωθυπουργού, με σκοπό να εισηγείται, να αναπτύσσει και να υποστηρίζει δράσεις και εφαρμογές ηλεκτρονικής Διακυβέρνησης. Σύμφωνα με την παρουσίαση της ομάδας [59], οι δράσεις που υλοποιήθηκαν εξυπηρετούν τον καλύτερο έλεγχο των δαπανών, την υποστήριξη της συλλογής εσόδων, τη διαφάνεια καθώς και την παρακολούθηση του Κυβερνητικού Έργου τόσο από την πολιτική ηγεσία όσο και από τους πολίτες. Χαρακτηριστικό παράδειγμα εφαρμογής της Νεφοϋπολογιστικής στο Δημόσιο Τομέα της Ελλάδας αποτελείτο πρόγραμμα «Διαύγεια» και το οποίο μελετάται ακολούθως.

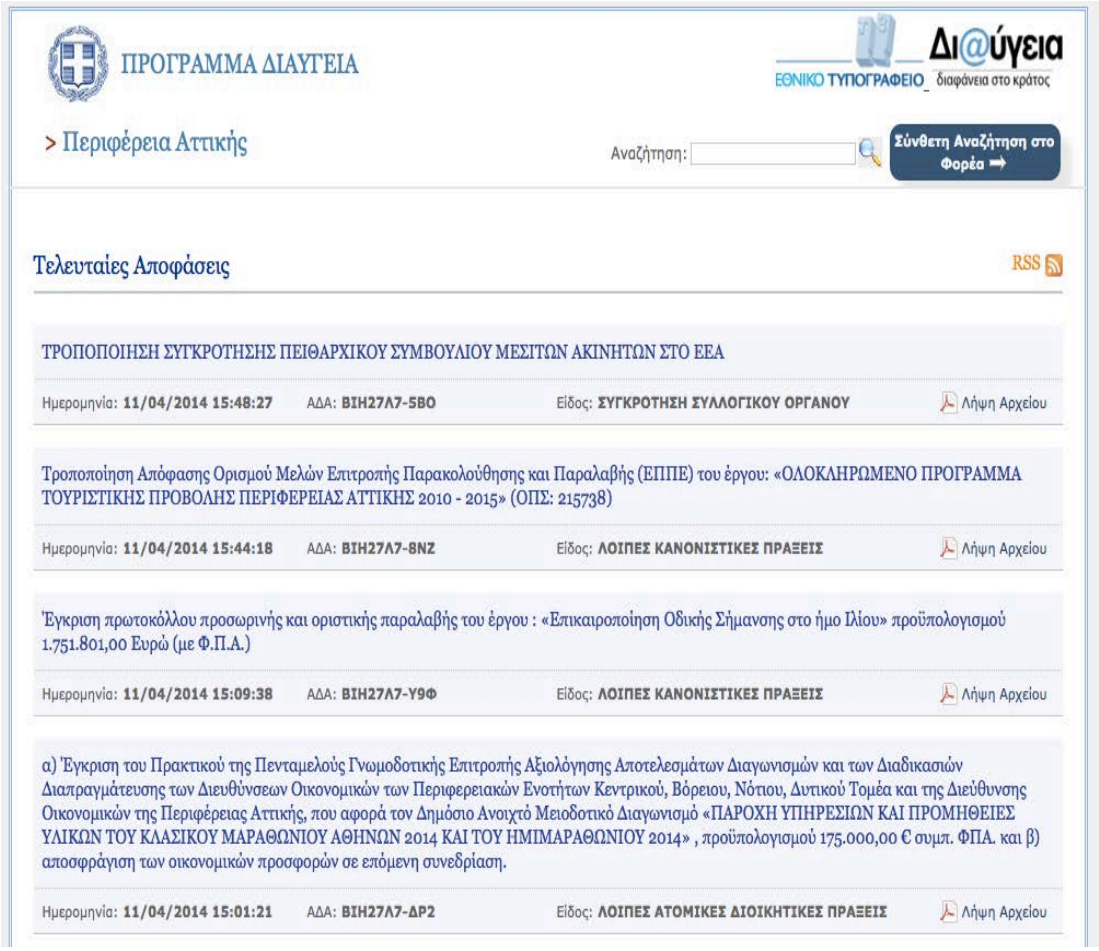
4.2.3.1 Το πρόγραμμα «Διαύγεια» (diavgeia.gov.gr) [61]

Σύμφωνα με την «Ομάδα Ηλεκτρονικής Διακυβέρνησης» [59], «*η διαφάνεια, ζήτημα μείζονος σημασίας για τη χώρα μας και προϋπόθεση για την εμπέδωση μίας σχέσης σεβασμού και εμπιστοσύνης ανάμεσα στον πολίτη και τη Δημόσια Διοίκηση, θωρακίστηκε και έλαβε θεσμική υπόσταση μέσω του Προγράμματος "Διαύγεια"*».Με το πρόγραμμα «Διαύγεια» εισάγεται για πρώτη φορά στην Ελλάδα η υποχρεωτική ανάρτηση των αποφάσεων των Δημόσιων Φορέων στο Διαδίκτυο. Η δράση αναπτύχθηκε και φιλοξενείται σε υποδομές της ΕΔΕΤ Α.Ε. (Εθνικό Δίκτυο Έρευνας και Τεχνολογίας) και υποστηρίζεται επιχειρησιακά από το Υπουργείο Διοικητικής Μεταρρύθμισης και Ηλεκτρονικής Διακυβέρνησης (http://www.ydmed.gov.gr/) [62] .

Από την 1/10/2010 όλοι οι φορείς του Δημοσίου, υποχρεούνται να αναρτούν τις αποφάσεις τους στο διαδικτυακό τόπο του προγράμματος «Διαύγεια». Με την ολοκλήρωση της ανάρτησης, η πράξη πιστοποιείται ότι έχει δημοσιευτεί αποκτώντας ένα μοναδικό Αριθμό Διαδικτυακής Ανάρτησης (ΑΔΑ), ενώ καμία απόφαση δεν είναι εκτελέσιμη πριν την ανάρτησή της στον τόπο του Προγράμματος. Ωστόσο, λαμβάνεται ειδική μέριμνα για τις πράξεις που αφορούν την εθνική άμυνα και τα ευαίσθητα προσωπικά δεδομένα [62]. Ο Πολίτης μπορεί να έχει πρόσβαση από ένα σημείο, στο σύνολο των νόμων και αποφάσεων που εκδίδουν τα κυβερνητικά όργανα, οι φορείς του στενού και του ευρύτερου δημόσιου τομέα, οι Ανεξάρτητες Αρχές και οι Οργανισμοί Τοπικής Αυτοδιοίκησης Α΄ και Β΄ βαθμού. Οι ενδιαφερόμενοι μπορούν να αναζητούν τις αποφάσεις των Υπουργείων και των Φορέων χρησιμοποιώντας λέξεις κλειδιά ή άλλα δεδομένα με τα οποία είναι καταχωρημένη η πράξη, μέσω μίας εύχρηστης φόρμας αναζήτησης. Έως τις 12/04/2014 έχουν ενταχθεί στο Πρόγραμμα 3.681 Φορείς του Δημοσίου και έχουν αναρτηθεί περισσότερες από 11.500.000 διοικητικές πράξεις και αποφάσεις.

Η εφαρμογή του προγράμματος Διαύγεια συμβάλει καθοριστικά στη δημιουργία ενός νέου μοντέλου στη σχέση του Πολίτη με το Κράτος, ενώ ενισχύεται η δυνατότητά του να απολαμβάνει τα συνταγματικά του δικαιώματα, όπως την πληροφόρηση και τη συμμετοχή του στην Κοινωνία της Πληροφορίας [62]. Το πρόγραμμα «Διαύγεια» έχει παρουσιαστεί με επιτυχία και ιδιαιτέρα θετικά σχόλια στην Ελλάδα, στην Ευρώπη και τις Η.Π.Α. όπου προκάλεσε το ενδιαφέρον και χαρακτηρίστηκε ως

επαναστατικό.



Πηγή:
http://et.diavgeia.gov.gr/f/perifereia_attikis

4.2.3.2 Οι υπηρεσίες του Ιδιωτικού Νέφους της Ελληνικής Κυβέρνησης

Η υλοποίηση όλων των δράσεων βασίζεται στη συστηματική συνεργασία της «Ομάδας της Ηλεκτρονικής Διακυβέρνησης» με τα στελέχη του κάθε Δημόσιου Φορέα και στην αξιοποίηση των υφιστάμενων Πληροφοριακών Συστημάτων και δομών. Όλες οι υπηρεσίες διατίθενται ως «Private Cloud» από διακομιστές του ΕΔΕΤ Α.Ε. και με την τεχνική υποστήριξη του Κέντρου Διαχείρισης Δικτύου του ΕΔΕΤ. Ακολούθως παρουσιάζονται όλες οι δράσεις με χρονολογική σειρά:

Φορέας	**Περιγραφή Υπηρεσίας**	**Δημόσια Διεύθυνση**
Προεδρία της Δημοκρατίας	Δικτυακός τόπος	http://www.presidency.gr
Γραφείο Πρωθυπουργού	Δικτυακός τόπος	http://www.primeminister.gr
Γραφείο Πρωθυπουργού	Υπηρεσία Ενημέρωσης	info.government.gov.gr
Γραφείο Πρωθυπουργού	Αποξήλωση παράνομων πινακίδων	illegalsigns.gov.gr
Κυβέρνηση	Δικτυακός τόπος	http://government.gov.gr
Αντιπρόεδρος της Κυβέρνησης	Δικτυακός τόπος	http://antiproedros.gov.gr
Κυβερνητικός Εκπρόσωπος	Δικτυακός τόπος	http://ekprosopos.gov.gr
Γενική Γραμματεία Κυβέρνησης	Δικτυακός τόπος - Υπηρεσία e-mail για τα στελέχη της ΓΓΚ	ggk.gov.gr
Υπουργείο Διοικητικής Μεταρρύθμισης και Ηλεκτρονικής Διακυβέρνησης	Πληροφοριακό σύστημα για το Πρόγραμμα ΔΙΑΥΓΕΙΑ	http://diavgeia.gov.gr
Υπουργείο Διοικητικής Μεταρρύθμισης και Ηλεκτρονικής Διακυβέρνησης /ΕΚΔΔΑ	Ηλεκτρονικές Υπηρεσίες προσκλήσεων & διαβουλεύσεων	http://www.opengov.gr

Υπουργείο Διοικητικής Μεταρρύθμισης & Ηλεκτρονικής Διακυβέρνησης	Μητρώο μισθοδοτούμενων ελληνικού δημοσίου	http://apografi.gov.gr
Υπουργείο Διοικητικής Μεταρρύθμισης & Ηλεκτρονικής Διακυβέρνησης	Μητρώο Νομικών Προσώπων Δημοσίου	https://registry.opengov.gr
Υπουργείο Διοικητικής Μεταρρύθμισης & Ηλεκτρονικής Διακυβέρνησης	Δράση για την ανοικτή δημόσια διοίκηση	http://openpad.gov.gr
Υπουργείο Διοικητικής Μεταρρύθμισης & Ηλεκτρονικής Διακυβέρνησης	Δικτυακός τόπος για τη παρουσίαση του επιχειρησιακού του Ν.3979	http://egovplan.gr
Υπουργείο Διοικητικής Μεταρρύθμισης & Ηλεκτρονικής Διακυβέρνησης / ΕΚΔΔΑ	Πλατφόρμα συνεργασίας για στελέχη πληροφορικής του δημόσιου τομέα	http://itdirectors.gov.gr
Υπουργείο Διοικητικής Μεταρρύθμισης & Ηλεκτρονικής Διακυβέρνησης / ΕΚΔΔΑ	Πλατφόρμα ηλεκτρονικής διαβούλευσης για δράσεις ΤΠΕ	http://labs.opengov.gr
Υπουργείο Οικονομικών	Δικτυακός τόπος	http://www.minfin.gr
Υπουργείο Οικονομικών - Γενική Γραμματεία Πληροφοριακών Συστημάτων		http://dict.opengov.gr www.gsis.gr
Υπουργείο Ανάπτυξης, Ανταγωνιστικότητας & Ναυτιλίας	Δικτυακός τόπος	http://www.mindev.gov.gr

Υπουργείο Ανάπτυξης, Ανταγωνιστικότητας & Ναυτιλίας	Πληροφοριακό σύστημα για το Πρόγραμμα ΑΓΟΡΑ	http://agora.gov.gr
Υπουργείο Ανάπτυξης, Ανταγωνιστικότητας & Ναυτιλίας- Γενική Γραμματεία Εμπορίου	Δικτυακός Τόπος Γενικής Γραμματείας Εμπορίου	http://gge.gov.gr
Υπουργείο Ανάπτυξης, Ανταγωνιστικότητας και Ναυτιλίας - Γενική Γραμματεία Εμπορίου	Παρατηρητήριο Διδάκτρων - Υποστηρικτικές εφαρμογές.	http://app.gge.gov.gr http://eysed.gge.gov.gr http://oil.gge.gov.gr http://app.gge.gov.gr http://parl.gge.gov.gr http://apod.gge.gov.gr http://metro.gge.gov.gr
Υπουργείο Ανάπτυξης, Ανταγωνιστικότητας και Ναυτιλίας-Γενική Γραμματεία Εμπορίου	Υπηρεσία Ταχυδρομείου στην πλατφόρμα ΕΛΛΑΚ - Πιλοτικό	http://mail.gge.gov.gr
Υπουργείο Ανάπτυξης Ανταγωνιστικότητας & Ναυτιλίας- Δικτυακός Τόπος Γενικής Γραμματείας Ναυτιλίας	Δικτυακός Τόπος Γενικής Γραμματείας Ναυτιλίας	shipping.gov.gr
Υπουργείο Ανάπτυξης, Ανταγωνιστικότητας &Ναυτιλίας- Ειδική Γραμματεία για την Ψηφιακή Σύγκλιση	Δικτυακός Τόπος Ειδικής Γραμματείας Ψηφιακής Σύγκλισης	digitalplan.gov.gr
Υπουργείο Ανάπτυξης, Ανταγωνιστικότητας & Ναυτιλίας - Επιχειρησιακή Μονάδα Ανάπτυξης	Δικτυακός τόπος	http://ema.mindev.gov.gr/
Υπουργείο Περιβάλλοντος και κλιματικής αλλαγής	Δικτυακός τόπος για τα ανοικτά γεωγραφικά δεδομένα	http://geodata.gov.gr
Υπουργείο	Εφαρμογή	http://wfd.opengov.gr/

Περιβάλλοντος και κλιματικής αλλαγή	διαβούλευσης της Διαβούλευση των Σχεδίων Διαχείρισης των υδατικών πόρων της χώρας	
Υπουργείο Περιβάλλοντος και κλιματικής αλλαγής	Μητρώο ταυτοτήτων υδάτων κολύμβησης της Ελλάδας	http://www.bathingwaterprofiles.gr/
Υπουργείο Υγείας και Κοινωνικής Αλληλεγγύης	Πλατφόρμα συνεργασίας για στελέχη του χώρου της Υγείας	ehealthforum.gov.gr
Υπουργείο Παιδείας, Δια Βίου Μάθησης και Θρησκευμάτων	Δράση Θαλής	https://apps.gov.gr/minedu/thalis
Υπουργείο Παιδείας, Δια Βίου Μάθησης και Θρησκευμάτων	Δράση Αρχιμήδης	-
Υπουργείο Παιδείας, Δια Βίου Μάθησης και Θρησκευμάτων	Δράση Υποτροφιών ξένων κυβερνήσεων σε Έλληνες υπηκόους	https://apps.gov.gr/minedu/scholarships
Υπουργείο Παιδείας, Δια Βίου Μάθησης και Θρησκευμάτων	Δράση Συνεργασία	https://apps.gov.gr/minedu/synergasia/
Υπουργείο Παιδείας, Δια Βίου Μάθησης και Θρησκευμάτων	Υποστήριξη ΙΚΥ	http://apps.gov.gr/minedu/iky_scholarships/
Υπουργείο Παιδείας, Δια Βίου Μάθησης και Θρησκευμάτων	Δράση Αριστεία	https://apps.gov.gr/minedu/aristeia/
Υπουργείο Παιδείας, Δια Βίου Μάθησης και Θρησκευμάτων	Δράση Δημιουργίας clusters	https://apps.gov.gr/minedu/clusters/

Υπουργείο Παιδείας, Δια Βίου Μάθησης και Θρησκευμάτων	"Business Support for the employment of highly qualified personnel	https://apps.gov.gr/minedu/employment
Υπουργείο Μεταφορών / ΕΕΤΤ	Δικτυακός τόπος για τη Δράση digitalgreece2020.gr	http://www.digitalgreece2020.gr/
Υπουργείο Πολιτισμού και Τουρισμού	Δικτυακός Τόπος Ελληνικού Οργανισμού Τουρισμού	http://blog.visitgreece.gr

Πηγή: http://egovict.blogspot.gr/

4.3 Εφαρμογές της Νεφοϋπολογιστικής στη Δημόσια Διοίκηση χωρών της Ασίας

Είναι γεγονός ότι εδώ και αρκετά χρόνια, οι περισσότερο αναπτυγμένες χώρες της Ασίας δείχνουν ιδιαίτερο ενδιαφέρον για την ανάπτυξη και υιοθέτηση λύσεων Νέφους στη Δημόσια Διοίκηση, προκειμένου να απολαύσουν τα σημαντικά οφέλη της τεχνολογίας αυτής. Σήμερα, τα περισσότερα κράτη της Ασίας διαθέτουν κυβερνητικό Νέφος με σκοπό να παρέχουν ολοκληρωμένες υπηρεσίες είτε προς τους πολίτες ή τις επιχειρήσεις είτε προς τους Δημόσιους οργανισμούς. Χαρακτηριστικά παραδείγματα τέτοιων Ασιατικών κρατών αποτελούν:

- Η Ιαπωνία: Το Ιδιωτικό Νέφος «Kasumigaseki»
- Η Ινδία: Το Ιδιωτικό Νέφος «MeghRaj»

Οι περιπτώσεις αυτές μελετώνται ακολούθως.

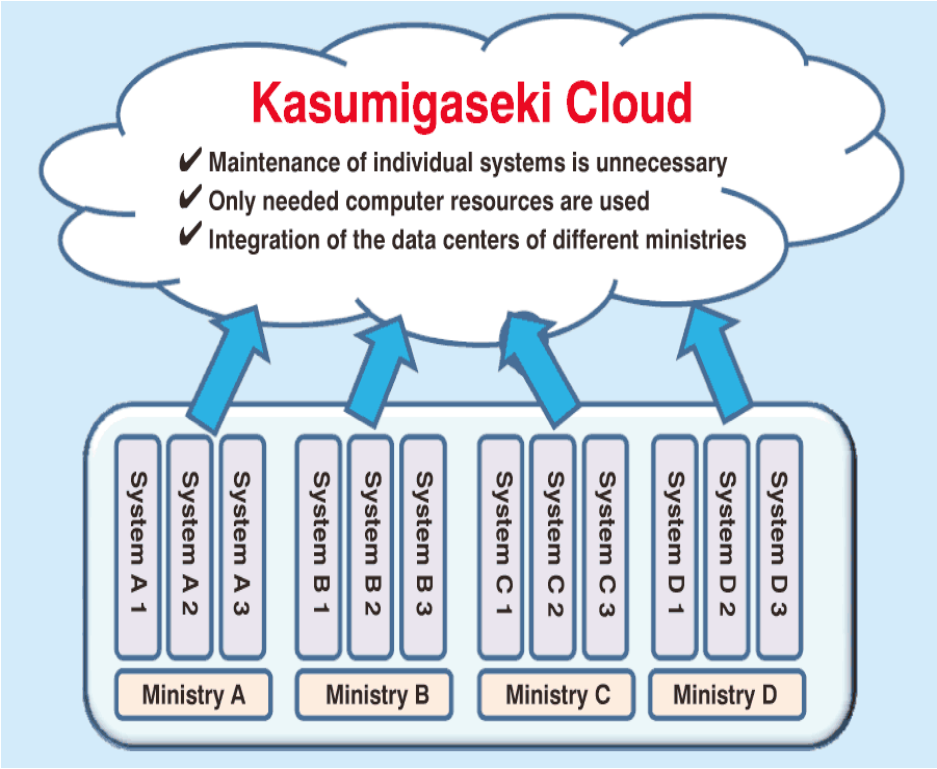
4.3.1 Ιαπωνία – Το Ιδιωτικό Νέφος «Kasumigaseki» [47][52][66]

Από το 2009, η Ιαπωνική κυβέρνηση έβαλε σε εφαρμογή το σχέδιο δημιουργίας της «Ψηφιακής Ιαπωνίας», με σκοπό την οικονομική ανάπτυξη της χώρας μέσω επενδύσεων στον τομέα της τεχνολογίας της Πληροφορικής. Ως μέρος του σχεδίου αυτού, η Ιαπωνική κυβέρνηση σε συνεργασία με το Ιαπωνικό Υπουργείο Εσωτερικών, ανέλαβε μία ιδιαίτερα σημαντική πρωτοβουλία για τη δημιουργία Ιδιωτικού Κυβερνητικού Νέφους. Το Νέφος αυτό ονομάστηκε «Kasumigaseki Cloud» εξαιτίας της ομώνυμης τοποθεσίας στο Τόκυο, όπου βρίσκονται οι περισσότεροι Κυβερνητικοί Φορείς του Κράτους.

Με τη δημιουργία του Νέφους «Kasumigaseki», το οποίο αναμένεται να ολοκληρωθεί έως το 2015, η Ιαπωνική κυβέρνηση φιλοδοξεί να μπορέσει να φιλοξενήσει το λογισμικό όλων των Δημόσιων Φορέων της Ιαπωνίας. Η πρωτοβουλία αυτή έχει ως στόχο τη δημιουργία μίας τεράστιας υποδομής Νέφους, η οποία θα μπορεί να ανταποκριθεί στις ολοένα αυξανόμενες απαιτήσεις των Πληροφοριακών Συστημάτων των Δημόσιων οργανισμών, χωρίς να απαιτείται η τήρηση ξεχωριστών IT τμημάτων ανά Δημόσιο Φορέα. Σύμφωνα με το Ιαπωνικό Υπουργείο Εσωτερικών, το Ιδιωτικό Κυβερνητικό Νέφος επιτρέπει τον εύκολο διαμοιρασμό των πληροφοριών ενώ προωθεί περισσότερο την τυποποίηση και την ενοποίηση των IT πόρων της Κυβέρνησης.

Με την ενοποίηση όλων των κυβερνητικών IT πόρων σε μία Cloud υποδομή, η Ιαπωνική Κυβέρνηση έχει ήδη αποκομίσει σημαντικά οφέλη, τα οποία αναφέρονται όχι μόνο στη μείωση του λειτουργικού κόστους των Δημόσιων οργανισμών αλλά και στην παροχή IT υπηρεσιών φιλικών προς το περιβάλλον. Εξάλλου, εκτός από τις χιλιάδες θέσεις εργασίας που δημιούργησε η τεράστια αυτή επένδυση για τη δημιουργία του Ιδιωτικού Κυβερνητικού Νέφους, η Ιαπωνική κυβέρνηση αναμένει ότι έως το 2020 θα έχει διπλασιάσει το μέγεθος της IT αγοράς της, τομέας ιδιαίτερης

στρατηγικής σημασίας για την Ιαπωνική οικονομία.



Πηγή:
THE CLOUDY FUTURE OF GOVERNMENT IT: CLOUD COMPUTING AND THE PUBLIC SECTOR AROUND THE WORLD, David C. Wyld [47]

4.3.2 Ινδία – Το Ιδιωτικό Νέφος «MeghRaj» [67] [68]

Η κυβέρνηση της Ινδίας, προκειμένου να εκμεταλλευτεί τα πολλαπλά οφέλη της Νεφοϋπολογιστικής, έχει ξεκινήσει μία πολύ φιλόδοξη πρωτοβουλία για την εφαρμογή Cloud τεχνολογιών στη Δημόσια Διοίκηση. Βασικός στόχος αυτής της πρωτοβουλίας αποτελεί η επιτάχυνση της παράδοσης των ηλεκτρονικών υπηρεσιών της χώρας μειώνοντας ταυτόχρονα τις IT δαπάνες των δημόσιων οργανισμών. Η πρωτοβουλία αυτή αναμένεται να εξασφαλίσει τη βέλτιστη χρησιμοποίηση της IT υποδομής καθώς και την επιτάχυνση της υλοποίησης εφαρμογών Ηλεκτρονικής Διακυβέρνησης.

Η πρωτοβουλία αυτή ονομάστηκε «MeghRaj» και σχεδιάστηκε και υλοποιήθηκε από το Εθνικό Κέντρο Πληροφορικής (National Informatics Centre)της Ινδίας σε συνεργασία με το Υπουργείο Επικοινωνιών και Πληροφορικής της χώρας. Το

αρχιτεκτονικό όραμα του Εθνικού Ιδιωτικού Νέφους «MeghRaj» περιλαμβάνει ένα σύνολο γεωγραφικά διάσπαρτων, νέων ή υφιστάμενων, υποδομών Νέφους οι οποίες ακολουθούν ένα κοινό πλαίσιο πρωτοκόλλων και προτύπων καθορισμένων από την Ινδική κυβέρνηση.

Το Ιδιωτικό Νέφος της Ινδικής κυβέρνησης παρέχει πλήθος Cloud υπηρεσιών προκειμένου να καλύψει τις αυξημένες IT απαιτήσεις των περισσότερων Δημόσιων οργανισμών της χώρας. Η παροχή των υπηρεσιών Νέφους πραγματοποιείται έπειτα από την υποβολή αίτησης του ενδιαφερόμενου Δημόσιου Φορέα. Οι τελευταία μπορούν μέσω του Ιδιωτικού Νέφους της κυβέρνησης να προμηθεύονται υπηρεσίες IaaS (Infrastructure as a Service), PaaS (Platform as a Service) και SaaS (Software as a Service), υπηρεσίες αποθήκευσης και υπηρεσίες hosting, για τη δημιουργία και φιλοξενία απομονωμένων εικονικών μηχανών (Virtual machines).

Πηγή: National Cloud by NIC
https://cloud.gov.in/index.php

Αναφορικά με τις παρεχόμενες hosting υπηρεσίες , το εθνικό Ιδιωτικό Νέφος της Ινδίας εκτός των άλλων παρέχει:

- Διακομιστή Εκτίμησης Ευπαθειών (Server Vulnerability Assessment)
- Διακομιστή Ελέγχου (Server Monitoring)

- Διακομιστή Αντιγράφων Ασφαλείας (Backup Server)
- Τείχος Προστασίας εφαρμογών και Δικτύου(Network/ Application Firewall)
- Domain Name Services

Κεφάλαιο 5ο

Στρατηγική Μετάβασης σε Τεχνολογίες Νέφους

Παρά το γεγονός ότι πολλοί ερευνητές εγείρουν σημαντικά ζητήματα γύρω από την ασφάλεια των Πληροφοριών σε μία υποδομή Νέφους, είναι αδιαμφισβήτητο το γεγονός ότι η Νεφοϋπολογιστική μπορεί να συμβάλλει καθοριστικά στη μείωση της γραφειοκρατίας, στην ενίσχυση της διαφάνειας και στο γενικότερο εκσυγχρονισμό της Δημόσιας Διοίκησης ενός Κράτους. Ωστόσο, η διαδικασία μετάβασης των Δημόσιων υπηρεσιών στο Νέφος απαιτεί το σχεδιασμό μίας καθολικής και ολοκληρωμένης στρατηγικής από την εκάστοτε Κυβέρνηση, έτσι ώστε η νέα δομή των Υπηρεσιών να λειτουργεί απρόσκοπτα και να εκπληρώνει τους σκοπούς των Δημόσιων Οργανισμών που εξυπηρετεί. Πολλές στρατηγικές έχουν προταθεί κατά καιρούς, ωστόσο, οι υπεύθυνοι για το σχεδιασμό της μετάβασης οφείλουν να εντοπίζουν εξαρχής τις ιδιαίτερες απαιτήσεις της Δημόσιας Διοίκησης και να σχεδιάσουν τη στρατηγική τους ανάλογα με αυτές. Στο πλαίσιο αυτό, θα πρέπει να ληφθούν σημαντικές αποφάσεις τόσο για την επιλογή των υπηρεσιών που πρόκειται να μεταβούν στο Νέφος όσο και για το μοντέλο του Νέφους που τελικά θα επιλεγεί. Στο Κεφάλαιο που ακολουθεί αναλύονται τα ζητήματα αυτά, ενώ ιδιαίτερη αναφορά γίνεται και στη σύναψη του συμβολαίου (Service Level Agreement -SLA) μεταξύ του Παρόχου και της Κυβέρνησης. Τέλος, περιλαμβάνεται μία εκτενής αναφορά για τη χρησιμότητα αλλά και τους Κινδύνους που ελλοχεύει η εφαρμογή της Νεφοϋπολογιστικής στις Κρίσιμες Υποδομές ενός Κράτους.

5.1 Στρατηγική μετάβασης της Δημόσιας Διοίκησης σε τεχνολογίες Νέφους

Είναι γεγονός ότι η μεταστροφή του παραδοσιακού IT μοντέλου στη Δημόσια Διοίκηση απαιτεί το σχεδιασμό και την εφαρμογή μίας ολοκληρωμένης στρατηγικής μετάβασης στο Νέφος. Παρά το γεγονός ότι οι προκλήσεις που αντιμετωπίζει μία Ιδιωτική επιχείρηση, κατά τη μετάβαση της στο Νέφος, δε διαφέρουν σε τίποτα από εκείνες που πρόκειται να αντιμετωπίσουν οι υπεύθυνοι ενός Δημόσιου οργανισμού, η προμήθεια των υπηρεσιών Νέφους αλλά και η ασφάλεια των δεδομένων χρήζουν ιδιαίτερης προσοχής από ένα Δημόσιο Φορέα. Η κάθε κυβέρνηση οφείλει τόσο την προστασία των Δεδομένων των πολιτών στο ακέραιο όσο και την εξασφάλιση της υψηλής διαθεσιμότητας των Κρίσιμων Υποδομών (Critical Infrastructure) του Κράτους, όπως η ενέργεια, η υγεία, το νερό, οι επικοινωνίες κτλ. Από την άλλη πλευρά, οι διαθέσιμοι οικονομικοί πόροι ενός Δημόσιου φορέα είναι συνήθως προϋπολογισμένοι αρκετούς μήνες ή χρόνια νωρίτερα, γεγονός που δυσκολεύει την προμήθεια καινοτόμων IT τεχνολογιών με χαμηλότερο κόστος, εάν συνυπολογιστεί και το γεγονός ότι η διαδικασία επιλογής προμηθευτή είναι ιδιαίτερα χρονοβόρα. Οι ιδιαιτερότητες αυτές που περιγράφηκαν ενισχύουν την άποψη ότι για την ομαλή μετάβαση της Δημόσιας Διοίκησης σε Cloud τεχνολογίες απαιτείται η ύπαρξη μίας προσεκτικά σχεδιασμένης στρατηγικής.

Κατά καιρούς έχουν προταθεί πλήθος στρατηγικών μετάβασης των Δημόσιων Υπηρεσιών στο Νέφος. Οι περισσότερες από αυτές προέρχονται από ερευνητές ή οργανισμούς των Ηνωμένων Πολιτειών της Αμερικής και λιγότερες από Ευρωπαϊκά κράτη. Μία τέτοια στρατηγική προτάθηκε από τον David Wyld[4] το 2009 για λογαριασμό της IBM. Η στρατηγική αυτή αποτελεί ένα γενικό πλαίσιο μετάβασης και θα πρέπει να προσαρμόζεται ανάλογα με την περίπτωση εφαρμογής, προκειμένου να ικανοποιήσει τις ιδιαίτερες απαιτήσεις του κάθε Δημόσιου Φορέα. Συνεπώς, οι υπεύθυνοι για την IT μετάβαση στο Νέφος θα πρέπει να αξιολογήσουν εκ των προτέρων τη δυνατότητα ενσωμάτωσης τεχνολογιών Νέφους στη συνολική IT στρατηγική του Δημόσιου οργανισμού, προκειμένου να υποστηρίξουν την αποστολή του. Σύμφωνα με τον David Wyld [05][47], η διαδικασία αυτή περιλαμβάνει έξι (6) στάδια, τα οποία παρουσιάζονται ακολούθως:

Στάδιο 1ο: Εκμάθηση –Εκπαίδευση

Η στρατηγική για τη μετάβαση σε τεχνολογίες Νέφους ξεκινά με την εκπαίδευση όλων των εμπλεκόμενων IT στελεχών σε θέματα που αφορούν τις βασικές λειτουργίες, αρχιτεκτονικές και υπηρεσίες που παρέχει η Νεφοϋπολογιστική. Η εκπαίδευση μπορεί να πραγματοποιηθεί με διάφορους τρόπους, όπως μέσω παρακολούθησης σεμιναρίων, προσωπικής έρευνας, επικοινωνίας με προμηθευτές υπηρεσιών Νέφους κτλ. Στη συνέχεια, δεδομένου ότι η Νεφοϋπολογιστική αποτελεί μία σχετικά νέα και διαρκώς εξελισσόμενη τεχνολογία των υπολογιστών, επιβάλλεται

[4] Department of Management, Southeastern Louisiana University, Hammond, LA USA

η ενημέρωση όλου του μελλοντικά εμπλεκόμενου προσωπικού (στελέχη των Δημόσιων οργανισμών, νομικούς, επιτελικά κυβερνητικά στελέχη κτλ) από τα εξειδικευμένα στελέχη για την πολιτική που πρόκειται να ακολουθηθεί και τα πλεονεκτήματα που θα προκύψουν από τη στροφή στη νέα αυτή τεχνολογία. Είναι ιδιαίτερα σημαντικό, η εκάστοτε κυβέρνηση να ενθαρρύνει πρωτοβουλίες και να παρέχει επαρκή χρηματοδότηση για έρευνα σχετικά με την παγκόσμια υιοθέτηση Cloud τεχνολογιών σε όλα τα επίπεδα της Δημόσιας Διοίκησης.

Στάδιο 2^{ο}: Αξιολόγηση των IT υποδομών του Δημόσιου οργανισμού

Το στάδιο αυτό περιλαμβάνει την αναλυτική αξιολόγηση της ικανότητας των υπάρχοντων IT υποδομών, προκειμένου να διαπιστωθεί το αν καλύπτουν τις υπάρχουσες ή μελλοντικές ανάγκες του οργανισμού. Σε ένα περιβάλλον Νέφους, όπου μπορούν εύκολα να προστεθούν ή να αφαιρεθούν υπολογιστικοί πόροι ανάλογα με τις ανάγκες του οργανισμού, είναι ιδιαίτερα σημαντική μία πλήρης καταγραφή και αξιολόγηση της IT υποδομής. Η αξιολόγηση θα πρέπει να περιλαμβάνει απαραίτητα την πλήρη καταγραφή της ημερήσιας κατανάλωσης υπολογιστικών πόρων με το υπάρχον IT μοντέλο αλλά και την πραγματική απαίτηση για την παροχή αξιόπιστων υπηρεσιών. Έτσι σε αυτή την περίπτωση, θα μπορεί να εκτιμηθεί εάν μπορεί ο οργανισμός να συνεχίσει να παρέχει εσωτερικά τις υπηρεσίες ή απαιτείται η μετάβαση του συνόλου ή μέρους αυτών στο Νέφος, προκειμένου να καλυφθούν περίοδοι αυξημένης ζήτησης υπολογιστικών πόρων.

Στάδιο 3^{ο}: Πιλοτική Εφαρμογή του Νέφους

Έπειτα από την αξιολόγηση των υπάρχοντων IT δομών, θα πρέπει να επιλεγεί μία συγκεκριμένη περιοχή ή τουλάχιστον ένα συγκεκριμένο έργο, προκειμένου να μεταφερθεί πιλοτικά στο Νέφος. Τα αποτελέσματα της πιλοτικής αυτής εφαρμογής θα πρέπει να αξιολογηθούν προσεκτικά, με σκοπό να καταγραφεί η απόδοσή τους. Όπως με κάθε νέα τεχνολογία, το εξειδικευμένο προσωπικό θα πρέπει να πειραματιστεί με τις εφαρμογές Νέφους έτσι ώστε να αποτιμήσει τη χρησιμότητα και την αποδοτικότητα των Cloud Computing εφαρμογών στη λειτουργία του οργανισμού.

Σημειώνεται ότι οι προσπάθειες αυτές, ανεξάρτητα από το αποτέλεσμά τους, θα πρέπει να ενθαρρύνονται από την κυβέρνηση, καθώς η εμπειρία που αποκομίζεται μπορεί να αποτελέσει πηγή γνώσης για την ευρύτερη IT κοινότητα με ενδιαφέρον στον τομέα της Νεφοϋπολογιστικής. Ο διαμοιρασμός αυτής της εμπειρίας μπορεί να διαμορφώσει πλαίσια «καλής πρακτικής» ή «παραδείγματα προς αποφυγή», τα οποία μπορούν να προωθήσουν και να διευκολύνουν την υιοθέτηση τεχνολογιών Νέφους ακόμη και σε μικρούς ή μεσαίους οργανισμούς.

Στάδιο 4^{ο}: Επιλογή δεδομένων και εφαρμογών για τη μετάβαση τους στο Νέφος

Κατόπιν της αξιολόγησης των αποτελεσμάτων που προέκυψαν από την πιλοτική εφαρμογή, οι υπεύθυνοι θα πρέπει να προβούν σε συνολική εκτίμηση των δεδομένων και των εφαρμογών του οργανισμού, έτσι ώστε να προσδιοριστούν εκείνα που μπορούν να μετακινηθούν σε περιβάλλον Νέφους. Στο σημείο αυτό και έπειτα από το διαχωρισμό των δεδομένων και των εφαρμογών, επιδιώκεται ο προσδιορισμός του μοντέλου του Νέφους (δημόσιο, ιδιωτικό, υβριδικό ή κοινότητας) στο οποίο αυτά θα μεταβούν. Η επιλογή του μοντέλου υπηρεσιών με τη χρήση SWOT ανάλυσης μελετάται στην επόμενη ενότητα.

Στάδιο 5^{ο}: Μετάβαση των δεδομένων και των εφαρμογών στο Νέφος

Σε αυτό το σημείο ξεκινά η σταδιακή μετάβαση των Δεδομένων και των εφαρμογών, που επιλέχθηκαν νωρίτερα, στο Νέφος με τη συμμετοχή της οργανωτικής ηγεσίας του οργανισμού και των εμπλεκόμενων IT στελεχών. Απαραίτητη κρίνεται η διαρκής επικοινωνία και υποστήριξη όλων των εμπλεκόμενων φορέων, εντός και εκτός του οργανισμού, προκειμένου να διασφαλιστεί η ομαλή πρόοδος κατά τη μετάβαση στο Νέφος. Σε αυτό το σημείο, το Νέφος καθίσταται από πιλοτική εφαρμογή σε κύριο εργαλείο για τη διαχείριση των Δεδομένων, των εφαρμογών και των υπηρεσιών του Δημόσιου οργανισμού.

Στάδιο 6^{ο}: Βελτίωση των υπηρεσιών Νέφους

Στο σημείο αυτό, η διαδικασία εισέρχεται στο τελικό στάδιο με σκοπό τη διαρκή βελτίωση των παρεχόμενων υπηρεσιών Νέφους. Εδώ, ο οργανισμός εξακολουθεί να μετακινεί κατάλληλα επιλεγμένα Δεδομένα και εφαρμογές στο Νέφος ή να επιστρέφει κάποια από αυτά στην παραδοσιακή IT μορφή, εφόσον αξιολογηθεί ότι η χρήση τους σε περιβάλλον Νέφους δεν απέδωσε τα αναμενόμενα αποτελέσματα. Η μετακίνηση όλο και περισσότερων εφαρμογών στο Νέφος θα βοηθήσει σημαντικά στη θεαματική αύξηση της διαλειτουργικότητας μεταξύ των Δημόσιων οργανισμών. Σε αυτό το σημείο, απαιτείται από πλευράς πολιτικής ηγεσίας η δημιουργία και εφαρμογή των σχετικών κανόνων λειτουργίας του Νέφους, όπως για παράδειγμα οι όροι πρόσβασης στα αρχεία κτλ.

The Six-Step Cloud Migration Strategy [47]

Όπως αναφέρθηκε και προηγουμένως, η στρατηγική αυτή αποτελεί ένα γενικό πλαίσιο που μπορεί να προσαρμοστεί ανάλογα με τις ανάγκες του κάθε οργανισμού. Ακολουθεί συνοπτική αναφορά με κάποιες από τις κατά καιρούς προτεινόμενες στρατηγικές μετάβασης στο Νέφος.

Αναφορά	***Στρατηγική Μετάβασης***
Cisco (2009) [71]	▪ Προσδιορισμός όλων των πιθανών εφαρμογών για μετάβαση από το υφιστάμενο καθεστώς στο Νέφος ▪ Επιβεβαίωση ότι η υπάρχουσα IT υποδομή μπορεί να υποστηρίξει και να επεκταθεί μέσω των υπηρεσιών Νέφους ▪ Ανάπτυξη ενός πλαισίου κόστους-οφέλους και αξιολόγηση των κινδύνων για τη λήψη αποφάσεων σχετικά με το που, πότε και πως μπορούν να μεταβούν οι υπηρεσίες στο Νέφος ▪ Ανάπτυξη συγκεκριμένης στρατηγικής για τη βελτιστοποίηση του υπάρχοντος IT περιβάλλοντος με τη χρήση τεχνολογιών Νέφους ▪ Εντοπισμός των δεδομένων που δε μπορούν να μετακινηθούν στο Νέφος για νομικούς λόγους ή για λόγους ασφάλειας κτλ

	▪ Εντοπισμός και εξασφάλιση in-house δυνατοτήτων για την αποτελεσματική διαχείριση των διαδικασιών υιοθέτησης υπηρεσιών Νέφους ▪ Δημιουργία μίας διατμηματικής ομάδας με σκοπό την παρακολούθηση νέων υπηρεσιών, Παρόχων και προτύπων στο χώρο της Νεφοϋπολογιστικής, τα οποία μπορούν να διαμορφώσουν την πολιτική του οργανισμού. ▪ Αξιολόγηση των τεχνικών προκλήσεων που πιθανόν προκύψουν κατά τη μετάβαση στο Νέφος και πιλοτική εφαρμογή ▪ Επιβεβαίωση ότι το δίκτυο των υπολογιστών είναι έτοιμο για μετάβαση στο Νέφος
Frost & Sullivan (2011) [65]	Προσδιορισμός: ▪ Προσδιορισμός των εφαρμογών που μπορούν να μεταφερθούν στο Νέφος ▪ Προσδιορισμός του μοντέλου Νέφους (Δημόσιο, Ιδιωτικό, Κοινότητας) με βάση την ασφάλεια των δεδομένων και τις απαιτήσεις του SLA συμβολαίου. Υλοποίηση: ▪ Καταγραφή της ζήτησης σε επίπεδο τμήματος ή οργανισμού ▪ Επιβεβαίωση της ενσωμάτωσης με την υφιστάμενη υποδομή ▪ Δημιουργία «πολιτικής των χρηστών», όπου διασφαλίζεται η ευχρηστία και η απλότητα ▪ Επιβεβαίωση ότι οι όροι του SLA συμβολαίου πληρούνται από τους Παρόχους και διασφαλίζουν το επιθυμητό επίπεδο ασφάλειας Βελτίωση: ▪ Λεπτομερή αναφορά των επιτυχιών & αποτυχιών στους χρήστες ▪ Αλλαγή της νοοτροπίας από την αγορά IT εξοπλισμού στη

	χρήση υπηρεσιών ▪ Επιβεβαίωση ότι το IT προσωπικό είναι κατάλληλα εκπαιδευμένο αναφορικά με τη διαχείριση των Παρόχων υπηρεσιών Νέφους και των SLA συμβολαίων
Federal Cloud Computing Strategy – Vivek Kundra (2011) [70]	Επιλογή: ▪ Επιλογή ποιών υπηρεσιών και πότε θα μεταφερθούν στο Νέφος Πρόβλεψη: ▪ Της συνολικής ζήτησης όπου είναι δυνατόν ▪ Εξασφάλιση της διαλειουργικότητας και της συμβατότητας με την υπάρχουσα IT υποδομή ▪ Σύναψη κατάλληλων συμβολαίων για την εξασφάλιση των απαιτήσεων του οργανισμού Διαχείριση: ▪ Μεταστροφή της αντίληψης για το IT μοντέλο από τα αγαθά στις υπηρεσίες ▪ Δημιουργία νέων δεξιοτήτων, όπου αυτές απαιτούνται ▪ Συστηματική παρακολούθηση των όρων του SLA συμβολαίου προκειμένου να διασφαλιστεί η συμμόρφωση του Παρόχου ▪ Περιοδική επαναξιολόγηση του Παρόχου και των μοντέλων των υπηρεσιών προκειμένου να μεγιστοποιηθούν τα οφέλη και να μειωθούν τα ρίσκα.

5.2 Επιλογή υπηρεσιών για μετάβαση στο Νέφος

Είναι γενικά παραδεκτό ότι οι τεχνολογίες Νέφους αποτελούν ένα εναλλακτικό τρόπο για την παροχή IT υπηρεσιών στη Δημόσια Διοίκηση, με πολλά σημαντικά οφέλη κατά την εφαρμογή του. Ωστόσο, το Νέφος καλύπτει ένα πλήθος υπηρεσιών και μοντέλων εφαρμογών, από in-house εικονικές μηχανές έως λογισμικό προσβάσιμο από πολλούς διαφορετικούς οργανισμούς μέσω Διαδικτύου. Συνεπώς, η αποτελεσματικότητα της εφαρμογής της Νεφοϋπολογιστικής εξαρτάται σε μεγάλο βαθμό από την επιλογή τόσο του κατάλληλου μοντέλου Νέφους όσο και του μοντέλου των υπηρεσιών, έτσι ώστε οι υπηρεσίες που μεταβαίνουν στο Νέφος να εξυπηρετούν στο ακέραιο τους στόχους του Οργανισμού.

5.2.1 Επιλογή του μοντέλου Νέφους

Όπως αναφέρθηκε και προηγουμένως, η επιλογή του σωστού μοντέλου Νέφους είναι καθοριστικής σημασία για μία επιτυχημένη μετάβαση στο Νέφος. Στο πλαίσιο αυτό, το European Network and Information Security (ENISA, 2011) παρουσίασε μία SWOT[5] ανάλυση για κάθε μοντέλο Νέφους (Δημόσιο, Ιδιωτικό και Κοινότητας), προκειμένου να βοηθήσει στην επιλογή του μοντέλου εκείνου που καλύπτει τις απαιτήσεις του Οργανισμού. Η SWOT ανάλυση παρουσιάζει τα πλεονεκτήματα, τις αδυναμίες, τις ευκαιρίες και τις απειλές αναφορικά με την ασφάλεια, την ανθεκτικότητα και τη νομική συμμόρφωση κάθε μοντέλου Νέφους. Η μελέτη αυτή παρουσιάζεται σε συνοπτικούς πίνακες ακολούθως [52][74].

Δημόσιο Νέφος στη Δημόσια Διοίκηση – SWOT Ανάλυση

Strengths:	**Weaknesses:**
▪ Υψηλή Διαθεσιμότητα & Αξιοπιστία ▪ Ανεκτικότητα & Ελαστικότητα ▪ Patch management ▪ Μικρός χρόνος απόκρισης ▪ Εξασφάλιση της επιχειρησιακής συνέχειας ▪ Ισχυρά μέτρα Ασφάλειας για τη φυσική πρόσβαση ▪ Ισχυρές διαδικασίες πρόληψης &	▪ Αδυναμία ελέγχου των προμηθευτών υπηρεσιών (SaaS, PaaS ή IaaS) ▪ Μειωμένη δυνατότητα διατήρησης αρχείων καταγραφής πρόσβασης, διαχείρισης και αναφοράς γεγονότων ▪ Αδυναμία πρόσβασης σε δεδομένα εγκληματικού χαρακτήρα ▪ Έλλειψη διαπραγματευτικής ισχύος για τη συμφωνία των όρων διαφάνειας με τον Πάροχο ▪ Υποχρέωση του παρόχου για

[5] Η **ανάλυση SWOT** είναι ένα εργαλείο στρατηγικού σχεδιασμού το οποίο χρησιμοποιείται για την ανάλυση του εσωτερικού και εξωτερικού περιβάλλοντος μίας επιχείρησης, όταν η επιχείρηση πρέπει να λάβει μία απόφαση σε σχέση με τους στόχους που έχει θέσει ή με σκοπό την επίτευξή τους [73].

Ανίχνευσης εισβολών	διατήρηση των δεδομένων του χρήστη εντός της επικράτειας (σε ορισμένες χώρες) ▪ Μειωμένες επιδόσεις σε περίπτωση κακής Διαδικτυακής συνδεσιμότητας ▪ Περιορισμένη διασπορά των data centers εντός της Ευρωπαϊκής Ένωσης, με πιθανές μειωμένες επιδόσεις των παρεχόμενων Υπηρεσιών ▪ Δύσκολη επιστροφή των δεδομένων στον πλήρη έλεγχο των χρηστών ή η μεταφορά τους σε άλλο Πάροχο
Opportunities: ▪ Ανάλυση και Αξιολόγηση των Κινδύνων ▪ Δοκιμές Ασφάλειας ▪ Παρακολούθηση της Ασφάλειας σε πραγματικό χρόνο ▪ Ανίχνευση ηλεκτρονικού εγκλήματος	**Threats:** ▪ Μία μεγάλη υποδομή Δημόσιου Νέφους είναι ελκυστικός στόχος επιθέσεων ▪ Μεγάλος αντίκτυπος από εσωτερικές επιθέσεις, λόγω του τεράστιου όγκου πληροφοριών που αποθηκεύονται στο Δημόσιο Νέφος ▪ Μία πιθανή αδυναμία απομόνωσης των χρηστών μπορεί να οδηγήσει σε σημαντική διαρροή πληροφοριών ▪ Έκθεση των αγαθών του οργανισμού σε περίπτωση λανθασμένου προσδιορισμού των απαιτήσεων ασφάλειας ▪ Κάθε αλλαγή στην διαδικασία ελέγχου του Παρόχου επιφέρει νέα αλλαγή στη στρατηγική ασφάλειας του Οργανισμού ▪ Οι SaaS και PaaS υπηρεσίες απαιτούν την αποθήκευση των δεδομένων σε συγκεκριμένη μορφή με αποτέλεσμα την αδυναμία μεταφοράς των Δεδομένων σε άλλο Πάροχο στην περίπτωση που τα Δεδομένα δε μπορούν να μετασχηματιστούν στη νέα αποδεκτή μορφή.

Ιδιωτικό Νέφος στη Δημόσια Διοίκηση – SWOT Ανάλυση

Strengths:	**Weaknesses:**
▪ Επιλογή των μεθόδων αξιολόγησης των Κινδύνων ▪ Δυνατότητα εκτέλεσης προγραμματισμένων patches ▪ Έλεγχος πρόσβασης ▪ Διατήρησης αρχείων καταγραφής (Log files) ▪ Auditing ▪ Έλεγχος της Διαθεσιμότητας, της κλιμάκωσης, της Αξιοπιστίας και της ελαστικότητας των Υπηρεσιών τους Νέφους ▪ Υποστήριξη σχεδίων επιχειρησιακής συνέχειας ▪ Πλήρης διαφάνεια και έλεγχος των νομικών απαιτήσεων, όπως η θέση των Δεδομένων	▪ Πιθανή έλλειψη οικονομικών πόρων μπορεί να οδηγήσει σε αδυναμία αγοράς και εφαρμογής μηχανισμών ασφαλείας ▪ Μικρότερη ευελιξία για κάλυψη περιόδων αυξημένης ζήτησης ▪ Η εμπιστοσύνη προς την Κυβέρνησης ή του Δημόσιου Οργανισμού καθίσταται ιδιαίτερα ευάλωτη από μία πιθανή διαρροή πληροφοριών σε περίπτωση κάποιου πιθανού επεισοδίου ασφάλειας ▪ Ο χρόνος ανάκαμψης ύστερα από ένα περιστατικό επίθεσης είναι αρκετά μεγαλύτερος από ένα Δημόσιο Νέφος, εκτός εάν τηρείται συγκεκριμένος μηχανισμός ασφάλειας. Στην περίπτωση αυτή κινδυνεύει η επιχειρησιακή συνέχεια. Επαρκής όροι προστασίας πρέπει να καθορίζονται στο SLA.
Opportunities:	**Threats:**
▪ Monitoring ▪ Έλεγχος Πρόσβασης	▪ Επιθέσεις με πιθανό πολιτικό κίνητρο ▪ Η συλλογή & Διαχείριση προσωπικών δεδομένων του Δημόσιου Οργανισμούς μπορεί να θεωρηθεί από τους τελικούς χρήστες ή τους πολίτες ως καθεστώς επιτήρησης. ▪ Ο αναποτελεσματικός σχεδιασμός του Νέφους και των Υπηρεσιών που φιλοξενούνται ▪ Η υψηλή μεταβλητότητα των αξιοποιούμενων πόρων μπορεί να οδηγήσει στη σταδιακή μετάβαση σε Δημόσιο Νέφος

Νέφος Κοινότητας στη Δημόσια Διοίκηση – SWOT Ανάλυση

Strengths:	**Weaknesses:**
▪ Οι κοινές απαιτήσεις, περιορισμοί και προφίλ κινδύνου των Δημόσιων οργανισμών μειώνουν αποτελεσματικά το κόστος ▪ Η διαμόρφωση των μηχανισμών και των εργαλείων για την προστασία των εφαρμογών απλοποιείται λόγω του κοινού προφίλ κινδύνου των Δημόσιων οργανισμών ▪ Οι Δημόσιοι οργανισμοί έχουν μεγαλύτερη διαπραγματευτική ισχύ έναντι του Παρόχου εφόσον λειτουργούν ομαδικά ▪ Καλύτερη ανταπόκριση κατά τις περιόδους υψηλής ζήτησης πόρων σε σχέση με ένα Ιδιωτικό Νέφος	▪ Μεγαλύτερος ανταγωνισμός των πόρων μεταξύ των εταίρων οργανισμών λόγο κοινών στόχων ▪ Το Νέφος Κοινότητας αποτελεί πιο ελκυστικό στόχο για πιθανές επιθέσεις σε σχέση με ένα Ιδιωτικό Νέφος ▪ Ο έλεγχος πρόσβασης και η αυθεντικοποίηση των χρηστών είναι πιο αδύναμοι σε σχέση με ένα Ιδιωτικό νέφος λόγω του μεγαλύτερου αριθμού των χρηστών ▪ Η ποιότητα της Διαδικτυακής σύνδεσης επηρεάζει την απόδοση των Παρεχόμενων υπηρεσιών.
Opportunities:	**Threats:**
▪ Οι κοινές απαιτήσεις ασφαλείας των έτερων οργανισμών μπορεί να βελτιώσει τις πολιτικές και τα πρότυπα ασφάλειας ▪ Κοινά συστήματα διαχείρισης ▪ Η ύπαρξη κοινών συστημάτων διαχείρισης συμβάντων μπορεί να απλοποιήσει την υιοθέτηση μηχανισμών για την αποθήκευση και διαχείριση αποδείξεων για ηλεκτρονικά εγκλήματα ▪ Ισχυρότερη ασφάλεια δεδομένου ότι οι πολιτικές ασφαλείας εφαρμόζονται αποκλειστικά για τους οργανισμούς εντός του Νέφους Κοινότητας	▪ Η έλλειψη συμφωνίας μεταξύ των Οργανισμών που εξυπηρετούνται από την ίδια υποδομή Νέφους, για τους κανόνες ασφαλείας που θα πρέπει να εφαρμοστούν ▪ Τα μέλη του Νέφους κοινότητας μπορεί να αυξηθούν, γεγονός που θα μειώσει τα πλεονεκτήματα που σχετίζονται με την ευελιξία των υπηρεσιών ▪ Δυσκολότερη πρόβλεψη των απαιτούμενων πόρων σε σχέση με το Ιδιωτικό Νέφος ▪ Μία αποτυχία απομόνωσης των χρηστών μπορεί να οδηγήσει σε σημαντική διαρροή πληροφοριών, γεγονός που είναι δύσκολο να διαγνωστεί λόγω του μεγάλου αριθμού των χρηστών

Όπως προκύπτει από τη SWOT ανάλυση των μοντέλων Νέφους, τα βασικά πλεονεκτήματα και οι ευκαιρίες του Δημόσιου Νέφους αφορούν την υψηλή διαθεσιμότητα των πόρων, την αξιοπιστία των συστημάτων και την αυστηρή πολιτική ασφάλειας που υιοθετούν. Από την άλλη πλευρά, το Ιδιωτικό Νέφος μπορεί να

προσφέρει στους Δημόσιους οργανισμούς ισχυρότερες υπηρεσίες ελέγχου (πρόσβασης, καταγραφής συμβάντων, αυθεντικοποίησης χρηστών κτλ). Αναφορικά με τις αδυναμίες και τους κινδύνους του κάθε Νέφους, στην περίπτωση του Δημόσιου Νέφους σχετίζονται με την απώλεια του ελέγχου των Δεδομένων, το μεγάλο αριθμό των χρηστών του Νέφους αλλά και τη μειωμένη διαπραγματευτική ισχύ του πελάτη-Οργανισμού κατά τη σύναψη συμβολαίου με τον Πάροχο. Στην περίπτωση Ιδιωτικού Νέφους, οι αδυναμίες σχετίζονται κυρίως με την πιθανή έλλειψη πόρων και ευελιξίας των συστημάτων. Αναφορικά με το Community Cloud, τα πλεονεκτήματα αναφέρονται κατά κύριο λόγο στη σημαντική μείωση του κόστους λόγο κοινών απαιτήσεων και πολιτικών μεταξύ των οργανισμών της κοινότητας, ενώ οι αδυναμίες επικεντρώνονται στον μεγάλο αριθμό χρηστών και στη μεγαλύτερη και μη προβλέψιμη κάποιες φορές ζήτηση πόρων.

5.2.2 Επιλογή του μοντέλου Υπηρεσιών

Όπως προαναφέρθηκε, ο κάθε Δημόσιος οργανισμός, στα πλαίσια της στρατηγικής που έχει αναπτύξει, υποχρεούται να διαχωρίσει τις υπηρεσίες που θα μεταβούν στο Νέφος από εκείνες που θα συνεχίζουν να παρέχονται μέσω των παραδοσιακών in-house τεχνολογιών IT. Ανάλογα με τις υπηρεσίες που πρόκειται να μεταβούν στο Νέφος, οι υπεύθυνοι του έργου οφείλουν να επιλέξουν το κατάλληλο μοντέλο παροχής υπηρεσιών, προκειμένου να διασφαλιστεί η αποδοτικότητα και η αξιοπιστία των υπηρεσιών. Σε αυτή την ενότητα ακολουθεί μία συνοπτική περιγραφή των μοντέλων παροχής Υπηρεσιών Νέφους και μερικές πιθανές εφαρμογές ανά περίπτωση [69].

- **Software as a Service (SaaS):** Η επιλογή του μοντέλου SaaS από ένα Δημόσιο οργανισμό συνδέεται με τη μείωση του κόστους που σχετίζεται κυρίως με την αγορά λογισμικού. Το μοντέλο αυτό επιτρέπει την άμεση πρόσβαση σε ένα τεράστιο πλήθος εξειδικευμένων και μη εφαρμογών, χωρίς να απαιτείται η αγορά των πλήρη δικαιωμάτων, ενώ παράλληλα παρέχεται η δυνατότητα αξιοποίησης των προηγμένων χαρακτηριστικών των εφαρμογών χωρίς επιπρόσθετη δαπάνη. Ταυτόχρονα, ο οργανισμός μπορεί να επωφεληθεί από την αξιοποίηση της τεχνογνωσίας και του προσωπικού του Παρόχου, χωρίς να απαιτείται η πρόσληψη επιπλέον εξειδικευμένου προσωπικού για θέματα τεχνικής υποστήριξης, αντιμετώπισης περιστατικών ασφαλείας και ανάκαμψης.

Παραδείγματα εφαρμογής του SaaS στη Δημόσια Διοίκηση: e-mail, εφαρμογές αυτοματισμού γραφείου, εφαρμογές ηλεκτρονικών πληρωμών, έργα ηλεκτρονικής Διακυβέρνησης κτλ

- **Platform as a Service (PaaS):** Το μοντέλο αυτό μπορεί να χρησιμοποιηθεί από ένα Δημόσιο οργανισμό για την αξιοποίηση περιβάλλοντος ανάπτυξης εφαρμογών, ενισχύοντας τη διαλειτουργικότητα μεταξύ των διαφορετικών και απομακρυσμένων ομάδων ανάπτυξης. Ο Πάροχος μπορεί να παρέχει όλα τα απαραίτητα εργαλεία στους προγραμματιστές για ανάπτυξη κάθε είδους

εφαρμογών σε κάθε πιθανό προγραμματιστικό περιβάλλον. Ο Οργανισμός μεταξύ άλλων επωφελείται και από τις διαθέσιμες εφαρμογές ελέγχου σε real-time συνθήκες αλλά και από τη χρέωση με βάση τη χρήση και όχι την εξολοκλήρου αγορά των εργαλείων.

Παραδείγματα εφαρμογής του PaaS στη Δημόσια Διοίκηση: Απαίτηση για κοινή χρήση εφαρμογών μεταξύ διαφορετικών χρηστών του ίδιου ή διαφορετικού οργανισμού, ανάπτυξη εφαρμογών από διαφορετικές ομάδες εργασίας, μετάβαση των υπάρχοντων εφαρμογών στο Νέφος, συγκέντρωση και ανάρτηση Δεδομένων από διαφορετικές πηγές για λόγους διαφάνειας.

- **Infrastructure as a Service (IaaS):** Το μοντέλο αυτό μπορεί να παρέχει στους Δημόσιους οργανισμούς data centers έτοιμα προς χρήση, έτσι ώστε να καλύψει πλήρως την ανάγκη τους για πόρους σε περιόδους αυξημένης ζήτησης. Ωστόσο, η συνολική διαχείριση των data centers παραμένει στον έλεγχο της κυβέρνησης ή του Δημόσιου οργανισμού, γεγονός που μπορεί να απαιτήσει την πρόσληψη νέου εξειδικευμένου προσωπικού από πλευράς Κυβέρνησης. Ωστόσο, το μεγαλύτερο όφελος που προκύπτει είναι η τεράστια μείωση του συνολικού κόστους αγοράς και συντήρησης hardware στη Δημόσια Διοίκηση. Έχει αποδειχτεί ότι το IaaS μοντέλο αποτελεί μία ιδιαίτερα ασφαλής λύση για παροχή υπηρεσιών στη Δημόσια Διοίκηση καθώς οι υπεύθυνοι IT μπορούν να αναπτύξουν και να εφαρμόσουν τη δική τους στρατηγική ασφάλειας.

Παραδείγματα εφαρμογής του PaaS στη Δημόσια Διοίκηση: Παροχή ηλεκτρονικών υπηρεσιών στους πολίτες, φιλοξενία web sites, δοκιμαστικός έλεγχος μεγάλης κλίμακας ευαίσθητων εφαρμογών και ασφαλής αποθήκευση μεγάλου όγκου Δεδομένων που χρήζουν ιδιαίτερης προστασίας από τυχόν επιθέσεις.

5.3 Service Level Agreement (SLA)

Παρά το γεγονός ότι η Νεφοϋπολογιστική μπορεί να προσφέρει σημαντικά οφέλη στη συνολική λειτουργία της Δημόσιας Διοίκησης, η μετάβαση στο Νέφος δε παύει να σημαίνει αναγκαστική παραχώρηση του ελέγχου των πόρων και των Δεδομένων σε μία Τρίτη οντότητα, στον Πάροχο. Η παραχώρηση τέτοιων δικαιωμάτων σημαίνει πλήθος ενδεχόμενων κινδύνων για τη λειτουργία και την αξιοπιστία του Δημόσιου οργανισμού που υιοθετεί τεχνολογίες Νέφους. Καθώς λοιπόν λαμβάνονται οι σχετικές αποφάσεις για τη στρατηγική μετάβασης στο Νέφος, οι υπεύθυνοι οφείλουν να διαπραγματευτούν και να καθορίσουν τους όρους που θα διέπουν τις σχέσεις με τον Πάροχο.

Σημαντικότερο εργαλείο για την αποφυγή ανάλογων κινδύνων αποτελεί η σύναψη του SLA (Service Level Agreement) συμβολαίου μεταξύ του Παρόχου και της Κυβέρνησης ή του Δημόσιου οργανισμού. Ουσιαστικά, το SLA αποτελεί ένα συμβόλαιο μεταξύ των δύο μερών, με το οποίο καθορίζονται με σαφήνεια και με μετρήσιμα μεγέθη, οι υπηρεσίες που οφείλει να παρέχει ο Πάροχος Νέφους (Cloud Provider). Το SLA αποτελεί ένα θεμέλιο εμπιστοσύνης του καταναλωτή προς τον Πάροχο και θα πρέπει κατ΄ ελάχιστον να ορίζει με σαφήνεια [80]:

- Τις υπηρεσίες που παρέχονται αλλά και τον τρόπο με τον οποίο πρόκειται να παρασχεθούν

- Τις διαδικασίες παρακολούθησης και μέτρησης της απόδοσης των παρεχόμενων υπηρεσιών. Ουσιαστικά κάθε υπηρεσία θα πρέπει να υπόκεινται σε μετρίσιμους ελέγχους και να πραγματοποιείται αναλυτική αναφορά των αποτελεσμάτων τους.

- Τις διαδικασίες διαχείρισης, ανάκαμψης και ελαχιστοποίησης των επιπτώσεων από πιθανά μη προγραμματισμένα περιστατικά

- Τις υποχρεώσεις και τις αρμοδιότητες τόσο του Παρόχου όσο και του καταναλωτή

- Μία σειρά από διαδικασίες ελέγχου και μετρίσιμα μεγέθη, έτσι ώστε να πιστοποιείται η παροχή των συμφωνηθέντων υπηρεσιών.

- Μία περιγραφή γα το πως μπορεί να διαμορφωθεί το SLA σε βάθος χρόνου

- Οι διαδικασίες με τις οποίες διασφαλίζεται η πολιτική ασφαλείας του οργανισμού για την πρόσβαση στα δεδομένα και τις εφαρμογές του.

Σε κάθε περίπτωση το SLA πρέπει να περιλαμβάνει ένα Service Level Objectives (SLO) στο οποίο περιλαμβάνονται τα μετρήσιμα χαρακτηριστικά του SLA (η ποιότητα των υπηρεσιών, η διαθεσιμότητα των πόρων, ο χρόνος απόκρισης κτλ). Τα μετρήσιμα αυτά μεγέθη είναι εκείνα που καθορίζουν την αναμενόμενη απόδοση του Παρόχου προς αποφυγή παρανοήσεων μεταξύ των δύο μερών. Συνεπώς, αποτελεί ευθύνη του κάθε Δημόσιου οργανισμού ή της Κυβέρνησης να εξετάζει ενδελεχώς και να διαπραγματεύεται τους όρους του SLA συμβολαίου, έτσι ώστε να διασφαλίζεται η επίτευξη των στόχων του. Να σημειωθεί ότι στην περίπτωση που κάποιος Οργανισμός επιλέξει τη σύναψη συμβολαίου με ένα μεταπωλητή (reseller) υπηρεσιών Νέφους και όχι απ΄ ευθείας με τον ίδιο τον Πάροχο, οι υπεύθυνοι για τη σύναψη της σύμβασης θα πρέπει να εξετάσουν τόσο την πολιτική του μεταπωλητή όσο και του πραγματικού Παρόχου.

Τα Service Level Agreements χωρίζονται σε δύο (2) κατηγορίες. Σε εκείνα που οι όροι τους είναι διαπραγματεύσιμοι μεταξύ των δύο μερών και σε εκείνα που είναι τυποποιημένα και μη διαπραγματεύσιμα. Να σημειωθεί ότι οι Πάροχοι Δημόσιου Νέφους (Public Cloud) προσφέρουν συνήθως τυποποιημένα, με μη διαπραγματεύσιμους όρους, SLA και συνεπώς δε συνίσταται η χρήση τους από οργανισμούς που διαχειρίζονται ευαίσθητα και κρίσιμα δεδομένα.

Σύμφωνα με τη δημοσίευση [78] του «Cloud Computing Use Cases Group», οι υπεύθυνοι για την ανάπτυξη του SLA θα πρέπει να εξετάσουν αν οι όροι του συμβολαίου καλύπτουν πλήρως τις απαιτήσεις και τους στόχους του οργανισμού, οι οποίοι θα πρέπει να έχουν προσδιοριστεί νωρίτερα. Πιο συγκεκριμένα, θα πρέπει να εξετάζονται οι παρακάτω απαιτήσεις για [78][79]:

1. Ασφάλεια: Ο Οργανισμός οφείλει να προσδιορίσει με σαφήνεια τις απαιτήσεις και την πολιτική ασφαλείας που πρόκειται να ακολουθήσει καθώς και τις διαδικασίες ελέγχου για τη διασφάλιση της απαιτήσεων του. Ο

Πάροχος από τη μεριά του οφείλει να παρέχει υπηρεσίες που διασφαλίζουν στις απαιτήσεις αυτές.

2. Κρυπτογράφηση Δεδομένων: Τα δεδομένα θα πρέπει να κρυπτογραφούνται τόσο κατά τη διάρκεια της μετάδοσης όσο και όταν αυτά δεν χρησιμοποιούνται. Οι αλγόριθμοι κρυπτογράφησης και η πολιτική ελέγχου πρόσβασης θα πρέπει να προσδιορίζονται ρητά μέσα στο SLA.

3. Ιδιωτικότητα: Οι βασικές αρχές της Ιδιωτικότητας θα πρέπει να διασφαλίζονται από τον προσδιορισμό συγκεκριμένων κανόνων όπως την κρυπτογράφηση, τη διατήρηση ή την οριστική διαγραφή των δεδομένων του Οργανισμού. Στο πλαίσιο αυτό ο Πάροχος θα πρέπει μέσα στο SLA να ορίζει ρητά τους τρόπους με τους οποίους επιτυγχάνει την απομόνωση των χρηστών σε ένα περιβάλλον πολλαπλών μισθώσεων (multi-tenant).

4. Διατήρηση δεδομένων ή διαγραφή: Ο Πάροχος θα πρέπει να είναι σε θέση να αποδεικνύει τη συμμόρφωσή του με τους νόμους και τις πολιτικές περί διατήρησης ή διαγραφής των δεδομένων του Οργανισμού.

5. Συμβατότητα: Ο Πάροχος θα πρέπει να είναι σε θέση να αποδείξει τη συμβατότητά του με τον τύπο των Δεδομένων που διαχειρίζεται ο Οργανισμός

6. Διαφάνεια: Οι Πάροχοι οφείλουν να ενημερώνουν άμεσα και χωρίς καμία καθυστέρηση τους υπεύθυνους του Οργανισμού για οποιαδήποτε παραβίαση των όρων του SLA. Τέτοια περίπτωση αποτελεί η διακοπή παροχής των προβλεπόμενων υπηρεσιών, η μειωμένη απόδοση του Παρόχου, ένα ενδεχόμενο περιστατικό ασφάλειας κτλ.

7. Πιστοποίηση: Ο Πάροχος θα πρέπει να κατέχει και να αποδεικνύει τις απαραίτητες πιστοποιήσεις.

8. Καθορισμός επιδόσεων: Οι εγγυημένες αποδόσεις του Παρόχου θα πρέπει να καθορίζονται ρητά στο SLA ενώ θα πρέπει να εξετάζεται εάν οι επιδόσεις αυτές καλύπτουν τις απαιτήσεις του Οργανισμού. Τα μετρήσιμα μεγέθη καθορίζονται στο SLA.

9. Monitoring: Οι υπεύθυνοι του οργανισμού θα πρέπει να εξετάζουν εάν στο SLA δίνεται η δυνατότητα παρακολούθησης και καταγραφής των επιδόσεων του Παρόχου (συνήθως πραγματοποιείται από Τρίτη Οντότητα)

10. Auditability: Για το λόγο ότι η αποκλειστική ευθύνη για την ασφάλεια των Δεδομένων ή τη διαθεσιμότητα των υπηρεσιών του Οργανισμού αποκλειστικά υπεύθυνος είναι ο Πάροχος, θα πρέπει να δίνεται η δυνατότητα στους υπεύθυνους του Οργανισμού να ελέγχουν τα συστήματα και τις διαδικασίες που ακολουθεί ο Πάροχος για τη διασφάλιση των δεδομένων και των παρεχόμενων υπηρεσιών. Το πως και το πότε θα πραγματοποιούνται οι έλεγχοι αυτοί θα πρέπει να ορίζεται ρητά στο SLA.

11. Μετρήσεις: Οι μετρήσεις της απόδοσης του Παρόχου θα πρέπει να υφίστανται με τις διαδικασίες και στις περιόδους που έχουν οριστεί στο SLA. Οι

μετρήσεις αυτές συνήθως αφορούν:

- την ταχύτητα απόκρισης του συστήματος
- τη διαθεσιμότητα του συστήματος
- την εξισορρόπηση του φόρτου εργασίας
- την ανθεκτικότητα του συστήματος
- την ελαστικότητα των πόρων του συστήματος
- την απόδοση του συστήματος καθώς αυξάνεται η ζήτηση για πόρους
- την ευελιξία του Παρόχου στην ανακατανομή των πόρων

12. Φυσική επικοινωνία: Όπως προαναφέρθηκε, ένα από τα βασικά χαρακτηριστικά του Cloud Computing είναι η κατ΄ απαίτηση και η αυτόματη δέσμευση πόρων. Ωστόσο, στο SLA θα πρέπει να προβλέπεται και η εξυπηρέτηση με φυσική παρουσία, σε περίπτωση που αυτό χρειαστεί.

Συμπερασματικά, το SLA θα πρέπει να ορίζει με σαφήνεια την οποιαδήποτε λεπτομέρεια που καθορίζει τη σχέση του Δημόσιου Οργανισμού ή της Κυβέρνησης με τον Πάροχο προς αποφυγή παρανοήσεων μεταξύ των δύο εταίρων. Καθοριστικό ρόλο στην αποτελεσματική διατύπωση των όρων του SLA αποτελεί ο εκ των προτέρων προσδιορισμός των αναγκών του Οργανισμού και η πολιτική ασφαλείας που επιθυμεί να ακολουθήσει. Να σημειωθεί ότι στη Δημόσια Διοίκηση, ένα SLA μπορεί να συναφθεί με τον Πάροχο είτε σε επίπεδο Κυβέρνησης είτε σε επίπεδο Οργανισμού.

5.4 Η Νεφοϋπολογιστική σε περιβάλλον Κρίσιμων Υποδομών (Critical Infrastructure)

Όπως έχει γίνει σαφές μέχρι τώρα, η Νεφοϋπολογιστική αποτελεί μία τεχνολογία η οποία μπορεί να εφαρμοστεί τόσο σε Ιδιωτικές επιχειρήσεις κάθε μεγέθους όσο και στη Δημόσια Διοίκηση. Ωστόσο, πολλοί είναι οι ερευνητές εκείνοι οι οποίοι εγείρουν σοβαρά ζητήματα ασφάλειας για την εφαρμογή των τεχνολογιών Νέφους σε περιβάλλοντα Κρίσιμων Υποδομών ενός Κράτους. Όπως σημειώνουν, η υιοθέτηση τεχνολογιών Νέφους σε περιβάλλοντα Κρίσιμων Υποδομών σημαίνει ότι η ανθεκτικότητα και η ασφάλεια των συστημάτων αυτών αποτελεί επιτακτική ανάγκη, με σκοπό την ελαχιστοποίηση των ανεπιθύμητων συμβάντων.

Πιο συγκεκριμένα, με τον όρο Κρίσιμες Υποδομές (Critical Infrastructures) εννοούνται «*όλες εκείνες οι υποδομές που σε περίπτωση υποβάθμισης ή διακοπή της λειτουργίας τους θα ανακύψουν σημαντικά προβλήματα στην εύρυθμη λειτουργία της Δημόσιας Διοίκησης και την παροχή βασικών υπηρεσιών στο κοινωνικό σύνολο*» [83]. Παραδείγματα τέτοιων υπηρεσιών αποτελούν η ηλεκτροδότηση, η υδροδότηση, οι μεταφορές, ο τραπεζικός τομέας, τα σώματα ασφαλείας και οι υγειονομικές υπηρεσίες. Η ασφάλεια των Υποδομών αυτών δεν αφορά μόνο την προστασία τους από επιθέσεις που στοχεύουν την αξιοπιστία και τη διαθεσιμότητά τους αλλά και από προστασία των πολιτών από επιθέσεις που μπορεί να επιφέρουν τη δημοσιοποίηση των προσωπικών και ευαίσθητων δεδομένων τους σε τρίτους [83]. Συνεπώς, η μετάβαση ενός Οργανισμού στο Νέφος προϋποθέτει τον εκ των προτέρων προσδιορισμό των Κρίσιμων Υποδομών του καθώς και τη μεταξύ τους αλληλεξάρτηση, προκειμένου να εκτιμηθεί το υπάρχον επίπεδο προστασίας τους αλλά και να αποφασιστεί η δυνατότητα υιοθέτησης τεχνολογιών Νέφους στους Τομείς αυτούς.

Στο πλαίσιο αυτό και υπό τη ραγδαία υιοθέτηση των τεχνολογιών Νέφους στη Δημόσια Διοίκηση σε παγκόσμιο επίπεδο, ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια των Δικτύων και των Πληροφοριών (European Network and Information Security Agency(ENISA)) δημοσίευσε το 2012, μεταξύ άλλων, μία μελέτη με τίτλο «Critical Cloud Computing: A CIIP perspective on Cloud Computing Services» [84]. Η μελέτη αυτή έχει σκοπό την παροχή οδηγιών για την προστασία των Πληροφοριών σε Κρίσιμες Υποδομές (Critical Information Infrastructure Protection (CIIP)) που αξιοποιούν τεχνολογίες Νέφους.

Σύμφωνα με τη μελέτη αυτή [84], το 80% των Δημόσιων και Ιδιωτικών Οργανισμών αναμένεται να λειτουργούν σύντομα εξαρτώμενοι από κάποια μορφή Νέφους. Αυτό αναπόφευκτα συνεπάγεται με τη συγκέντρωση των IT πόρων σε μεγάλα Κέντρα Δεδομένων. Το γεγονός αυτό, μπορεί να θεωρηθεί ως μέτρο για την ενίσχυση της Ασφάλειας των Ζωτικών Πληροφοριών μίας Κρίσιμης Υποδομής, καθώς ο Πάροχος μπορεί να εφαρμόσει και να ενισχύσει την πολιτική ασφαλείας του Οργανισμού αλλά και να εξασφαλίσει την αποδοτικότητα και τη διαθεσιμότητα των Υπηρεσιών του με μικρότερο κόστος. Από την άλλη πλευρά, σε περίπτωση παραβίασης της Ασφάλειας του Οργανισμού, οι συνέπειες μπορεί να αποβούν καταστροφικές, ως αποτέλεσμα της συγκέντρωσης των πόρων, εφόσον θα επηρεάσουν μεγάλο πλήθος χρηστών ή Οργανισμών. Συνεπώς, οι Υπηρεσίες της Νεφοϋπολογιστικής μπορούν να θεωρηθούν

από μόνες τους ως Κρίσιμες καθώς μπορούν να επηρεάσουν καθοριστικά τη λειτουργία πλήθους άλλων Κρίσιμων Υποδομών.

Όπως αναφέρθηκε και προηγουμένως, μια ενδεχόμενη διακοπή των Υπηρεσιών στις Κρίσιμες Υποδομές μπορεί να επιφέρει πλήθος σοβαρών επιπτώσεων (ακόμη και ζωτικών) τόσο στη συνολική λειτουργία της Δημόσιας Διοίκησης όσο και στους πολίτες ενός Κράτους. Η μελέτη του ENISA, βασιζόμενη στη μελέτη παλαιότερων ανεπιθύμητων περιστατικών ασφάλειας, καταγράφει τους βασικούς Κινδύνους οι οποίοι μπορούν να επηρεάσουν τη λειτουργία μίας Κρίσιμης Υποδομής ενώ παράλληλα εξετάζει τη χρησιμότητα της Νεφοϋπολογιστικής σε ανεπιθύμητα περιστατικά ασφαλείας. Πιο συγκεκριμένα:

1. **Φυσικές Καταστροφές ή διακοπή της ηλεκτροδότησης:** Όπως είναι φυσικό, η άμεση αντιμετώπιση των συνεπειών από μία τοπική φυσική καταστροφή (σεισμός, πλημμύρα, φωτιά κτλ) ή από μία ξαφνική διακοπή της ηλεκτροδότησης σε μία Κρίσιμη Υποδομή θεωρείται αδύνατη με την ύπαρξη ενός μόνο παραδοσιακού IT Κέντρου Δεδομένων. Ωστόσο, μία υποδομή Νέφους μπορεί να διασφαλίσει τη συνέχεια της λειτουργίας των Υποδομών αυτών, εξαιτίας του μεγάλου πλήθους και μεγέθους των Κέντρων Δεδομένων που διαθέτει. Η ανθεκτικότητα της Νεφοϋπολογιστικής σε τέτοιες περιπτώσεις βασίζεται στο γεγονός οτι τα Κέντρα Δεδομένων που διαχειρίζεται ο Πάροχος βρίσκονται τοποθετημένα σε διάσπαρτα γεωγραφικά σημεία, με αποτέλεσμα οι Υπηρεσίες να συνεχίζουν να παρέχονται από διαφορετικό γεωγραφικό σημείο, κάθε φορά που αυτό απαιτείται.

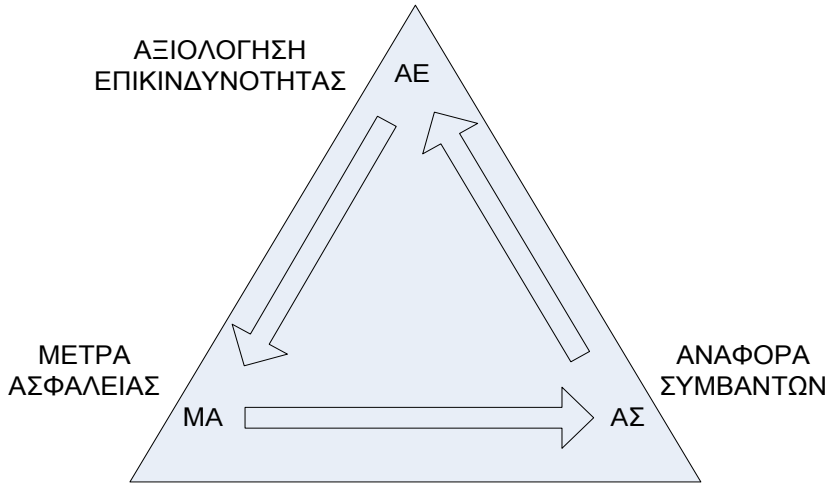
2. **Εξάντληση των IT πόρων (λόγω υπερφόρτωσης ή DDoS επιθέσεων):** Είναι γνωστό ότι η διασφάλιση της λειτουργίας μίας Υποδομής εξαρτάται από τη διαθεσιμότητα των IT πόρων κάθε στιγμή που αυτοί απαιτούνται. Οι παραδοσιακές μορφές IT μπορούν να παρέχουν συγκεκριμένους πόρους, οι οποίοι πιθανόν να μην είναι σε πολλές περιπτώσεις αρκετοί για να εξυπηρετήσουν τις ανάγκες μίας Κρίσιμης Υποδομής. Για παράδειγμα, κάποιες Υποδομές πιθανόν να απαιτούν αυξημένους πόρους σε συγκεκριμένες χρονικές περιόδους (περίοδοι υψηλής ζήτησης) ενώ σε κάποιες άλλες όχι. Ενώ οι παραδοσιακές μορφές IT μπορούν, κυρίως λόγω υψηλού κόστους, να διαχειρίζονται συγκεκριμένους πόρους, μία Υποδομή Νέφους έχει τη δυνατότητα να προσφέρει κάθε φορά τους πόρους εκείνους που απαιτεί η Κρίσιμη Υποδομή για τα διασφαλίσει τη λειτουργία της, αποφεύγοντας περιπτώσεις υπερφόρτωσης και εξάντλησης των πόρων του συστήματος. Αξίζει να σημειωθεί, ότι μία υποδομή Νέφους μπορεί να μετριάσει τις συνέπειες από μία ενδεχόμενη υπερφόρτωση του συστήματος όχι μόνο εξαιτίας της αυξημένης ζήτησης σε περιόδους αιχμής αλλά και σε περιπτώσεις DDoS επιθέσεων, όπου προκαλείται εσκεμμένα από τον επιτιθέμενο υπερφόρτωση του συστήματος.

3. **Διαδικτυακές επιθέσεις:** Είναι γεγονός ότι οι διαδικτυακές επιθέσεις που εκμεταλλεύονται αδυναμίες του χρησιμοποιούμενου Λογισμικού μπορούν να προκαλέσουν μεγάλες παραβιάσεις στα Δεδομένα των χρηστών. Να σημειωθεί ότι στις Κρίσιμες Υποδομές συχνά διατηρούνται προσωπικά Δεδομένα, ακόμη και ευαίσθητα, εκατομμυρίων χρηστών. Η χρήση τεχνολογιών Νέφους για τη φύλαξη μεγάλου όγκου Δεδομένων μπορεί να

εξασφαλίζει την εφαρμογή αποτελεσματικών μέτρων και πολιτικών Ασφαλείας, ωστόσο, μία ενδεχόμενη επίθεση μπορεί να πολλαπλασιάσει τις επιπτώσεις εξαιτίας τη συγκέντρωσης των Δεδομένων εκατομμυρίων χρηστών στα μεγάλα Κέντρα Δεδομένων.

4. **IaaS και PaaS Υπηρεσίες Νέφους:** Μία υποδομή Νέφους μπορεί να παρέχει IaaS και PaaS υπηρεσίες σε άλλους IT προμηθευτές, οι οποίοι με τη σειρά τους προσφέρουν Υπηρεσίες σε Κρίσιμες Υποδομές. Συνεπώς, μία ενδεχόμενη αδυναμία παροχής των IaaS ή PaaS υπηρεσιών από την υποδομή Νέφους μπορεί να επηρεάσει τη συνολική λειτουργία της Κρίσιμης Υποδομής που έμμεσα εξυπηρετεί.

Σύμφωνα με τα προαναφερόμενα, δεν είναι δύσκολο να αντιληφθεί κανείς ότι μία υποδομή Νέφους αποτελεί από μόνη της μία Κρίσιμη Υποδομή, καθώς μπορεί να επηρεάσει άμεσα ή έμμεσα τη λειτουργία και τις υπηρεσίες άλλων Οργανισμών ή Κρίσιμων Υποδομών. Σε πολλές περιπτώσεις, η Νεφοϋπολογιστική μπορεί να διασφαλίσει τη λειτουργία και τη συνέχεια μίας κρίσιμης Υποδομής, ωστόσο σε κάποιες περιπτώσεις η συγκέντρωση των πόρων μπορεί να επιφέρει δυσμενής συνέπειες. Μέσα στο πλαίσιο αυτό, η μελέτη παρέχει μία σειρά συστάσεων προς τους υπεύθυνους για τον καθορισμό της στρατηγικής μετάβασης των Κρίσιμων Υποδομών ενός Κράτους σε τεχνολογίες Νέφους. Η στρατηγική αυτή που προτείνεται περιλαμβάνει τρία στάδια και απεικονίζεται ακολούθως:



Διαδικασία Διαχείριση της Ασφάλειας Κρίσιμων Υποδομών
Πηγή: ENISA: «Critical Cloud Computing: A CIIP Perspective on Cloud Computing services» [84]

1. **Αξιολόγηση της Επικινδυνότητας (Risk Assessment):** Η Αξιολόγηση της επικινδυνότητας αποτελεί τη βάση για τη ασφαλή μετάβαση μίας Κρίσιμης Υποδομής στο Νέφος. Περιλαμβάνει τον προσδιορισμό των Κρίσιμων υπηρεσιών Νέφους σε μία Υποδομή, την αξιολόγηση της εξάρτησης των

υπηρεσιών Νέφους από άλλους παράγοντες (όπως το δίκτυο επικοινωνιών ή ηλεκτροδότησης) αλλά και τη δημιουργία μίας σαφής εικόνας για την αλληλεξάρτηση των Κρίσιμων Υπηρεσιών με τις Υπηρεσίες Νέφους.

2. **Μέτρα Ασφάλειας (Security Measures):** Στο στάδιο αυτό, οι υπεύθυνοι για τη στρατηγική μετάβασης στο Νέφος θα πρέπει να επιλέξουν τα κατάλληλα μέτρα Ασφάλειας, έτσι ώστε να ελαχιστοποιηθούν οι πιθανότητες για ανεπιθύμητα συμβάντα. Εδώ περιλαμβάνονται η διαρκή βελτίωση των πρακτικών Ασφάλειας που θα επιλέξουν οι υπεύθυνοι, η αποφυγή διατήρησης του Λογισμικού σε περιττά Κέντρα Δεδομένων, η αποφυγή του «one point of failure» μέσω της τυποποίησης του software που χρησιμοποιείται έτσι ώστε να επιτρέπεται η φορητότητα του Λογισμικού σε άλλο Πάροχο και η πραγματοποίηση τακτικών ελέγχων για την πιστοποίηση τήρησης της διαδικασίας Ασφάλειας από την πλευρά του Παρόχου.

3. **Αναφορά συμβάντων (Incident Reporting):** Η αναφορά των συμβάντων συμβάλει στον έλεγχο της αποτελεσματικότητας των μέτρων Ασφάλειας που έχουν εφαρμοστεί. Τα αποτελέσματα των ελέγχων αυτών αποτελούν την είσοδο για τη βελτίωση της Αξιολόγηση της Επικινδυνότητας (Στάδιο $1^{ο}$). Να σημειωθεί ότι η Αναφορά ανεπιθύμητων συμβάντων θα πρέπει να έχει υποχρεωτικό χαρακτήρα από την πλευρά του Παρόχου και να καθορίζεται ρητά στο Service Level Agreement (SLA).

Κεφάλαιο 6ο

Συμπεράσματα

Σύμφωνα με τα προαναφερόμενα, δεν είναι δύσκολο να αντιληφθεί κανείς ότι η Νεφοϋπολογιστική βρίσκεται σήμερα σε μία φάση ραγδαίας ανάπτυξης σε παγκόσμιο επίπεδο. Κατά καιρούς, πολλοί μεγάλοι Οργανισμοί και πλήθος ερευνητών έχουν ασχοληθεί με τη μελέτη της τεχνολογίας της Νεφοϋπολογιστικής, ενώ παράλληλα επιδιώκουν τη διεύρυνση του πεδίου εφαρμογής της. Η ταχύτατη εξέλιξή της οφείλεται στα χαρακτηριστικά της εκείνα από τα οποία προκύπτει ένα πλήθος σημαντικών ωφελημάτων στα πεδία όπου εφαρμόζεται. Τα χαρακτηριστικά αυτά αναφέρονται στην κατ΄ απαίτηση δέσμευση των πόρων, στη δυνατότητα διαμοιρασμού των πόρων του συστήματος μεταξύ πολλών χρηστών αλλά και στην ταχεία δέσμευση και αποδέσμευσή τους χωρίς να γίνεται αντιληπτό από τους χρήστες. Σήμερα, η Νεφοϋπολογιστική διακρίνεται σε τέσσερα (4) μοντέλα Νέφους (Public, Private, Community, Hybrid) ενώ οι προσφερόμενες υπηρεσίες διακρίνονται σε τρείς (3) βασικές κατηγορίες (SaaS, PaaS και IaaS). Το κάθε μοντέλο Νέφους ή Υπηρεσίας μπορεί να χρησιμοποιηθεί ξεχωριστά ή συνδυαστικά προκειμένου να εξυπηρετήσει τους σκοπούς του Οργανισμού ή του προσώπου που επιθυμεί τη μετάβαση σε τεχνολογίες Νέφους.

Τα προηγμένα αυτά χαρακτηριστικά αλλά και η δυναμική εισχώρηση της Νεφοϋπολογιστικής τόσο στο Δημόσιο όσο και στον Ιδιωτικό Τομέα διαμορφώνουν σήμερα σημαντικά πλεονεκτήματα έναντι των παραδοσιακών μορφών IT. Τα πιο χαρακτηριστικά από αυτά είναι η μείωση του κόστους για την αγορά και συντήρηση εξοπλισμού (hardware, software), η εύκολη πρόσβαση σε Δεδομένα και εφαρμογές ανά πάσα στιγμή και από οποιοδήποτε υπολογιστή, η ενίσχυση της Ασφάλειας των πληροφοριών και των συστημάτων με την εφαρμογή αυστηρότερων πολιτικών Ασφάλειας, η προώθηση της συνεργασίας μεταξύ διαφορετικών ομάδων εργασίας ή Οργανισμών καθώς και η πρόσβαση σε Υποδομές με μεγάλη υπολογιστική ισχύ και υψηλές επιδόσεις. Από την άλλη πλευρά, θα πρέπει να αναφερθεί ότι όπως κανένα υπολογιστικό σύστημα δε μπορεί να θεωρηθεί απολύτως ασφαλές έτσι και η μεταφορά των Δεδομένων ή των Υπηρεσιών σε περιβάλλον Νέφους εγείρει, σε

πολλές περιπτώσεις, σημαντικά ζητήματα Ασφάλειας και Ιδιωτικότητας των πληροφοριών.

Στο Κεφάλαιο 2 επικεντρωθήκαμε στην εφαρμογή της Νεφοϋπολογιστικής στη Δημόσια Διοίκηση, αναλύοντας συγχρόνως την έννοια της Ηλεκτρονικής Διακυβέρνησης και τη δυνατότητα διεύρυνσης του πεδίου εφαρμογής της υιοθετώντας τεχνολογίες Νέφους. Τα αποτελέσματα που προκύπτουν από τη διεθνή εμπειρία σχετικά με την παροχή e-Government υπηρεσιών σε περιβάλλον Νέφους είναι ιδιαίτερα ενθαρρυντικά, γεγονός που ωθεί τις Κυβερνήσεις στη διαρκή ανάληψη νέων πρωτοβουλιών στο πεδίο αυτό. Ωστόσο, μία σειρά από ζητήματα Ασφάλειας και Ιδιωτικότητας που εγείρουν πολλοί ερευνητές, έχουν αποτρέψει τις Κυβερνήσεις πολλών Κρατών παγκοσμίως να σχεδιάσουν μια γενικευμένη πολιτική για την καθολική μετάβαση των Δημόσιων Υπηρεσιών τους στο Νέφος. Συνεπώς, επιβάλλεται ο εκ των προτέρων εντοπισμός και καταγραφή των Κινδύνων, που ενδέχεται να προκύψουν βραχυπρόθεσμα και μακροπρόθεσμα, ώστε να ληφθούν τα κατάλληλα μέτρα προστασίας και αντιμετώπισης. Οι Κίνδυνοι αυτοί αφορούν είτε τεχνικά ζητήματα (αδυναμία απομόνωσης των χρηστών, εξάντληση των διαθέσιμων πόρων, κακόβουλες επιθέσεις εναντίον του Παρόχου) είτε Νομικά ζητήματα (π.χ. μεταφορά των Δεδομένων σε κράτη με διαφορετική Νομοθεσία) ή ακόμη και ζητήματα με επιπτώσεις στη λειτουργία των Δημόσιων Οργανισμών (π.χ. αδυναμία μεταφοράς των Δεδομένων σε άλλο Πάροχο, απώλεια ελέγχου των Δεδομένων, μη συμμόρφωση του Παρόχου με τις προκαθορισμένες απαιτήσεις κτλ). Σήμερα, πολλά από αυτά τα ζητήματα έχουν παρακαμφθεί, με αποτέλεσμα η Νεφοϋπολογιστική να κατακτά την εμπιστοσύνη πολλών Κυβερνήσεων. Ωστόσο, κάποια από αυτά είναι ακόμη υπαρκτά και συνεπώς απαιτείται η προσεκτική αξιολόγησή τους προτού αποφασιστεί η μετάβαση μίας Υπηρεσίας στο Νέφος.

Αξίζει να σημειωθεί ότι η ταχεία εξάπλωση της Νεφοϋπολογιστικής δημιούργησε την ανάγκη για τη θέσπιση ενός Νομικού Πλαισίου με το οποίο καθορίζεται το πλαίσιο λειτουργίας των Παρόχων, τα δικαιώματα των χρηστών και πλήθος άλλων ζητημάτων. Σε γενικές γραμμές, τα κράτη-μέλη της Ευρωπαϊκής Ένωσης (έπειτα των σχετικών οδηγιών που εξέδωσε η Ευρωπαϊκή επιτροπή) τηρούν ένα ιδιαίτερα αυστηρό Νομικό Πλαίσιο για την προστασία των προσωπικών και των ευαίσθητων Δεδομένων, σε κάθε περίπτωση που αυτά υφίστανται επεξεργασία. Από την άλλη πλευρά, οι Ηνωμένες Πολιτείες της Αμερικής, παρά το γεγονός ότι θεωρούνται πρωτοπόροι στην υιοθέτηση τεχνολογιών Νέφους στη Δημόσια Διοίκηση, δεν διαθέτουν ένα πλήρες Νομικό Πλαίσιο για την προστασία των Δεδομένων στις Υποδομές Νέφους. Απεναντίας, διαθέτουν πλήθος ισχυρών Νόμων οι οποίοι επιβάλλουν στους Παρόχους της επικράτειας την αποκάλυψη των Πληροφοριών που τηρούν στις Υποδομές τους, χωρίς την προηγούμενη συγκατάθεση του κατόχου των Δεδομένων ή την εισαγγελική παρέμβαση. Στο κεφάλαιο 3 περιγράφηκε το Νομικό Πλαίσιο που τηρείται στις Η.Π.Α. και στην Ευρώπη καθώς και οι αρχές του «Ασφαλούς Λιμένα» που καθορίζει του όρους λειτουργίας των Αμερικανικών επιχειρήσεων στην Ευρωπαϊκή Ένωση, αναφορικά με την προστασίας της Ιδιωτικότητας των πληροφοριών που αυτές διαχειρίζονται.

Σύμφωνα με τα προαναφερόμενα, ο περιορισμός των Κινδύνων που περιγράφησαν στο 2^{ο} Κεφάλαιο, η θέσπιση συγκεκριμένου Νομικού πλαισίου αλλά και η αναγνώριση των ωφελημάτων που προκύπτουν από τη χρήση των υποδομών Νέφους συνετέλεσαν στο γεγονός ότι πολλές Κυβερνήσεις παγκοσμίως ανέκτησαν την

εμπιστοσύνη τους έναντι των τεχνολογιών Νέφους. Στο πλαίσιο αυτό, τα τελευταία χρόνια παρατηρείται μία συστηματική προσπάθεια για την υιοθέτηση τεχνολογιών Νέφους στη Δημόσια Διοίκηση από πολλά Κράτη. Οι Ηνωμένες Πολιτείες της Αμερικής θεωρούνται πρωτοπόροι στη μετάβαση της Δημόσιας Διοίκησης σε υποδομές Νέφους, ενώ ακολουθούν με ταχύτατους ρυθμούς τα προηγμένα κράτη της Ευρωπαϊκής Ένωσης. Στο σημείο αυτό, η Ελλάδα φαίνεται να υστερεί, ωστόσο, τα τελευταία χρόνια έχουν γίνει αρκετά βήματα προς αυτήν την κατεύθυνση, αφού οι Κυβερνήσεις αντιλήφθηκαν ότι η Νεφοϋπολογιστική μπορεί να γίνει σπουδαίος ουραγός στη Διοικητική μεταρρύθμιση που προωθείται. Στο Κεφάλαιο 4 μελετήθηκαν κάποιες από αυτές τις περιπτώσεις που έχουν ήδη υλοποιηθεί και εφαρμοστεί παγκοσμίως.

Ωστόσο, η μετάβαση των Δημόσιων Υπηρεσιών στο Νέφος απαιτεί τον καθορισμό μίας καλά σχεδιασμένης στρατηγικής προς αυτή την κατεύθυνση. Στο πλαίσιο αυτό, οι υπεύθυνοι σχεδιασμού της στρατηγικής οφείλουν να λάβουν σημαντικές αποφάσεις, έτσι ώστε να διασφαλίσουν την απρόσκοπτη λειτουργία και συνέχεια των Δημόσιων οργανισμών. Ιδιαίτερη βαρύτητα θα πρέπει να δοθεί τόσο στην επιλογή των υπηρεσιών που θα μεταβούν στο Νέφος όσο και στην επιλογή του μοντέλου Νέφους που θα εξυπηρετήσει καλύτερα τους σκοπούς του οργανισμού. Να σημειωθεί ότι ο σχεδιασμός μίας σωστής στρατηγικής προϋποθέτει τον εντοπισμό των ιδιαίτερων χαρακτηριστικών και απαιτήσεων της Δημόσιας Διοίκησης όπου πρόκειται να εφαρμοστεί. Εκτός όμως από τη χάραξη μία συνολικής στρατηγικής μετάβασης, θεωρείται εξίσου σημαντικός ο προσδιορισμός των όρων που θα διέπουν τις σχέσεις της Κυβέρνησης με τον Πάροχο υπηρεσιών Νέφους. Οι όροι αυτοί θα πρέπει να καθορίζονται με κάθε λεπτομέρεια στο Service Level Agreement (SLA συμβόλαιο) το οποίο αποτελεί ένα θεμέλιο εμπιστοσύνης μεταξύ των δύο μερών.

Συμπερασματικά, διαπιστώνουμε ότι οι δυνατότητες της Νεφοϋπολογιστικής στη Δημόσια Διοίκηση είναι πραγματικά ανεξάντλητες. Αυτό το επιβεβαιώνει η διεθνής εμπειρία, η οποία υπόσχεται την υλοποίηση ιδιαίτερα πρωτοποριακών λύσεων και εφαρμογών σε βάθος χρόνου. Συνεπώς, η νέα αυτή τεχνολογία αναμένεται να μας απασχολήσει για αρκετά χρόνια ακόμα καθώς το ενδιαφέρον των μελετητών, των ερευνητών, των Κυβερνήσεων και των επιχειρήσεων παγκοσμίως αυξάνεται με εντυπωσιακά ταχύτατους ρυθμούς.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[01] NIST – National Institute of Standards and Technology http://www.nist.gov/itl/cloud/index.cfm

[02] Academia.edu: «Cloud Computing: Όταν τα δεδομένα "πετούν" στα σύννεφα» by Marina Markellou.

http://www.academia.edu/4882290/Cloud_Computing_

[03] Softone blog: «Cloud Computing: Πλεονεκτήματα για τις μικρές & μεσαίες επιχειρήσεις»

http://blog.softone.gr/archives/2011/03/23/cloud-computing-πλεονεκτήματα-για-τις-μικρές-μεσα/

[04] DataLine: «Government Cloud Computing», www.dataline.com.

[05] David C. Wyld: «Moving to the Cloud: An Introduction to Cloud Computing in Government», IBM Center for "The Business of Government".

[06] IT Security Professional:
http://www.itsecuritypro.gr/contents_article.php?id=93&catid=4

[07] Intracom Telecom:
http://www.intracomtelecom.com/gr/products/ict_services_solutions/solutions/security.htm

[08] Wikipedia, «Ασφάλεια Δικτύων Υπολογιστών»:
http://el.wikipedia.org/wiki/%CE%91%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1_%CE%B4%CE%B9%CE%BA%CF%84%CF%8D%CF%89%CE%BD_%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CF%8E%CE%BD

[09] Patrick Hφne, «Cloud Computing Security Requirements and Solutions: a Systematic Literature Review».

[10] Δημήτριος Ζήσης, Δημήτριος Λέκκας: «Addressing cloud computing security issues», http://www.sciencedirect.com/science/article/pii/S0167739X10002554

[11] Rizwana Shaikh, M. Sasikumar: «Security Issues in Cloud Computing: A survey».

[12] Σ. Κατσικάς, Δ. Γκρίτζαλης, Σ. Γκρίτζαλης (Επιστημονική Επιμέλεια). «Ασφάλεια Πληροφοριακών Συστημάτων». Εκδόσεις Νέων Τεχνολογιών, Αθήνα2004.

[13] Αρχή Προστασίας Δεδομένων – Νόμος 2472/1997: http://www.dpa.gr/portal/page?_pageid=33,123437&_dad=portal&_schema=PORTAL

[14] Αρχή Προστασίας Δεδομένων – Νόμος 3471/2006: http://www.dpa.gr/portal/page?_pageid=33,123437&_dad=portal&_schema=PORTAL

[15] Αρχή Προστασίας Δεδομένων, «Ερωτήσεις - Απαντήσεις για τα Προσωπικά Δεδομένα» http://www.dpa.gr/portal/page?_pageid=33,18990&_dad=portal&_schema=PORTAL

[16] Εθνική Σχολή Δημόσιας Διοίκησης: «Ηλεκτρονική Διακυβέρνηση: Μια ευκαιρία για καλύτερη Διακυβέρνηση με επίκεντρο τον πολίτη – Η ελληνική περίπτωση», Κατερίνα Σαρρή

[17] Europa – Σύνοψη της Νομοθεσίας της Ε.Ε. -(Ανακοίνωση της Ευρωπαϊκής Επιτροπής COM(2003)567): http://europa.eu/legislation_summaries/internal_market/businesses/public_procurement/l24226b_el.htm#KEY , ή http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=el&type_doc=COMfinal&an_doc=2003&nu_doc=567

[18] Ιγκλεζάκης Ιωάννης:«E-Government in Greece», University of Thessaloniki: http://www.academia.edu/240742/eGovernment_in_Greece

[19] Szilard Molnar, «Η ηλεκτρονική διακυβέρνηση στην Ευρωπαϊκή Ένωση».

[20] Κέντρο Εξυπηρέτησης Πολιτών (ΚΕΠ): www.kep.gov.gr

[21] Ίδρυμα Κοινωνικών Ασφαλίσεων (ΙΚΑ): www.ika.gr

[22] ΣΥΖΕΥΞΙΣ: http://www.syzefxis.gov.gr/

[23] Κυβερνητική Πύλη Δημόσιας Διοίκησης «Ερμής»: www.ermis.gov.gr

[24] International Journal of Advanced Research in Computer Science and Software Engineering: «A REVIEW OF CLOUD COMPUTING AND E- GOVERNANCE», Kuldeep Vats, Shravan Sharma, Amit Rathee

[25] Kamal Dahbur, Bassil Mohammad, Ahmad Bisher Tarakji: «A Survey of Risks, Threats and Vulnerabilities in Cloud Computing», School of Engineering and Computing Sciences, New York Institute of Technology Amman, Jordan.

[26] The Council of European Professional Informatics Societies (CEPIS): «Cloud Computing Security and Privacy Issues»

[27] European Network and Information Security Agency (ENISA): «Cloud Computing – Benefits, Risks and Recommendations for information security», November 2009.

[28] New York Times: «What Cloud Computing Really Means», By ERIC KNORR and GALEN GRUMAN, InfoWorld, April 2008. http://www.nytimes.com/idg/IDG_002570DE00740E180025742400363509.html?ex=1365307200&en=3aa8122436bda02f&ei=5088&partner=rssnyt&emc=rss

[29] Γραφείο επιτρόπου προστασίας Δεδομένων προσωπικού χαρακτήρα (Κυπριακή Δημοκρατία) http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/eu_gr/eu_gr?OpenDocument

[30] Ομάδα Εργασίας του Άρθρου 29 για την προστασία των προσωπικών Δεδομένων: « Γνώμη 05/2012 σχετικά με τη Νεφοϋπολογιστική, της 01/07/2012».

[31] Κίτσος Παναγιώτης – Διδακτορική Διατριβή: « Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της Ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών: Ενσωμάτωση των ρυθμίσεων της Ευρωπαϊκής Ένωσης στο ελληνικό δίκαιο », (2011, Πανεπιστήμιο Μακεδονίας, Οικονομικών και Κοινωνικών Επιστημών). http://thesis.ekt.gr/thesisBookReader/id/26521#page/91/mode/1up

[32] Αρχή Προστασίας Δεδομένων – Νομοθεσία: http://www.dpa.gr/portal/page?_pageid=33,15145&_dad=portal&_schema=PORTAL

[33] Το Σύνταγμα της Ελλάδος –Άρθρο 9Α με το ψήφισμα της Ζ΄ Αναθεωρητικής Βουλής (2001)

[34] Πειρατικό Παπαγαλάκι, «Υποκλοπή Επικοινωνιών: Ιδιωτικότητα εναντίον Ασφάλειας»: http://waves.pirateparty.gr/

[35] Wikipedia, «Information Privacy Law »: http://en.wikipedia.org/wiki/Information_privacy_law#United_States

[36] HG Legal Resources.org, «Data Protection Law»: http://www.hg.org/data-protection.html

[37] Wikipedia, «Σύνταγμα των Ηνωμένων Πολιτειών»: http://el.wikisource.org/wiki/%CE%A3%CF%8D%CE%BD%CF%84%CE%B1%CE%B3%CE%BC%CE%B1_%CF%84%CF%89%CE%BD_%CE%97%CE%BD%CF%89%CE%BC%CE%AD%CE%BD%CF%89%CE%BD_%CE%A0%CE%BF%CE%BB%CE%B9%CF%84%CE%B5%CE%B9%CF%8E%CE%BD#.CE.A4.CF.81.CE.BF.CF.80.CE.BF.CE.BB.CE.BF.CE.B3.CE.AF.CE.B1_4_.E2.80.93_.CE.88.CF.81.CE.B5.CF.85.CE.BD.CE.B1_.CE.BA.CE.B1.CE.B9_.CE.BA.CE.B1.CF.84.CE.AC.CF.83.CF.87.CE.B5.CF.83.CE.B7_.281791.29

[38] The United States Department of Justice, «Overview of the Privacy Act of 1974», 2012 edition: http://www.justice.gov/opcl/1974privacyact-overview.htm

[39] «Data Protection and Privacy in the United States and Europe» by Jean Slemmons Stratford & Juri Stratford, Fall 1998

[40] Wikipedia, « Privacy Act of 1974 »: http://en.wikipedia.org/wiki/Privacy_Act_of_1974

[41] Wikipedia, «Electronic Communications Privacy Act»: http://en.wikipedia.org/wiki/Electronic_Communications_Privacy_Act

[42] Congressional Research Service: «Reauthorization of the FISA Amendments Act» , Edwart C. Liu, April 2013

[43] PC Magazine: «Απειλούνται τα δεδομένα μας στο Cloud από τις Η.Π.Α.», Γιάννης Τζώρτζος, Φεβρουάριος 2013 . http://www.e-pcmag.gr/techtalk/apeilountai-ta-dedomena-mas-sto-cloud-apo-tis-ipa

[43] Υπουργείο Εμπορίου των Η.Π.Α.: «US- EU Harbor Overview». http://export.gov/safeharbor/eu/eg_main_018476.asp

[44] Wikipedia, «International Safe Harbor Privacy Principles»: http://en.wikipedia.org/wiki/International_Safe_Harbor_Privacy_Principles

[45] Eur-Lex, Access to European Union Law, «EUR-Lex - 32000D0520 – EN»:

http://eur-lex.europa.eu/legal-content/el/ALL/;jsessionid=2PtVTyWdPwQSG7hGltKFGflHhZ1P2RByjKh33T2zT9hgBrnfKvBB!-1514564281?uri=CELEX:32000D0520

[46] CIO: «Cloud Computing Gains in Federal Government», By Kenneth Corbin, 2012. http://www.cio.com/article/705545/Cloud_Computing_Gains_in_Federal_Government?page=2&taxonomyId=3133

[47] International Journal of Web & Semantic Technology, «The cloudy future of Government IT: Cloud Computing and the public sector around the world», David C. Wyld

[48] Cloud Book, Government Clouds: http://www.cloudbook.net/directories/gov-clouds/government-cloud-computing.php

[49] GSA Advantage online shopping: https://www.gsaadvantage.gov/advantage/main/home.do

[50] Cloud.cio.gov: http://cloud.cio.gov/

[51] NASA: «NASA Nebula Cloud Computing Platform, Cloud Computing for a Universe of Data». http://www.nasa.gov/open/plan/nebula.html

[52] Δερμεντζή Ελένη, «CLOUD COMPUTING IN E-GOVERNMENT», Διπλωματική Εργασία, Πανεπιστήμιο Μακεδονίας, Φεβρουάριος 2013

[53] DISA – Defence Information Systems Agency, Department of Defence: http://www.disa.mil/About/Our-Work

http://www.disa.mil/Services/Enterprise-Services/Infrastructure/RACE

http://www.disa.mil/Services/Enterprise-Services/Applications/Forge-Mil

[54] UK Cloud Store: http://govstore.service.gov.uk/cloudstore/

[55] Joinup – European Commission: «German Government Cloud: Open source where possible»: https://joinup.ec.europa.eu/community/osor/news/german-government-cloud-open-source-where-possible

[56] Bernd Zwattendorfer, Klaus Stranacher, Arne Tauber, Peter Reichstδdter: «Cloud Computing in E-Government across Europe - A Comparison»

[57] epractice.eu – German Administration Services Directory (DVDV): http://www.epractice.eu/cases/dvdv

[58] Sucre (SUpporting Cloud Research Exploitation): «State of the art analysis: Cloud solutions in the Public sector», Project No: 318204, Project Runtime: 10/2012 - 09/2014

[59] Παρουσίαση Δράσεων Ομάδας Ηλεκτρονικής Διακυβέρνησης στην Ελλάδα: http://egovict.blogspot.gr/

[60] e-Government Conference - Μεταμορφώνοντας το Δημόσιο Τομέα με εφαλτήριο την ανάπτυξη:

http://www.netweek.gr/default.asp?pid=9&cID=6&arId=25244&la=1

[61] Υπουργείο Διοικητικής Μεταρρύθμισης και Ηλεκτρονικής Διακυβέρνησης: http://www.ydmed.gov.gr/

[62] Διαύγεια: http://diavgeia.gov.gr/

[63] egov-ict ιστολόγιο: http://egovict.blogspot.gr/

[64] NSN - Computing industry leaders form Asia Cloud Computing Association to drive regional adoption, security and policy:

http://nsn.com/news-events/press-room/press-releases/computing-industry-leaders-form-asia-cloud-computing-associati

[65] FROST & SULLIVAN 2011 – «State of Cloud Computing in the Public Sector – A Strategic analysis of the business case and overview of initiatives across Asia Pacific»: http://www.sucreproject.eu/sites/default/files/cloud_computing_adoption_in_the_public_sector.pdf

[66] Information Week – «Japan Hopes IT Investment, Private Cloud Will Spur Economic Recovery»: http://www.informationweek.com/it-strategy/japan-hopes-it-investment-private-cloud-will-spur-economic-recovery/d/d-id/1079624

[67] Asia Pacific Future Gov: «Indian IT Minister launches national cloud», http://www.futuregov.asia/articles/2014/feb/05/indian-it-minister-launches-national-cloud/

[68] MeghRaj Cloud Initiative –Government of India, https://cloud.gov.in/index.php

[69] International Journal of Engineering and Innovative Technology (IJEIT) : «Security Risks & Migration Strategy For Cloud Sourcing: A Government Perspective», Dr Mansaf Alam, Shuchi Sethi, January 2013

[70] Vivek Kundra : «Federal Cloud Computing Strategy» , February 2011

[71] Cisco White Paper: «Cloud Computing in the Public Sector: Public Manager's Guide to Evaluating and Adopting Cloud Computing», November 2009

[72] ComputerWeekly.com: «Cloud choices: How to select the right hosted services», http://www.computerweekly.com/opinion/Cloud-Choices

[73] Wikipedia: «Ανάλυση SWOT». http://el.wikipedia.org/wiki/%CE%91%CE%BD%CE%AC%CE%BB%CF%85%CF%83%CE%B7_SWOT

[74] ENISA: «Security & Resilience in Governmental clouds», January 2011.

[75] Systems Engineering at MITRE, Cloud Computing SERIES: «Cloud SLA Considerations for the Government Consumer», Kevin Buck-Diane Hanf, September 2010.

[76] Cloud Computing Use Cases Group: «Moving to the Cloud », Version 01, February 2011. http://cloudusecases.org/

[77] Search IT Channel: «Service Level Agreement». http://searchitchannel.techtarget.com/definition/service-level-agreement

[78] Cloud Computing Use Cases Group: «Cloud Computing Use Cases», Version 04, July 2010.

[79] IBM Developer Works: «Review and summary of cloud service level agreements». http://www.ibm.com/developerworks/cloud/library/cl-rev2sla.html

[80] IEEE International Conference on Services Computing 2009: «Cloud Security Issues». Advanced Software Technologies, International Institute of Information Technology, Pune India. Balachandra Reddy, Kandukuri Ramakrishna Paturi V, Dr. Atanu Rakshit.

[81] Wikipedia: «Service Level Objective (SLO)». http://en.wikipedia.org/wiki/Service_level_objective

[82] Cloud Security Alliance Industry Blog: «Critical Infrastructure and the Cloud», February 2013. https://blog.cloudsecurityalliance.org/2013/02/01/critical-infrastructure-and-the-cloud/

[83] DigitalGreece2020: «Καταγραφή των Κρίσιμων Υποδομών στο Δημόσιο και τον Ιδιωτικό Τομέα», June 2011. http://www.digitalgreece2020.gr/archives/399

[84] ENISA: «Critical Cloud Computing: A CIIP Perspective on Cloud Computing services», December 2012, Version 01.

[85] Edwin Schouten – Cloud & IT Architecture: «A Critical Information Infrastructure Protection (CIIP) perspective on Cloud Computing».

http://edwinschouten.nl/2013/02/19/ciip-perspective-on-cloud-computing/

[86] IT Law Wiki: «Critical Cloud Computing - A CIIP Perspective on Cloud Computing Services».

http://itlaw.wikia.com/wiki/Critical_Cloud_Computing_-_A_CIIP_Perspective_on_Cloud_Computing_Services