Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Προηγμένα Συστήματα Πληροφορικής»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	Ταξινομία ρυθμιστικών πλαισίων και ασφάλειας σε περιβάλλοντα Υπολογιστικών Νεφών Cloud Computing: Law and Regulations
Ονοματεπώνυμο Φοιτητή	**Χαλδαίος Χρήστος**
Πατρώνυμο	**Αυγουστής**
Αριθμός Μητρώου	**ΜΠΣΠ/12089**
Επιβλέπων	**Χρήστος Δουληγέρης, Καθηγητής**

Ημερομηνία Παράδοσης **Ιούλιος 2014**

Τριμελής Εξεταστική Επιτροπή

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

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα κ. Δημήτρη Καλλέργη για τις παρατηρήσεις και πάντα εύστοχες επισημάνσεις του, τον καθηγητή κ. Δουληγέρη Χρήστο καθώς και την οικογένεια μου για τη στήριξη που μου έχει δύσει όλα αυτά τα χρόνια.

Περίληψη

Το υπολογιστικό νέφος αποτελεί την αρχιτεκτονική προσέγγιση που ευελπιστεί να ηγεμονεύσει και κυριότερα να αντικαταστήσει τις λύσεις εκείνες που γνωρίζαμε έως σήμερα. Είναι ένα φαινόμενο που αναπτύσσεται συνεχώς και παρέχει πλεονεκτήματα που το καθιστούν εξαιρετικά ελκυστικό είτε αφορά τον ιδιωτικό είτε τον δημόσιο τομέα, καθώς δίνει τη δυνατότητα να μειωθεί το κόστος των εγκαταστάσεων που φιλοξενούν τις υποδομές πληροφοριακών συστημάτων και να ενοποιηθούν υπάρχουσες λύσεις σε νέες, αξιοποιώντας την ελάχιστη δυνατή τεχνογνωσία. Από την άλλη πλευρά, συνδέεται με μειονεκτήματα όπως η προστασία των ευαίσθητων δεδομένων, η έλλειψη ελέγχου από πλευράς του χρήστη και η ασφάλεια των δεδομένων αυτών. Σύμφωνα με όσα καταγράφονται στο κείμενο της στρατηγικής «Ορίζοντας 2020» η ανάπτυξη της ψηφιακής οικονομίας μπορεί να αποφέρει τεράστια οφέλη για τους πολίτες, αλλά και συνολικά για την οικονομία μίας χώρας. Όμως, για να στραφούν οι φορείς προς την κατεύθυνση των λύσεων υπολογιστικού νέφους θα πρέπει να αναπτυχθεί κλίμα ασφάλειας και εμπιστοσύνης, το οποίο θα προκύψει μέσω των κατάλληλων ρυθμιστικών και νομικών πλαισίων που θα θεσπίσει η Ευρωπαϊκή Ένωση αλλά και η κάθε χώρα ξεχωριστά.

Στην παρούσα μεταπτυχιακή διατριβή εξετάζουμε και αναλύουμε την πιθανότητα ύπαρξης προβλημάτων λόγω της αλληλεπίδρασης των συστημάτων μεταξύ φορέων που διέπονται από διαφορετικά κανονιστικά πλαίσια λειτουργίας, μεταξύ χωρών με διαφορετικά νομικά πλαίσια και μεταξύ διαφορετικών θεσμικών παραγόντων. Θα πραγματοποιήσουμε καταγραφή, σύγκριση και ανάλυση του ισχύοντος ρυθμιστικού και νομικού πλαισίου σχετικά με τις υλοποιήσεις υπολογιστικών νεφών σε διαφορές χώρες της Ευρωπαϊκής Ένωσης, είτε αφορά τον ιδιωτικό τομέα είτε τον δημόσιο. Τέλος, θα γίνει αποτίμηση και σύγκριση στην υπάρχουσα πολιτική της Ελλάδας και των αντίστοιχων ευρωπαϊκών χωρών.

Abstract

Cloud computing is an architectural approach that hopes to take over and mainly to replace all these solutions that we know today. It is a phenomenon that is continuously growing and offers advantages that make it extremely attractive either in the private or in the public sector, as it gives the possibility to reduce the cost of hosting infrastructure facilities and information systems to integrate existing solutions to new, utilizing the minimum possible expertise. On the other hand, it is associated with disadvantages such as the protection of sensitive data, the lack of control on the part of the user and the security of such data. According to what is recorded in the text of the strategy 'Horizon 2020' , the development of the digital economy can bring huge benefits for citizens, but also for the overall economy of a country. However, for the transition towards cloud computing public and private bodies must develop security and trust, which will occur through appropriate regulatory and legal frameworks to be adopted by the European Union and individual countries.

In this master thesis we examine and analyze the possibility of problems due to the interaction between systems of entities governed by different regulatory frameworks operation between countries with different legal frameworks and between different institutional actors. We will carry out a recording, comparison and analysis of the current regulatory and legal frameworks for cloud computing implementations in various countries of the European Union, either in the private sector or the public. Finally, we will make an assessment and comparison of the existing policy of Greece and the respective European countries.

Περιεχόμενα

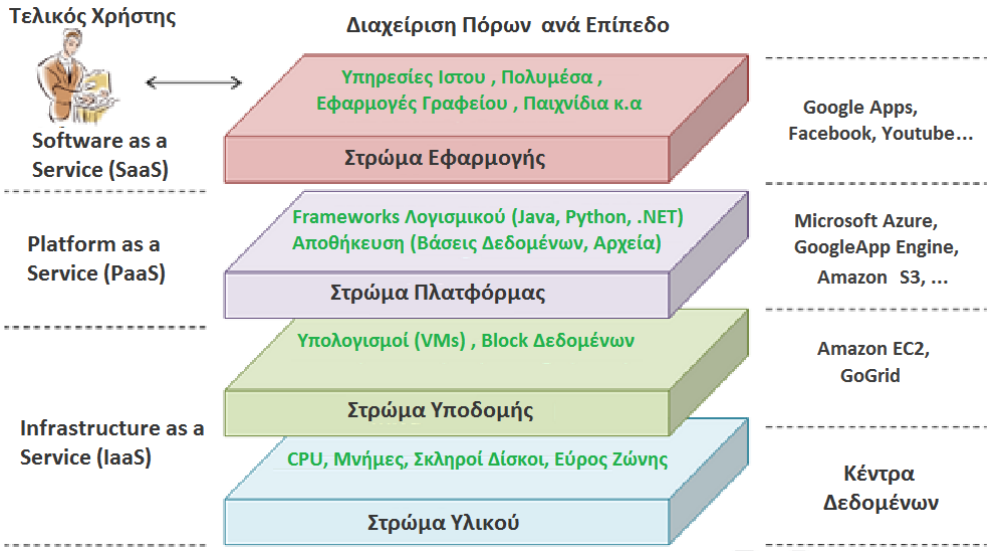
Λίστα Εικόνων

Λίστα Πινάκων

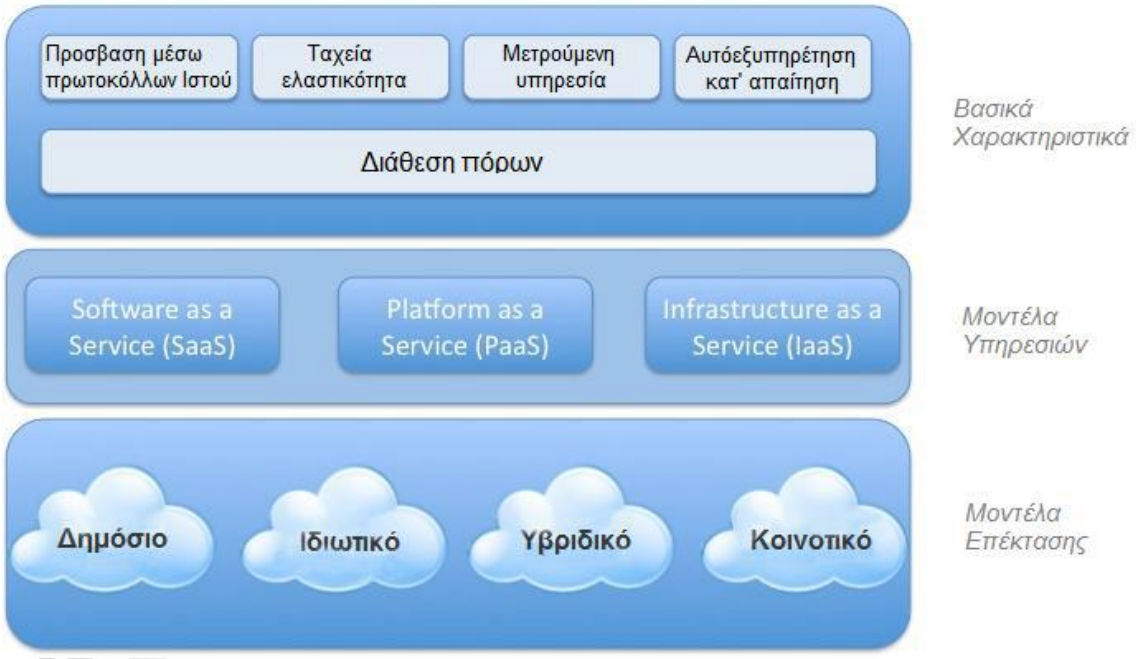
Η Ευρωπαϊκή Επιτροπή έχει θέσει ως στόχο να γίνει πιο «παραγωγική» στον τομέα του υπολογιστικού νέφους ώστε η Ευρώπη να προσφέρει λύσεις και να μην χρησιμοποιεί λύσεις που παράγονται αλλού. Ο ψηφιακός τομέας, είτε πρόκειται για υπηρεσίες είτε για προϊόντα είτε για περιεχόμενο, κυριαρχείται από επιχειρήσεις τρίτων χωρών, κυρίως από τη Βόρεια Αμερική ή την Ασία. Στην εποχή μας η ψηφιακή βιομηχανία είναι ένας σημαντικός παράγοντας ανάπτυξης, παρόλα αυτά η Ευρώπη παρουσιάζει καθυστέρηση στον τομέα αυτόν. Η ανακατανομή του μεριδίου της αγοράς μπορεί να επηρεαστεί από το υπολογιστικό νέφος. Αυτό μπορεί να συμβάλει ώστε περισσότεροι παράγοντες να μπορούν να συναγωνιστούν εκ νέου για την κατάκτηση θέσης στην παγκόσμια αγορά. Η θέση των εταιριών που κυριαρχούν αυτή τη στιγμή θα αμφισβητηθεί από υπάρχοντες ανταγωνιστές ή από νεοεμφανιζόμενους παράγοντες. Ο παγκόσμιος ρόλος του υπολογιστικού νέφους απαιτεί την ανάπτυξη παγκόσμιων αρχών και προτύπων. Η ΕΕ πρέπει να ηγηθεί της προσπάθειας δημιουργίας και υποστήριξης σε πρότυπα πιστοποίησης σε πανευρωπαϊκή κλίμακα για αξιόπιστους παρόχους υπολογιστικού νέφους και να εγγυηθεί την εξασφάλιση υψηλού επίπεδου προστασίας των προσωπικών δεδομένων, το οποίο προβλέπεται από την ευρωπαϊκή νομοθεσία.

1.1 Ορισμός του υπολογιστικού νέφους

Το **Υπολογιστικό Νέφος** (Cloud Computing) αναφέρεται στις εφαρμογές που παραδίδονται ως υπηρεσίες μέσω του διαδικτύου και στα υπολογιστικά μηχανήματα (hardware) και στο λογισμικό (software) που βρίσκονται σε ένα κέντρο πληροφοριών που παρέχει αυτές τις υπηρεσίες. Όταν αυτές οι υπηρεσίες παρέχονται από έναν ανεξάρτητο πάροχο ή από εξωτερικούς πελάτες, τότε το υπολογιστικό νέφος βασίζεται σε ένα επιχειρηματικό μοντέλο μίσθωσης ανάλογα με τη χρήση. Το Εθνικό Ινστιτούτο Τυποποιήσεων και Τεχνολογίας (NIST–National Institute of Standards and Technology) είναι ένα ίδρυμα ευρέως γνωστό σε παγκόσμιο επίπεδο στο πεδίο της τεχνολογίας πληροφοριών. Το NIST [1] όρισε την αρχιτεκτονική του υπολογιστικού νέφους περιγράφοντας πέντε χαρακτηριστικά, τρία μοντέλα υπηρεσίας νέφους και τέσσερα μοντέλα ανάπτυξης νέφους.



Εικόνα 1.1 Απεικόνιση ορισμού NIST για την αρχιτεκτονική του Cloud Computing *(Πηγή: Q. Zhang, L. Cheng, R. Boutaba. (2010) Cloud computing: state-of-the-art and research challenges". Springer)*



Εικόνα 1.2 Οπτική αναπαράσταση του ορισμού του νέφους κατά τον NIST *(Πηγή: http://csrc.nist.gov/groups/sns/cloud-computing/index.html)*

1.2 Τα χαρακτηριστικά του Cloud Computing

Όπως αναφέρθηκε, υπάρχουν 5 χαρακτηριστικά του Cloud Computing, τα οποία εξηγούν τη σχέση και τη διαφορά που υφίσταται συγκριτικά με τις παραδοσιακές υπολογιστικές μεθόδους.

Αυτό εξυπηρέτηση κατά απαίτηση (on-demand-self-service)

Οι καταναλωτές μπορούν να αξιοποιήσουν ή να απορρίπτουν την παροχή υπηρεσιών, χωρίς ανθρώπινη αλληλεπίδραση με τον πάροχο υπηρεσιών έως και ένα σημαντικό επίπεδο χωρίς να διαταράξουν τις εργασίες υποδοχής.

Ευκολία πρόσβασης

Οι χρήστες μπορούν να έχουν πρόσβαση στα δεδομένα και στις εφαρμογές τους από οποιοδήποτε σημείο και από οποιαδήποτε συσκευή (smartphone, laptop,tablet) αρκεί να διαθέτουν σύνδεση στο Διαδίκτυο

Κλιμακωσιμότητα

Ο προμηθευτής προσαρμόζει σε πραγματικό χρόνο την υπολογιστική ισχύ στις ανάγκες του εκάστοτε χρήστη. Αυτό σημαίνει ότι σε περίοδο που ο πελάτης χρειαστεί παραπάνω ισχύ, θα μπορεί να καλύπτει τις ανάγκες του χωρίς να επενδύσει σε εξοπλισμό πληροφορικής που μπορεί μετά από ένα διάστημα να μην θέλει να το χρησιμοποιήσει.

Διάθεση πόρων (resource pooling).

Οι πόροι του παρόχου που χρησιμοποιούνται για υπολογιστικές διαδικασίες διατίθενται για να εξυπηρετούν πολλαπλούς χρήστες. Οι πόροι χρησιμοποιούν ένα μοντέλο «πολύ-ενοικιαστή» και συνδυάζοντας δυναμικά φυσικούς και εικονικούς πόρους ανταποκρίνονται στην εκάστοτε καταναλωτική ζήτηση.

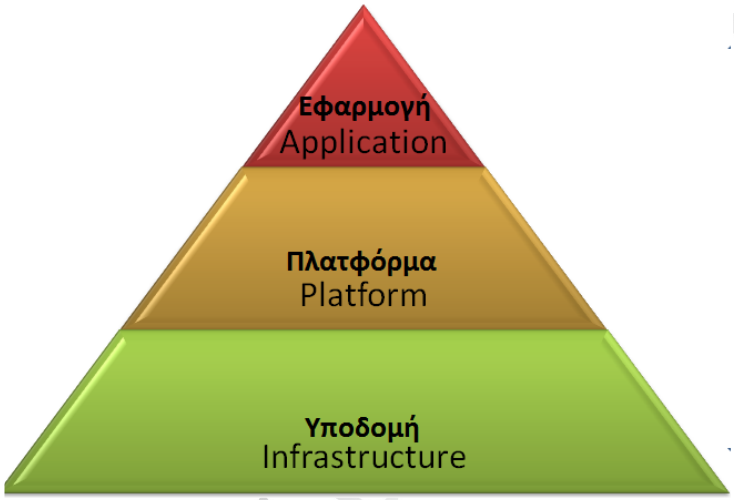
Τιμολόγηση ανάλογη με τη χρήση

Με τα συστήματα νέφους δίνεται η δυνατότητα μέτρησης των πόρων και υπηρεσιών ανάλογα το είδος (π.χ. αποθήκευσης, επεξεργασίας, εύρους ζώνης ή διαθέσιμων λογαριασμών χρηστών) που χρησιμοποιεί ο καταναλωτής. Έτσι παρέχεται διαφάνεια

τόσο για τον παροχή αλλά και ο καταναλωτής πληρώνει μόνο το πόσο που αντιστοιχεί στις υπηρεσίες που χρησιμοποιεί πραγματικά

1.3 Μοντέλα υπηρεσίας νέφους

Υπάρχουν 3 μοντέλα υπηρεσίας νέφους, οι οποίες συχνά αναφέρονται και ως «μοντέλο SPI» (Software, Platform or Infrastructure as a service –Λογισμικό, Πλατφόρμα ή Δομή μιας υπηρεσίας).



Εικόνα 1.3 πυραμίδα παροχής υπηρεσιών

Λογισμικό νέφους ως υπηρεσία (SaaS)

Η δυνατότητα που παρέχεται στον καταναλωτή είναι να χρησιμοποιούν τις εφαρμογές που διατίθενται στο νέφος. Οι εφαρμογές είναι προσβάσιμες από διάφορες συσκευές του πελάτη (π.χ. Web-based e-mail). Ο καταναλωτής δεν διαχειρίζεται ή ελέγχει την υποκείμενη υποδομή νέφους, συμπεριλαμβανομένου του δικτύου, των servers, των λειτουργικών συστημάτων. Για παράδειγμα, το Google Apps προσφέρει λογισμικό on-line για την επιχείρηση ή ιδιωτικούς φορείς οι οποίοι μπορούν να κάνουν τις θεμελιώδεις επιχειρησιακές δραστηριότητες που μια συνηθισμένη σουίτα εφαρμογών γραφείου μπορεί να παρέχει. Το Google Apps περιλαμβάνει συνεργασία στα έγγραφα κειμένου, παρουσίαση και υπολογισμούς με λογιστικά φύλλα καθώς και ημερολόγια και υπηρεσίες ηλεκτρονικού ταχυδρομείου.

Πλατφόρμα νέφους ως υπηρεσία (PaaS)

Η δυνατότητα που παρέχεται στον καταναλωτή να αναπτύξει εφαρμογές σε περιβάλλον cloud. Ο καταναλωτής χρησιμοποιεί γλώσσες προγραμματισμού και εργαλεία που υποστηρίζονται από τον πάροχο της υπηρεσίας στη δομή του νέφους.. Η PaaS προσφέρει τη διευκόλυνση της επέκτασης των εφαρμογών χωρίς το κόστος και την πολυπλοκότητα της αγοράς και της διαχείρισης υλικού και λογισμικού. Ένα παράδειγμα πλατφόρμας νέφους ως υπηρεσία (PaaS) είναι η Azure[1] των Microsoft Windows η οποία παρέχει ένα περιβάλλον βασισμένο στα Windows για να τρέχει εφαρμογές και να αποθηκεύει τα δεδομένα στους servers των κέντρων δεδομένων για να καλύψει τους χρήστες.

Δομή του νέφους ως υπηρεσία (IaaS)

Αντί για την αγορά διακομιστών, λογισμικού, κέντρου δεδομένων, ή εξοπλισμού δικτύων, οι καταναλωτές αγοράζουν αντ' αυτού τους πόρους αυτούς πλήρως ως υπηρεσία. Επιπλέον, παρέχεται στον καταναλωτή η δυνατότητα λειτουργιών επεξεργασίας, αποθήκευσης και άλλων θεμελιωδών υπολογιστικών πόρων στους οποίους ο χρήστης μπορεί να αναπτύξει και να τρέξει οποιαδήποτε λειτουργικά συστήματα ή προγράμματα. Οι Amazon Web Services[2] είναι ένα τέτοιο παράδειγμα, όπου η υποδομή είναι διαθέσιμη με έναν τρόπο πληρωμής βάσει χρήσης (pay as you go) με αυτοεξυπηρέτηση και κατέχει servers, αποθήκευση και διαμόρφωση δικτύου.

1.4 Μοντέλα ανάπτυξης νέφους

Ανεξάρτητα από το πρότυπο υπηρεσιών που χρησιμοποιείται (SaaS, PaaS, ή IaaS), υπάρχουν τέσσερα πρότυπα επέκτασης για τις υπηρεσίες νέφους με παράγωγες παραλλαγές που εξετάζουν συγκεκριμένες απαιτήσεις. Είναι σημαντικό να σημειωθεί ότι υπάρχουν παράγωγα πρότυπα επέκτασης νέφους που προκύπτουν λόγω της ωρίμανσης των προσφορών της αγοράς και της απαίτησης των πελατών.

Δημόσιο νέφος (Public cloud)

Η υποδομή cloud διατίθεται στο ευρύ κοινό ή σε μεγάλες ομάδες βιομηχανίας και ανήκει σε κάποιον πάροχο υπηρεσιών νέφους. Τα δημόσια νέφη προσφέρουν διάφορα

[1] http://azure.microsoft.com/en-us/
[2] http://aws.amazon.com/

οφέλη στους φορείς παροχής υπηρεσιών, συμπεριλαμβανομένης της μηδενικής αρχικής επένδυσης για υποδομή αλλά υστερούν στον έλεγχο το δεδομένων μέσα στο νέφος, το δίκτυο και τις ρυθμίσεις ασφαλείας.

Ιδιωτικό νέφος (Private cloud)

Σε αυτού του είδους το νέφους, η δομή λειτουργεί αποκλειστικά και μόνο για έναν οργανισμό και δίνει την αποκλειστική πρόσβαση και χρήση της υποδομής και των υπολογιστικών πόρων. Μπορεί να ρυθμιστεί είτε από τον οργανισμό είτε από κάποιον τρίτο, και μπορεί να φιλοξενηθεί στις εγκαταστάσεις του ίδιου του). Ένα ιδιωτικό νέφος προσφέρει τον υψηλότερο βαθμό ελέγχου της απόδοσης, της αξιοπιστίας και της ασφάλειας. Εντούτοις μοιάζει με τα παραδοσιακά κέντρα δεδομένων και δεν παρέχουν την ευκολία της μηδενικής αρχικής δαπάνης.

Κοινοτικό Νέφος (Community cloud)

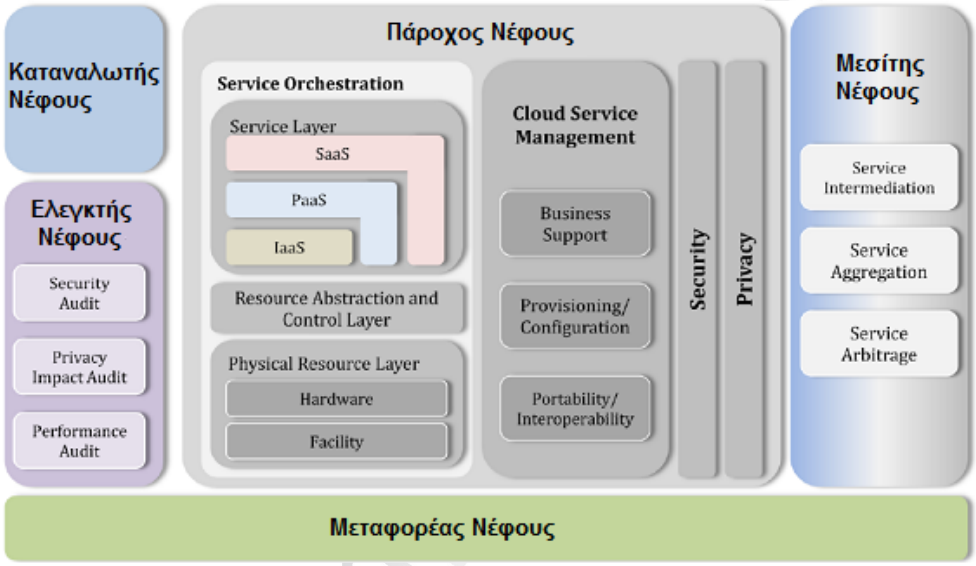
Η υποδομή νέφους μοιράζεται από κοινού από διάφορους οργανισμούς και υποστηρίζει μια συγκεκριμένη που έχει κοινά ενδιαφέροντα και τακτικές. Μπορεί να ρυθμιστεί από τον οργανισμό ή κάποιον τρίτο και μπορεί να είναι τοποθετημένη εντός ή εκτός των εγκαταστάσεων του οργανισμού. Ένας καταναλωτής μπορεί να έχει πρόσβαση στους τοπικούς πόρους του νέφους, και επίσης στους πόρους άλλων συμμετεχόντων οργανισμών.

Υβριδικό νέφος (Hybrid cloud)

Η υποδομή cloud αποτελείται από δύο ή περισσότερων σύννεφα νέφη διαφορετικού είδους (ιδιωτικών, κοινότητας, ή δημόσιες) που παραμένουν μοναδικές οντότητες, αλλά συνδέονται μεταξύ τους τυποποιημένη τεχνολογία που επιτρέπει φορητότητα των δεδομένων και της εφαρμογής (πχ cloud bursting για εξισορρόπηση φορτίου μεταξύ νεφών).

1.5 Τύποι Χρηστών – Ρόλοι

Η αρχιτεκτονική αναφοράς υπολογισμού νέφους του NIST καθορίζει πέντε σημαντικούς ρόλους: καταναλωτής νέφους, πάροχος νέφους, μεταφορέας νέφους, ελεγκτής νέφους και μεσίτης νέφους. Κάθε ρόλος είναι μια οντότητα (ένα πρόσωπο ή οργανισμός) που συμμετέχει σε μια συναλλαγή ή μια διαδικασία ή εκτελεί στόχους στο υπολογιστικό νέφους. Η παρακάτω εικόνα προσδιορίζει τους σημαντικότερους ρόλους, δραστηριότητες και τις λειτουργίες του υπολογιστικού νέφους.



Εικόνα 1.4 Το εννοιολογικό πρότυπο αναφοράς του NIST

(Πηγή: F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, D. Leaf (2011). NIST: Recommendations of the National Institute of Standards and Technology)

Καταναλωτής νέφους

Οι καταναλωτές νέφους είναι ένα πρόσωπο ή οργανισμός (δημόσιος η ιδιωτικός) που διατηρεί μια επιχειρησιακή σχέση και χρησιμοποιεί την υπηρεσία από τους προμηθευτές νέφους. Οι καταναλωτές νέφους χρειάζονται συμφωνητικά παροχής υπηρεσιών(SLAs)[3] για να διευκρινίσουν τις τεχνικές απαιτήσεις απόδοσης που ικανοποιούνται από έναν προμηθευτή νέφους. Τα SLAs μπορούν να καλύψουν τους όρους σχετικά με την ποιότητα της υπηρεσίας, την ασφάλεια, κάλυψη για πιθανές αποτυχίες απόδοσης κ.α. Ένας καταναλωτής νέφους μπορεί ελεύθερα να επιλέξει έναν προμηθευτή νέφους με καλύτερες τιμές και περισσότερους ευνοϊκούς όρους.

[3] http://en.wikipedia.org/wiki/Service-level_agreement

Πάροχος νέφους

Ένας Πάροχος νέφους είναι ένα πρόσωπο ή οργανισμός. Είναι η αρμόδια οντότητα για να καταστήσει μια υπηρεσία διαθέσιμη στα ενδιαφερόμενα συμβαλλόμενα μέρη. Ένας πάροχος νέφους αποκτά και διαχειρίζεται την υποδομή υπολογισμού που απαιτείται για την παροχή των υπηρεσιών, τρέχει το λογισμικό νέφους που παρέχει τις υπηρεσίες, και κάνει τη ρύθμιση για να παραδώσει τις υπηρεσίες νέφους στους καταναλωτές νέφους μέσω της πρόσβασης στο δίκτυο.

Ελεγκτής νέφους

Ένας ελεγκτής νέφους είναι ένα συμβαλλόμενο μέρος το οποίο συνήθως είναι ένας ιδιωτικός οργανισμός που μπορεί να εκτελέσει μια ανεξάρτητη εξέταση ελέγχου των υπηρεσιών νέφους με την πρόθεση να εκφράσει μια άποψη επ'αυτού. Οι έλεγχοι εκτελούνται για να ελέγξουν την προσαρμογή στα πρότυπα μέσω της αναθεώρησης των αντικειμενικών δεδομένων. Ένας ελεγκτής νέφους μπορεί να αξιολογήσει τις υπηρεσίες που παρέχονται από έναν πάροχο νέφους από την άποψη των ελέγχων ασφάλειας, του αντίκτυπου της ιδιωτικότητάς, της απόδοσης, κ.λπ. Για τον έλεγχο ασφάλειας, ένας ελεγκτής νέφους μπορεί να κάνει μια αξιολόγηση των ελέγχων ασφάλειας στο πληροφοριακό σύστημα για να καθορίσει το βαθμό στον οποίο οι έλεγχοι εφαρμόζονται σωστά, λειτουργούν όπως θα έπρεπε, και παράγουν το επιθυμητό αποτέλεσμα όσον αφορά τις απαιτήσεις ασφάλειας για το σύστημα.

Μεσίτης νέφους

Δεδομένου ότι το υπολογιστικό νέφος εξελίσσεται, η ολοκλήρωση των υπηρεσιών νέφους μπορεί να είναι αρκετά σύνθετη για να διαχειριστεί από τους καταναλωτές νέφους. Ένας καταναλωτής νέφους μπορεί να ζητήσει τις υπηρεσίες νέφους από έναν μεσίτη νέφους, αντί να έρθει σε επαφή με έναν προμηθευτή νέφους άμεσα. Ένας μεσίτης νέφους είναι μια οντότητα που διαχειρίζεται τη χρήση, την απόδοση και την παράδοση των υπηρεσιών νέφους και διαπραγματεύεται τις σχέσεις μεταξύ των παρόχων νέφους και των καταναλωτών νέφους.

Μεταφορέας νέφους

Ένας μεταφορέας νέφους ενεργεί ως μεσάζων που παρέχει τη μεταφορά των υπηρεσιών νέφους μεταξύ παρόχων νέφους και των καταναλωτών νέφους. Οι μεταφορείς νέφους παρέχουν πρόσβαση στους καταναλωτές μέσω του δικτύου, των τηλεπικοινωνιών και

άλλων συσκευών πρόσβασης. Ένας πάροχος νέφους θα υπογράψει SLAs με έναν μεταφορέα νέφους για να παρέχει υπηρεσίες σύμφωνες με το επίπεδο των SLAs που προσφέρονται για να καλύψει τις απαιτήσεις των καταναλωτών, και μπορεί να απαιτήσει από το μεταφορέα νέφους να παρέχει αφιερωμένες και ασφαλείς συνδέσεις μεταξύ των καταναλωτών νέφους και των παρόχων

1.6 Ορισμός του προβλήματος

Με τη ραγδαία αύξηση των υλοποιήσεων σε αρχιτεκτονικές υπολογιστικού νέφους δεν αυξήθηκαν μόνο τα ζητήματα ασφάλειας αλλά και τα προβλήματα λόγω της αλληλεπίδρασης των συστημάτων μεταξύ φορέων που διέπονται από διαφορετικά κανονιστικά πλαίσια λειτουργίας, μεταξύ χωρών με διαφορετικά νομικά πλαίσια και μεταξύ διαφορετικών θεσμικών παραγόντων. Επιπλέον δημιουργήθηκαν προβλήματα που προέρχονται από πολιτικοοικονομικά και κοινωνικά ζητήματα όπως η έλλειψη ελέγχου και ελευθερίας έκφρασης και ζητήματα εμπιστοσύνης, ιδιωτικότητας και ηθικής

Λόγω των παραπάνω δημιουργήθηκαν διάφορα ερωτήματα που πρέπει να απαντηθούν . Για παράδειγμα τι σημαίνει αν τα δεδομένα του χρήστη βρίσκονται σε πάνω από μία χώρες; Τι νομικό καθεστώς ισχύει σε κάθε χώρα; Πρέπει εκ των προτέρων να υπάρχει συναίνεση από τον οργανισμό ή την εταιρία για την τοποθεσία των δεδομένων του; Ένα άλλο ερώτημα είναι τι συμβαίνει αν εταιρία και πάροχος έχουν διαφορετική νομοθεσία; Επίσης ο πάροχος γίνεται να μην είναι σε θέση να προσφέρει υπηρεσίες όπως παροχή στοιχείων για να διερευνηθεί μία υπόθεση ή να αρνηθεί να το κάνει για να προστατεύσει τα δεδομένα των άλλων πελατών του ή γιατί δεν του το επιβάλλει η τοπική νομοθεσία. Άλλο ένα ερώτημα είναι η περίοδος διατήρησης των δεδομένων που διαφέρει ανά χώρα. Ένα άλλο ζήτημα είναι η εξασφάλιση της πρόσβασης των πελατών (το αντικείμενο των δεδομένων) σε δεδομένα που τους αφορούν. Τι συμβαίνει όταν αλλάζει η γεωπολιτική στρατηγική δυο χωρών οι οποίες έχουν πρόσβαση σε κέντρα δεδομένων μεταξύ τους; Τέλος τι συμβαίνει στην Ευρωπαϊκή Ένωση και σε τι επίπεδο έχουν αναπτυχθεί υποδομές του υπολογιστικού νέφους; Υπάρχει Ευρωπαϊκή Ένωση δυο ταχυτήτων σε ανάπτυξη έργων με χρήση υπολογιστικού νέφους;

Η μη λήψη μέτρων για την αντιμετώπιση των συμβάντων και των παραπάνω απαντήσεων θα μπορούσε να αποτελέσει πλήγμα στην εμπιστοσύνη των πολιτών προς στις κυβερνητικές ηλεκτρονικές υπηρεσίες υπολογιστικών νεφών. επομένως για τον εκδημοκρατισμό των καναλιών επικοινωνίας.

1.7 Δομή Διατριβής

Στο πρώτο κεφάλαιο όπως είδαμε, πραγματοποιήθηκε μια σύντομη εισαγωγή για το υπολογιστικό νέφος, τα χαρακτηριστικά του και τα είδη χρηστών που υπάρχουν. Επιπλέον θέσαμε τα προβλήματα που έχουν δημιουργηθεί από τη χρήση υποδομών του νέφους. Στο δεύτερο κεφάλαιο παρουσιάζονται διάφορες δράσεις της Ευρωπαϊκής Ένωσης που αφορούν το υπολογιστικό νέφος όπως η στρατηγική Ευρώπη 2020, ο Ορίζοντας 2020 και το Ψηφιακό Θεματολόγιο. Στο τρίτο κεφάλαιο έχει ως στόχο να παρουσιάσει το νομικό πλαίσιο της Ευρωπαϊκής Ένωσης που διέπει το υπολογιστικό νέφος σε ζητήματα όπως η διεθνής διαβίβαση δεδομένων. Στο τέταρτο κεφάλαιο γίνεται εκτενής αναφορά στο υπάρχον κανονιστικό πλαίσιο 3 χώρων (Ιταλία, Ηνωμένο Βασίλειο και Δανία) της Ευρωπαϊκής Ένωσης και σε έργα υποδομής και χρήσης υπολογιστικού νέφους στις χώρες αυτές. Τέλος το πέμπτο κεφάλαιο αφόρα τα κοινωνικοπολιτικά και ηθικά ζητήματα που έχουν προκύψει από την χρήση υπολογιστικού νέφους.

ΚΕΦΑΛΑΙΟ 2: Δράσεις Ευρωπαϊκής Ένωσης

Ο τομέας των ΤΠΕ έχει αλλάξει δραστικά από το 2001 και τα αποτελέσματα αυτών των αλλαγών έχουν επηρεάσει σημαντικά τις οικονομίες και τις κοινωνίες των χωρών. Το υπολογιστικό νέφος αναδεικνύονται σε βασικό καταλύτη των ΤΠΕ. Οι μεγάλοι οργανισμοί και οι κυβερνήσεις μεταφέρουν σταδιακά τα συστήματα τους σε συστήματα νέφους, ενώ ταυτόχρονα όλοι οι εμπλεκόμενοι αναπτύσσουν ενιαία πρότυπα για τη γρήγορη διάδοση των υπηρεσιών νέφους. Η συγκεκριμένη τεχνολογία έχει άμεση σχέση με την ανάγκη της Ευρωπαϊκής Ένωσης για αύξηση του ανταγωνισμού της επιχειρηματικότητας αλλά και της απασχόλησης. Σύμφωνα με τη Ευρωπαϊκή Ένωση το υπολογιστικό νέφος θα γίνει καταλύτης της εθνικής και περιφερειακής ανταγωνιστικότητας ενώ η στρατηγική που θα ακολουθηθεί θα οδηγήσει σε καθαρό ετήσιο κέρδος 160 δισεκατομμύρια € του ΑΕΠ της ΕΕ κατά το 2020. Σε αυτό συντελεί η στρατηγική Ευρώπη 2020 της Ευρωπαϊκής Επιτροπής και συγκεκριμένα το Ψηφιακό Θεματολόγιο.

2.1 Ευρώπη 2020

Η Ευρωπαϊκή Επιτροπή δρομολόγησε τον Μάρτιο 2010 [2] την αντικατάσταση της στρατηγικής της **Λισαβόνας** του 2000 με τη **στρατηγική Ευρώπη 2020**, για έξοδο από την κρίση και προετοιμασία της οικονομίας της Ένωσης για τις προκλήσεις της επόμενης δεκαετίας. Ο στόχος της στρατηγικής είναι η επίτευξη υψηλών επιπέδων απασχόλησης, παραγωγικότητας και κοινωνικής συνοχής, που θα υλοποιηθούν μέσω συγκεκριμένων δράσεων σε ευρωπαϊκό και εθνικό επίπεδο. Η ανάγκη για την οικονομική ενίσχυση και την απασχόληση απαιτεί κινητοποίηση από όλους τους φορείς στην Ευρώπη. Η Ευρωπαϊκή Επιτροπή προσδιορίζει τρεις κύριους μοχλούς ανάπτυξης, οι οποίοι θα υλοποιηθούν με συγκεκριμένες δράσεις σε επίπεδο ΕΕ και κρατών μελών:

- **έξυπνη ανάπτυξη** (προώθηση της γνώσης, της καινοτομίας, της εκπαίδευσης και της ψηφιακής κοινωνίας),
- **βιώσιμη ανάπτυξη** (βελτίωση της αποτελεσματικής χρήσης των πόρων στο πλαίσιο της παραγωγικής διαδικασίας και ενίσχυση της ανταγωνιστικότητάς μας)

- **ανάπτυξη χωρίς αποκλεισμούς** (αύξηση της συμμετοχής στην αγορά εργασίας και ενίσχυση της απόκτησης δεξιοτήτων και της καταπολέμησης της φτώχειας).

2.1.1 Στόχοι και εμβληματικές πρωτοβουλίες

Η Στρατηγική έθεσε πέντε πρωταρχικούς στόχους (targets) με ορίζοντα το 2020:

1. Αύξηση του ποσοστού απασχόλησης του πληθυσμού ηλικίας 20 έως 64 ετών σε 75%,
2. Αύξηση του επιπέδου επενδύσεων σε 3 % του ΑΕΠ στον τομέα της Έρευνας & Ανάπτυξης,
3. Μείωση των εκπομπών αερίων του θερμοκηπίου κατά 20% σε σχέση με το 1990 (ή και 30%, υπό τον όρο ότι και άλλες ανεπτυγμένες χώρες θα δεσμευθούν για ανάλογες μειώσεις και ότι οι αναπτυσσόμενες χώρες θα συμβάλουν επαρκώς, ανάλογα με τις ευθύνες και τις αντίστοιχες δυνατότητές τους), αύξηση κατά 20% του ποσοστού των ανανεώσιμων πηγών ενέργειας, γ. αύξηση κατά 20% της ενεργειακής απόδοσης,
4. Μείωση των ποσοστών πρόωρης εγκατάλειψης της σχολικής εκπαίδευσης σε λιγότερο από 10% και αύξηση του ποσοστού των πτυχιούχων τριτοβάθμιας εκπαίδευσης σε 40 % και
5. Απεγκλωβισμό 20 εκατομμυρίων ανθρώπων από τη φτώχεια, τον κοινωνικό αποκλεισμό.

Για την επίτευξη των στόχων η Επιτροπή πρότεινε 7 εμβληματικές πρωτοβουλίες για την Ε.Ε. όσο και για τα Κράτη-Μέλη οι όποιες είναι *η Ένωση της Καινοτομίας, Νεολαία σε κίνηση, το Ψηφιακό θεματολόγιο για την Ευρώπη, Μια Ευρώπη που χρησιμοποιεί αποτελεσματικά της πόρους της, Μια βιομηχανική πολιτική για την εποχή της παγκοσμιοποίησης, Ατζέντα για νέες δεξιότητες και θέσεις εργασίας και Ατζέντα για νέες δεξιότητες και θέσεις εργασίας*.

Πολλοί από τους άξονες της συγκεκριμένης στρατηγικής θα ωφεληθούν με τη χρήση του υπολογιστικού νέφους. Τα οφέλη του υπολογιστικού νέφους όπως η μείωση του κόστους για την αγορά εξοπλισμού θα βοηθήσει στην τόνωση της ανάπτυξης, της απασχόλησης και την υποστήριξη των μικρομεσαίων επιχειρήσεων ώστε να γίνουν πιο ανταγωνιστικές. Επιπλέον, λόγω της μείωσης των κέντρων δεδομένων θα συμβάλει στη

μετάβαση προς μια ενεργειακά αποδοτική οικονομία με χαμηλές εκπομπές διοξειδίου του άνθρακα.

2.2 Ορίζοντας 2020

Από τα πιο κύρια προγράμματα για τη στρατηγική επένδυση για το υπολογιστικό νέφος είναι ο "Ορίζοντας 2020" [3] της Ε.Ε. για Έρευνα και Καινοτομία (2014 – 2020). Το Πρόγραμμα "Ορίζοντας 2020" ("Horizon 2020") αποτελεί βασικό κορμό της στρατηγικής "Ευρώπη 2020", της Ένωσης Καινοτομίας και του Ευρωπαϊκού Χώρου Έρευνας. Συγκεκριμένα, το πρόγραμμα αποτελεί προσπάθεια για:

- «**Επιστημονική αριστεία**», δηλαδή επιστημονική έρευνα παγκόσμιου επιπέδου που θα οδηγήσει στις τεχνολογίες του μέλλοντος και θα προσελκύσει στην ΕΕ τους καλύτερους επιστήμονες στον κόσμο.
- «**Βιομηχανική υπεροχή**», δηλαδή στρατηγική επένδυση σε τεχνολογίες-κλειδιά όπως η νανοτεχνολογία και το υπολογιστικό νέφος, συμμετοχή του ιδιωτικού τομέα και δημιουργία καινοτόμων μικρομεσαίων επιχειρήσεων υψηλής τεχνολογίας που θα στηρίξουν την ανάπτυξη της ΕΕ
- «**Κοινωνικές προκλήσεις**», δηλαδή στράτευση της επιστημονικής έρευνας για αντιμετώπιση των προκλήσεων όπως είναι η γήρανση του πληθυσμού, η εξάντληση των ενεργειακών πόρων, η αντιμετώπιση της κλιματικής αλλαγής, και η μετατροπή της επιστημονικής γνώσης σε εφαρμοσμένες λύσεις για τα καθημερινά προβλήματα των πολιτών.

2.3 Ψηφιακό Θεματολόγιο

Όπως αναφέραμε παραπάνω μια από τις βασικές δράσεις της ευρωπαϊκής στρατηγικής είναι το **Ψηφιακό Θεματολόγιο (Digital Agenda)** [4]. Το **Ψηφιακό Θεματολόγιο** δραστηριοποιείται στους τομείς του Διαδικτύου και των Τεχνολογιών Πληροφορίας και Επικοινωνιών (ΤΠΕ) ώστε να συμβάλει σε σημαντικό βαθμό στην οικονομική ανάπτυξη της ΕΕ και να επεκτείνει τα οφέλη της ψηφιακής εποχής σε ολόκληρο το κοινωνικό φάσμα.

Στο Ψηφιακό Θεματολόγιο σκιαγράφονται επτά πεδία προτεραιότητας:

- Υλοποίηση της ενιαίας ψηφιακής αγοράς
- Αύξηση της διαλειτουργικότητας και των προτύπων
- Εδραίωση της εμπιστοσύνης και της ασφάλειας στο διαδίκτυο
- Προώθηση της ταχείας και υπερταχείας πρόσβασης στο διαδίκτυο για όλους
- Επένδυση στην έρευνα και την καινοτομία
- Βελτίωση του ψηφιακού γραμματισμού, των δεξιοτήτων και της κοινωνικής ένταξης
- Οφέλη για την κοινωνία χάρη στην έξυπνη αξιοποίηση της τεχνολογίας.

Για την αύξηση χρήσης των υποδομών του υπολογιστικού νέφους το Ψηφιακό Θεματολόγιο έχει προτείνει τις παρακάτω δράσεις:

- Η Επιτροπή σκοπεύει να προβεί σε επανεξέταση του κανονιστικού πλαισίου της ΕΕ για την προστασία των δεδομένων. Οι online αγορές στην ΕΕ εξακολουθούν να χωρίζονται από φραγμούς που εμποδίζουν την πρόσβαση σε πανευρωπαϊκές υπηρεσίες και περιεχόμενο. Η ευρωπαϊκή διαδικτυακή αγορά πάσχει από έλλειψη εμπιστοσύνης των χρηστών όσον αφορά την ασφάλεια των πληρωμών και την προστασία της ιδιωτικής ζωής.

- Πρέπει να ενισχυθεί περαιτέρω από την ΕΕ η διαλειτουργικότητα μεταξύ εφαρμογών και υπηρεσιών. Για να γίνει αυτό, έχει πρωταρχική σημασία να συνεχίσει η Επιτροπή την αναθεώρηση της ευρωπαϊκής πολιτικής τυποποίησης.

- Η ΕΕ πρέπει να υλοποιήσει δίκτυα πρόσβασης νέας γενιάς τα οποία θα βοηθήσουν στη ανάπτυξη του υπολογιστικού νέφους. Η Επιτροπή σκοπεύει να καταφύγει στα ευρωπαϊκά ταμεία για να χρηματοδοτήσει τις επενδύσεις για τις ευρυζωνικές συνδέσεις.

2.4 Αξιοποίηση των δυνατοτήτων του υπολογιστικού νέφους στην Ευρώπη

Η αύξηση της χρήσης του υπολογιστικού νέφους στην Ευρώπη οδήγησε στην αύξηση των πιέσεων που δημιουργήθηκαν από τα κενά νομικού πλαισίου μέχρι τότε (Πίνακας 2.1). Αυτό είχε ως αποτέλεσμα στις 27 Σεπτεμβρίου 2012, η Ευρωπαϊκή Επιτροπή να δημοσιεύσει στρατηγική για την «Αξιοποίηση των δυνατοτήτων του υπολογιστικού νέφους στην Ευρώπη [5]». Η στρατηγική εκπονήθηκε από μια ομάδα εμπειρογνωμόνων με σκοπό την αύξηση της χρήσης του υπολογιστικού νέφους σε ολόκληρη την οικονομία.

Το έργο της βασίζεται σε άλλες νομοθετικές πρωτοβουλίες που έχουν ήδη αναληφθεί, όπως η πρόταση ευρωπαϊκού δικαίου των πωλήσεων. Η ομάδα έχει ως σκοπό την παροχή βοήθειας στην Επιτροπή προκειμένου να διερευνήσει τρόπους βελτίωσης του νομικού πλαισίου για τις συμβάσεις υπολογιστικού νέφους για καταναλωτές ώστε να ενισχυθεί η εμπιστοσύνη των καταναλωτών στη χρήση συμβάσεων υπολογιστικού νέφους καθώς επίσης και στην τροποποίηση της οδηγίας για την προστασία των δεδομένων της ΕΕ.

Βασικοι χρηστες	**Κίνητρα**	**Παραδείγματα δρασεων**
Προμηθευτές και εταιρειες	Να επιφέρει αλλαγές στις πολιτικές που σχετίζονται με το cloud και τους κανονισμούς της ΕΕ στα κράτη μέλη της για την προώθηση της περιφερειακής ανταγωνιστικότητας , την ανάπτυξη και την καινοτομία.	Η Oracle, Cisco Systems, η SAP , η Apple, η Google και η Microsoft έχουν ασκήσει πίεσεις για τον εξορθολογισμό των κατακερματισμένων εθνικων αρχων προστασίας δεδομένων της ΕΕ. Στις 24 Ιανουαρίου 2011, ο Brad Smith, γενικός σύμβουλος της Microsoft, άσκησε εφεση ενώπιον της Γαλλικής Εθνοσυνέλευσης για τη μείωση των εμποδίων στη χρήση του νέφους. Τον Αύγουστο του 2011, το Ευρωπαϊκό Δίκτυο Τηλεπικοινωνιών Σύνδεσμος Χειριστών (ETNO) το οποίο εκπροσωπεί 41 μεγάλους τηλεπικοινωνιακούς οργανισμούς σε 34 ευρωπαϊκές χώρες, πίεσε για ένα διεθνή πρότυπο για την προστασία της ιδιωτικής ζωής

		και την απλοποίηση των κανόνων που διέπουν τις μεταφορές δεδομένων. Επιπλέον, υποστήριξε ότι τα μέτρα αυτά θα επιτρέψουν σε ευρωπαϊκες εταιρείες να ανταγωνίζονται στο ίδιο επίπεδο με εκείνες στις ΗΠΑ. Τον Ιανουάριο του 2012 , ο Andy Mulholland, CTO της Cap Gemini, εξέφρασε την ανησυχία ότι οι περισσότεροι από τους σημαντικότερους παρόχους στο cloud στην Ευρώπη είναι εταιρείες με έδρα τις ΗΠΑ και υποστήριξε ότι η αναθεώρηση της νομοθεσίας για τα προσωπικά δεδομένα της ΕΕ θα βοηθήσει τις εταιρείες αυτές να πωλούν τις υπηρεσίες τους στους ευρωπαίους χρήστες.
Ακτιβιστές, ομάδες ενδιαφέροντος και εκπροσώποι χρηστών	Διασφάλιση της αξιοπιστίας και της διαθεσιμότητας των υπηρεσιών cloud, καθώς και η θεσπιση ένος υψηλού επιπέδου προστασίας των δεδομένων από τις διάφορες απειλές.	Τον Δεκέμβριο του 2012, το Ευρωπαϊκό Κοινοβούλιο δημοσίευσε μια έκθεση τονίζοντας τη σημασία της έναρξης των διαπραγματεύσεων ΕΕ-ΗΠΑ για προστασίας των προσωπικών δεδομένων στο σύννεφο. Τον Ιανουάριο του 2013, η Gus Hosein , επικεφαλής της βρετανικού ΜΚΟ Διεθνής Προστασίας Προσωπικών Δεδομένων, δήλωσε ότι οι αμερικάνικες μυστικες υπηρεσιες ενδέχεται να έχουν πρόσβαση στα δεδομένα πολιτών της ΕΕ που είναι αποθηκευμένα σε εταιρείες των ΗΠΑ το οποιο μπορει να σημάνει την απώλεια της εθνικής κυριαρχίας των δεδομένων. Στις 25 Ιανουαρίου 2013, Caspar Bowden, πρώην επικεφαλης ασφαλείας της Microsoft, προειδοποίησε κατά τη διάρκεια μιας συζήτησης στην 6η Διεθνη Διάσκεψη για την τεχνολογία, προστασίας προσωπικών δεδομένων και την ιδιωτικότητα (CSDP 13) ότι οι νέες προτάσεις της ΕΕ περί προστασίας των δεδομένων δεν έχουν διατάξεις για την αντιμετώπιση της προστασίας των προσωπικών δεδομένων στο νέφος.
Εθνικές κυβερνήσεις	Πρόληψη της κυριαρχία των πολιτικών για το νέφος της ΕΕ.	Η επιτροπή της Ρουμανίας για τις Τεχνολογίες Πληροφορικής και Επικοινωνιών σε ένα ερωτηματολόγιο τον Οκτ 2012 απευθύνθηκε

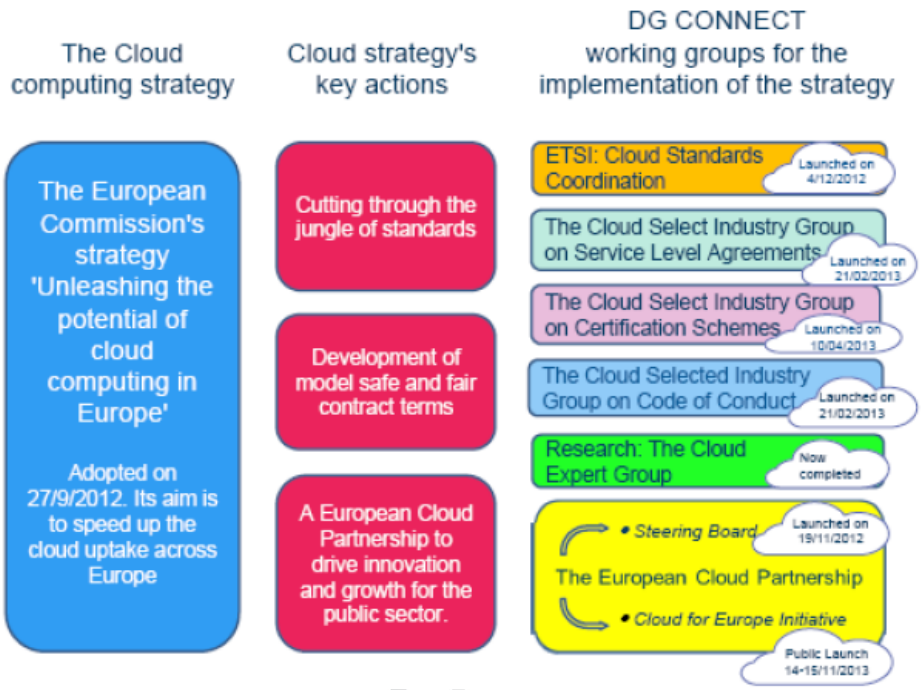
της ΕΕ	Ανταπόκριση στις απαιτήσεις για την εναρμόνιση των νομικών συστημάτων και των μηχανισμών επιβολής της νομοθεσίας με εκείνα των άλλων χωρών μελών της Ευρωπαϊκής Ένωσης.	στα εθνικά κοινοβούλια της ΕΕ, όπου εξέφρασε την άποψη ότι το νέο πλαίσιο προστασίας δεδομένων της ΕΕ θα αυξήσει σημαντικά τις διοικητικές και οικονομικές επιβαρύνσεις για τους υπεύθυνους επεξεργασίας δεδομένων. Η επιτροπή υποστήριξε επίσης ότι ορισμένες από τις προτεινόμενες υποχρεώσεις θα πρέπει να αναλυθούν περαιτέρω για να εξετασθεί η δυνατότητα μείωσης των πρόσθετων επιβαρύνσεων
ΕΕ και άλλοι διεθνείς οργανισμοί	Απάντηση σε πιέσεις από τους προμηθευτές-παρόχους,τους καταναλωτες, ακτιβιστές και άλλους. Παρέχει ένα περιβάλλον που προωθεί την χρήση του cloud computing, συμβάλλοντας έτσι στην οικονομική ανάπτυξη των χωρών μελών. Την εναρμόνιση και την ευθυγράμμιση των νομικών συστημάτων και μηχανισμών επιβολής.	Τον Σεπτέμβριο του 2012, η Ευρωπαϊκή Επιτροπή δημοσίευσε την «Αξιοποίηση των δυνατοτήτων του υπολογιστικού νέφους στην Ευρώπη», μια έκθεση-ορόσημο για την χάραξη μιας νέας στρατηγικής για το cloud computing για την Ευρωπαϊκή Ένωση

Πίνακας 2.1 Βασικές κινητήριες δυνάμεις για τη χάραξη ευρωπαϊκής πολιτικής στο υπολογιστικό νέφος
(*Πηγή: Nir Kshetri San Murugesan " Cloud Computing and EU Data Privacy Regulations" , 2013)*

Οι τρεις κύριες δράσεις (εικόνα 2.1) της στρατηγικής είναι:

- Η δημιουργία και η υποστήριξη σε πρότυπα πιστοποίησης σε πανευρωπαϊκή κλίμακα για αξιόπιστους παρόχους υπολογιστικού νέφους για την αντιμετώπιση των κυκεώνα των προτύπων, ώστε οι χρήστες του υπολογιστικού νέφους να διαθέτουν διαλειτουργικότητα και ακεραιότητα των δεδομένων.
- Η εκπόνηση πρότυπων ασφαλών και δίκαιων συμβατικών όρων για συμβάσεις υπολογιστικού νέφους
- Η συγκρότηση ευρωπαϊκής σύμπραξης για το υπολογιστικό νέφος (ECP), με σκοπό να φέρνει σε επαφή τις δημόσιες αρχές με τις εταιρίες προκειμένου να αναπτύξουν ένα κοινό κανονιστικό πλαίσιο για την αξιοποίηση της αγοραστικής δύναμης του δημόσιου τομέα, για τη διαμόρφωση της ευρωπαϊκής αγοράς

υπολογιστικού νέφους, και την επίτευξη καλύτερης και φτηνότερης ηλεκτρονικής διακυβέρνησης.



Εικόνα 2.1 Η Ευρωπαϊκή στρατηγική για το υπολογιστικό νέφος
(Πηγή: http://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy)

Βασική δράση 1 - Αντιμετώπιση του κυκεώνα των προτύπων

Η πιστοποίηση των υπηρεσιών νέφους ότι πληρούν πρότυπα τα οποία έχουν την έγκριση από ρυθμιστικές αρχές θα συμβάλει στην επιτυχία του υπολογιστικού νέφους ως ένδειξη συμμόρφωσης με τις νομικές υποχρεώσεις. Η ύπαρξη προτύπων στο υπολογιστικό νέφος θα επηρεάσει τους καταναλωτές, τους χρήστες του δημόσιου τομέα καθώς επίσης και τις μικρομεσαίες επιχειρήσεις. Οι χρήστες δεν είναι σε θέση να αξιολογήσουν την εκάστοτε υπηρεσία υπολογιστικού νέφους βάσει των ισχυρισμών των προμηθευτών και των παρόχων. Για τον σκοπό αυτό η λήψη ανεξάρτητης και πιστοποίησης είναι αναγκαία. Αυτή τη στιγμή υπάρχουν δυο ινστιτούτα προτύπων.

Το αμερικανικό εθνικό ινστιτούτο προτύπων και τεχνολογίας (NIST), έχει δημοσιεύσει μια σειρά εγγράφων και ορισμών ενώ το Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών Προτύπων (ETSI), έχει συστήσει ομάδα για το υπολογιστικό νέφος προκειμένου να εξετάσει τις ανάγκες τυποποίησης και τη συμμόρφωση με τα πρότυπα διαλειτουργικότητας. Η Επιτροπή πρόκειται: [5]

- *"να προωθήσει έμπιστες και αξιόπιστες προσφορές υπολογιστικού νέφους αναθέτοντας στο ETSI να συντονίσει με τους ενδιαφερόμενους φορείς, με διαφανή και ανοιχτό τρόπο, τον προσδιορισμό, έως το 2013, λεπτομερούς χάρτη των απαραίτητων προτύπων (μεταξύ άλλων για την ασφάλεια, τη διαλειτουργικότητα, τη φορητότητα των δεδομένων και την αντιστρεψιμότητα)".*
- *"να ενισχύσει την εμπιστοσύνη στις υπηρεσίες υπολογιστικού νέφους με αναγνώριση, σε ενωσιακή κλίμακα, τεχνικών προδιαγραφών στο πεδίο των τεχνολογιών πληροφοριών και επικοινωνιών για την προστασία πληροφοριών προσωπικού χαρακτήρα, σύμφωνα με τον νέο κανονισμό για την ευρωπαϊκή τυποποίηση".*
- *"να συνεργαστεί με την υποστήριξη του ENISA και άλλων σχετικών φορέων για να συμβάλουν στην ανάπτυξη, σε ενωσιακή κλίμακα, εθελοντικών συστημάτων πιστοποίησης στο πεδίο του υπολογιστικού νέφους (συμπεριλαμβανομένης της προστασίας των δεδομένων) και στην κατάρτιση καταλόγου των εν λόγω συστημάτων έως το 2014".*
- *"να αντιμετωπίσει τις περιβαλλοντικές προκλήσεις από την αυξημένη χρήση υπολογιστικού νέφους μέσω συμφωνίας - με τη βιομηχανία – εναρμονισμένων μετρήσεων για την κατανάλωση ενέργειας, την κατανάλωση νερού και τις εκπομπές διοξειδίου του άνθρακα των υπηρεσιών υπολογιστικού νέφους, έως το 2014."*

Βασική δράση 2: Ασφαλείς και δίκαιοι συμβατικοί όροι και προϋποθέσεις

Οι συμβάσεις υπολογιστικού νέφους είναι ιδιαίτερα σημαντικές γιατί αφορούν πολλά είδη χρηστών. Ωστόσο η τωρινή κατάσταση δημιουργεί αβεβαιότητα στον χρήστη εξαιτίας ελλιπώς διατυπωμένων συμβάσεων με τους παρόχους υπολογιστικού νέφους. Η πολυπλοκότητα του νομικού πλαισίου για παρόχους υπηρεσιών νέφους συνεπάγεται ότι συχνά χρησιμοποιούν πολύπλοκες συμβάσεις ή συμφωνίες για το επίπεδο των παρεχόμενων υπηρεσιών. Οι συμβάσεις αυτές ενδέχεται να έχουν ανεπαρκείς όρους όπως την ανάκτηση δεδομένων, ευθύνη για την ακεραιότητα της ροής των δεδομένων, το απόρρητο και την αδιάλειπτη παροχή των υπηρεσιών.

Οι συμφωνίες επιπέδου υπηρεσιών καθορίζουν τη σχέση μεταξύ του παρόχου υπολογιστικού νέφους και των επαγγελματικών χρηστών, και έτσι παρέχουν ουσιαστικά τη βάση της εμπιστοσύνης που μπορούν να έχουν οι χρήστες στην

ικανότητα ενός παρόχου υπηρεσιών υπολογιστικού νέφους για παροχή υπηρεσιών. Μολονότι η υφιστάμενη νομοθεσία της ΕΕ προστατεύει τους χρήστες των υπηρεσιών υπολογιστικού νέφους, οι καταναλωτές συχνά δεν γνωρίζουν τα σχετικά δικαιώματά τους, ιδίως του εφαρμοστέου δικαίου και της διεθνούς δικαιοδοσίας. Οι προτάσεις της Ευρωπαϊκής Επιτροπής για τη θέσπιση ενός κοινού ευρωπαϊκού δίκαιου των πωλήσεων αποσκοπεί στον προσδιορισμό ασφαλών και δίκαιων συμβατικών όρων και προϋποθέσεων μεταξύ παρόχων υπηρεσιών υπολογιστικού νέφους και καταναλωτών. Επίσης η μεταρρύθμιση του καθεστώτος προστασίας δεδομένων θα διασφαλίσει τη βιωσιμότητα και την καταλληλότητα των κανόνων για την προστασία των δεδομένων, θα δημιουργήσει ένα πλαίσιο που θα βοηθήσει στην ανάπτυξη των υπηρεσιών υπολογιστικού νέφους και θα συμβάλει ώστε οι καταναλωτές να επωφεληθούν πλήρως από την ανάπτυξη των ψηφιακών υπηρεσιών και του υπολογιστικού νέφους.

Η Επιτροπή πρόκειται, έως το τέλος του 2013: [5]

- *"Να εκπονήσει, με τα ενδιαφερόμενα μέρη, πρότυπους όρους όσον αφορά τις συμφωνίες για το επίπεδο υπηρεσιών υπολογιστικού νέφους για συμβάσεις μεταξύ των παρόχων και των επαγγελματικών χρηστών υπολογιστικού νέφους, συνεκτιμώντας την ανάπτυξη του κεκτημένου της ΕΕ στο εν λόγω πεδίο"*.

- *"Σύμφωνα με την ανακοίνωση σχετικά με ένα κοινό ευρωπαϊκό δίκαιο των πωλήσεων, να προτείνει στους καταναλωτές και στις μικρές επιχειρήσεις ευρωπαϊκούς πρότυπους συμβατικούς όρους και προϋποθέσεις για τα θέματα που εμπίπτουν στο πεδίο της πρότασης για κοινό ευρωπαϊκό δίκαιο των πωλήσεων. Στόχος είναι να τυποποιηθούν οι βασικοί συμβατικοί όροι και προϋποθέσεις, η παροχή συμβατικών όρων βέλτιστης πρακτικής για την παροχή υπηρεσιών υπολογιστικού νέφους για τις πτυχές που σχετίζονται με την προμήθεια «ψηφιακού περιεχομένου»"*.

- *"Να αναθέσει σε ομάδα εμπειρογνωμόνων που θα συσταθεί επί ταυτού, συμπεριλαμβανομένου του κλάδου, να προσδιορίσει πριν από το τέλος του 2013, ασφαλείς και δίκαιους συμβατικούς όρους και προϋποθέσεις για τους καταναλωτές και τις μικρές επιχειρήσεις, και - με βάση παρόμοια προσέγγιση προαιρετικού*

εργαλείου - για τα συναφή με το νέφος θέματα πέραν του κοινού ευρωπαϊκού δικαίου των πωλήσεων. Να διευκολύνει τη συμμετοχή της Ευρώπης στην παγκόσμια ανάπτυξη του υπολογιστικού νέφους: με αναθεώρηση τυποποιημένων συμβατικών ρητρών που ισχύουν για τη μεταφορά δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες και την προσαρμογή τους, όπως απαιτείται, για υπηρεσίες υπολογιστικού νέφους. Καθώς και να καλέσει τις εθνικές αρχές προστασίας των δεδομένων να εγκρίνουν δεσμευτικούς εταιρικούς κανόνες για τους παρόχους υπολογιστικού νέφους".

- *"Να συνεργαστούν με τον κλάδο για να συμφωνήσουν σε έναν κώδικα δεοντολογίας για παρόχους υπολογιστικού νέφους με σκοπό την υποστήριξη ομοιόμορφης εφαρμογής των κανόνων προστασίας των δεδομένων που μπορεί να υποβληθεί στην ομάδα του άρθρου 29 για έγκριση, προκειμένου να εξασφαλιστεί η ασφάλεια δικαίου και η συνοχή μεταξύ του κώδικα δεοντολογίας και της ενωσιακής νομοθεσίας."*

Βασική δράση 3 – Προαγωγή πρωταγωνιστικού ρόλου του δημοσίου τομέα μέσω ευρωπαϊκής σύμπραξης για το υπολογιστικό νέφος

Ο δημόσιος τομέας είναι ο μεγαλύτερος καταναλωτής των υπηρεσιών ΤΠΕ στην ΕΕ. Αυτό του δίνει τη δυνατότητα να έχει ισχυρό ρόλο στη διαμόρφωση της αγοράς του υπολογιστικού νέφους. Επίσης μπορεί να καθορίσει τις απαιτήσεις για τα χαρακτηριστικά, τις επιδόσεις, την ασφάλεια, τη διαλειτουργικότητα και τη φορητότητα των δεδομένων, καθώς τη συμμόρφωση με τις τεχνικές απαιτήσεις και να καθορίσει απαιτήσεις για την πιστοποίηση.

Αρκετά κράτη μέλη έχουν δρομολογήσει εθνικές στρατηγικές, όπως η Andromède[4] στη Γαλλία και η GCloud στο Ηνωμένο Βασίλειο. Η ομαδοποίηση των δημόσιων απαιτήσεων θα μπορούσε να επιφέρει αύξηση της αποδοτικότητας ενώ θα μπορούσε να μειωθεί το κόστος και να καταστήσουν δυνατή τη διαλειτουργικότητα. Ο ιδιωτικός τομέας θα επωφεληθεί επίσης από υπηρεσίες υψηλότερης ποιότητας, περισσότερο ανταγωνισμό, ταχεία τυποποίηση καθώς και θα δοθούν ευκαιρίες στην αγορά για μικρομεσαίες επιχειρήσεις. Η Επιτροπή δημιούργησε την ευρωπαϊκή σύμπραξη για το

[4] http://www.challenges.fr/high-tech/20120421.ZDN6981/cloud-andromede-orange-et-thales-se-felicitent-et-se-disent-prets-a-demarrer.html

υπολογιστικό νέφος (ECP) προκειμένου να στεγάσει παρόμοιες πρωτοβουλίες σε επίπεδο κρατών μελών.

Η ευρωπαϊκή σύμπραξη για το υπολογιστικό νέφος (ECP) είναι αρμόδια για τις προμήθειες δημοσίων ευρωπαϊκών φορέων και καθοριστικής σημασίας παράγοντες του κλάδου της ΤΠ και των τηλεπικοινωνιών. Οι κύριες αποστολές [5] του διοικητικού συμβουλίου περιλαμβάνει:

- *Την σύναψη συμβάσεων που θα προωθηθούν από τα συμμετέχοντα κράτη μέλη και τις δημόσιες αρχές προς χρήση σε όλη την ΕΕ, στόχος της είναι να διασφαλίσει ότι η εμπορική προσφορά στην Ευρώπη είναι προσαρμοσμένη στις ευρωπαϊκές ανάγκες.*

- *Τη συγκέντρωση τεχνογνωσίας του κλάδου και των χρηστών για την σύναψη συμβάσεων για το υπολογιστικό νέφος με ανοιχτό και πλήρως διαφανή τρόπο*

- *Την αποφυγή κατακερματισμού και τη διασφάλιση ασφαλούς και πράσινης δημόσιας χρήσης του υπολογιστικού νέφους, σε πλήρη ευθυγράμμιση με τους ευρωπαϊκούς κανόνες*

- *Την παροχή βοήθειας σχετικά με τις στρατηγικές προτεραιότητες ώστε να καταστεί το υπολογιστικό νέφος κινητήρια δύναμη για την οικονομική ανάπτυξη*

- *Τη διατύπωση συστάσεων για την ανάπτυξη πολιτικής για ασφαλές και διαλειτουργικό υπολογιστικό νέφος που να συμβάλλει στην ευρωπαϊκή ψηφιακή ενιαία αγορά."*

ΚΕΦΑΛΑΙΟ 3: Νομικό πλαίσιο χωρών Ευρωπαϊκής Ένωσης

Η ραγδαία ανάπτυξη και διάδοση του υπολογιστικού νέφους θέτει διαρκώς και με αυξανόμενη ένταση σε δοκιμασία τη ρυθμιστική ικανότητά των νομικών κανόνων ως προς την προστασία των δικαιωμάτων στην πληροφοριακή ιδιωτικότητα. Σε αυτό το κεφάλαιο θα αναλύσουμε το νομικό πλαίσιο. Η αποθήκευση δεδομένων σε πολλούς και διαφορετικούς διακομιστές με διαφορετικές δικαιοδοσίες είναι η κύρια διαφορά μεταξύ του νέφους με άλλες τεχνολογίες. Παρακάτω παραθέτουμε το ήδη υπάρχον νομικό πλαίσιο και τα ζητήματα τα οποία σχετίζονται στην χρήση του υπολογιστικού νέφους και τι ισχύει στην Ευρωπαϊκή Ένωση που βάσει της νέας στρατηγικής της Ευρωπαϊκής επιτροπής θα πρέπει να αλλάξει.

3.1 Το πλαίσιο προστασίας των δεδομένων

Από τις βασικές αρχές της γενικής οδηγίας για την προστασία των δεδομένων, είναι η οδηγία 95/46/ΕΚ [6] ,που ισχύει για τους υπεύθυνους της επεξεργασίας και τους εκτελούντες την επεξεργασία, όπως, τη διαγραφή δεδομένων και τα τεχνικά και οργανωτικά μέτρα. Οι κανόνες της ΕΕ για την προστασία των δεδομένων (η οδηγία του 1995 για την προστασία των δεδομένων 95/46/ΕΚ) αποσκοπούν στην προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων και ιδίως του δικαιώματος της προστασίας των δεδομένων, καθώς και της ελεύθερης ροής των δεδομένων.

Αυτή η οδηγία για την προστασία των δεδομένων συμπληρώθηκε από άλλες νομοθετικές πράξεις όπως με την οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες. Το δικαίωμα της προστασίας των δεδομένων προσωπικού χαρακτήρα αναγνωρίζεται από τη συνθήκη της Λισαβόνας και από το άρθρο 8 του Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ. Η συνθήκη προβλέπει τη θέσπιση κανόνων σχετικά με την προστασία των δεδομένων σε όλες τις δραστηριότητες που εμπίπτουν στο πεδίο εφαρμογής του δικαίου της ΕΕ, δυνάμει του άρθρου 16. Το 2009, η Επιτροπή άρχισε να επανεξετάζει το ισχύον νομικό πλαίσιο για την προστασία των δεδομένων, διοργανώνοντας αρχικά διάσκεψη υψηλού επιπέδου τον Μάιο του 2009 και στη συνέχεια δημόσια διαβούλευση που ολοκληρώθηκε στα τέλη του 2009. Καθ' όλη τη

διάρκεια του έτους 2010 οργανώθηκαν διαβουλεύσεις με συγκεκριμένους ενδιαφερόμενους φορείς.

Στην οδηγία 95/46/ΕΚ, υπάρχουν πολλές πτυχές στο θέμα της προστασίας της ιδιωτικής ζωής, πληροφορίες που χρειάζονται προσοχή. Πρώτα απ 'όλα το άρθρο 8 της οδηγίας 95/46/ΕΚ δηλώνει ότι τα προσωπικά δεδομένα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, τη συμμετοχή σε συνδικαλιστικές οργανώσεις και τα δεδομένα που αφορούν την υγεία ή το φύλο πρέπει να προστατεύονται με ορισμένες εξαιρέσεις. Κάθε παραβίαση της ασφάλειας των πληροφοριών πρέπει να αναφέρεται στις αρχές, εάν πιθανόν επηρεάζει αρνητικά κάποιο άτομο, το οποίο στη συνέχεια, θα πρέπει να ενημερώνεται. Στο άρθρο 10-11 της οδηγίας 95/46/ΕΚ αναφέρεται ότι θα πρέπει να γνωρίζει και να ενημερώνεται το πρόσωπο από το οποίο συλλέγονται δεδομένα για τους αποδέκτες των δεδομένων του εκτός από μερικές περιπτώσεις όπως η συλλογή δεδομένων για σκοπούς στατιστικούς ή ιστορικής ή επιστημονικής έρευνας. Σύμφωνα με το άρθρο 25 του 95/46/ΕΚ, τα κράτη μέλη βασικά μπορούν να μεταφέρουν τα δεδομένα προσωπικού χαρακτήρα εκτός της Ευρωπαϊκής Κοινότητας παρά μόνον εάν η τρίτη χώρα έχει επαρκή προστασία των προσωπικών δεδομένων. Σύμφωνα με το άρθρο 29 της Οδηγίας 95/46/ΕΚ δημιουργήθηκε η "Ομάδα προστασίας των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα", γνωστή και ως "Ομάδα του Άρθρου 29", για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Η Ομάδα έχει συμβουλευτικό χαρακτήρα ως προς την Ευρωπαϊκή Επιτροπή αλλά είναι ανεξάρτητη ως προς αυτήν. Η εξέταση των θεμάτων γίνεται είτε μετά από αίτηση της Ευρωπαϊκής Επιτροπής είτε με πρόταση των μελών της Ομάδας. Η Ομάδα εκδίδει γνωμοδοτήσεις και κείμενα εργασίας.

Παρά τη θέσπιση της οδηγίας 95/46/ΕΚ κάθε κράτος μέλος της ΕΕ έχει δημιουργήσει ανομοιογένεια όσον αφορά την προστασία δεδομένων προσωπικού χαρακτήρα η οποία διαφέρει ανάλογα με το πού διαμένει ένα άτομο ή από πού αγοράζει αγαθά και υπηρεσίες. Παράλληλα πρέπει να εκσυγχρονιστούν οι ισχύοντες κανόνες οι οποίοι θεσπίστηκαν όταν το Διαδίκτυο έκανε ακόμη τα πρώτα του βήματα μιας και η μεταρρύθμιση του καθεστώτος προστασίας δεδομένων θα διασφαλίσει τη βιωσιμότητα και την καταλληλότητα των κανόνων μας για την ψηφιακή εποχή.

3.2 Εφαρμοστέο Δίκαιο

Η συμμόρφωση της προστασίας δεδομένων, ιδίως τα προσωπικά δεδομένα, υπήρξε αντικείμενο πολλών μελετών. Η οδηγία του Ευρωπαίου Επόπτης Προστασίας Δεδομένων είναι η κύρια νομοθεσία σχετικά με τα προσωπικά δεδομένα. Θα είναι σημαντικό να κατανοήσουμε το νομικό ορισμό των προσωπικών δεδομένων, και να καθορίσουμε ποιος είναι υπεύθυνος για την προστασία και την ασφάλεια στο νέφος. Θέματα δικαιοδοσίας είναι στο επίκεντρο οποιασδήποτε νομικής συζήτησης σχετικά με το υπολογιστικό νέφος. Πολλές νομικές διατάξεις, σε πολλές χώρες έχουν εξελιχθεί κατά τα τελευταία 30 με 40 χρόνια προσπαθεί να ασχοληθούν με το ζήτημα της προστασίας των δεδομένων. Τα περισσότερα κράτη του ΕΟΧ έχουν συμμορφωθεί από την οδηγία για την προστασία των δεδομένων της Ευρωπαϊκής Ένωσης το 1995. Από την άλλη πλευρά η Αμερική δεν έχει ενιαία νομοθεσία για την προστασία των δεδομένων συγκρίσιμη με την οδηγία για την προστασία των δεδομένων της Ευρωπαϊκής Ένωσης. Η έλευση του υπολογιστικού νέφους έχει αυξήσει τις ανησυχίες των εταιριών μιας και τα δεδομένα δεν αποθηκεύονται τοπικά. Υπάρχουν πάντα κίνδυνοι για παραβίαση της ασφάλειας είτε από εσωτερικές είτε από εξωτερικές απειλές.

Η Ευρωπαϊκή Οδηγία για την προστασία των δεδομένων έχει σοβαρές συνέπειες για τους παρόχους του νέφους εντός Ευρωπαϊκού Οικονομικού Χώρου (ΕΟΧ), γι 'αυτό είναι πολύ σημαντικό να καθοριστεί τι σημαίνει «προσωπικά δεδομένα». Η Οδηγία ισχύει μόνο για προσωπικά δεδομένα και ορίζει ως « δεδομένα προσωπικού χαρακτήρα»**:**

"κάθε πληροφορία που αναφέρεται σε φυσικό πρόσωπο του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί «το πρόσωπο στο οποίο αναφέρονται τα δεδομένα» ως πρόσωπο του οποίου η ταυτότητα μπορεί να εξακριβωθεί λογίζεται το πρόσωπο εκείνο που μπορεί να προσδιοριστεί, άμεσα ή έμμεσα, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός ή περισσοτέρων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από φυσική, βιολογική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική άποψη"

Οι πάροχοι του νέφους πρέπει να τηρούν όλα τα κατάλληλα μέτρα και είναι σε θέση να εξασφαλίσουν την προστασία των προσωπικών δεδομένων. Υπάρχει όμως ενα πεδίο της οδηγίας, που ο πάροχος του νέφους μπορεί να καταστήσει τα δεδομένα «μη

προσωπικά» και επομένως να αποφύγει να υπόκεινται στις απαιτήσεις προστασίας των δεδομένων. Μια τέτοια περίπτωση είναι όταν τα δεδομένα δεν μπορούν να θεωρηθούν ότι αναφέρονται σε κάποιο άτομο ή όταν δεν μπορεί να θεωρηθεί ότι η ταυτότητα του ατόμου είναι γνωστή ή μπορεί να εξακριβωθεί. Όταν οι υπό επεξεργασία πληροφορίες δεν εμπίπτουν στην έννοια των «δεδομένων προσωπικού χαρακτήρα», τότε η οδηγία για την προστασία των προσωπικών δεδομένων δεν εφαρμόζεται. Σε αυτή την περίπτωση μπορεί να είναι εφαρμοστέα η εθνική νομοθεσία για την προστασία δεδομένων. Μια τέτοια περίπτωση μπορεί να είναι π.χ. η περίπτωση των κωδικοποιημένων δεδομένων, άσχετα με το αν είναι ή όχι δεδομένα προσωπικού χαρακτήρα.

Σύμφωνα με το δίκαιο της Ευρωπαϊκής Ένωσης την προστασία των δεδομένων, την ευθύνη για τα προσωπικά δεδομένα επιβάλλεται στον «υπεύθυνο της επεξεργασίας», ο οποίος μπορεί να χρησιμοποιεί «επεξεργαστές δεδομένων», για την επεξεργασία των δεδομένων για λογαριασμό του. Από τη σκοπιά του νέφους, το « υπεύθυνος της επεξεργασίας» κατά κύριο λόγο, παραμένει ο φορέας που ωφελείται από την υπηρεσία cloud, και ο πάροχος θεωρείται ως «επεξεργαστής δεδομένων». Αυτό σημαίνει ότι πλήρης ευθύνη για την προστασία των δεδομένων συνήθως βρίσκεται εξ ολοκλήρου στην εταιρία ή οργανισμός που χρησιμοποιεί την υπηρεσία νέφους. Το γεγονός αυτό αναδεικνύει ακόμη περισσότερο τη σημασία των συμφωνητικό παροχής υπηρεσιών (SLA) μεταξύ των πελατών και των προμηθευτών νέφους.

3.3 Δικαιοδοσία

Η δικαιοδοσία επί των δραστηριοτήτων στο Διαδίκτυο έχει γίνει ένα από τα κύρια πεδία μάχης για τον αγώνα για την εδραίωση του κράτους δικαίου στην Κοινωνία της Πληροφορίας. Η Οδηγία είχε προβλέψει την έννοια της απομακρυσμένης επεξεργασίας των δεδομένων όπου η επεξεργαστής είναι εγκατεστημένος σε άλλη χώρα και δεν περιέχει διατάξεις σχετικά με το εφαρμοστέο δίκαιο και τη δικαιοδοσία του.

Σύμφωνα με το άρθρο 4 της Οδηγίας 95/46/ΕΚ τρεις λόγοι για την εφαρμογή των κανόνων της Ευρωπαϊκής Ένωσης σε πράξη της επεξεργασίας δεδομένων προσωπικού χαρακτήρα είναι:

1. **Εγκατάσταση** - Σύμφωνα με το άρθρο 4 (1) (α) κάθε κράτος μέλος του ΕΟΧ πρέπει να εφαρμόζει την οδηγία όπως εφαρμόζεται στο εν λόγω κράτος μέλος, εάν *"επεξεργασία εκτελείται στα πλαίσια των δραστηριοτήτων υπευθύνου εγκατεστημένου στο έδαφος του κράτους μέλους*". Αυτό σημαίνει ότι, εάν ο υπεύθυνος της επεξεργασίας είναι εγκατεστημένος στο έδαφος περισσότερων του ενός κρατών μελών και προβαίνει σε επεξεργασία των δεδομένων στο πλαίσιο των δραστηριοτήτων του στις χώρες αυτές, τότε εφαρμόζεται το δίκαιο καθενός εκ των κρατών μελών στο οποίο λαμβάνει χώρα η εν λόγω επεξεργασία.

2. **Διεθνές δίκαιο** - άρθρο 4 (1) (β) προβλέπει ότι η προστασία των δεδομένων ενός κράτους μέλους δίκαιο εφαρμόζεται "*όταν ο υπεύθυνος δεν είναι εγκατεστημένος στο έδαφος του κράτους μέλους, αλλά σε τόπο όπου εφαρμόζεται η εθνική του νομοθεσία δυνάμει του δημοσίου διεθνούς*".

3. **Εξοπλισμός** - Το άρθρο 4 παράγραφος 1 γ) αναφέρεται στον τρόπο εφαρμογής της νομοθεσίας περί προστασίας των δεδομένων στους υπεύθυνους της επεξεργασίας που δεν είναι μεν εγκατεστημένοι στον ΕΟΧ, αλλά χρησιμοποιούν μέσα, αυτοματοποιημένα ή όχι, ευρισκόμενα στο έδαφος κράτους μέλους, εκτός εάν τα μέσα αυτά χρησιμοποιούνται μόνο με σκοπό τη διέλευση. Αυτό σημαίνει ότι εάν κάποιος πελάτης υπηρεσιών νέφους είναι εγκατεστημένος εκτός του ΕΟΧ αλλά έχει προσλάβει πάροχο υπηρεσιών νεφοϋπολογιστικής εγκατεστημένο εντός του ΕΟΧ, η νομοθεσία περί προστασίας των δεδομένων που διέπει τον πάροχο επεκτείνεται και στον πελάτη.

3.4 Διεθνής διαβίβαση δεδομένων

Μια από τις βασικές αρχές της Οδηγίας είναι ότι τα κράτη – μέλη πρέπει να προνοούν για την μεταφορά των προσωπικών δεδομένων, που υποβάλλονται σε επεξεργασία ή που προορίζονται για επεξεργασία σε μια τρίτη χώρα, μόνο αν η μεταφορά αυτών θα πραγματοποιηθεί χωρίς προκατάληψη στο να συμμορφωθεί ανάλογα με τους εθνικούς όρους, οι οποίοι υιοθετούνται σύμφωνα με άλλους όρους της οδηγίας, η εν λόγω τρίτη χώρα εγγυάται ένα επαρκές επίπεδο προστασίας.

Αυτό εφαρμόζεται εφόσον διατηρούνται δεδομένα εντός της ίδιας οντότητας ή εφόσον η εξαγωγή είναι σε μια εταιρία του ίδιου ομίλου της χώρας ή σε τρίτο πρόσωπο/ εταιρία στην εν λόγω χώρα. Ο συγκεκριμένος όρος αυτός είχε ως στόχο να θέσει τις τρίτες

χώρες υπό κάποια πίεση, ούτως ώστε να υιοθετήσουν τα πρότυπα προστασίας δεδομένων παρόμοια με εκείνων της ΕΟΧ.

Σύμφωνα με την Οδηγία η εξαγωγή ή η μεταφορά δεδομένων εξακολουθεί να αποτελεί «επεξεργασία», για την οποία απαιτείται μια νομική αιτιολόγηση με τον συνήθη τρόπο. Για παράδειγμα το υποκείμενο των δεδομένων τίθεται υπό επεξεργασία, ακόμα και όταν η εξαγωγή επιτρέπεται βάσει του άρθρου 25 ή του άρθρου 26. Η Ευρωπαϊκή Επιτροπή έχει δηλώσει ότι ορισμένες χώρες παρέχουν τέτοια επαρκή προστασία, που έχει ως συνέπεια τα προσωπικά δεδομένα να μπορούν να εξαχθούν ελεύθερα στις εν λόγω χώρες. Έως τώρα μόνο λίγες χώρες από τις οποίες κάποιες είναι μικρές περιοχές της Ευρώπης έχουν δηλωθεί για να εξασφαλίσουν ένα επαρκές επίπεδο με αυτόν τον τρόπο: Ανδόρα, Αργεντινή, Καναδάς, Ελβετία, Φερόες Νήσοι, Γκέρνσεϊ, Ισραήλ. Η Γαλλία, η Πορτογαλία και η Ισπανία επιτρέπουν στην εθνική αρχή προστασίας δεδομένων να κάνει τις δικές τους διαπιστώσεις επάρκειάς τους, καθώς και στο Βέλγιο, την Ολλανδία, τη Σουηδία, το Υπουργείο Δικαιοσύνης ή η κυβέρνηση μπορούν εξίσου να το πράξουν, αλλά αυτές οι διαπιστώσεις είναι σπάνιες. Στην πράξη, τα Κράτη - Μέλη απλώς επιβεβαιώνουν τοπικά ευρήματα επάρκειας της Ευρωπαϊκής Επιτροπής και ποτέ δεν έχουν εκδοθεί πορίσματα επάρκειας για τις χώρες που δεν έχουν ήδη κριθεί επαρκείς από την Επιτροπή.

Στην ουσία η Οδηγία απαγορεύει την εξαγωγή των προσωπικών δεδομένων από τον ΕΟΧ προς τρίτες χώρες εκτός εάν ισχύουν εξαιρέσεις ή ειδικές ρυθμίσεις για τη διασφάλιση της επάρκειας. Η ουσία των πολλών ρυθμίσεων του υπολογιστικού νέφους είναι η εξ' αποστάσεως αποθήκευση δεδομένων και η επεξεργασία των δεδομένων με τέτοιο τρόπο ώστε η γεωγραφική θέση των δεδομένων και / ή οι λειτουργίες των δεδομένων να μπορούν να αλλάξουν και εύκολα να αναπαραχθούν σε άλλες χώρες, συμπεριλαμβανομένων των χωρών εκτός του ΕΕ. Ως εκ τούτου, οι κανόνες για την εξαγωγή στατιστικών στοιχείων έχουν δημιουργήσει σημαντικές προκλήσεις για το υπολογιστικό νέφος, οι οποίες από την φύση τους βασίζονται στη μεταφορά δεδομένων από τον χρήστη στο νέφος (και αντίστροφα), και την αυτοματοποιημένη μεταφορά δεδομένων μέσα στο νέφος.

Συνδυάζοντας τις δικαιοδοτικές διατάξεις με τις διατάξεις για την εξαγωγή των δεδομένων μπορεί να σημαίνει ότι ένας πάροχος νέφους χωρίς ένταξη στον ΕΟΧ μπορεί, ωστόσο, να υπόκειται στο καθεστώς εξαγωγής δεδομένων της ΕΕ όταν

προσπαθεί να μεταφέρει δεδομένα από τον ΕΟΧ προς τόπου ένταξής του ή σε κάποια άλλη θέση εκτός του ΕΟΧ, ακόμη και αν τα δεδομένα που συλλέχθηκαν αρχικά εκτός του ΕΟΧ, αφορούν άτομα εκτός του ΕΟΧ.

Αυτό μπορεί να έχει ως αποτέλεσμα η Οδηγία να εμποδίζει τους παρόχους υπηρεσιών υπολογιστικού νέφους εκτός ΕΟΧ να προσφέρουν τις υπηρεσίες τους εξ αποστάσεως σε χρήστες εντός του ΕΟΧ. εκτός εάν ο πάροχος πληροί τις απαιτήσεις της σχετικής εθνικής εφαρμογής, ή αν ισχύει κάποια εξαίρεση. Θέτει επίσης σοβαρά ζητήματα σχετικά με την εκτέλεση των νόμων προστασίας δεδομένων της ΕΕ στην πράξη. Για παράδειγμα, ένας πάροχος cloud με έδρα τις ΗΠΑ προσφέρει εξ' αποστάσεως αποθήκευση και επεξεργασία των φωτογραφιών στο cloud με κέντρα δεδομένων που βασίζονται σε διάφορες τοποθεσίες των ΗΠΑ, δεν θα μπορεί να προσφέρουν αυτή την υπηρεσία στους εντός του ΕΟΧ χρήστες (εκτός εάν ισχύουν εξαιρέσεις / ειδικές ρυθμίσεις). Ωστόσο, είναι δύσκολο να δούμε ποια εθνική αρχή προστασίας δεδομένων του ΕΟΧ θα κάνει την επιβολή του νόμου κατά του εν λόγω εξ' αποστάσεως παρόχου cloud στις ΗΠΑ.

Υπάρχουν τρεις μέθοδοι, για μια μη ευρωπαϊκή οντότητα («τρίτη χώρα») για να μπορεί να υποστηρίζει και να έχει επαρκή προστασία σύμφωνα με το άρθρο 25.

- Safe Harbor ή "σφαίρας ασφαλείας"
- Τυποποιημένες συμβατικές ρήτρες
- Δεσμευτικοί εταιρικοί κανόνες (Binding Corporate Rules)

Περαιτέρω, το άρθρο 26 της οδηγίας, επιτρέπει μια σειρά από άλλες εξαιρέσεις, όπως την νόμιμη διαβίβαση δεδομένων προσωπικού χαρακτήρα εκτός Ευρώπης , ακόμη και σε μια «τρίτη χώρα» που αποτυγχάνει να προσφέρει ένα "επαρκές επίπεδο προστασίας".

Ένας υπεύθυνος επεξεργασίας των δεδομένων μπορεί να στείλει νόμιμα προσωπικά δεδομένα εκτός της Ευρώπης προς τις Ηνωμένες Πολιτείες ή προς οποιαδήποτε άλλη χώρα, εφόσον :

- το πρόσωπο στο οποίο αναφέρονται τα δεδομένα έχει συναινέσει ρητώς στη διαβίβαση
- η διαβίβαση είναι αναγκαία για την εκτέλεση σύμβασης μεταξύ του προσώπου στο οποίο αναφέρονται τα δεδομένα και του υπευθύνου επεξεργασίας ή για την εκτέλεση προσυμβατικών μέτρων ληφθέντων κατ' αίτηση του προσώπου αυτού
- η διαβίβαση είναι αναγκαία για τη συνομολόγηση ή την εκτέλεση σύμβασης που έχει συναφθεί ή πρόκειται να συναφθεί μεταξύ του υπευθύνου επεξεργασίας και τρίτου προς το συμφέρον του προσώπου στο οποίο αναφέρονται τα δεδομένα
- η διαβίβαση είναι αναγκαία ή απαιτείται εκ του νόμου για τη διασφάλιση σημαντικού δημοσίου συμφέροντος ή για την αναγνώριση, άσκηση ή υπεράσπιση ενός δικαιώματος ενώπιον του δικαστηρίου
- η διαβίβαση είναι αναγκαία για τη διασφάλιση ζωτικού συμφέροντος του προσώπου στο οποίο αναφέρονται τα δεδομένα
- η διαβίβαση πραγματοποιείται από δημόσιο μητρώο το οποίο προορίζεται βάσει νομοθετικών ή κανονιστικών διατάξεων για την παροχή πληροφοριών στο κοινό και είναι προσιτό είτε στο κοινό γενικά είτε σε οποιοδήποτε πρόσωπο μπορεί να αποδείξει έννομο συμφέρον, εφόσον στη συγκεκριμένη περίπτωση πληρούνται οι σχετικές νόμιμες προϋποθέσεις.

Επίσης δεν υπάρχει καμία απαγόρευση μεταφοράς ανώνυμων δεδομένων εκτός της ΕΕ και δεν εμπίπτει στο πεδίο εφαρμογής της οδηγίας εάν η ταυτότητα του υποκειμένου των δεδομένων είναι αδύνατον να προσδιοριστεί. Ως εκ τούτου, ακόμη και μια επιχείρηση σε μια χώρα που δεν είναι μέλος της Ευρώπης των χωρών δεδομένων δικαίου μπορεί να λάβει νόμιμα πληροφορίες σχετικά με μεμονωμένους Ευρωπαίους, αλλά μόνο αν η διαβίβαση πληροί τις εξαιρέσεις του άρθρου 26 ή η διαβίβαση είναι προστατευμένη κάτω από μία από τις τρεις εξατομικευμένων μεθόδων για τη μεταφορά δεδομένων που αναλύονται παρακάτω: safe harbor, τυποποιημένες συμβατικές ρήτρες, και των δεσμευτικών εταιρικών κανόνων BCR

3.4.1 Safe Harbor

Οι περισσότερες υπηρεσίες υπολογιστικού νέφους προσφέρονται από αμερικανικές επιχειρήσεις. Οι ΗΠΑ και η ΕΕ έχουν συμφωνήσει μέσω ενός καθεστώς της εφαρμογής του Safe Harbor ή "σφαίρας ασφαλείας" το οποίο επιτρέπει στους οργανισμούς στις ΗΠΑ (συμπεριλαμβανομένων των παρόχων υπηρεσιών cloud) που εισάγουν τα προσωπικά δεδομένα από την ΕΕ να αποδείξουν την ύπαρξη επαρκούς επιπέδου προστασίας για τους σκοπούς του άρθρου 25. Το επίπεδο επαρκούς προστασίας για τη μεταφορά των δεδομένων από την Ευρωπαϊκή Ένωση στις Ηνωμένες Πολιτείες της Αμερικής πρέπει να ικανοποιείται εφόσον οι οργανισμοί σέβονται τις αρχές της "σφαίρας ασφαλείας" για την προστασία της ιδιωτικής ζωής. Σύμφωνα με τα παραπάνω οι αμερικανικοί οργανισμοί που επιθυμούν να λαμβάνουν δεδομένα από την Ευρωπαϊκή Ένωση θα πρέπει να δηλώνουν ενώπιον του αμερικανικού αρμόδιου φορέα, στην Ομοσπονδιακή Επιτροπή Εμπορίου των ΗΠΑ (FTC), ότι σέβονται τις εν λόγω αρχές. Στις υπηρεσίες υπολογιστικού νέφους, δεν τίθεται ζήτημα μόνο μεταφοράς δεδομένων από την ΕΕ στις ΗΠΑ αλλά τα δεδομένα αποθηκεύονται και μεταφέρονται σε διάφορους διακομιστές ή κέντρα δεδομένων εγκατεστημένα σε οποιοδήποτε μέρος του κόσμου. Επίσης, η εφαρμογή του safe harbor εξαρτάται αποκλειστικά και μόνο από τη σύμβαση η οποία συνάπτεται μεταξύ αυτού και του πελάτη του. Επομένως, είναι ζήτημα κατάλληλων συμβατικών ρητρών οι οποίες να επιτρέπουν στον πάροχο να προσφέρει τις επαρκείς εγγυήσεις για την προστασία της ιδιωτικής ζωής.

3.4.2 Binding Corporate Rules (BCR)

Οι δεσμευτικοί εταιρικοί κανόνες BCR είναι το νομικό εργαλείο που δίνει τη δυνατότητα σε ομίλους εταιριών (πολυεθνικές επιχειρήσεις) να διαβιβάζουν προσωπικά δεδομένα από εταιρείες του ομίλου που είναι εγκατεστημένες στην Ευρωπαϊκή Ένωση, σε εταιρίες του ίδιου ομίλου που είναι εγκατεστημένες σε τρίτες χώρες (εκτός της Ε.Ε.), οι οποίες δεν εξασφαλίζουν ικανοποιητικό επίπεδο προστασίας. Αποτελούν ένα σύνολο νομικά δεσμευτικών κανόνων με το οποίο μία ομάδα εταιρειών που συνιστούν όμιλο, μπορεί να παράσχει τις ως άνω απαιτούμενες επαρκείς εγγυήσεις αναφορικά με τις διαβιβάσεις προσωπικών δεδομένων στο εσωτερικό του ομίλου. Πρόκειται δηλαδή για μία από τις υπάρχουσες βάσεις νομιμότητας της διαβίβασης προσωπικών δεδομένων

μεταξύ εταιρειών που ανήκουν μεν στον ίδιο όμιλο, εδρεύουν ωστόσο σε διαφορετικές έννομες τάξεις, και δη εκτός Ε.Ε.

Τα βασικά χαρακτηριστικά των BCR είναι τα εξής:

1. **Είναι νομικά δεσμευτικοί**. Μόνο υπό αυτόν τον όρο μπορούν να αποτελούν "επαρκείς εγγυήσεις" υπό την έννοια του άρθρου 26 παρ. 2 της Οδηγίας 95/46/ΕΚ. Για να αποκτήσουν δε νομική δεσμευτικότητα, τα BCR μπορει να έχουν τη μορφή είτε μονομερούς δήλωσης είτε μιας "εταιρικής συμφωνίας", ήτοι μιας σύμβασης μεταξύ των εταιριών του ομίλου.
2. **Είναι εταιρικοί**. Αυτό σημαίνει ότι ισχύουν για όλα τα μέλη μιας πολυεθνικής ή ενός ομίλου, αφού συνήθως έχουν δημιουργηθεί και επιβληθεί από την κεντρική διοίκηση του ομίλου. Επισημαίνεται δε ότι τα BCR καλύπτουν τις διαβιβάσεις δεδομένων αποκλειστικά μεταξύ εταιριών του ίδιου ομίλου (π.χ. από BP Γαλλίας σε BP Ιαπωνίας ή BP Ταϋλάνδης) και όχι τις διαβιβάσεις σε άλλες εταιρίες που δεν ανήκουν στον όμιλο (π.χ. από BP Γαλλίας σε Shell Ιαπωνίας).
3. **Ρυθμίζουν τη διασυνοριακή ροή δεδομένων**. Αυτός είναι και ο κύριος λόγος ύπαρξής τους, καθώς τα BCR εξασφαλίζουν την παροχή επαρκούς προστασίας των δεδομένων που καλύπτονται από την Οδηγία 95/46/ΕΚ και διαβιβάζονται εκτός Ε.Ε., σε χώρες που δεν παρέχουν ικανοποιητικό επίπεδο προστασίας. Άλλα προσωπικά δεδομένα που τυγχάνουν επεξεργασίας από τον όμιλο, αλλά δεν τυγχάνουν καμιάς επεξεργασίας εντός της Ε.Ε., δεν χρειάζεται να καλύπτονται από τα BCR.

3.4.3 Τυποποιημένες συμβατικές ρήτρες

Οι τυποποιημένες συμβατικές ρήτρες που έχει θεσπίσει η Ευρωπαϊκή Επιτροπή για τον σκοπό της οριοθέτησης της διεθνούς διαβίβασης δεδομένων μεταξύ δύο υπευθύνων της επεξεργασίας ή ενός υπεύθυνου και ενός εκτελούντα την επεξεργασία βασίζονται σε διμερή προσέγγιση. Όταν ο πάροχος υπηρεσιών νεφοϋπολογιστικής είναι ταυτόχρονα ο εκτελών την επεξεργασία, οι τυποποιημένες ρήτρες δυνάμει της απόφασης 2010/87/ΕΚ της επιτροπής συνιστούν μέσο που θα μπορούσε να χρησιμοποιηθεί ως βάση μεταξύ του εκτελούντος την επεξεργασία και του υπευθύνου της επεξεργασίας για την παροχή επαρκών εγγυήσεων όσον αφορά τη διεθνή διαβίβαση δεδομένων σε περιβάλλοντα

νεφοϋπολογιστικής. Το ίδιο το κείμενο της Οδηγίας αφήνει να εγκρίνει τη μεταφορά προσωπικών δεδομένων ακόμη και σε τρίτες χώρες που αδυνατούν να εξασφαλίσουν ένα «επαρκές επίπεδο προστασίας», εάν ο ελεγκτής ανεγείρει «επαρκείς εγγυήσεις», με «ορισμένες τυποποιημένες συμβατικές ρήτρες» συνεπή με την απόφαση της Επιτροπής.

3.5 Το ζήτημα της εμπιστευτικότητας των δεδομένων

Σύμφωνα με την USA Patriot Act [7], εάν η υπηρεσία νέφους παρέχεται από έναν αμερικανικό φορέα, τότε η Αμερικανική Κυβέρνηση έχει τη δυνατότητα στα πλαίσια μίας τρομοκρατικής έρευνας, να συμβουλευθεί όλα τα αποθηκευμένα δεδομένα στους διακομιστές της αμερικανικής εταιρείας, ακόμα και αν αυτά βρίσκονται εκτός αμερικανικού εδάφους. Η εμπιστευτικότητα των δεδομένων δεν είναι πια εγγυημένη και τα υποκείμενα των δεδομένων δεν λαμβάνουν γνώση περί αυτής της αμερικανικής εισχώρησης. Ο Καναδάς από το 2004 και η Ολλανδία έχουν εκφράσει τις ιδιαίτερες ανησυχίες τους σχετικά με το θέμα αυτό με την Ολλανδία να εξετάζει το ενδεχόμενο να απαγορεύσει στη δημόσια διοίκηση να συνεργάζεται με αμερικανικούς παρόχους για online υπηρεσίες στις οποίες τα δεδομένα είναι δεκτικά φιλοξενίας από τους αμερικανικούς παρόχους.

Από την πλευρά της **Επιτροπή των Περιφερειών (ΕτΠ)**, η οποία αποτελεί πολιτική συνέλευση και συμμετέχει στη διαδικασία κατάρτισης των νέων κοινοτικών νόμων, εφιστά την προσοχή στο γεγονός ότι ένα από τα κυριότερα εμπόδια στην αξιοποίηση του υπολογιστικού νέφους στον δημόσιο και στον ιδιωτικό τομέα είναι το ζήτημα των νόμων και των κανόνων που θα πρέπει να εφαρμόζονται κατά τη χρήση της τεχνολογίας αυτής (εθνικοί και ευρωπαϊκοί κανόνες προστασίας προσωπικών δεδομένων, νομοθεσία σχετικά με την κοινωνική προστασία και την προστασία της υγείας, κλπ.). Η προστασία των δεδομένων συνδέεται εξάλλου με ορισμένα προβλήματα και ορισμένους κινδύνους που πρέπει επίσης να αντιμετωπιστούν. Επίσης επιδοκιμάζει τις τρεις βασικές δράσεις που προτείνει η Επιτροπή, αλλά κρίνει ότι θα πρέπει να συμπληρωθούν από συγκεκριμένα μέτρα που να εστιάζουν στην ανάπτυξη των γνώσεων των χρηστών. Αυτό θα έχει ως αποτέλεσμα την αύξηση της ζήτησης στην αγορά, της μείωσης της ασύμμετρης κατανομής των κινδύνων μεταξύ καταναλωτών και προμηθευτών υπηρεσιών και να δημιουργηθεί μια πιο ισορροπημένη κατανομή των πλεονεκτημάτων που απορρέουν από την ανάπτυξη αυτής της νέας τεχνολογίας.

Τέλος θεωρεί ότι τα μέτρα θα πρέπει να επικεντρωθούν στην προώθηση της ψηφιακής εκπαίδευσης και της ψηφιακής παιδείας ενώ να είναι αξιοποιήσιμα ακόμα και σε σκόπιμο τοπικό επίπεδο.

3.6 Ομάδα Εργασίας Άρθρου 29

Η **Ομάδα Εργασίας του Άρθρου 29** συστάθηκε βάσει του άρθρου 29 της Οδηγίας 95/46/ΕΚ στις της 24ης Οκτωβρίου 1995 σχετικά με την προστασία των φυσικών προσώπων όσον αφορά την επεξεργασία των δεδομένων προσωπικού χαρακτήρα. Έχει συμβουλευτικό ρόλο και ενεργεί ανεξάρτητα ενώ οι αρμοδιότητες της είναι κυρίως η εξέταση της εφαρμογής της Οδηγίας 95/46/ΕΚ στα κράτη μέλη, αλλά και στις μεταγενέστερες Οδηγίες 2002/58/ΕΚ και 2006/24/ΕΚ. Η Ομάδα γνωμοδοτεί, επίσης, για κάθε νομοθετικό ή διοικητικό μέτρο ή δράση των οργάνων της Ευρωπαϊκής Ένωσης που αφορά στην προστασία των προσωπικών δεδομένων στην Ευρωπαϊκή Ένωση, καθώς και αν η νομοθεσία τρίτης χώρας παρέχει ικανοποιητικό επίπεδο προστασίας, το οποίο επιτρέπει τη διαβίβαση προσωπικών δεδομένων από κράτος μέλος της ΕΕ προς αυτή. Σε επίπεδο γνωμοδοτήσεων η Ομάδα ασχολήθηκε με τα εξής θέματα: α) το νέο νομοθετικό πλαίσιο για την προστασία των προσωπικών δεδομένων, β) τις νέες τεχνολογίες, γ) τις διαβιβάσεις δεδομένων σε τρίτες χώρες.

Η Ομάδα Εργασίας εξέδωσε δυο γνωμοδοτήσεις σχετικά με τις ιδιαιτερότητες και τα ζητήματα που δημιουργούνται από την εφαρμογή της τεχνολογίας του υπολογιστικού νέφους, το οποίο εξαπλώνεται διαρκώς. Συγκεκριμένα η Ομάδα εξέδωσε τη Γνώμη 5/2012 [8] στην οποία τέθηκαν οι υποχρεώσεις του παρόχου υπηρεσιών υπολογιστικής νέφους και του πελάτη, ο οποίος θεωρείται υπεύθυνος επεξεργασίας, και δίδεται ιδιαίτερη έμφαση στα μέτρα ασφάλειας. Επίσης η Ομάδα εξέδωσε τη Γνώμη 6/2012 σχετικά με την υποχρέωση των παρόχων ηλεκτρονικών επικοινωνιών, να γνωστοποιούν στα θιγόμενα πρόσωπα περιστατικά παραβίασης των προσωπικών τους δεδομένων.

3.7 Πρόταση για νέα οδηγία για την προστασία προσωπικών δεδομένων

Στις 25.1.2012 η Ευρωπαϊκή Επιτροπή ανακοίνωσε την πρόταση αναθεώρησης των κανόνων του 1995 για την προστασία των προσωπικών δεδομένων, προκειμένου να ενισχύσει τα δικαιώματα ιδιωτικότητας στον ψηφιακό κόσμο και να ενισχύσει την ψηφιακή οικονομία στην Ευρώπη. Η τεχνολογική εξέλιξη και η παγκοσμιοποίηση έχουν μεταβάλει τον τρόπο συλλογής των δεδομένων, καθώς και την πρόσβαση και την χρήση τους. Επιπλέον, τα 27 κράτη μέλη της ΕΕ έχουν εφαρμόσει τους ευρωπαϊκούς κανόνες με αποκλίσεις, έχοντας ως αποτέλεσμα ένα ανομοιογενές πλαίσιο. Ένας ενιαίος ευρωπαϊκός νόμος θα εναρμόνιζε πλήρως το σχετικό πλαίσιο, αποτρέποντας απώλειες που κατά την Ευρωπαϊκή Επιτροπή ανέρχονται σε περίπου 2,3 δισεκατομμύρια ευρώ τον χρόνο. Η πρωτοβουλία της Επιτροπής θα ενισχύσει την αξιοπιστία των διαδικτυακών υπηρεσιών απέναντι στους καταναλωτές, προωθώντας την ανάπτυξη, την απασχόληση και την καινοτομία στην Ευρώπη.

Πρακτικά, η Ευρωπαϊκή Επιτροπή προτείνει την θέσπιση ενός Κανονισμού άμεσης εφαρμογής σε όλα τα κράτη μέλη που θα αντικαταστήσει τους εθνικούς νόμους. Πρόκειται για τον Γενικό Κανονισμό Προστασίας Δεδομένων. Παράλληλα, προτείνει την ψήφιση μιας Οδηγίας "για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, και για την ελεύθερη κυκλοφορία των δεδομένων αυτών". Μερικά από τα πιο βασικά στοιχεία που προστίθενται με τον προτεινόμενο Κανονισμό [9] είναι τα παρακάτω:

- Η καθιέρωση ενός νέου «δικαιώματος στη λήθη» θα βοηθήσει τα άτομα στην καλύτερη διαχείριση των κινδύνων που κρύβει το διαδίκτυο για την προστασία δεδομένων. Όταν κάποιος δεν επιθυμεί πλέον την επεξεργασία των δεδομένων του και εφόσον δεν συντρέχουν νόμιμοι λόγοι για τη διατήρησή τους, τα δεδομένα θα διαγράφονται. Οι κανόνες έχουν ως στόχο την ενίσχυση των δικαιωμάτων των ατόμων και όχι τη διαγραφή γεγονότων του παρελθόντος ή τον περιορισμό της ελευθερίας του Τύπου.

- Η απαίτηση για συγκατάθεση για τη διαχείριση δεδομένων, αυτή θα πρέπει να δίδεται ρητά, και όχι να λαμβάνεται ως δεδομένη.
- Η διευκόλυνση της πρόσβασης των χρηστών στα δεδομένα τους και θέσπιση του δικαιώματος φορητότητας δεδομένων, δηλαδή διευκόλυνση τη μεταφοράς προσωπικών δεδομένων από έναν πάροχο υπηρεσιών σε άλλον.
- Οι εταιρείες και οι οργανισμοί θα υποχρεούνται να γνωστοποιούν σοβαρές παραβιάσεις δεδομένων χωρίς καθυστέρηση, και, εφόσον είναι εφικτό, εντός 24 ωρών. Οφείλουν να σας γνωστοποιούν παραβιάσεις των δεδομένων σας που θα μπορούσαν να είναι επιζήμιες για εσάς. Θα πρέπει επίσης να ειδοποιούν την αρμόδια αρχή προστασίας δεδομένων.
- Ενιαίο σύνολο κανόνων για την προστασία δεδομένων, οι οποίοι θα ισχύουν σε όλη την ΕΕ. Βελτιωμένα διοικητικά και δικαστικά μέτρα αποκατάστασης για τις περιπτώσεις παραβίασης του δικαιώματος προστασίας δεδομένων.
- Οι εταιρείες θα είναι υπόλογες σε μία μόνο εθνική αρχή προστασίας δεδομένων στη χώρα της ΕΕ στην οποία έχουν την έδρα τους.
- Τα άτομα θα έχουν δικαίωμα να αναφέρουν όλες τις υποθέσεις στην εθνική αρχή προστασίας δεδομένων της χώρας τους, ακόμη και αν τα προσωπικά δεδομένα τους υποβάλλονται σε επεξεργασία εκτός της χώρας τους.
- Οι κανόνες της ΕΕ εφαρμόζονται σε εταιρείες μη εγκατεστημένες στην ΕΕ, εφόσον αυτές παρέχουν εμπορεύματα ή υπηρεσίες στην ΕΕ ή παρακολουθούν τη διαδικτυακή συμπεριφορά πολιτών της Ένωσης.
- Θα αυξηθεί η ευθύνη και υποχρέωση λογοδοσίας για όσους επεξεργάζονται δεδομένα προσωπικού χαρακτήρα.
- Θα ενισχυθούν οι εθνικές αρχές προστασίας δεδομένων ώστε να είναι σε θέση να επιβάλλουν πιο αποτελεσματικά τους κανόνες της ΕΕ στην εκάστοτε χώρα
- Θα υπάρχει ευκολότερη πρόσβαση στα δεδομένα σας.
- Αυξημένη ευθύνη και υποχρέωση λογοδοσίας για τα άτομα που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα, μέσω της διενέργειας εκτιμήσεων κινδύνου για την προστασία δεδομένων, του διορισμού υπευθύνων προστασίας δεδομένων και συμμόρφωσης με τις αρχές προστασίας της ιδιωτικής ζωής

Οι νέοι κανόνες θα διασφαλίσουν ότι ο χρήστης ή καταναλωτής θα ενημερώνεται με σαφήνεια και κατανοητό τρόπο ότι τα προσωπικά δεδομένα του έχουν υποβληθεί σε επεξεργασία. Όταν θα γίνεται η επεξεργασία των προσωπικών δεδομένων ενός χρήστη θα πρέπει να απαιτείται η συγκατάθεσή του εκ των προτέρων από την εταιρεία. Η Ευρωπαϊκή Επιτροπή θα ενισχύσει επίσης το δικαίωμα στη λήθη, σύμφωνα με το οποίο όταν κάποιος δεν επιθυμεί πλέον την επεξεργασία των δεδομένων του και εφόσον δεν συντρέχουν νόμιμοι λόγοι για τη διατήρησή τους, τα δεδομένα θα διαγράφονται. Η Επιτροπή επιδιώκει επίσης τη διασφάλιση της ελεύθερης και εύκολης πρόσβασης στα προσωπικά δεδομένα ώστε να είναι πιο εύκολο αφενός να γνωρίζει ο χρήστης ποιες προσωπικές πληροφορίες βρίσκονται στα χέρια εταιρειών και δημόσιων αρχών και αφετέρου να μπορούν να μεταφέρουν τα προσωπικά δεδομένα από έναν πάροχο υπηρεσιών σε άλλο – η λεγόμενη αρχή της «φορητότητας των δεδομένων».

Η μεταρρύθμιση απαιτεί από τους οργανισμούς να ειδοποιούν χωρίς αδικαιολόγητη καθυστέρηση και, εφόσον είναι εφικτό, εντός 24 ωρών τόσο τα άτομα όσο και την αρμόδια αρχή προστασίας δεδομένων σε περίπτωση τυχαίας ή παράνομης καταστροφής, απώλειας, παραποίησης, απόκτησης ή γνωστοποίησης δεδομένων σε μη εξουσιοδοτημένα πρόσωπα. Η «προστασία της ιδιωτικής ζωής ήδη από τον σχεδιασμό» και η «προστασία της ιδιωτικής ζωής εκ κατασκευής» θα αποτελέσουν επίσης κεντρικές αρχές στους κανόνες προστασίας δεδομένων της ΕΕ· αυτό σημαίνει ότι οι διασφαλίσεις προστασίας δεδομένων πρέπει να ενσωματώνονται σε προϊόντα και υπηρεσίες από τα πρώτα κιόλας στάδια της ανάπτυξής τους και ότι οι φιλικές προς την προστασία της ιδιωτικής ζωής προεπιλεγμένες ρυθμίσεις πρέπει να είναι ο κανόνας – π.χ. στα κοινωνικά δίκτυα. Οι κανόνες αυτοί θα ενισχύσουν τα δικαιώματα των ατόμων στην πράξη. Η Επιτροπή θα αναλάβει την ενημέρωση των πολιτών για τα δικαιώματα αυτά καθώς και για την πιο αποτελεσματική αξιοποίησή τους.

3.8 Συμφωνητικό παροχής υπηρεσιών (SLA)

Στο προηγούμενο κεφάλαιο αναφέραμε την αναγκαιότητα των συμφωνητικών παροχής υπηρεσιών (SLA). Ένα SLA είναι η μόνη νομική συμφωνία που εγγυάται την ποιότητα και την ποσότητα των υπηρεσίες που παρέχονται από τον πάροχο υπηρεσιών cloud. Κατά τη διαπραγμάτευση και τη δημιουργία ενός σύμφωνου SLA, ένας οργανισμός θα

πρέπει να συμπεριλαμβάνει λεπτομέρειες σχετικά με την ασφάλεια και την προστασία που αναμένεται από το νέφος παροχής υπηρεσιών έτσι ώστε εμπιστευτικότητα, ακεραιότητα και τη διαθεσιμότητα των ευαίσθητων πληροφοριών να είναι εγγυημένα. Επιπλέον, ένα SLA θα πρέπει να περιλαμβάνουν ρήτρες που σχετίζονται με το θέμα της αποζημίωσης για απώλεια των επιχειρήσεων και τα έσοδα που προκαλούνται από διακοπές λειτουργίας των υπηρεσιών λόγω δικτύου ή / και αστοχίες υλικού, παραβιάσεις της ασφάλειας. Το μειονέκτημα του υπολογιστικού νέφους, σε σχέση με SLAs, είναι η δυσκολία στον προσδιορισμό για τη διακοπή παροχής υπηρεσιών, λόγω της πολύπλοκης φύσης του περιβάλλοντος. Οι ακόλουθοι τομείς θα πρέπει προσεκτικά να αξιολογηθούν και διαπραγματευτούν με τον πάροχο υπηρεσιών νέφους κατά τη δημιουργία SLA διαδικασία:

- Λεπτομερή περιγραφή του περιβάλλοντος της υπηρεσίας, συμπεριλαμβανομένης της τοποθεσίας των εγκαταστάσεων και των κατάλληλων απαιτήσεων ασφάλειας
- Πολιτικές, διαδικασίες και πρότυπα συμπεριλαμβανομένων της εξέτασης και διαχείρισης του προσωπικού
- Προκαθορισμένα επίπεδα υπηρεσίας και των δαπανών τους
- Διαδικασία αξιολόγησης και συμμόρφωσης στο επίπεδο που έχει συμφωνηθεί από τον πάροχο, συμπεριλαμβανομένων των ελέγχων και των δοκιμών
- Επιπρόσθετη νομική αποκατάσταση για μη συμμόρφωση ή για βλάβη που προκλήθηκε από τον πάροχο
- Βαθμός αλληλεπίδρασης μεταξύ του παρόχου και του οργανισμού
- Τις αρμοδιότητες του οργανισμού να παρέχει σχετικές πληροφορίες και πόρους στον πάροχο
- Διαδικασίες, μέτρα προστασίας και περιορισμούς για δεδομένα που έχουν να κάνουν με τον οργανισμό, καθώς και την διαχείριση ευαίσθητων δεδομένων
- Υποχρεώσεις του παρόχου κατά τον τερματισμό της συμφωνίας, όπως η επιστροφή και η εκκαθάριση των δεδομένων
- Πριν την σύναψη κάθε σύμβασης είναι καλό να υπάρχει ένας έμπειρος νομικός σύμβουλος για επανεξέταση των όρων. Οι συμβάσεις που δεν έχουν διαπραγματευτεί βάσει του SLA, συντάσσονται κατά κανόνα υπέρ του παρόχου και μπορεί να αποδειχθούν παγίδες και μη εφαρμόσιμες για κάθε οργανισμό.

Η Ευρωπαϊκή Ένωση ήδη μέσω του έβδομου προγράμματος πλαισίου χρηματοδοτεί διάφορα ερευνητικά προγράμματα [10] όπως το SLA@SOI, το οποίο στοχεύει προς μια οικονομικότερη παροχή υπηρεσιών, όπου οι υπηρεσίες που βασίζονται στις τεχνολογίες μπορούν να διαπραγματεύονται με ευελιξία ως οικονομικά αγαθά, δηλαδή υπό καθορισμένες συνθήκες θα επιτρέψει να προσαρμοστεί με ευελιξία και να οδηγήσει έτσι την καινοτομία και την ανταγωνιστικότητα.

Άλλα προγράμματα του έβδομου προγράμματος πλαισίου είναι το VISION Cloud και το IRMOS [10] τα οποία διερευνούν να γεφυρωθεί το χάσμα μεταξύ των προσδοκιών από τη πλευρά του πελάτη του νέφους και των μηχανισμών διαχείρισης πόρων.

Με τη στρατηγική της Ευρωπαϊκής Επιτροπής με τίτλο «Αξιοποίηση των δυνατοτήτων του υπολογιστικού νέφους στην Ευρώπη» κατέδειξε μια σειρά καίριων δράσεων, μεταξύ των οποίων αναφέρεται στην εκπόνηση πρότυπων ασφαλών και δίκαιων συμβατικών όρων για συμβάσεις υπολογιστικού νέφους. Για το σκοπό αυτό, η DG ConNECT έχει ξεκινήσει ειδικές ομάδες εργασίας για την υλοποίηση της συνολικής στρατηγικής και των βασικών δράσεων που προσδιορίζονται. Μια ομάδα εργασίας (Cloud Select Industry Group) περιλαμβάνει εκπροσώπους από τη βιομηχανία και από ενδιαφερόμενα μέρη του υπολογιστικού νέφους, με σκοπό να υποστηρίξει τις δράσεις της Ευρωπαϊκής Επιτροπής και να παράσχει στοιχεία στην ευρωπαϊκή σύμπραξη για το υπολογιστικό νέφος (ECP) που αφορούν συμφωνητικά παροχής υπηρεσιών. Οι αρχικές δραστηριότητες της ομάδας εργασίας επικεντρώθηκε στην κατάρτιση ενός προκαταρκτικού καταλόγου των χαρακτηριστικών που πρέπει να περιληφθούν στα SLA, έθεσε την ανάγκη για ορισμούς, την ταξινόμηση και τις περιγραφές των διαφόρων μετρήσεων, καθώς και για την αποτελεσματική των παρακολούθηση προσεγγίσεων του SLA.

3.9 Πρότυπα και υπολογιστικό νέφος

Μολονότι αναδύονται νέα πρότυπα δεν έχει επιτευχθεί συμφωνία ως προς τα ποια πρότυπα θα εξασφαλίσουν την απαιτούμενη διαλειτουργικότητα, φορητότητα και αναστρεψιμότητα των δεδομένων. Πολλές ερευνητικές ομάδες, forums και οργανισμοί προτυποποίησης εργάζονται για τη δημιουργία προτύπων που να καλύπτουν επαρκώς όλες τις πτυχές του νέφους ώστε να καθιερωθούν στην ανάπτυξη συστημάτων υπολογιστικού νέφους Η Επιτροπή επιθυμεί να προσδιοριστούν συνεκτικές δέσμες

χρήσιμων προτύπων για να καταστεί ευκολότερη η οργάνωση τόσο της ζήτησης όσο και της προσφοράς. Η Επιτροπή θα συνεργαστεί με τον ENISA[5] και άλλους σχετικούς φορείς για να συμβάλει στην ανάπτυξη εκούσιου ενωσιακής κλίμακας συστημάτων πιστοποίησης στον τομέα του υπολογιστικού νέφους (συμπεριλαμβανόμενης της προστασίας των δεδομένων) και θα καταρτίσει κατάλογο των εν λόγω συστημάτων από το 2014.

Αυτή τη χρονική στιγμή υπάρχει ένας μεγάλος αριθμός οργανισμών τυποποίησης στον τομέα τυποποίησης νέφους [11]. Κάποια από τα πιο γνωστά είναι το IEEE. Τον Απρίλιο του 2011 το IEEE προώθησε μια πρωτοβουλία υπολογιστικού νέφους που επιδιώκει να καθορίσει πρότυπα για τη διαλειτουργικότητα νέφους. Για αυτόν τον λόγο, η IEEE έχει αναγγείλει δύο ομάδες εργασίας. Η μια ομάδα, η P2301, μισθώνεται για να συντάξει πρότυπα για την καθιέρωση της φορητότητας ενώ η δεύτερη ομάδα εργασίας, η P2302, επικεντρώνεται στο να επιτρέψει σε ένα σύστημα που βρίσκεται σε ένα νέφος να λειτουργήσει με ένα σύστημα σε ένα άλλο νέφος. Τα πρότυπα αυτά θα παράσχουν μια οικονομία κλίμακας που είναι διαφανής στους χρήστες. Το Cloud Security Alliance[6] "λειτουργεί ως μια ομάδα χρηστών" με το να βρίσκει τις καλύτερες πρακτικές, αλλά δεν εφαρμόζει απαραιτήτως αυστηρό έλεγχο στην έκδοση των εγγράφων, όπως πρέπει να κάνει ένα σώμα προτύπων όπως ο ISO ή ο ANSI. Στις ΗΠΑ παίζει πρωτοπόρο ρόλο στο νέφος τυποποίησης το NIST.

Σε ευρωπαϊκό επίπεδο το ETSI θα χρησιμεύσει ως συντονιστής. Το ETSI είναι ένα Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών Προτύπων που παράγει σε παγκόσμιο επίπεδο-τα ισχύοντα πρότυπα για τις Τεχνολογίες Επικοινωνιών (ΤΠΕ), συμπεριλαμβανομένων των σταθερών, κινητών, ραδιόφωνων, ραδιοτηλεοπτικών εκπομπών και τεχνολογιών διαδικτύου. Το ETSI είναι μια οργάνωση μη κερδοσκοπική με περισσότερες από 700 οργανώσεις Μέλη του ETSI που προέρχονται από 62 χώρες σε 5 ηπείρους σε όλο τον κόσμο.

Ένας άλλος οργανισμός που δραστηριοποιείται στην Ευρώπη είναι ο EuroCloud[7], ο οποίος είναι ένας ανεξάρτητος μη κερδοσκοπικός οργανισμός όπου κάθε ευρωπαϊκή

[5] http://www.enisa.europa.eu/
[6] https://cloudsecurityalliance.org/
[7] http://www.eurocloud.org/

χώρα μπορεί να ζητήσει να συμμετάσχει υπό την προϋπόθεση ότι σέβεται το καταστατικό EuroCloud. Το EuroCloud εχει μεγάλη επιρροή σε πανευρωπαϊκούς παρόχους νέφους.

Τέλος, ο διεθνής οργανισμός τυποποίησης International Organization for Standardization, (ISO) είναι μια διεθνής οργάνωση δημιουργίας και έκδοσης προτύπων που αποτελείται από αντιπροσώπους των εθνικών οργανισμών τυποποίησης. Ενώ ο οργανισμός ορίζεται ως μη κυβερνητική οργάνωση, η ικανότητα του να θέτει πρότυπα τα οποία αργότερα οι κυβερνήσεις αποφασίζουν πως πρέπει να τηρούνται δια νόμων ή συνθηκών, τον καθιστά πιο ισχυρό από άλλες μη κυβερνητικές οργανώσεις και στην πράξη λειτουργεί σαν μια κοινοπραξία με ισχυρούς συνδέσμους με κυβερνήσεις. Όσον αφορά το υπολογιστικό νέφος το 2015 θα παρουσιαστεί το πρότυπο ISO / IEC 27017 το οποίο θα βασιστεί στο πρότυπο ISO / IEC 27002 ώστε να καλύψει τις πτυχές της ασφάλειας των πληροφοριών και των σχέσεων προμηθευτή με υπολογιστικό νέφος αλλά και των ISO / IEC 27018 σχετικά με τις πτυχές της ιδιωτικής ζωής του νέφους. Επίσης το έργο έχει ευρεία στήριξη από τους εθνικούς φορείς προτύπων καθώς και από το Cloud Security Alliance, μεταξύ άλλων.

ΚΕΦΑΛΑΙΟ 4: Περιπτώσεις μελέτης έργων

Στο παρακάτω κεφάλαιο αρχικά θα αναλύσουμε το κανονιστικό και νομικό πλαίσιο που διέπει τρεις χώρες της Ευρωπαϊκής Ένωσης σε ζητήματα που αφορούν την τεχνολογία του υπολογιστικού νέφους. Συγκεκριμένα της Ιταλίας, της Δανίας και του Ηνωμένου Βασίλειου καθώς και περιπτώσεις έργων πληροφορικής με χρήση υπολογιστικού νέφους. Επιπλέον θα αναλυθεί το ελληνικό νομικό πλαίσιο και θα γίνει ανάλυση ενός έργου πληροφορικής ενώ θα γίνει αναφορά περιπτώσεων παραβίασης προσωπικών δεδομένων. Τέλος θα γίνει σύγκριση όλων των χώρων σε σχέση με τη χρήση και τη λειτουργία των έργων αυτών.

4.1 Νομικό και κανονιστικό πλαίσιο χώρων Ε.Ε

Αν και το υπολογιστικό νέφος έχει εξαπλωθεί στην Ευρώπη καμιά χώρα της ευρωπαϊκής ένωσης δεν έχει θεσπίσει ακόμα κάποιο συγκεκριμένο νομικό και κανονιστικό πλαίσιο που να αφορά αποκλειστικά τη χρήση του. Όλες οι χώρες όμως έχουν εφαρμόσει νόμους περί επεξεργασίας δεδομένων προσωπικού χαρακτήρα και έχουν ενσωματώσει την οδηγία 95/46/ΕΚ με κάποιες παραλλαγές της.

Συγκεκριμένα στην **Δανία** ο νόμος για τα προσωπικά δεδομένα τέθηκε σε ισχύ την 1η Ιουλίου 2000. Η ανεξάρτητη αρχή DatatiIsynet [12] είναι υπεύθυνη για τον έλεγχο της εφαρμογής του νόμου. Μέχρι το 2009 ο αριθμός των ερευνών ο οποίος περιλαμβάνει όλες τις υποθέσεις που διεκπεραιώθηκαν ήταν 2000. Στην **Ιταλία** η οδηγία 95/46/ΕΚ εφαρμόστηκε και τέθηκε σε ισχύ στις 8 Μάιου του 1997 [13] και περιλαμβάνει διατάξεις για τα προσωπικά δεδομένα. Ο νόμος ισχύει για δεδομένα που αφορούν φυσικά και νομικά πρόσωπα. Η υπεύθυνη ρυθμιστική αρχή είναι η Garante. Κατά τη διάρκεια του 2004, η Garante πραγματοποίησε περίπου 100 ελέγχους και οι έρευνες κατέληξαν σε περίπου 20 ποινικές διαδικασίες. Στο **Ηνωμένο Βασίλειο** η οδηγία 95/46/ΕΚ έχει εφαρμοστεί από την Αρχή Προστασίας Δεδομένων του 1998 με ημερομηνία 16 Ιουλίου 1998. Η πλειοψηφία των διατάξεων τέθηκε σε ισχύ την 1η Μαρτίου 2000.Η υπεύθυνη ρυθμιστική αρχή είναι η ICO **(**Information Commissioner's office) [14]. Οι παραβιάσεις τιμωρούνται με αστική ευθύνη ή ποινικές κυρώσεις, αλλά όχι με ποινές φυλάκισης και περιλαμβάνουν απεριόριστα πρόστιμα. Το 2004-2005 20.138 υποθέσεις περατώθηκαν από την Αρχή και υπήρχαν 12 ποινικές διώξεις. Οι

κυρώσεις που επιβλήθηκαν κυμάνθηκαν από £ 1000 σε £ 3.150. Τα τελευταία χρόνια οι καταγγελίες και τα ποσά αυξηθήκαν αλματωδώς και φτάνουν ακόμα και τα 250.000£ ανά πρόστιμο.

4.2 Διαφορές κανονιστικών πλαισίων χωρών Ε.Ε

Παρακάτω έχουμε κατηγοριοποιήσει τις διαφορές των χωρών μεταξύ τους σύμφωνα με το κανονιστικό πλαίσιο που διέπει το κάθε κράτος για την προστασία των προσωπικών δεδομένων.

4.2.1 Διαβίβαση δεδομένων

Στην **Δανία** μπορεί να πραγματοποιείται η διαβίβαση δεδομένων προσωπικού χαρακτήρα στα κράτη μέλη της ΕΕ και του ΕΟΧ μπορεί να πραγματοποιείτε απλώς, θα πρέπει να τηρούνται οι γενικοί κανόνες για την επεξεργασία σύμφωνα με την Αρχή Προστασία Δεδομένων (ΑΠΔ). Η ΑΠΔ απαγορεύει τη μεταφορά εκτός του ΕΟΧ, εκτός εάν ο προορισμός εξασφαλίζει επαρκή προστασία για τα δεδομένα. Επιπλέον, η Αρχή μπορεί να χορηγήσει άδεια για τη μεταφορά των δεδομένων (τα οποία μπορεί να είναι υπό όρους), εάν ο υπεύθυνος επεξεργασίας παρέχει επαρκείς εγγυήσεις για την προστασία των δικαιωμάτων των υποκειμένων των δεδομένων.

Στην **Ιταλία** η ΑΠΔ επιτρέπει τη μεταφορά δεδομένων εντός του ΕΟΧ χωρίς περιορισμούς ενώ σε χώρες εκτός του ΕΟΧ επιτρέπεται μόνο αν :

1. η τρίτη χώρα του ΕΟΧ εξασφαλίζει ικανοποιητικό επίπεδο προστασίας, όπως αναγνωρίζεται από την Garante (π.χ. με τον Καναδά, την Ουγγαρία, την Ελβετία, την Αργεντινή, Isle of Man, και με εταιρείες της ΗΠΑ που έχουν προσχωρήσει στις αρχές του safe harbor)
2. ή μέσω της υιοθέτησης των τυποποιημένων συμβατικών ρητρών
3. τηρούνται ορισμένες προϋποθέσεις, όπως: η συγκατάθεση του υποκειμένου των δεδομένων, η επεξεργασία αφορά δεδομένα προσωπικού χαρακτήρα που αφορούν νομικά πρόσωπα και η διαβίβαση είναι αναγκαία για την άσκηση ή υπεράσπιση δικαιώματος.

Στο **Ηνωμένο Βασίλειο** η ΑΠΔ επιτρέπει τις μεταφορές εντός του ΕΟΧ χωρίς όρους ενώ απαγορεύει τις μεταφορές εκτός του ΕΟΧ, εκτός εάν ο προορισμός εξασφαλίζει επαρκή προστασία για τα δεδομένα. Η επαρκής προστασία αξιολογείται από τον υπεύθυνο της επεξεργασίας. Προσωπικά δεδομένα μπορεί να μεταφερθούν εκτός του ΕΟΧ υπό τις συνήθεις συνθήκες (π.χ. εάν έχει υπάρξει μια κοινοτική διαπίστωση επάρκειας, ο εισαγωγέας δεδομένων έχει υπογράψει το Safe Harbor ή το υποκείμενο των δεδομένων έχει δώσει τη συγκατάθεση).

4.2.2 Ευαίσθητα δεδομένα

Στην **Ιταλία** τα ευαίσθητα δεδομένα μπορούν να υποστούν επεξεργασία μόνο με γραπτή συγκατάθεση του υποκειμένου των δεδομένων και την έγκριση της Garante του. Στην **Δανία** οι υπεύθυνοι επεξεργασίας δεδομένων του ιδιωτικού τομέα μπορούν να τα επεξεργαστούν μόνο σε ορισμένες περιπτώσεις. Τα προσωπικά δεδομένα δεν μπορούν να αποκαλυφθούν χωρίς τη ρητή συγκατάθεση του υποκειμένου των δεδομένων, εκτός εάν μια τέτοια αποκάλυψη γίνεται για σκοπούς δημόσιου ή ιδιωτικού συμφέροντος, που υπερτερούν σαφώς των συμφερόντων του υποκειμένου των δεδομένων, ή εάν η αποκάλυψη πληροί τις απαιτήσεις για την επεξεργασία των ευαίσθητων δεδομένων. Στο **Ηνωμένο Βασίλειο** παρέχεται ειδική προστασία για τα προσωπικά δεδομένα που είναι ευαίσθητα (δηλαδή σχετικά με τη φυλετική ή εθνοτική καταγωγή του υποκειμένου των δεδομένων, τα πολιτικά φρονήματα, τις θρησκευτικές ή παρόμοιες πεποιθήσεις, τη συμμετοχή σε συνδικαλιστική οργάνωση) και τα οποία μπορεί να επεξεργαστούν μόνο με τη συγκατάθεση του υποκείμενου των δεδομένων.

4.2.3 Κυρώσεις

Στην **Δανία** κάθε φυσικό ή νομικό πρόσωπο που διαπράττει αδίκημα σύμφωνα με την Αρχή υπόκειται σε πρόστιμο ή φυλάκιση. Η ΑΠΔ της Δανίας δεν μπορεί να επιβάλει κυρώσεις, αλλά μπορεί να ζητήσει από τη δανέζικη εισαγγελία να κινήσει τις διαδικασίες. Οι διατάξεις της Αρχής ισχύουν μόνο για ιδιώτες. Στην **Ιταλία** η ΑΠΔ θέτει αστικές, ποινικές και διοικητικές κυρώσεις. Ο υπεύθυνος της επεξεργασίας είναι υπεύθυνος για τις ζημίες που προκαλούνται από την ακατάλληλη χρήση ή την απώλεια δεδομένων. Η Αρχή μπορεί να επιβάλει διοικητικές κυρώσεις σε περίπτωση μη τήρησης των υποχρεώσεων του στο υποκείμενο των δεδομένων ή ελλιπούς κοινοποίησης στην Garante. Η ΑΠΔ προβλέπει ποινή φυλάκισης και τη δημοσίευση της

απόφασης, σε περίπτωση παράνομης επεξεργασίας των προσωπικών δεδομένων, σε περίπτωση που προκύψει απώλεια ή η μη εφαρμογή των απαιτούμενων μέτρων ασφαλείας. Η Garante έχει αρμοδιότητες έρευνας και μπορεί να χρησιμοποιήσει επίσης την Οικονομική Αστυνομία (Guardia di Finanza). Εκτός από την γενική υποχρέωση να εφαρμόσουν τα μέτρα ασφαλείας για την προστασία των δεδομένων προσωπικού χαρακτήρα από τυχαία ή αθέμιτη καταστροφή, ο νόμος απαιτεί, στο πλαίσιο ποινικών κυρώσεων, την εφαρμογή ειδικών τεχνικών προδιαγραφών (disciplinare Tecnico) , οι οποίες επισυνάπτεται στο νόμο. Στο **Ηνωμένο Βασίλειο** ο νόμος θέτει αστικές ή ποινικές κυρώσεις οι οποίες περιλαμβάνουν απεριόριστα πρόστιμα αλλά όχι ποινές φυλάκισης.

4.2.4 Πρότυπα

Στη **Δανία** δεν υπάρχει κάποιος νόμος για τη θέσπιση προτύπων ασφαλείας στη χρήση υπολογιστικού νέφους. Τα πρότυπα ασφαλείας που χρησιμοποιούνται συνήθως για πιστοποίηση είναι η σειρά του ISO 27000 και ISAE 3000. Το Digitaliseringsstyrelsen[8] είναι η δημόσια αρχή που είναι υπεύθυνη για την ενίσχυση της ανάπτυξης, την εξασφάλιση της αποτελεσματικότητας του δημόσιου τομέα καθώς και υπεύθυνη για τα πρότυπα ασφάλειας σε έργα με χρήση υπολογιστικού νέφους. Στην **Ιταλία** όπως και στην Δανία δεν υπάρχει κάποιο νομικό πλαίσιο για την θέσπιση πρότυπων ασφαλείας. Το μόνο που ισχύει είναι ένα γενικό πλαίσιο κανόνων ασφάλειας που εξέδωσε η υπηρεσία Agency Digital Italy[9] που είναι υπεύθυνη για τη ψηφιακή μετάβαση του δημοσίου τομέα. Στο **Ηνωμένο Βασίλειο** το Cabinet Office έχει προτείνει την θέσπιση προτύπων ασφάλειας και την πιστοποίηση των έργων με χρήση υπολογιστικού νέφους στο δημόσιο τομέα αλλά ακόμα δεν έχουν εφαρμοστεί.

4.3 Παραδείγματα χρήσης υπολογιστικού νέφους στην Ευρωπαϊκή Ένωση

4.3.1 Ιταλία

Με την εφαρμογή του Ψηφιακού Θεματολογίου η Ιταλία ήταν από τις πρώτες χώρες που μετέφεραν το υπολογιστικό νέφος στη δημόσια διοίκηση. Από τα πρώτα έργα

[8] http://www.digst.dk/
[9] http://www.agid.gov.it/

χρήσης στην ιταλική δημόσια διοίκηση ήταν το DT Cloud [15]. Το DT Cloud ξεκίνησε να υλοποιείται το 2011 από μια ανώνυμη εταιρεία (Consip) που ανήκει στο ιταλικό Υπουργείο Οικονομικών και ολοκληρώθηκε το 2013 με στόχο να αναπτύξει μια ιδιωτική πλατφόρμα cloud υπηρεσιών για το Υπουργείο Οικονομικών ώστε να μειωθεί το κόστος της κυβέρνησης ΤΠ και θα ενισχύσει τις υπηρεσίες προς τους πολίτες. Το συνολικό κόστος της πρωτοβουλίας ανέρχεται σε περίπου € 2εκ.
Το συγκεκριμένο έργο προορίζεται για τη μετάβαση των υφισταμένων εφαρμογών και υπηρεσιών στο νέφος. Η μετάβαση των εφαρμογών αφορά κυρίως IaaS (π.χ. εικονικές μηχανές ή υποστήριξη των φυσικών πόρων) και PaaS (web hosting) υπηρεσίες μέχρι στιγμής. Οι χρήστες που χρησιμοποιήσουν το έργο είναι κυρίως εσωτερικοί χρήστες του DT (π.χ. πιστωτικά ιδρύματα, την αστυνομία και την ίδια τη διοίκηση της DT). Ωστόσο , στο μέλλον θα επεκταθεί και σε άλλα υπουργεία.

Το έργο περιλαμβάνει :

1. Την εικονικοποίηση της υποδομής για την ανταλλαγή των διακομιστών, αποθηκευτικών και δικτυακών πόρων.
2. Την εισαγωγή νέων διαδικασιών διαχείρισης υπηρεσιών και SLA, με σκοπό την αύξηση της αυτοματοποίησης και της ευελιξίας στις διαδικασίες.
3. Μια πλατφόρμα με την προοπτική για την ανάπτυξη ενός εθνικού ιδιωτικού νέφους οργανωμένη με πολλές δημόσιες διοικήσεις ως ενοικιαστές, προκειμένου να διευκολυνθεί η απόκτηση και η κατανομή των υπηρεσιών μεταξύ των διοικήσεων

Υποδομή νέφους

Η υποδομή cloud του κέντρου δεδομένου (IaaS) υλοποιήθηκε από εξωτερικούς προμηθευτές όπως η VMware και HP για την αγορά των διακομιστών.

Απαιτήσεις ασφάλειας και ιδιωτικό απόρρητο

Μαζί με το Cloud DT, η Consip εφαρμόζει ένα σχέδιο ανάκτησης των δεδομένων με σκοπό τη διασφάλιση της λειτουργικής συνέχειας της υπηρεσίας. Ένα κέντρο δεδομένων εγκαταστάθηκε ειδικά για την αντιμετώπιση καταστροφών ώστε να διασφαλίζει την ομαλή λειτουργία των κρίσιμων υπηρεσιών. Επιπλέον, ένα πλαίσιο ασφάλειας του σύννεφου έχει ξεκινήσει με το έργο, με μια νέα προσέγγιση για την

προστασία των δεδομένων και νέες διαδικασίες για τη διαχείριση του κινδύνου έχουν ξεκινήσει, προκειμένου να παρακολουθούν περιστατικά ασφάλειας. Επίσης το έργο ακολουθεί τον ιταλικό νόμο περί Προστασίας Προσωπικών Δεδομένων και τον Κώδικα ψηφιακής διοίκησης (CAD). Στο πλαίσιο του ορισμού και της εφαρμογής των νέων διαδικασιών, νέα SLA έχουν καθοριστεί, που περιλαμβάνουν απαιτήσεις αξιοπιστίας και χρονοδιάγραμμα για την παροχή και συνδρομή. Τέλος τα αποτελέσματα από τη χρήση του έργου ήταν η μείωση χρήσης υλικού κατά 60%. Ωστόσο, ακόμα είναι σύντομο το χρονικό διάστημα που λειτουργεί η πλατφόρμα για να γίνει εκτίμηση των οφελών της μετάβασης στο υπολογιστικό νέφος.

4.3.2 Ηνωμένο Βασίλειο

Το 2011 η βρετανική κυβέρνηση ξεκίνησε τη στρατηγική για το υπολογιστικό νέφος, μια πρωτοβουλία για την προώθηση της χρήσης του νέφους στο Ηνωμένο Βασίλειο και το δημόσιο τομέα με το πρόγραμμα G-Cloud [16]. Οι δύο βασικοί στόχοι της στρατηγικής νέφους είναι η μείωση των κυβερνητικών δαπανών και η βελτίωση των δημόσιων υπηρεσιών. Το πρόγραμμα στοχεύει στη δημιουργία ενός νέου πλαισίου για το πώς η δημόσια διοίκηση προμηθεύεται υπηρεσίες τεχνολογιών πληροφοριών και επικοινωνιών (ΤΠΕ) με στόχο την προώθηση της χρήσης των τεχνολογιών νέφους. Όσον αφορά τη βελτίωση των υφιστάμενων υπηρεσιών ο στόχος είναι να διασφαλιστεί ότι η δημόσια διοίκηση έχει την επιλογή ανάμεσα σε ένα ευρύ φάσμα παρόχων και των εφαρμογών κατά την αγορά μιας υπηρεσίας ΤΠΕ. Για τον ιδιωτικό τομέα, ο στόχος είναι αυξηθεί η ανταγωνιστικότητα στην διαδικασία προμηθειών στην οποία είναι σε θέση να λάβει μέρος ένας μεγαλύτερος αριθμός εταιριών ΤΠΕ (ιδίως των μικρομεσαίων επιχειρήσεων). Το G-Cloud καλύπτει κάθε είδος υπηρεσιών νέφους που μπορούν να αγοραστούν από τον δημόσιο τομέα, συμπεριλαμβανομένων των κεντρικών και των τοπικών δημόσιων αρχών.

Το CloudStore είναι ένα βασικό εργαλείο για την υποστήριξη αυτών των αλλαγών. Το CloudStore αποτελεί καταλύτη για την Ψηφιακή Στρατηγική του Ηνωμένου Βασιλείου. Το κόστος του έργου για την εγκατάσταση ανέρχεται σε £ 2.175εκ και επιτρέπει σε εταιρίες ΤΠΕ να προσφέρουν τις υπηρεσίες νέφους τους διαδικτυακά σε στη δημόσια διοίκηση για την αγορά αυτών των υπηρεσιών. Επιπλέον το CloudStore φέρνει νέους πελάτες από την κοινότητα των προμηθευτών (ιδίως των μικρομεσαίων επιχειρήσεων). Το CloudStore εισήγαγε ένα νέο τρόπο για την αγορά των υπηρεσιών πληροφορικής

που καθιστά εύκολη και αυτοματοποιημένη όσο το δυνατόν για τους ανθρώπους να χρησιμοποιούν και να συνδέονται με τους προμηθευτές και τους αγοραστές. Επιπλεον ενθαρρύνει την ανταλλαγή και την επαναχρησιμοποίηση των υπηρεσιών νέφους και τις εφαρμογές του με στόχο να μειώσει το κόστος για τις δημόσιες αρχές.

Το CloudStore λειτουργεί με διαφανή και ανοικτό τρόπο, με στόχο την αύξηση της ανταγωνιστικότητας μεταξύ των προμηθευτών. Επιπλέον οι προμηθευτές μπορούν να συμμετέχουν σε μια πιο ανοικτή και δίκαιη αγορά που θα αυξήσει τη διαφάνεια σχετικά με τις υπηρεσίες νέφους που προσφέρονται και να οδηγήσει σε πιο καινοτόμες υπηρεσίες. Το CloudStore ξεκίνησε τη λειτουργία του στις 19 Φεβρουαρίου του 2012 και κατά το πρώτο χρόνο λειτουργιάς του προσέφερε περίπου 1.700 υπηρεσίες νέφους από 257 προμηθευτές. Η δεύτερη χρονιά του συγκέντρωσε 459 προμηθευτές (εκ των οποίων το 75% είναι μικρομεσαίες επιχειρήσεις) και 32000 υπηρεσίες. Επί του παρόντος, οι μελλοντικές εξελίξεις είναι να καταστεί η ιστοσελίδα του CloudStore όσο πιο φιλική στο χρήστη.

Υποδομή νέφους

Το CloudStore δημιουργήθηκε από την εταιρία ανάπτυξης λογισμικού SolidSoft σε έξι εβδομάδες σε συνεργασία με την ομάδα του G-Cloud. Η εφαρμογή φιλοξενείται στην υποδομή της Microsoft Azure Cloud.

Απαιτήσεις ασφάλειας και ιδιωτικό απόρρητο

Σύμφωνα με την ειδική συμφωνία (call-off) που έχει υπογράψει ο προμηθευτής θα πρέπει να τηρεί τις παρακάτω απαιτήσεις :

- Ο προμηθευτής πρέπει να ειδοποιήσει έγκαιρα για οποιαδήποτε παραβίαση των μέτρων ασφαλείας που εφαρμόζονται για την προστασία των προσωπικών δεδομένων.
- Τα προσωπικά δεδομένα θα πρέπει να υποβάλλονται σε επεξεργασία μόνο σε τέτοιο βαθμό που είναι απαραίτητα για την παροχή των υπηρεσιών G -Cloud ή όπως απαιτείται από το νόμο.
- Ο προμηθευτής πρέπει να εφαρμόζει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την προστασία των δεδομένων προσωπικού χαρακτήρα δημόσιας

υπηρεσίας (μη εξουσιοδοτημένη ή παράνομη επεξεργασία, καταστροφή, βλάβη, αλλοίωση ή αποκάλυψη και να αποτρέπει μη εξουσιοδοτημένη ή παράνομη επεξεργασία των προσωπικών δεδομένων.

- Ο προμηθευτής θα πρέπει να συμμορφώνεται με τις υποχρεώσεις των υπευθύνων επεξεργασίας δεδομένων στο πλαίσιο του νόμου περί προστασίας δεδομένων.
- Θα πρέπει επίσης να συμμορφώνεται με οποιεσδήποτε άλλες οδηγίες που κοινοποιήθηκαν από το υπουργικό συμβούλιο ή να ενσωματώνει τα πρότυπα ή / και πρότυπες ρήτρες (τα οποία έχουν εγκριθεί από την Ευρωπαϊκή Επιτροπή και να προσφέρει επαρκείς διασφαλίσεις σύμφωνα με την νομοθεσία περί προστασίας δεδομένων).
- Όταν πρόκειται για μη προσωπικά δεδομένα, απαγορεύεται στον προμηθευτή να αποθηκεύσει, να αντιγράψει ή να χρησιμοποιήσει τα δεδομένα των πελατών του εκτός εάν καταγράφεται στην ειδική συμφωνία (call-off) και θα πρέπει να εξασφαλίζουν ότι κάθε σύστημα στο οποίο ο προμηθευτής κατέχει οποιαδήποτε στοιχεία πελατών είναι ένα ασφαλές σύστημα που συμμορφώνεται με την πολιτική ασφαλείας.
- Στο πλαίσιο της προστασίας των στόχων πληροφορίες η συμφωνία-πλαίσιο ορίζει ότι η επιθεώρηση και ο έλεγχος των δραστηριοτήτων επεξεργασίας δεδομένων του προμηθευτή μπορεί να διεξαχθεί από δημόσιους φορείς που έχουν αγοράσει υπηρεσίες του.

Αναμενόμενα οφέλη

Σύμφωνα με τη στρατηγική του υπολογιστικού νέφους η εξοικονόμηση κόστους αναμένεται από την εφαρμογή του G - Cloud και του CloudStore μεταξύ 2012 και 2015 περίπου στα € 208εκ. Ο στόχος για την εφαρμογή είναι το 50% των έργων πληροφορικής του δημόσιου τομέα να χρησιμοποιεί υπηρεσίες νέφους μέχρι το 2015. Μέχρι τις 19 Μαρτίου, 2013, 11 εκ. λίρες συνολικής αξίας υπηρεσίες είχαν αγοραστεί μέσω του πλαισίου για τις δημόσιες συμβάσεις G – cloud.

4.3.3 Δανία

Στις σκανδιναβικές χώρες υπάρχει μια ισχυρή πρωτοβουλία και συνεργασία όσο αφορά το υπολογιστικό νέφος από όλες τις χώρες (Σουηδία, Νορβηγία, Ισλανδία και τη Φινλανδία). Έχει τεθεί σε ισχύ μια ομάδα εργασίας και ένα φόρουμ για την εφαρμογή του υπολογιστικού νέφους στο δημόσιο τομέα. Ο στόχος τους είναι να αυξηθεί η αξιοποίηση του υπολογιστικού νέφους στον δημόσιο τομέα, ο καθορισμός κοινών προτύπων, η ανταλλαγή βέλτιστων πρακτικών, η άρση των εμποδίων και η έκθεση των οφελών. Στη Δανία έχουν τεθεί σε πιλοτικό επίπεδο διάφορες περιπτώσεις στο δημόσιο τομέα προκειμένου να αποκτήσουν εμπειρία από περιπτώσεις τα οποία στη συνέχεια να μοιραστούν με τον υπόλοιπο δημόσιο τομέα. Ωστόσο δεν υπάρχει κάποια ειδική στρατηγική αλλά είναι περισσότερο ένα γενικό πλαίσιο και θεωρείται ως μέρος της συνολικής στρατηγικής της ηλεκτρονικής διακυβέρνησης. Παρόλο που δεν υπάρχει καμία στρατηγική, υπάρχουν δύο είδη έργων μέχρι σήμερα. Από τη μια πλευρά είναι η δημιουργία ενός στρατηγικού σχεδίου για την άρση των εμποδίων που παρακωλύουν άσκοπα τη χρήση του υπολογιστικού νέφους στο δημόσιο τομέα κυρίως ζητήματα σε σχέση με τη ρύθμιση και την ασφάλεια. Επιπλέον στα σχέδια της στρατηγικής είναι η προσαρμογή της νομοθεσίας της Δανίας για τα δεδομένων προσωπικού χαρακτήρα, την ενημέρωση και την ερμηνεία του κανονισμού, έτσι ώστε να είναι πιο σύγχρονο και να μην εμποδίζει τη χρήση του νέφους άσκοπα. Από την άλλη πλευρά ήδη λειτουργούν κάποια έργα προκειμένου να πειραματιστούν και να αξιολογηθεί η απόδοση τους, π.χ. :

- Ένα πιλοτικό έργο για τη μετάβαση της κεντρικής πλατφόρμας NemHandel, ένα σύστημα ηλεκτρονικής τιμολόγησης έτσι ώστε να αποκτήσουν εμπειρία με τις νέες τεχνολογίες
- μια πιλοτική δοκιμή με τη μετάβαση της πύλης Digitalisér.dk, μιας κοινότητας για την ανταλλαγή πληροφοριών μεταξύ του δημόσιου τομέα, τις επιχειρήσεις και τους πολίτες
- Η μονάδα στατιστικών στοιχείων της πύλης πληροφοριών για τους πολίτες Borger.dk

Το **NemHandel** [17] είναι μια υπηρεσία που έχει μεταφερθεί σε περιβάλλον υπολογιστικού νέφους και απευθύνεται σε επιχειρήσεις ή οποιαδήποτε οντότητα που πρέπει να λάβει και να στείλει ψηφιακά τιμολόγια προς και από το δημόσιο τομέα. Η

ηλεκτρονική τιμολόγηση είναι μέρος της δανέζικης στρατηγικής ηλεκτρονικής διακυβέρνησης, η οποία έχει ως στόχο να παρέχει την καλύτερη ποιότητα, την αποτελεσματικότητα στο δημόσιο τομέα. Η μετάβαση έγινε διότι το προηγούμενο περιβάλλον ήταν ασταθής λόγω των υψηλών διακυμάνσεων του όγκου της κυκλοφορίας για την μείωση του λειτουργικού κόστους και να αποκτήσουν την εμπειρία σχετικά με το υπολογιστικό νέφος.

Οι συζητήσεις για τη μετάβαση στο νέφος ξεκίνησαν το 2009 από τη Δανέζικη Υπηρεσία (Digitaliseringsstyrelsen) για την ψηφιοποίηση του δημόσιου τομέα και η εγκατάσταση ξεκίνησε τον Ιούνιο του 2010. Από την 1η Μαΐου 2011, είναι υποχρεωτικό οι δημόσιες αρχές να λαμβάνουν τιμολόγια μέσω της υποδομής NemHandel. Η υποδομή του Nemhandel διευκολύνει την κυβέρνηση και των επιχειρήσεων στις μεταξύ τους συναλλαγές.

Υποδομή νέφους

Το έργο υλοποιήθηκε από δύο προμηθευτές:

- Η Amazon με την AWS για την υποδομή. Η Amazon θεωρήθηκε ως ο πιο έμπειρος προμηθευτής σε ανάλογα έργα.
- Η Netic, δανέζικος πάροχος της πληροφορικής η οποία έχει το ρόλο του μεσίτη νεφους μεταξύ του Amazon και του Οργανισμού για την ψηφιοποίηση.

Απαιτήσεις ασφάλειας και ιδιωτικό απόρρητο

Στην περίπτωση του NemHandel η συμφωνία με το πάροχο είναι να εξασφαλίζει τη διαθεσιμότητα της υπηρεσίας 24 ώρες το 24ωρο εφαρμογής και να τηρεί το νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων

Αναμενόμενα οφέλη

Όσον αφορά το κόστος εκτιμάται ότι η εξοικονόμηση κόστους είναι περίπου 50%. Το αρχικό κόστος της μετανάστευσης ήταν 725.000 DKK αλλά τελικά ανήλθε σε 1.650.000 DKK. Αν και υπήρχαν συμπληρωματικές δαπάνες λειτουργίας όπως η παρακολούθηση των εφαρμογών και των πόρων, τη συντήρηση, τη διαχείριση βάσεων δεδομένων, λειτουργίες υποστήριξης, η υπέρβαση του προϋπολογισμού ήταν λόγω των

επενδύσεων στην παραγωγή αλλά οφείλεται λόγο έλλειψη εμπειρίας με την AWS και την έλλειψη σταθερότητας του περιβάλλοντος AWS.

4.4 Ελλάδα

Σύμφωνα από τα αποτελέσματα έρευνας [18] του 2012, που πραγματοποιήθηκε από την Ipsos Public Affairs για τη BSA, με τη συμμετοχή σχεδόν 4.000 χρηστών υπολογιστών σε εννέα χώρες της Ευρωπαϊκής Ένωσης (Αυστρία, Βέλγιο, Γαλλία, Γερμανία, Ελλάδα, Ουγγαρία, Πολωνία, Ρουμανία, Ηνωμένο Βασίλειο), μόλις το 24% των συμμετεχόντων χρησιμοποιούν εφαρμογές «cloud» (όπως online υπηρεσίες email ή online επεξεργασία κειμένων) σε σύγκριση με 34% των χρηστών σε διεθνές επίπεδο. Η εξοικείωση με το «υπολογιστικό νέφος» διαφέρει σημαντικά στην ενιαία Ευρωπαϊκή Αγορά, με 1 στους 4 χρήστες υπολογιστών στο Ηνωμένο Βασίλειο (28%) και στην Ελλάδα (24%), να καταγράφουν υψηλά επίπεδα εξοικείωσης, σε σύγκριση με έναν στους δέκα χρήστες στην Πολωνία (9%) και τη Γαλλία (10%). Η χρήση του υπολογιστικού νέφους στην Ελλάδα καταγράφει πολύ υψηλό ποσοστό (39%), αρκετά υψηλότερο τόσο από τον Ευρωπαϊκό, όσο και από το διεθνή μέσο όρο. Τα αντίστοιχα ποσοστά στις πιο ανεπτυγμένες Ευρωπαϊκές αγορές είναι σημαντικά χαμηλότερα, καθώς μόλις το 17% των Γερμανών, 18% των Βέλγων και 19% των Γάλλων, δηλώνουν ότι έχουν πρόσβαση σε εφαρμογές του «νέφους».

Σε αυτό συνέβαλε η εθνική αναπτυξιακή στρατηγική 2007-2013. Σύμφωνα με το ΕΣΠΑ 2007-2013, πριν τη στρατηγική 2007-2013, η θέση της Ελλάδας στις τεχνολογίες πληροφορικής και επικοινωνιών, συγκρινόμενη τόσο με τις υπόλοιπες χώρες της ΕΕ όσο και παγκοσμίως, βρισκόταν στα χαμηλότερα επίπεδα. Κατά την τελευταία δεκαετία, οι νέες τεχνολογίες δεν συνέβαλαν σε μεγάλο βαθμό στη βελτίωση της παραγωγικότητας της ελληνικής οικονομίας και στη βελτίωση της ποιότητας ζωής των πολιτών

Ο στόχος της εθνικής αναπτυξιακής στρατηγική ήταν η διεύρυνση των αναπτυξιακών δυνατοτήτων της χώρας, στην επιτάχυνση του ρυθμού οικονομικής μεγέθυνσης και στην αύξηση της παραγωγικότητας σε επίπεδα υψηλότερα του μέσου κοινοτικού όρου, για την επίτευξη της πραγματικής σύγκλισης και τη βελτίωση της ποιότητας ζωής όλων των πολιτών χωρίς αποκλεισμούς. Ένα από τα βασικά προγράμματα που βοήθησαν είναι η Ψηφιακή Σύγκλιση και αποτέλεσε προπομπός του Ορίζοντα 2020. Η Ψηφιακή

Σύγκλιση κατά κύριο λόγο συμβάλει στον 6ο Γενικό Στόχο του ΕΣΠΑ, εντάσσεται στη 2η θεματική προτεραιότητα που αφορά στην Κοινωνία της Γνώσης και Καινοτομίας και στοχεύει στην αποτελεσματικότερη αξιοποίηση των τεχνολογιών πληροφορικής και επικοινωνιών (ΤΠΕ). Στόχος του προγράμματος είναι να αναδείξει τις αναπτυξιακές κατευθύνσεις και να εξειδικεύσει τη στρατηγική, τα μέσα και τις παρεμβάσεις για την αποδοτική και βιώσιμη αξιοποίηση των Τεχνολογιών Πληροφορικής και Επικοινωνιών (ΤΠΕ) στην Ελληνική οικονομία και κοινωνία.

Το **Ε.Π. «Ψηφιακή Σύγκλιση» 2007-2013** [19] έχει προϋπολογισμό συνολικής δημόσιας δαπάνης της τάξης των 1,147 εκ €, (κοινοτική συνδρομή Κ.Σ. της τάξη 860,0 εκ €), τα οποία κατανέμονται ανά Άξονα. Ο συνολικός συγχρηματοδοτούμενος προϋπολογισμός από την Ε.Ε. ανέρχεται σε 1,07 δισεκατομμύρια ΕΥΡΩ, εκ των οποίων τα 860 εκατομμύρια είναι η κοινοτική συνδρομή και τα 215 εκατομμύρια εθνική συμμετοχή. Για την υλοποίηση των έργων αναμένεται να αξιοποιηθεί και ιδιωτική συμμετοχή ύψους 320 εκατομμυρίων ΕΥΡΩ. Το σύνολο των ανωτέρω ποσών υπολογίζεται να ανέλθει στα 1,47 δισεκατομμύρια ΕΥΡΩ.

4.5 Νομικό πλαίσιο Ελλάδος

Παρόλο την ύπαρξη εθνικής στρατηγικής για την χρήση υπηρεσιών νέφους η Ελλάδα είναι από τις χώρες στις όποιες δεν υπάρχει νομικό πλαίσιο για να ρυθμίζει τη χρήση αυτών. Παρόλο αυτά υπάρχει νομικό και ρυθμιστικό πλαίσιο που αφορά τη ρύθμιση των ευαίσθητων και προσωπικών δεδομένων και έχει ενσωματώσει κοινοτικές οδηγίες με κάποιες αλλαγές.

4.5.1 Ανεξάρτητοι φορείς

Επιπλέον υπάρχουν 2 ανεξάρτητοι φορείς (ΑΔΑΕ, ΑΠΔΠΧ) οι όποιοι είναι αρμόδιοι για την προστασία και διασφάλιση των προσωπικών δεδομένων.

- Η **Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα** είναι ο αρμόδιος φορέας για την εφαρμογή αυτής της νομοθεσίας στην Ελλάδα (νόμοι 2472/1997 και 3471/2006). Αποστολή της Αρχής αποτελεί η προστασία των δικαιωμάτων της προσωπικότητας και της ιδιωτικής ζωής του ατόμου στην Ελλάδα, σύμφωνα με τις

διατάξεις των Ν. 2472/1997 και 3471/2006. Ο πρωταρχικός σκοπός της Αρχής [20] είναι η προστασία του πολίτη από την παράνομη επεξεργασία των προσωπικών του δεδομένων αλλά και η συνδρομή προς αυτόν σε κάθε περίπτωση που διαπιστώνεται παραβίαση των σχετικών δικαιωμάτων του σε κάθε επιχειρησιακό τομέα (χρηματοπιστωτικό, υγεία, ασφάλιση, εκπαίδευση, δημόσια διοίκηση, μεταφορές, ΜΜΕ, κ.ο.κ). Επιπλέον σκοπός της Αρχής είναι η υποστήριξη και καθοδήγηση των υπεύθυνων επεξεργασίας στην εκπλήρωση των υποχρεώσεων τους απέναντι στο νόμο και την αντιμετώπιση των νέων τεχνολογιών και εφαρμογών λαμβάνοντας υπόψη τις νέες ανάγκες υπηρεσιών της ελληνικής κοινωνίας. Επίσης η Αρχή ασκεί έλεγχους για να εξακριβώσει αν γίνεται άμεσα η έμμεσα η συναίνεση του αντικειμένου των δεδομένων με τον υπεύθυνο επεξεργασίας τους, για ποιο λόγο θέλει να τα χρησιμοποιήσει και ποια στοιχεία μας. Ο ανεξάρτητος φορέας τα τελευταία χρόνια λαμβάνει ολοένα αυξανόμενο αριθμό καταγγελιών για περιστατικά παραβίασης προσωπικών δεδομένων από διάφορες κατηγορίες υπευθύνων επεξεργασίας που σχετίζονται κυρίως με παραβίαση της ασφάλειας των δεδομένων, δηλαδή παραβίαση του άρθρου 10 ν. 2472/1997.

- Με το άρθρο 1 συστάθηκε, σύμφωνα με την παράγραφο 2 του άρθρου 19 του Συντάγματος, η **Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ)** [21] με σκοπό την προστασία του νόμου 3115/2003 απορρήτου των επιστολών, της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο καθώς και την ασφάλεια των δικτύων και πληροφοριών. Στην έννοια της προστασίας του απορρήτου των επικοινωνιών περιλαμβάνεται και ο έλεγχος της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου, που προβλέπονται από τον νόμο.

4.5.2 Ενσωμάτωση κοινοτικών οδηγιών

Παρακάτω παραθέτουμε τις κοινοτικές οδηγίες που έχουν ενσωματωθεί στο εσωτερικό δίκαιο της Ελλάδας

- Η **Οδηγία 95/46/ΕΚ** Η Ελλάδα υπήρξε από τις πρώτες χώρες που μετέφεραν την κοινοτική Οδηγία στο εσωτερικό δίκαιο. Το ελληνικό νομοθετικό πλαίσιο για την προστασία προσωπικών δεδομένων συγκροτείται από το συνταγματικό δικαίωμα προστασίας προσωπικών δεδομένων όπως κατοχυρώνεται στο άρθρο

9 Α του Συντάγματος, τον νόμο 2472/97 (ΦΕΚ Α' 50/10.04.1997) για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Ο βασικός σκοπός του νόμου [22] είναι η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και σκοπός του η προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής. Οι διατάξεις και επιταγές του νόμου καταλαμβάνουν, χωρίς διαφοροποιήσεις και τον δημόσιο και ιδιωτικό τομέα. Ο ν. 2472/97 συνιστά ένα πλαίσιο κανόνων που εδράζεται σε τέσσερις πυλώνες: α) σε ένα σύστημα ουσιαστικών ρυθμίσεων που θέτει αφενός τις προϋποθέσεις νομιμότητας της επεξεργασίας προσδιορίζοντας δεσμευτικά το σημείο ισορροπίας μεταξύ των αντιτιθεμένων δικαιωμάτων και συμφερόντων και αφετέρου τις βασικές αρχές του νόμου με έμφαση στην αρχή του σκοπού και της αναλογικότητας (άρθρα 4-10), β) στην απονομή δικαιωμάτων στα πρόσωπα ώστε να προστατεύσουν τα δικαιώματα και συμφέροντά τους (άρθρα 11-14), γ) στην εισαγωγή και οργάνωση ανεξάρτητου θεσμικού ελέγχου της προστασίας προσωπικών δεδομένων ώστε να εξασφαλίζεται η εφαρμογή της νομοθεσίας (άρθρα 15-20) και δ) στους κανόνες που προβλέπουν διοικητικές, ποινικές και αστικές κυρώσεις σε περιπτώσεις παράβασης του νόμου (άρθρα 21-23).

- Η **Οδηγία 97/66/ΕΚ** του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα, η οποία εισήχθη στο ελληνικό δίκαιο με το **ν. 2774/1999**, "Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα". Από τις σημαντικότερες ρυθμίσεις που επιβάλλονται από την οδηγία και από το άρθρο 9 του Ν. 2774/97 [23] συνίσταται ότι η αποστολή ηλεκτρονικών μηνυμάτων "για κάθε είδους διαφημιστικούς σκοπούς" είναι επιτρεπτή μόνο στην περίπτωση συνδρομητών που έχουν δώσει εκ των προτέρων τη ρητή συγκατάθεσή τους. Έτσι η αποστολή μη ζητηθέντος ηλεκτρονικού μηνύματος συνιστά παράνομη επεξεργασία, εφόσον τα υποκείμενα δεν είχαν δώσει ρητή συγκατάθεσή τους προηγουμένως

- Η **Οδηγία 2002/58/ΕΚ**[24] του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Ιουλίου 2002 αποτελεί μέρος των ρυθμίσεων για τις τηλεπικοινωνίες

και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών. Ο βασικός σκοπός είναι ότι ο πάροχος υπηρεσιών ηλεκτρονικών υπηρεσιών να εξασφαλίζει την πρόσβαση στα προσωπικά δεδομένα έχει μόνο εξουσιοδοτημένο προσωπικό και διασφαλίζει ότι τα δεδομένα αυτά από τυχαία καταστρέφει η αλλοίωση. Επίσης θέτει ότι για φυσικά πρόσωπα η συγκατάθεση των αντικειμένων εμπορικής επικοινωνίας είναι υποχρεωτική ενώ για τα νομικά πρόσωπα δίδεται στα κράτη-μέλη η κατά διακριτική ευχέρεια δυνατότητα επιλογής μεταξύ ενός συστήματος.

- **Η Οδηγία 2009/136/ΕΚ**[25] τροποποίησε την παραπάνω οδηγία και θέτει ότι παρόλο τη ενημέρωση του χρήστη μέσω των όρων πολιτικής απορρήτου της ιστοσελίδας πλέον καθίσταται υποχρεωτική η συγκατάθεση του. Η συγκατάθεση του χρήστη μπορεί να δίνεται μέσω ρυθμίσεων στον φυλλομετρητή ή μέσω άλλων εφαρμογών. Ο νόμος εξουσιοδοτεί την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ.) για τον προσδιορισμό των τρόπων παροχής πληροφοριών και δήλωσης της συγκατάθεσης. Στο πεδίο εφαρμογής εμπίπτουν τα cookies που χρησιμοποιούνται για διαφήμιση είτε αυτά εγκαθίστανται από τον ίδιο τον κάτοχο της ιστοσελίδας, είτε από άλλα διαφημιστικά δίκτυα μέσω της επισκεπτόμενης ιστοσελίδας.

Με τον νόμο 3471/06 (ΦΕΚ Α’ 133/28.06.2006) και τις τροποποιήσεις που εισήχθησαν στον Ν. 2472/97 θα πρέπει να γίνεται η γνωστοποίηση περιστατικών παραβίασης προσωπικών δεδομένων, η υποχρέωση των παρόχων για τη λήψη κατάλληλων μέτρων και στην εγκατάσταση cookies.

Το 2001 κατά την αναθεώρηση του Συντάγματος περιλήφθηκε ένα νέο άρθρο (9Α) που ορίζει ότι «καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει. Η διασφάλιση της προστασίας των προσωπικών δεδομένων ανατίθεται από τον αναθεωρητικό νομοθέτη σε ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, όπως νόμος ορίζει». Την εποπτεία της εφαρμογής των άνω νομοθετικών κειμένων έχει στην Ευρώπη Ο Ευρωπαίος Επόπτης Προσωπικών Δεδομένων και στην Ελλάδα η Αρχή Προστασίας Προσωπικών Δεδομένων. Η Αρχή Προστασίας Προσωπικών Δεδομένων

έχει από το νόμο αρμοδιότητα να εκδίδει οδηγίες και αποφάσεις και να γνωμοδοτεί για κάθε ρύθμιση που αφορά την επεξεργασία και προστασία δεδομένων προσωπικού χαρακτήρα. Επιπλέον οι πάροχοι των υπηρεσιών ηλεκτρονικών επικοινωνιών υποχρεούνται να γνωστοποιούν στις αρμόδιες αρχές (ΑΠΔΠΧ, ΑΔΑΕ), καθώς και στους θιγόμενους συνδρομητές ή χρήστες, περιστατικά παραβίασης προσωπικών δεδομένων. Επίσης υποχρεούνται να τηρούν σχετικό αρχείο παραβιάσεων. Αυτά ορίζει το άρθρο 12 του ν. 3471/2006 μετά την τελευταία τροποποίησή του. Η Ε.Ε. θα ορίσει σύντομα τις λεπτομέρειες, τις περιστάσεις και τον τρόπο της γνωστοποίησης, που θα ισχύουν για όλα τα κράτη μέλη.

Πλήγμα στο σύστημα προστασίας επέφερε το άρθρο 8 του ν. 3625/07 [26] που εισήγαγε την εξαίρεση ενός ευρύτατου φάσματος επεξεργασίας προσωπικών δεδομένων, συγκεκριμένα αυτής που πραγματοποιείται από τις δικαστικές, εισαγγελικές αρχές και τις διωκτικές αρχές για την εξυπηρέτηση των αναγκών της λειτουργίας τους με σκοπό τη βεβαίωση εγκλημάτων, από το πεδίο εφαρμογής του νόμου και κατ' επέκταση από την εποπτεία της Αρχής. Η εξαίρεση αυτή που αφορά έναν τομέα εντασσόμενο στον σκληρό πυρήνα της κρατικής δράσης θέτει μείζονα ζητήματα συνταγματικότητας.

4.5.3 Παράδειγμα χρήσης υπολογιστικού νέφους στην Ελλάδα

Από τα πιο σημαντικά έργα που πρόκειται να υλοποιηθούν στον δημόσιο τομέα με την χρήση της τεχνολογίας του υπολογιστικού νέφους και προέρχεται από το Επιχειρησιακό Πρόγραμμα «Ψηφιακή Σύγκλιση» είναι η δημιουργία του κόμβου G-Cloud της Γενικής Γραμματείας Πληροφοριακών Συστημάτων (ΓΓΠΣ) [27] και αφορά τις Κεντρικές Υπολογιστικές Υποδομές της ΚτΠ ΑΕ (Κοινωνία της Πληροφορίας ΑΕ) προκηρύχτηκε με ανοιχτό διεθνή διαγωνισμό το 2013.Πρόκειται για ένα έργο για τον εκσυγχρονισμό του δημοσίου τομέα και τη μετάβασή του σε συστήματα νέφους computing με προϋπολογισμό 14.709.570 ευρώ ενώ ο χρόνος υλοποίησης έχει οριστεί σε 24 μήνες από την υπογραφή της Σύμβασης.

Αναλυτικότερα το αντικείμενο του έργου αποτελεί ο σχεδιασμός, η υλοποίηση και η θέση σε πλήρη λειτουργία δύο Κεντρικών Υπολογιστικών Κέντρων της ΚτΠ ΑΕ και της ΓΓΠΣ, τα οποία θα παρέχουν υπολογιστική και αποθηκευτική ισχύ μέσω

προηγμένων οριζόντιων υποδομών υλικού και λογισμικού ΤΠΕ. Τα δύο Κέντρα Δεδομένων θα λειτουργούν αυτόνομα. Οι υποδομές που θα αναπτυχθούν θα χρησιμοποιηθούν για την προσφορά υπηρεσιών οι οποίες θα καλύπτουν τις ανάγκες της ευρύτερης Δημόσιας Διοίκησης, πιο συγκεκριμένα, τις ανάγκες σε υπολογιστική και αποθηκευτική ισχύ των κεντρικών συστημάτων πρωτίστως δράσεων για τις οποίες οι Φορείς Λειτουργίας του Έργου (ΦΛτΕ) είναι οι τελικοί δικαιούχοι στα πλαίσια της τέταρτης προγραμματικής περιόδου αλλά και λοιπών κεντρικών συστημάτων τρίτων Φορέων της Δημόσιας Διοίκησης που θα υποδειχθούν. Τα υπολογιστικά κέντρα θα εγκατασταθούν σε ειδικά διαμορφωμένο αυτοτελή χώρο, ο οποίος θα διαμορφωθεί και εξοπλισθεί με κατάλληλο εξοπλισμό μέσω ξεχωριστού διαγωνισμού. Το φυσικό αντικείμενο του έργου περιλαμβάνει προμήθεια εξοπλισμού, τυποποιημένου λογισμικού και εφαρμογών – στοιχεία τα οποία θα εξασφαλίσουν την τεχνολογική ικανότητα στους ΦΛτΕ να λειτουργούν αυτόνομα και ανεξάρτητα τα νέα Κέντρα Δεδομένων παρέχοντας ψηφιακές υπηρεσίες προστιθέμενης αξίας υψηλής ποιότητας προς συνεργαζόμενους φορείς, με τρόπο ασφαλή, ελαστικό, και ευέλικτο.

Με την υλοποίηση του παρόντος προτεινόμενου έργου οι ΦΛτΕ, αφενός θα έχουν επιτύχει την προετοιμασία και θέση σε πλήρη λειτουργία προηγμένων υπολογιστικών εξοπλισμών και λογισμικών υποδομής private και public cloud και αφετέρου θα έχουν καθορίσει και υλοποιήσει όλες τις αναγκαίες διαδικασίες για την βέλτιστη διαχείριση και χρήση τους με απώτερο σκοπό την προσφορά των σχετικών εσωστρεφών και εξωστρεφών υπηρεσιών. Επιπρόσθετα, θα είναι σε θέση να συμβάλουν στην αποδοτικότερη Υλοποίηση και Παραγωγική Λειτουργία έργων ΤΠΕ των φορέων της Δημόσιας Διοίκησης για τους οποίους είναι τελικοί δικαιούχοι, επιτρέποντας τους να αποκτήσουν εύκολη και γρήγορη πρόσβαση σε νέες προηγμένες υπηρεσίες που θα προσφέρονται πάνω από τεχνολογίες οριζόντιων υποδομών παροχής υπολογιστικής και αποθηκευτικής ισχύος με τρόπο ευέλικτο και ελαστικό. Πιο συγκεκριμένα, στα αναμενόμενα οφέλη συμπεριλαμβάνονται:

- Αύξηση της διαθεσιμότητας και της απόδοσης των πληροφοριακών συστημάτων της Δημόσιας Διοίκησης με την υιοθέτηση του μοντέλου ευέλικτων και αποτελεσματικών κέντρων δεδομένων τα οποία παρέχουν πόρους ελαστικά και με βελτιωμένη ανθεκτικότητα σε αστοχίες και άλλες καταστροφές.

- Αύξηση της αποδοτικότητας και της ασφάλειας των πληροφοριακών συστημάτων της Δημόσιας Διοίκησης.
- Οικονομίες κλίμακας μέσω της μείωσης του συνολικού κόστους που προκύπτει από την διαχείριση και συντήρηση πληροφοριακών συστημάτων.
- Βελτίωση της συνολικής "εμπειρίας του Πολίτη", λόγω της κεντρικής υπόστασης των υπηρεσιών των Κέντρων Δεδομένων, μέσω της οποίας θα επιτυγχάνεται μικρότερο χρονικό διάστημα για την παροχή των εφαρμογών και κατ' επέκταση άμεση ανταπόκριση στην αύξηση των αναγκών κλπ.
- Βελτίωση της δυνατότητας διαλειτουργικότητας και διασυνδεσιμότητας των φιλοξενούμενων πληροφοριακών συστημάτων και ως εκ τούτου διευκόλυνση της εφαρμογής ψηφιακών υπηρεσιών προστιθέμενης αξίας για τις επιχειρήσεις και τους πολίτες της χώρας.

Ασφάλεια και προστασία των συστημάτων και των δεδομένων της υποδομής του Κέντρου Δεδομένων

Η σχεδίαση του έργου σύμφωνα με την προκήρυξη θα πρέπει να διασφαλίζεται ο δυναμικός και ελαστικός τρόπος διάθεσης των ενοποιημένων υποδομών των φορέων που θα συμμετέχουν στο νέφος με τρόπο διαφανή προς τον συνεργαζόμενο φορέα και κυρίως ασφαλή όσον αφορά την ακεραιότητα των διακινούμενων και αποθηκευμένων προσωπικών δεδομένων των πολιτών (Ν. 2472/1997, 3471/2006). Πέρα από τα παραπάνω, ο υποψήφιος Ανάδοχος θα πρέπει να λάβει ειδική μέριμνα και να δρομολογήσει τις κατάλληλες δράσεις για:

- την ασφάλεια των Πληροφοριακών Συστημάτων, Εφαρμογών, Μέσων και Υποδομών του κάθε Κέντρου Δεδομένων

- την προστασία της ακεραιότητας και της διαθεσιμότητας των πληροφοριών που αφορούν στην λειτουργία των υποδομών του κάθε Κέντρου Δεδομένων (infrastructure data)

- την προστασία τυχόν προς επεξεργασία και αποθηκευμένων προσωπικών δεδομένων στις βάσεις δεδομένων της υποδομής ή αλλού των αναζητώντας και

εντοπίζοντας με μεθοδικό τρόπο τα τεχνικά μέτρα και τις οργανωτικό-διοικητικές διαδικασίες που απαιτούνται.

Επιπλέον για τον σχεδιασμό και την υλοποίηση των τεχνικών μέτρων ασφαλείας του έργου, ο ανάδοχος θα πρέπει να λάβει υπόψη του:

- το θεσμικό και νομικό πλαίσιο που ισχύει (π.χ. προστασία των προσωπικών δεδομένων Ν. 2472/97, προστασία των προσωπικών δεδομένων στον τηλεπικοινωνιακό τομέα Ν. 2774/99)
- τις σύγχρονες εξελίξεις στις ΤΠΕ
- τις βέλτιστες πρακτικές στο χώρο της Ασφάλειας στις ΤΠΕ
- τα επαρκέστερα διατιθέμενα προϊόντα λογισμικού και υλικού
- τυχόν πρότυπα (ISO27001) τα οποία θα περιλαμβάνονται στο «Πλάνο Ενεργειών για τη Ασφάλεια και προστασία των συστημάτων και των δεδομένων της υποδομής των Κέντρων Δεδομένων» που θα παραδοθεί από τον Ανάδοχο στην Αναθέτουσα Αρχή.

Ο ανάδοχος, στην πρόταση του, θα πρέπει να διατυπώσει τη μεθοδολογία ανάλυσης και αντιμετώπισης των ζητημάτων ασφαλείας που άπτονται των παραπάνω ζητημάτων, περιγράφοντας τους μηχανισμούς ελέγχου και τις τεχνολογικές λύσεις που περιέχονται στην προτεινόμενη λύση. Κατ' ελάχιστον θα πρέπει να γίνει καταγραφή των εξής:

- Καταγραφή Απαιτήσεων Συμμόρφωσης με Θεσμικό, Νομικό και Κανονιστικό Πλαίσιο
- Συμφωνία πεδίου εφαρμογής της Διαχείρισης της Ασφάλειας
- Ανάλυση Επιχειρηματικών Επιπτώσεων, απειλών και αδυναμιών
- Ανάπτυξη Σχεδίου Διαχείρισης Κινδύνων ISO27001
- Ανάπτυξη Πολιτικών Ασφάλειας Πληροφοριών,
- Ανάπτυξη Διαδικασιών Ασφάλειας

Επιθεωρητές (auditors) Έργου

Στο πλαίσιο υλοποίησης του Έργου, η ΚτΠ Α.Ε δύναται να αναθέσει σε στελέχη της ή τρίτο ανεξάρτητο όργανο τη διενέργεια τακτικών ή έκτακτων επιθεωρήσεων Έργου (project audits) για την πιστοποίηση της πορείας των εργασιών και την καταγραφή συμπερασμάτων και περιοχών παρέμβασης ή βελτίωσης. Ο Ανάδοχος οφείλει να συμμορφωθεί με τις υποδείξεις κατόπιν σχετικής έγκρισης που θα επικυρώνεται από το αρμόδιο όργανο της ΚτΠ Α.Ε. Οι ΦΛτΕ διατηρούν το δικαίωμα να αναθέσουν σε ανεξάρτητο εξειδικευμένο φορέα τη διεξαγωγή δοκιμών ασφάλειας στα έτη υποχρεωτικής εγγύησης, τα συμπεράσματα των οποίων πρέπει να ληφθούν υπόψη από τον ανάδοχο ο οποίος και υποχρεούται να προβεί στις απαραίτητες διορθωτικές ενέργειες.

4.6 Περιπτώσεις παραβίασης δεδομένων

Παρακάτω παραθέτουμε διάφορες περιπτώσεις και καταγγελίες παραβίασης προσωπικών δεδομένων που αφορούν χώρες της Ευρωπαϊκής Ένωσης.

4.6.1 Δανία

Το 2011 ο δήμος της Οντένσε [28] ζήτησε τη γνωμοδότηση από την Datatilsynet για να χρησιμοποιήσει τις υπηρεσίες νέφους της Google σε όλα τα σχολεία. Η αρχή προστασίας προσωπικών δεδομένων Datatilsynet απέρριψε την χρήση των εφαρμογών της Google επειδή ο δήμος δεν είχε τεκμηριώσει ότι τα στοιχεία που πρέπει να υποβάλλονται σε επεξεργασία με τη Google δεν θα μεταφέρονται σε κέντρα δεδομένων εκτός της ΕΕ. Επίσης η ανάλυση επικινδυνότητας και η εκτίμηση των κινδύνων σε σχέση με την ασφάλεια των δεδομένων δεν κρίθηκε ικανοποιητική ενώ η συμφωνία επεξεργασίας δεδομένων μεταξύ του δήμου και Google δεν συμμορφώνεται με τις απαιτήσεις του νομικού πλαισίου της Δανίας.

4.6.2 Ηνωμένο Βασίλειο

Τον Μάρτιο του 2014 η Αρχή Προστασίας Προσωπικών δεδομένων ICO που έχει συσταθεί για την υπεράσπιση των δικαιωμάτων πληροφοριών προς το δημόσιο συμφέρον επέβαλε πρόστιμο ύψους £200.000 στην βρετανική Υπηρεσία Συμβούλων

Εγκυμοσύνης [29] (BPA) για την έκθεση χιλιάδων προσωπικών στοιχείων χρηστών οι όποιοι είχαν ζητήσει τηλεφωνικώς συμβουλές σε θέματα εγκυμοσύνης. Τα προσωπικά δεδομένα δεν αποθηκεύθηκαν με ασφάλεια και μια ευπάθεια στην ιστοσελίδα επέτρεψε χάκερς να έχουν πρόσβαση στο σύστημα. Σύμφωνα με την Αρχή το συγκεκριμένο πρόβλημα συνέβηκε γιατί η βρετανική υπηρεσία δεν γνώριζε ότι στην ιστοσελίδα τους αποθηκεύονταν οι συγκεκριμένες πληροφορίες και δεν διατηρούσε υψηλά επίπεδα ασφάλειας. Επίσης το προσωπικό δεν ήταν εκπαιδευμένο κατάλληλα ενώ οι πόροι που χρησιμοποιούνταν ήταν περιορισμένοι. Επίσης στην αναφορά της η Αρχή επισημαίνει ότι είναι σημαντικό να χρησιμοποιείτε ένας αξιόπιστος πάροχος νέφους που είναι πιο πιθανό να εξασφαλίσει την ασφάλεια της υποδομής. Ωστόσο, προσθέτουν ότι αν μια εφαρμογή είναι ανασφαλές, θα είναι επίσης σε κίνδυνο στο σύννεφο.

Επίσης η εταιρεία της Sony Computer Entertainment Europe τον Μάρτιο του 2013 έλαβε χρηματική ποινή [30] £250.000 από τη Αρχή Προστασίας Προσωπικών δεδομένων (ICO), μετά από μια σοβαρή παραβίαση του νόμου περί προστασίας δεδομένων. Συγκεκριμένα η ποινή προήρθε μετά από κυβερνοεπίθεση στη πλατφόρμα Sony PlayStation Network Platform τον Απρίλιο του 2011. Η επίθεση έθεσε σε κίνδυνο τα προσωπικά στοιχεία των εκατομμυρίων πελατών, όπως ονόματα, διευθύνσεις, διευθύνσεις ηλεκτρονικού ταχυδρομείου, ημερομηνίες γέννησης, κωδικούς πρόσβασης λογαριασμού ακόμα και στοιχεία καρτών. Μια έρευνα της ICO διαπίστωσε ότι η επίθεση θα μπορούσε να είχε αποφευχθεί, αν το λογισμικό της εταιρίας ήταν up-to-date.

4.6.3 Ιταλία

Η περίπτωση της Google [31] Ιταλία είναι ένα παράδειγμα της ερμηνείας της φράσης «στο πλαίσιο των δραστηριοτήτων μιας εγκατάστασης» από εθνικό δικαστήριο στην Ευρωπαϊκή Ένωση. Στην περίπτωση αυτή, το 2010 τρία στελέχη της Google καταδικάστηκαν για αδικήματα για παράβαση της ιταλικής νομοθεσίας προστασίας δεδομένων σε σχέση με ένα βίντεο που ανέβηκε στο Google Video που δείχνει τον ξυλοδαρμό ενός άτομου με ειδικές ανάγκες

Το δικαστήριο αποφάσισε ότι η ιταλική νομοθεσία περί προστασίας των δεδομένων ήταν εφαρμοστέα στην προκειμένη περίπτωση. Το δικαστήριο ανέφερε ότι η κατηγορία στα 3 στελέχη της Google δεν οφείλεται στο περιεχόμενο του βίντεο αλλά ότι η επεξεργασία του βίντεο έγινε σε διακόμιστες στις ΗΠΑ / Ιρλανδία παρόλο που η

Google είχε μια εγκατάσταση στην Ιταλία. Ενώ πρόσθεσε ότι ο ρόλος της Google Italy είναι βοηθητικός και δεν πραγματοποιείται επεξεργασία δεδομένων. Από την άλλη πλευρά οι δικηγόροι της Google ανέφεραν ότι η εταιρία έχει συμμορφωθεί με τους κανόνες της Ευρωπαϊκής Ένωσης και χαρακτήρισαν την απόφαση ως πλήγμα για την ελευθερία του διαδικτύου

4.6.4 Ελλάδα

Στην Ελλάδα η Αρχή Προστασίας Δεδομένων λαμβάνει ολοένα αυξανόμενο αριθμό καταγγελιών για περιστατικά παραβίασης προσωπικών δεδομένων από διάφορες κατηγορίες υπευθύνων επεξεργασίας που σχετίζονται κυρίως με παραβίαση της ασφάλειας των δεδομένων, δηλαδή παραβίαση του άρθρου 10 ν. 2472/1997. Κατά τη διάρκεια του έτους 2012, η Αρχή Προστασίας Δεδομένων επιλήφθηκε 2000 περίπου προσφυγών-αιτήσεων και ερωτημάτων. Παρακάτω έχουμε καταγράψει κάποια ενδεικτικά περιστατικά [32]:

- **Sony Music Entertainment A.E:** Η Αρχή εξέτασε περιστατικό παράνομης δημοσιοποίησης προσωπικών δεδομένων εγγεγραμμένων χρηστών του διαδικτυακού τόπου της εταιρείας που έγινε μετά από παραβίαση ιστοσελίδας της με χρήση της τεχνικής SQL Injection. (59/2012).
- **Τραπεζικά ιδρύματα:** Η Αρχή επέβαλε χρηματικά πρόστιμα σε τραπεζικά ιδρύματα για την έλλειψη μέτρων ασφαλείας κατά την καταστροφή προσωπικών δεδομένων και τα κάλεσε να εφαρμόσουν πλήρως τις σχετικές διατάξεις της Οδηγίας 1/2005. (76/2012).
- **ΟΚΑΝΑ:** Η Αρχή επέβαλε πρόστιμο ύψους τριών χιλιάδων ευρώ στον «Οργανισμό Κατά των Ναρκωτικών - ΟΚΑΝΑ» για την παραβίαση της ασφάλειας προσωπικών δεδομένων. Ειδικότερα, έγγραφα με στοιχεία θεραπευομένων-μελών απορρίφθηκαν εκ παραδρομής, χωρίς προηγουμένως να καταστραφούν, σε κάδους απορριμμάτων κατά τη διάρκεια της μετεγκατάστασης μονάδας του ΟΚΑΝΑ (114/2012).
- **Γενική Γραμματεία Πληροφοριακών Συστημάτων** (Απόφαση 98/2013) πρόστιμο ύψους 150.000 ευρώ για τη μη λήψη κατάλληλων μέτρων ασφάλειας

και τη διαρροή δεδομένων που αφορούν το σύνολο σχεδόν των φορολογουμένων στην Ελλάδα.

Μια περίπτωση καταγγελίας η οποία είναι σε εξέλιξη και αφορά έργο πληροφορικής με τη χρήση υπηρεσιών νέφους. Συγκεκριμένα το Διοικητικό Συμβούλιο της ΟΛΜΕ κατέθεσε στις 7 Μαρτίου 2014 [33] προσφυγή στην Αρχή Προστασίας Προσωπικών Δεδομένων για τη λειτουργία του ηλεκτρονικού συστήματος MySchool του υπουργείου Παιδείας. Το MySchool είναι μια ηλεκτρονική πύλη του Υπουργείου Παιδείας με στόχο τη ενοποίηση των υφιστάμενων πληροφοριακών συστημάτων υποστήριξης της καθημερινής λειτουργίας των σχολικών μονάδων. Το πιο σημαντικό, όμως, είναι ότι το MySchool περιλαμβάνει και καταγράφει πλέον, κάθε τι που αφορά στα διοικητικά των σχολείων της Α/μιας και Β/μιας εκπαίδευσης. Το MySchool εγκαταστάθηκε στους servers του Υπουργείο Παιδείας, προκειμένου να εντοπιστούν και επιλυθούν τα προβλήματα της νηπιακής ηλικίας του. Από τα παραπάνω διαπιστώνουμε ότι ο ρόλος της συγκεκριμένης πλατφόρμας σχεδιάστηκε για να δίνει πληροφορίες οποιαδήποτε στιγμή σε ότι αφορά προσωπικά στοιχεία του ανθρώπινου δυναμικού (Μαθητές και Εκπαιδευτικοί).

Εκτός από την ΟΛΜΕ ο Σύλλογος Εκπαιδευτικών Π.Ε. Κεντρικής και Νότιας Χαλκιδικής μετά από ομόφωνη απόφαση του Δ.Σ. του (18/11/2013) κατέθεσε στις 26/11/2013 έγγραφη καταγγελία στην Αρχή Προστασίας Προσωπικών με το αίτημα για έλεγχο νομιμότητας της ψηφιακής εφαρμογής του συστήματος Myschool ως προς την προστασία προσωπικών δεδομένων μαθητών, γονέων και κηδεμόνων, νομιμότητας και δικαιοδοσίας διευθυντών και προϊσταμένων σχολικών μονάδων να συγκεντρώσουν τα στοιχεία που απαιτούνται από την ψηφιακή εφαρμογή για τους μαθητές. Στις 9 Ιανουαρίου 2014, ο Σύλλογος παρέλαβε έγγραφο από της Αρχής Προστασίας Προσωπικών Δεδομένων, σύμφωνα με το οποίο απευθύνεται στο Υπουργείο Παιδείας και Θρησκευμάτων και ζητάει να απαντήσουν για τα ζητήματα που τίθενται από την καταγγελία. Ένα από τα βασικά ερωτήματα είναι η γνωστοποίηση των νομοθετικών διατάξεων των οποίων προκύπτει η αρμοδιότητα του Υπουργείου Παιδείας και Θρησκευμάτων να συλλέγει και επεξεργάζεται τα δεδομένα των μαθητών και των γονέων-κηδεμόνων τους στο πλαίσιο του ως άνω πληροφοριακού συστήματος και το σκοπό της επεξεργασίας καθώς και το είδος των προσωπικών δεδομένων που

συλλέγονται. Παρόλο αυτά το υπουργείο δεν έχει απαντήσει ακόμα στα ερωτήματα της Αρχής.

4.7 Συμπεράσματα

Σε αυτό το κεφάλαιο μπορούμε να βγάλουμε 2 ειδή συμπερασμάτων. Πρώτο όσον αφορά το νομικό και κανονιστικό πλαίσιο των τεσσάρων χώρων και δεύτερο το τεχνικό μέρος των έργων που έχουν δημιουργηθεί.

Με την ερεύνα της Ipsos για την χρήση του υπολογιστικού νέφους στην Ελλάδα και των άλλων νότιων χωρών της Ευρώπης διαπιστώνουμε μια ευρύτερη τάση στην οποία οι αναπτυσσόμενες αγορές έχουν προσπεράσει πιο ώριμες αγορές με υψηλότερη χρήση υπηρεσιών. Αυτό αποδεικνύεται και στην ανάλυση των παραπάνω χωρών. Πολλές χώρες της νοτίου Ευρώπης ήδη σχεδιάζουν τη μετανάστευση στο υπολογιστικό νέφος ενώ υπάρχουν ήδη αρκετά έργα σε εξέλιξη. Από την άλλη ανεπτυγμένες χώρες που έχουν πιο αυστηρούς κανόνες όσο αφορά το νομικό και κανονιστικό πλαίσιο βρίσκονται ακόμα σε πρώιμο στάδιο.

Το 2013 η Ιταλία και το Ηνωμένο Βασίλειο σύμφωνα με τη BSA ήταν στις πρώτες θέσεις σε ζητήματα ασφάλειας. Σύμφωνα με τις περιπτώσεις παραβίασης δεδομένων στο Ηνωμένο Βασίλειο οφειλόταν σε περιπτώσεις που δεν είχαν τηρηθεί πολιτικές ασφάλειας. Αυτό είχε ως αποτέλεσμα να προστεθεί σαν όρος στη συμφωνία μεταξύ προμηθευτή και κράτους στο Cloudstore ότι η εταιρία θα πρέπει να έχει πιστοποιηθεί από κάποιο πρότυπο ασφαλείας(συνήθως iso 27001). Στην Ελλάδα αν και υπάρχουν αρκετά έργα στον ιδιωτικό και δημόσιο τομέα δεν υπάρχει συγκεκριμένη στρατηγική. Συγκεκριμένα δεν υπάρχει ένα γενικό πλαίσιο κανόνων για έργα που αφορούν υπολογιστικό νέφος αλλά γίνεται ξεχωριστά. Στο τομέα της ασφάλειας οι περιπτώσεις παραβίασης οφείλεται στη μη τήρηση των νόμων και των κανόνων της Αρχής προστασίας δεδομένων προσωπικού χαρακτήρα. Στο τομέα των έργων τα έργα που δημιουργούνται σε νότιες χώρες στοχεύουν σε μεγαλύτερο εύρος χρηστών από την βόρεια Ευρώπη. Για παράδειγμα χώρες όπως η Ιταλία και η Ελλάδα κατασκευάζουν κέντρα δεδομένων ώστε να φιλοξενήσουν και να παρέχουν υπηρεσίες στο δημόσιο τομέα σε αντίθεση με τη Δανία που ακόμα είναι σε επίπεδο εφαρμογών.

Τέλος στο κομμάτι της εξαγωγής δεδομένων όλες οι χώρες ακολουθούν την οδηγία 95/46/ΕΚ δηλαδή η διαβίβαση δεδομένων προσωπικού χαρακτήρα στα κράτη μέλη της ΕΕ και του ΕΟΧ μπορεί να πραγματοποιείτε ενώ απαγορεύουν τη μεταφορά εκτός του

ΕΟΧ, εκτός εάν ο προορισμός εξασφαλίζει επαρκή προστασία για τα δεδομένα ή υπό ειδικές συνθήκες.

ΚΕΦΑΛΑΙΟ 5: Κοινωνικοπολιτικά και ηθικά ζητήματα με τη χρήση υπολογιστικού νέφους

Το παρακάτω κεφάλαιο έχει ως σκοπό να γνωστοποιήσει διάφορα κοινωνικά, ηθικά και πολιτικά ζητήματα τα οποία οφείλονται στην τεχνολογική ανάπτυξη αλλά και στην αλματώδη χρήση του υπολογιστικού νέφους. Με τον πολλαπλασιασμό των κοινωνικών δικτύων και τη χρήση του από τον ευρύτερο δημόσιο και ιδιωτικό τομέα θα δημιουργούνται συνεχώς νέα ζητήματα.

5.1 Ηθικά ζητήματα

Ο γρήγορος ρυθμός της επιστημονικής και τεχνολογικής προόδου του υπολογιστικού νέφους μπορεί να προκαλέσει σοβαρά ερωτήματα ηθικής φύσης που να απασχολούν όλους τους Ευρωπαίους. Αυτά τα ερωτήματα μπορούν επίσης να έχουν πιθανές επιπτώσεις στις μελλοντικές γενιές. Παρακάτω καταγράφουμε κάποια από αυτά:

- Δημοκρατία και κοινωνικά δίκτυα
- Παγκοσμιοποίηση και πολιτιστικός ιμπεριαλισμός
- Ηλεκτρονική αποξένωση

Το ζήτημα της ελεύθερης έκφρασης είναι πολλές φορές στο επίκεντρο των γεγονότων και ειδικά στα κοινωνικά δίκτυα. Τα τελευταία χρόνια βγαίνουν στην δημοσιότητα διάφορα θέματα και ζητήματα που αφορούν κυβερνήσεις και μυστικές υπηρεσίες που κατηγορούνται για έλεγχο ή απαγόρευση της λειτουργία των κοινωνικών δικτύων. Για παράδειγμα στις 20 Απρίλιου ο ιδρυτής του ρωσικού ιστότοπου κοινωνικής δικτύωσης VKontakte[10] (VK) Πάβελ Ντούροφ εγκατέλειψε τη Ρωσία επικαλούμενος εντάσεις με τις αρχές[34]. Ο ιστότοπος κοινωνικής δικτύωσης υπερβαίνει στην πρώην ΕΣΣΔ τον αμερικανό ανταγωνιστή του, το Facebook, με περισσότερους από 100 εκατ. Χρήστες. Ο Ντούροφ δήλωσε πως το Δεκέμβριο είχε αρνηθεί να παραδώσει στη ρωσική Ομοσπονδιακή Υπηρεσία Ασφαλείας (FSB, πρώην KGB) τα προσωπικά δεδομένα των στελεχών της οργάνωσης Ευρωμαϊντάν, η οποία είχε κεντρική θέση στη φιλοευρωπαϊκή αμφισβήτηση στην Ουκρανία. "Η μεταβίβαση προσωπικών δεδομένων

[10] *https://vk.com/*

Ουκρανών στις ρωσικές αρχές θα ήταν όχι μόνον αντίθετη προς το νόμο, αλλά θα συνιστούσε επίσης προδοσία όλων αυτών των εκατομμυρίων κατοίκων της Ουκρανίας που μας έδειξαν εμπιστοσύνη", είχε εξηγήσει τότε από τη σελίδα του στον VK. Ύστερα από τη παραίτηση του εξαγοράστηκε ο ιστοτοπος από δύο στενούς συνεργάτες του Βλαντίμιρ Πούτιν.

Ένα άλλο πρόσφατο παράδειγμα απαγόρευσης αλλά και χρήσης του περιεχομένου του κοινωνικού δικτύου για την εξυπηρέτηση κυβερνητικών συμφερόντων κατηγορήθηκε η Τουρκία. Συγκεκριμένα ο πρωθυπουργός της χώρας Ρετζέπ Ταγίπ Ερντογάν απαγόρευσε τη λειτουργίας[35] του δημοφιλούς κοινωνικού δικτύου twitter. Η Ρυθμιστική Αρχή Τηλεπικοινωνιών, ανήρτησε στην ιστοσελίδα της τρεις δικαστικές αποφάσεις, εξηγώντας πως η απαγόρευση του twitter γίνεται για λόγους προστασίας των πολιτών επειδή η εφαρμογή δεν σεβάστηκε την απόφαση του δικαστηρίου να αποσύρει κάποια συγκεκριμένα links, που υποδείχθηκαν από τις εισαγγελικές αρχές και έπειτα από αγωγές πολιτών για παραβίαση της ιδιωτικότητάς από την πλατφόρμα κοινωνικής δικτύωσης. Η απόφαση της κυβέρνησης της Τουρκίας προκάλεσε κατακραυγή στον διεθνή τύπο που καταγγέλλει λογοκρισία και πλήγμα για την δημοκρατία. Στην Ουάσινγκτον αλλά και στην Ευρωπαϊκή Ένωση εξέφρασαν την ανησυχία τους για την απόφαση της τουρκικής κυβέρνησης λέγοντας ότι η ελευθερία έκφρασης είναι βασική αρχή της ΕΕ.

5.1.1 Πολιτιστικός ιμπεριαλισμός[11]

Οι διαφορετικές απόψεις σχετικά με την ιδιωτική ζωή ενισχύεται περαιτέρω με πολιτιστικές διαφορές. Ως εκ τούτου, οι χρήστες των υπηρεσιών νέφους θα πρέπει να ασχοληθούν με τις διαφορετικές κουλτούρες που επικρατούν σε διάφορες περιοχές οι όποιες επηρεάζουν την προστασία της ιδιωτικής ζωής[36]. Ειδικά δεδομένου ότι οι μεγάλες εταιρείες που είναι κυρίαρχες στο υπολογιστικό νέφος ως επί το πλείστον προέρχονται από δυτικούς πολιτισμούς κυρίως από τις ΗΠΑ. Με την εφαρμογή δυτικών αξίων σε εφαρμογές νέφους, τα πλαίσια και τους κανονισμούς του , μπορεί να οδηγήσει σε αύξηση της πολιτιστικής ομογενοποίησης, την καταστολή τοπικών πολιτισμών. Η παγκοσμιοποίηση μπορεί να διαδραματίσει ένα ρόλο τόνωσης της

[11] Tomlinson, J. (1991). Cultural imperialism: A critical introduction. Bloomsbury Publishing.

αλληλεπίδρασης μεταξύ των άτομα που ανήκουν σε διαφορετικές κοινότητες και κατά συνέπεια, η ανταλλαγή των ηθικών κανόνων και αξιών συμβάλλοντας σε μια παγκόσμια συναίνεση σχετικά με τις ΤΠΕ - ηθική. Στην Κίνα, για παράδειγμα, η επέκταση του πεδίου εφαρμογής της ιδιωτικής ζωής απορρέει από την παγκοσμιοποίηση, ενσωματώνοντας τόσο τις παραδοσιακές κινεζικές αξίες αλλά και τις δυτική αξίες. Το υπολογιστικό νέφος παρέχει όχι μόνο μια επείγουσα ανάγκη για διάλογο μεταξύ διαφορετικών πολιτισμών μπορεί επίσης να συμβάλει παρέχοντας τη σφαιρική υποδομή που είναι αναγκαία για να ανταλλαγή, συνεργασία και επικοινωνία μεταξύ των πολιτισμικών συνόρων.

5.1.2 Ηλεκτρονική αποξένωση

Τέλος ένα άλλο ζήτημα είναι της τεχνολογικής αποξένωσης. Ένα μεγάλο ποσοστό του παγκόσμιου πληθυσμού δεν έχει πρόσβαση στο Internet. Το υπολογιστικό νέφος μπορεί να παρέχει την ελεύθερη έκφραση, την ανταλλαγή πληροφοριών, ιδεών και μπορεί να γίνει μέσο για όλους τους ανθρώπους. Σύμφωνα με μια ερεύνα η Ινδία έχει 100 εκατομμύρια χρήστες του Διαδικτύου η οποία είναι μια τεράστια αγορά. Αλλά εξακολουθεί να αφήνει περισσότερο από 9/10 του πληθυσμού της χώρας δεν μπορεί να εκμεταλλευτούν τα πλεονεκτήματα από το υπολογιστικό νέφος. Για να λυθεί το πρόβλημα οι κυβερνήσεις θα πρέπει να υιοθετήσουν τις τεχνολογίες του νέφους αφού θα αποτελέσει σημαντική συνιστώσα των εθνικών υποδομών ζωτικής σημασίας.

5.2 Πολιτικές επιπτώσεις

Η σημασία των ηθικών ζητημάτων που θέτει το υπολογιστικό νέφος ως τεχνολογική επανάσταση αυξάνει τις κοινωνικές τους επιπτώσεις. Το υπολογιστικό νέφος έχει παρουσιαστεί από πολλούς ως σημαντική μετατόπιση παραδείγματος (paradigm shift). Αυτό οφείλεται ότι η αποθήκευση δεδομένων και η υπολογιστική ισχύς προσφέρονται σαν υπηρεσίες κοινής ωφέλειας, όπως ο ηλεκτρισμός αλλά δημιουργεί αρκετούς κινδύνους και αποτελεί πολιτισμική απόφαση και όχι μόνο τεχνολογική[12]. Αν υποθέσουμε ότι τα συστήματα ασφαλείας των υπολογιστών δεν είναι άριστα και επιρρεπή σε προβλήματα τότε το άλμα προς το νέφος μπορεί να είναι καταστροφικό. Οι πάροχοι του νέφους υποστηρίζουν ότι εφόσον οι πληροφορίες θα γίνουν πιο

[12] http://www.bbc.co.uk/news/business-12779201

συγκεντρωτικές τότε και οι ίδιοι θα μπορούν να επενδύσουν περισσότερα χρήματα σε συστήματα ασφαλείας. Η συγκέντρωση των πληροφοριών και η χρήση του υπολογιστικού νέφους από πολλές εταιρείες είχε ως αποτέλεσμα την αύξηση των κυβερνο-επιθέσεων. Για παράδειγμα η Google το 2010 [37] σταμάτησε τις δραστηριότητες της στην Κίνα λόγω σοβαρών επιθέσεων. Οι επιθέσεις ήταν οργανωμένες και φάνηκαν αρκετά επικίνδυνες για την εταιρεία αφού εγκατέλειψε ένα πολύ μεγάλο μερίδιο της αγοράς παγκοσμίως. Ως αποτέλεσμα, μπορούμε να συμπεράνουμε ότι η Google ως πάροχος δεν είναι σε θέση να διαβεβαιώσει την αποτελεσματική προστασία των συστημάτων τους.

Σύμφωνα με την Google οι επιθέσεις στόχευαν σε λογαριασμούς ηλεκτρονικού ταχυδρομείου Κινέζων ακτιβιστών υπέρ των ανθρωπίνων δικαιωμάτων. Συνεπώς μπορούμε να υποθέσουμε ότι υπήρχε μια σχέση με τις πολιτικές ιδεολογίες των χρηστών. Ωστόσο, το πρόβλημα μπορεί να γίνει πιο ισχυρό εάν συμβάλλουν στην συγκέντρωση των πληροφοριών σε ένα μικρότερο αριθμό συστημάτων ενώ μπορεί να αποτελέσει σοβαρή απειλή για την κοινωνία και θέτει σε κίνδυνο την ελευθερία του λόγου. Όπως και στην περίπτωση της Google στην Κίνα το ίδιο μπορεί να γίνει με οργανώσεις τρομοκρατών ή κυβερνήσεις για τον έλεγχο και την παρακολούθηση των δράσεων των πολιτών τους ή αντίπαλων κρατών. Ένα άλλο παράδειγμα είναι το διακρατικό πρόβλημα μεταξύ Ρωσίας και Ουκρανίας. Αν και δεν υπάρχει κάποια συγκριμένη στρατηγική για το υπολογιστικό νέφος στην Ουκρανία, δραστηριοποιούνται πολλοί ρώσικοι πάροχοι με τα κέντρα δεδομένων να βρίσκονται σε ρώσικο έδαφος. Ενώ αρκετές εφαρμογές του υπολογιστικού νέφους (πχ κοινωνικά δίκτυα) έχουν τεράστιο αριθμό δεδομένων χρηστών με τα κέντρα δεδομένων να υπάρχουν και στις δυο χώρες. Όπως γίνεται αντιληπτό με την έναρξη της πολιτικής διαμάχης πολλά κυβερνητικά δεδομένα αλλά και των πολιτών να βρίσκονται και στις δυο πλευρές. Αυτό θα είχε ως αποτέλεσμα να εξυπηρετήσει τα συμφέροντα της εκαστοτε χώρας εναντίον της άλλης.

Από την άλλη πλευρά η χρήση των εφαρμογών νέφους όπως τα κοινωνικά δίκτυα facebook και twitter βοήθησε σε διάφορες κοινωνικές διεργασίες όπως η λεγομένη «Αραβική Άνοιξη» και στην Ουκρανία. Στην περίπτωση της «Αραβικής Άνοιξης» υπάρχουν ενδείξεις ότι οι διαδηλώσεις υποστηρίχθηκαν από τη χρήση των social media ενώ πολιτικοί αναλυτές τα θεωρούν βασικό καταλύτη στη εξέγερση. Το Twitter

χρησιμοποιήθηκε ως πολιτικό εργαλείο για πρώτη κατά τη διάρκεια των ιρανικών εκλογών του 2009 όπου πολίτες της χώρας διαμαρτυρηθήκαν για την επανεκλογή του προέδρου Μαχμούντ Αχμαντινετζάντ. Στην Τυνησία και στην Αίγυπτο το Twitter και το Facebook ήταν τα ισχυρά εργαλεία των πολιτών να εκφράσουν τις απόψεις τους και να τις γνωστοποιήσουν σε όλο τον κόσμο και να ζητήσουν την αποκατάσταση της ελευθερίας στις χώρες τους. Σε ορισμένες χώρες με πιο αυταρχικά καθεστώτα τα ίδια εργαλεία χρησιμοποιήθηκαν για κατασκοπεία η να συγκεντρώσουν στοιχεία χρηστών οι οποίοι έχουν αντίθετη άποψη με τη κυβέρνηση (π.χ. Τουρκία).

Η άνοδος του Wikileaks [37] και η δημοσίευση 90.000 εγγράφων είχε ως αποτέλεσμα η Υπουργός Εξωτερικών των ΗΠΑ Χίλαρι Κλίντον, σε ομιλία της τον Φεβρουάριο του 2011 να ζητήσει :
«Μια σοβαρή συζήτηση » σχετικά με τους κανόνες για να διασφαλιστεί ένα ανοικτό Διαδίκτυο, σημειώνοντας ότι είχε βοηθήσει υπέρ της δημοκρατίας στην Αίγυπτο, αλλά επίσης υπηρετήσει ως ένα εργαλείο για τους τρομοκράτες και καταπιεστικές κυβερνήσεις».

Σύμφωνα με το Wikileaks ο σκοπός του είναι η υπεράσπιση της ελευθερίας του λόγου και τη δημοσίευση των μέσων ενημέρωσης και την υποστήριξη των δικαιωμάτων όλων των ανθρώπων και στηρίζεται στις αρχές από την Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου. Ειδικότερα, το άρθρο 19 εμπνέει το έργο των δημοσιογράφων μας και άλλους εθελοντές. Ενώ ο ιδρυτής της ιστοσελίδας αναφέρει ότι ο καθένας έχει το δικαίωμα στην ελευθερία της γνώμης και της έκφρασης το δικαίωμα αυτό περιλαμβάνει την ελευθερία γνώμης χωρίς παρεμβάσεις και να αναζητεί, να λαμβάνει και να διαδίδει πληροφορίες και ιδέες με οποιοδήποτε μέσο και ανεξαρτήτως συνόρων.

5.3 Επίδραση πολιτών –κυβερνήσεων

Η τεχνολογία των πληροφοριών επηρεάζει περισσότερο τις κυβερνήσεις από τις εταιρίες. Ωστόσο αν και οι εταιρίες και οι καταναλωτές χρησιμοποιούν τις νέες τεχνολογίες οι κυβερνήσεις υστερούν να καλύψουν τη διαφορά. Αυτό όμως αφήνει τις κυβερνήσεις να εκτεθούν σε πολλούς τομείς και μπορεί να έχει αρνητικό αντίκτυπο σε αυτές. Ως αποτέλεσμα θα πρέπει να δαπανηθούν μεγάλα ποσά για να καλύψουν τις

ανάγκες εξοπλισμού και εκπαίδευσης του προσωπικού. Οδηγεί επίσης σε μεγαλύτερη αναποτελεσματικότητα, όπως τα νέα συστήματα συγχέονται με τα παλιά και δημιουργούνται πολλά προβλήματα.

Δεύτερον, οι κυβερνήσεις κατέχουν εμπιστευτικές πληροφορίες με απόρρητα στοιχεία πολιτών και δεδομένα ασφαλείας της χώρας τους. Αν και πολλές εταιρείες έχουν παραβιάσεις ή επιθέσεις όσον αφορά τις πληροφορίες των πελατών, τα δεδομένα που κατέχουν οι κυβερνήσεις είναι πιο ευαίσθητα ενώ τείνουν να αντιδρούν μετά το γεγονός και όχι προληπτικά.

Το τρίτο θέμα είναι η εμπιστοσύνη των πολιτών και κατά πόσο γνωρίζουν την νέα τάση της τεχνολογίας. Όσοι πολίτες είναι ενημερωμένοι και γνωρίζουν το υπολογιστικό νέφος έχουν αντιρρήσεις για θέματα ιδιωτικότητάς έτσι ώστε να χρησιμοποιηθεί σε κυβερνητικές υπηρεσίες. Αυτό έρχεται σε συνδυασμό με τον Σνόουντεν [38] και με την αναφορά του διεθνούς φόρουμ των οργανώσεων των καταναλωτών (TACD) των ΗΠΑ και της ΕΕ η οποία αναπτύσσει κοινές συστάσεις πολιτικής των καταναλωτών προς την κυβέρνηση των ΗΠΑ και της Ευρωπαϊκής Ένωσης για την προώθηση των συμφερόντων των καταναλωτών στη χάραξη πολιτικής της ΕΕ και των ΗΠΑ.

5.3.1 Υπόθεση Σνόουντεν

Ο Σνόουντεν αποκάλυψε πληροφορίες για μία σειρά από απόρρητα προγράμματα των μυστικών υπηρεσιών, συμπεριλαμβανομένης της παρεμπόδισης των αμερικανικών και ευρωπαϊκών τηλεφωνικών επικοινωνιών και των προγραμμάτων παρακολούθησης PRISM και Tempora. Ο Σνόουντεν ανέφερε ότι οι διαρροές ήταν μία προσπάθεια *«να ενημερωθεί το κοινό ως προς το τι συμβαίνει στο όνομά του και τι εναντίον του»*. Αυτό οδήγησε πολλές εταιρίες αλλά και κάτοικους χώρων να μην θέλουν να χρησιμοποιούν παροχους του νέφους και να αυξηθούν οι ανησυχίες για τα κοινωνικά δίκτυα που δραστηριοποιούνται στις Ηνωμένες Πολιτείες. Οι αποκαλύψεις σχετικά με τις ΗΠΑ και ΕΕ για την συλλογή πληροφοριών έχουν προκαλέσει σοβαρές ανησυχίες σχετικά με την έλλειψη διαφάνειας και τη δέουσα διαδικασία. Η πραγματική έκταση της εν λόγω πρακτικής, αν ήταν νόμιμη η συλλογή πληροφοριών ή το φάσμα των δραστηριοτήτων που αφορούν εταιρείες, όπως η Google, Facebook και Yahoo είναι ακόμα ασαφής.

5.3.2 Διατλαντική εταιρική σχέση Εμπορίου και Επενδύσεων (TTIP)

Από την άλλη πλευρά το TACD[13] σε αναφορά της τον Οκτώβριο του 2013 σχολίασε [39] την διατλαντική εταιρική σχέση Εμπορίου και Επενδύσεων (TTIP) η οποία είναι μια εμπορική συμφωνία που είναι προς το παρόν στο στάδιο των διαπραγματεύσεων μεταξύ της Ευρωπαϊκής Ένωσης και των Ηνωμένων Πολιτειών. Στοχεύει στη μείωση των δασμών σε όλους τους τομείς, η ΕΕ και οι ΗΠΑ θέλουν να αντιμετωπίσουν τα εμπόδια όπως διαφορές των τεχνικών κανονισμών, προτύπων και διαδικασιών έγκρισης για να καταστεί ευκολότερη για να αγοράζουν και να πωλούν αγαθά και υπηρεσίες μεταξύ της ΕΕ και των ΗΠΑ. Οι διαπραγματεύσεις θα εξετάσουν επίσης το άνοιγμα των δύο αγορών για τις υπηρεσίες, τις επενδύσεις και τις δημόσιες συμβάσεις. Θα μπορούσαν επίσης να διαμορφώσουν την παγκόσμια κανόνες για το εμπόριο.

Είναι αδύνατο να αντιμετωπιστεί το θέμα της ροής δεδομένων, όταν τα καθεστώτα προστασίας των δεδομένων στις ΗΠΑ και την ΕΕ είναι εκ διαμέτρου διαφορετικά και άνισα. Χωρίς επαρκή εποπτεία και διαφάνεια, σε κάθε προσπάθεια να περιλαμβάνουν μέτρα προστασίας των δεδομένων στις διατλαντικές εμπορικές διαπραγματεύσεις θα μπορούσε εύκολα να οδηγήσουν σε σημαντική αποδυνάμωση της προστασίας του καταναλωτή. Το TACD πιστεύει ακράδαντα ότι οι πληροφορίες σχετικά με το Διαδίκτυο θα πρέπει να ρέουν ελεύθερα και να εξασφαλίσουν την ελευθερία της έκφρασης και της επιλογής των καταναλωτών. Οι αρχές της διαφάνειας και της ουδετερότητας είναι θεμελιώδη στοιχεία της αρχιτεκτονικής του Διαδικτύου και να επιτρέπουν στους καταναλωτές και τις επιχειρήσεις να μοιραστούν τις ζωτικής σημασίας πληροφορίες. Οι διαπραγματεύσεις μεταξύ της Ευρωπαϊκής Ένωσης και των Ηνωμένων Πολιτειών θα πρέπει να αφαιρέσουν οποιοδήποτε περιορισμό στην ελεύθερη ροή των πληροφοριών στο διαδίκτυο.

Οι καταναλωτές υπόκεινται σε αυξημένη παρακολούθηση καθώς κινούνται μέσω online και offline κόσμους, μπορεί να έχουν τη δυνατότητα να υπονομεύσει ατομική προστασία της ιδιωτικής ζωής και της ασφάλειας. Μια εμπορική συμφωνία δεν μπορεί να επιλύσει το γεγονός ότι δύο συστήματα είναι εξαιρετικά αποκλίνουσα και μη

[13] http://tacd.org/

διαλειτουργικά ούτε θα πρέπει να χρησιμοποιούνται για την παράκαμψη της νομοθετικής διαδικασίας. Η ΕΕ και οι ΗΠΑ θα πρέπει πρώτα να διαπραγματευτούν τους κανόνες προστασίας των προσωπικών δεδομένων ώστε να υπάρξει ένα κοινό πλαίσιο και ύστερα σε εμπορικό επίπεδο.

Οι συστάσεις του TACD για τις κυβερνήσεις της ΕΕ και των ΗΠΑ είναι :

1. Η διασφάλιση του δικαιώματος των καταναλωτών να στέλνουν και να λαμβάνουν περιεχόμενο της επιλογής τους και το δικαίωμα να χρησιμοποιούν τις υπηρεσίες χωρίς καμία διακρίσεις.
2. Συνέχιση της νομοθετικής διαδικασίας για την προστασία των δεδομένων και της ιδιωτικής ζωής.
3. Η Επιδίωξη ψήφισης του Κογκρέσου ψήφιση νόμου για τη θέσπιση των δικαιωμάτων του καταναλωτή. Σε περίπτωση απουσίας της νομοθεσίας, οι ΗΠΑ δεν μπορούν να προσφέρουν στην ΕΕ καμία διαβεβαίωση ότι υπάρχει επαρκής προστασία για τα προσωπικά δεδομένα που αποθηκεύονται ή χρησιμοποιούνται από εταιρείες των ΗΠΑ.
4. Η ΕΕ θα πρέπει να αναμένει την έγκρισης της δέσμης μεταρρυθμίσεων της προστασίας των δεδομένων από το Ευρωπαϊκό Κοινοβούλιο και τα κράτη μέλη και ύστερα να συνεχίσει τις διαπραγματεύσεις.
5. Βελτίωση της συνεργασίας μεταξύ των ρυθμιστικών αρχών ώστε να εφαρμόζονται οι νόμοι που αφορούν την ιδιωτική ζωή σε διασυνοριακές υποθέσεις
6. Συμφωνία για κοινά πρότυπα προστασίας προσωπικών δεδομένων εκτός των προτεινόμενων διαπραγματεύσεων TTIP. Τα πρότυπα αυτά πρέπει να πληρούν τις απαιτήσεις της κοινοτικής νομοθεσίας.
7. Ανεξάρτητη αξιολόγηση της αποτελεσματικότητας του Safe Harbour και να γίνουν οι απαραίτητες αλλαγές για να εξασφαλίσουν ότι είναι επαρκώς εναρμονισμένες με τις διατάξεις της νομοθεσίας της ΕΕ περί προστασίας δεδομένων.

5.4 Συμπεράσματα

Βάσει των παραπάνω συμπεραίνουμε την ανάγκη για πληροφόρηση όλων των πολιτών όπως και την ευαισθητοποίηση των κυβερνήσεων για τη λήψη μέτρων. Ειδικοί σε θέματα ηθικής μπορούν να διαδραματίσουν σημαντικό ρόλο στην επίτευξη και τη γεφύρωση του χάσματος μεταξύ ηθικής και πρακτικής εφαρμογής. Η Ευρωπαϊκή Επιτροπή έχει αναπτύξει σειρά πρωτοβουλιών για την ολοκληρωμένη αντιμετώπιση ζητημάτων ηθικής και δεοντολογίας, ιδιαίτερα για τα ερευνητικά έργα που χρηματοδοτούνται από το 7ο Πρόγραμμα Πλαίσιο για την έρευνα και εκδίδει κατευθυντήριες οδηγίες. Στην Ελλάδα με πρωτοβουλία του υπουργείου Υποδομών για την βελτίωση της ψηφιακής εικόνας της χώρας συγκροτήθηκε το φόρουμ «Ψηφιακή Ελλάδα 2020». Το φόρουμ[14] συστάθηκε το 2010 και ένα από τα αντικείμενα του είναι η δημόσια διοίκηση και η κοινωνία, το ψηφιακό χάσμα, η εμπιστοσύνη και η ασφάλεια. Ωστόσο παρόλο που τέθηκαν οι στόχοι δεν έχει πραγματοποιηθεί ακόμα καμία ενέργεια σε εθνικό και επίπεδο.

[14] Ψηφιακή Ελλάδα 2020 www.digitalgreece2020.gr

Επίλογος-Συμπεράσματα

Το υπολογιστικό νέφος ήδη εξελίσσεται στο μεγαλύτερο κλάδο παροχής υπηρεσιών που επαγγέλλεται μεγάλες ευκαιρίες για τις ευρωπαϊκές τηλεπικοινωνίες και τις εταιρείες τεχνολογίας. Από την άλλη γνωρίζουμε ότι το υπολογιστικό νέφος οπως κάθε νέα τεχνολογία, έχει πολλούς κινδύνους. Οι κίνδυνοι εξαρτώνται από το είδος των δεδομένων και των υπηρεσιών, από το ποιος διαχειρίζεται και με ποιο τρόπο τα δεδομένα και τις υπηρεσίες, από τους μηχανισμούς ασφαλείας που έχουν υλοποιηθεί, από το κανονιστικό πλαίσιο και τα ηθικά ζητήματα που δημιουργούνται.

Η Ευρωπαϊκή Ένωση σκοπεύει ήδη μέσω κατάλληλων δράσεων (Ευρώπη 2020) την προώθηση του ώστε πολίτες και επιχειρήσεις να επωφεληθούν με τον καλύτερο τρόπο από αυτή την τεχνική εξέλιξη. Παράλληλα προωθεί μια στρατηγική για το σύννεφο που έχει ως σκοπό να διερευνήσει τρόπους βελτίωσης του νομικού πλαισίου για τις συμβάσεις υπολογιστικού νέφους για καταναλωτές ώστε να ενισχυθεί η εμπιστοσύνη των καταναλωτών καθώς επίσης και στην τροποποίηση της οδηγίας για την προστασίας των δεδομένων της ΕΕ. Το κανονιστικό πλαίσιο παίζει σημαντικό ρόλο στις αποφάσεις των οργανισμών. Έτσι και με τη χρήση υπηρεσιών στο Σύννεφο κάθε οργανισμός πρέπει να αξιολογήσει κρίσιμα θέματα, τα οποία αν δεν έχει εξετάσει ενδελεχώς, οι επιπτώσεις θα είναι μεγάλες. Τα κανονιστικά θέματα αφορούν την υφιστάμενη νομοθεσία για μετακίνηση/ επεξεργασία/ αποθήκευση δεδομένων εκτός της χώρας του οργανισμού, είτε προς χώρες της Ευρωπαϊκής Ένωσης είτε σε άλλες τρίτες χώρες με την πιθανή άγνοια του οργανισμού για την τοποθεσία των δεδομένων του.

Πολλά από τα ζητήματα που τέθηκαν θα επιλυθούν με την αναθεώρηση της Οδηγίας 95/46/ΕΚ περί προστασίας δεδομένων της Ε.Ε και του θεσμικού πλαισίου που αναπτύχθηκε από τότε μέχρι σήμερα, για την ενίσχυση των online δικαιωμάτων στην ιδιωτικότητα και την ενδυνάμωση της ψηφιακής οικονομίας στην Ευρώπη. Επιπλέον κάθε οργανισμός ή εταιρία που θέλει να κάνει μετάβαση στο Σύννεφο, θα πρέπει να καλύψει τις σύγχρονες απαιτήσεις ασφαλείας, με την προϋπόθεση ότι ο πάροχος πρέπει να εξασφαλίζει α) την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των πληροφοριών, σύμφωνα με τις καθορισμένες απαιτήσεις ασφαλείας, β) το επίπεδο

υπηρεσιών σύμφωνα με τις επιχειρησιακές απαιτήσεις, γ) τη συμμόρφωση με το κανονιστικό πλαίσιο.

Ένα συμπέρασμα που μπορούμε να βγάλουμε είναι για την χρήση του Σύννεφου στην Ευρώπη. Συγκεκριμένα διαπιστώνουμε μια ευρύτερη τάση στην οποία οι αναπτυσσόμενες αγορές έχουν προσπεράσει πιο ώριμες αγορές με υψηλότερη χρήση υπηρεσιών. Αυτό αποδεικνύεται και στην ανάλυση των παραπάνω χωρών. Πολλές χώρες της νοτίου Ευρώπης ήδη έχουν ήδη μεταφέρει τις υπολογιστικές υποδομές τους στο νέφος. Από την άλλη πλευρά, ανεπτυγμένες χώρες της βόρειας Ευρώπης που έχουν πιο αυστηρούς κανόνες όσο αφορά το νομικό και κανονιστικό πλαίσιο, βρίσκονται ακόμα σε πρώιμο στάδιο. Επιπλέον αν και η Ε.Ε. έχει θέσει ως προτεραιότητα τη μείωση των χρηματοδοτήσεων του κεντρικού κράτους με σύμπραξη δημόσιου – ιδιωτικού τομέα (ΣΔΙΤ), τα έργα με χρήση υπολογιστικού νέφους κατά κύριο λόγο χρηματοδοτούνται από το κράτος.

Όσον αφορά στα κοινωνικοπολιτικά και ηθικά ζητήματα που θέσαμε, θα πρέπει να δοθούν απαντήσεις από την πλευρά των κυβερνήσεων, των παρόχων και των κοινωνικών ομάδων. Παρατηρούμε ότι τα πλεονεκτήματα του Σύννεφου, προωθούν τον εκδημοκρατισμό των καναλιών επικοινωνίας και υπόσχονται νέες μορφές ηλεκτρονικής δημοκρατίας, αλλά από την άλλη πλευρά ενισχύει και τους αντίπαλους της. Όπως δεν πρέπει να υπάρχουν περιορισμοί ή έλεγχος στο υπολογιστικό νέφος (πχ. κοινωνικά δίκτυα). Αυτό θα οδηγήσει στην απομάκρυνση των καταναλωτών και στην έλλειψη αξιοπιστίας των εταιριών για τη συγκεκριμένη τεχνολογία και θα περιορίσει την αύξηση της ψηφιακής οικονομίας. Ένα ζήτημα που δεν έχει απαντηθεί ακόμα είναι σε περίπτωση γεωπολιτικής αλλαγής μιας χώρας (πχ. πολεμική διαμάχη μεταξύ δυο χωρών, έξοδος χώρας από την Ε.Ε) πως θα εξασφαλίσει την ακεραιότητα, τον έλεγχο και την ασφάλεια των δεδομένων της. Επιπλέον, η Ευρωπαϊκή Επιτροπή θα πρέπει να αναπτύξει σειρά πρωτοβουλιών για την ολοκληρωμένη αντιμετώπιση ζητημάτων ηθικής και δεοντολογίας.

Τέλος το υπολογιστικό νέφος και οι εφαρμογές του θα είναι μια πηγή προκλητικών ερευνητικών θεμάτων στην επιστήμη της πληροφορικής για αρκετά από τα επόμενα χρόνια.

Βιβλιογραφία και Αναφορές

1. F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, D. Leaf (2011). *NIST Cloud Computing Reference Architecture: Recommendations of the National Institute of Standards and Technology*, National Institute of Standards and Technology
2. European Commission. *Europe 2020*. Διαθέσιμο: http://ec.europa.eu/europe2020/index_el.htm [Προσπελάστηκε στις 1/1/2014]
3. European Commission. *Horizon 2020*. Διαθέσιμο: http://ec.europa.eu/programmes/horizon2020/en/what-horizon-2020 [Προσπελάστηκε στις 1/1/2014]
4. European Commission (2012). *Commission presses 16 Member States to implement new EU telecoms rules*, IP/11/1429.
5. European Commission (2012). *Unleashing the Potential of Cloud Computing in Europe*.
6. European Parliament (1995). *Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data on the free movement of such data*, OJ L 281.
7. Joris van Hoboken, Axel Arnbak (2012). *Obscured by Clouds*, Privacy Law Scholars Conference 2013, 6-7 June, Berkeley, CA.
8. European Commission. *Opinion 05/2012 on Cloud Computing*. Διαθέσιμο: http://ec.europa.eu/justice/data-protection/article29/documentation/opinionrecommendation/files/2012/wp196_en.pdf [Προσπελάστηκε 10/1/2014]
9. European Commission (2012). *Regulation of the European Parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data*.
10. European Commission (2013). *Cloud Computing Service Level Agreements - Exploitation of Research Results*, Dimosthenis Kyriazis (ed.). June 2013, Brussels.
11. Cloud Standards Wiki. *Cloud Standards*. Διαθέσιμο: http://www.cloud-standards.org [Προσπελάστηκε στις 1/2/2014]
12. Digitaliser (2012). *Cloud computing and the legal framework*. Διαθέσιμο: http://digitaliser.dk/resource/2368677/artefact/Cloud+computing+and+the+legal+framework-a1.pdf. [Προσπελάστηκε στις 15/2/2014]

13. Garante Privacy. *Italian Legislation*. Διαθέσιμο: http://www.garanteprivacy.it/web/guest/home_en/italian-legislation [Προσπελάστηκε στις 1/2/2014]
14. ICO (2012) *Guidance on the use of cloud computing version 1.1* Διαθέσιμο: http://ico.org.uk/news/latest_news/2012/~/media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx [Προσπελάστηκε στις 20/2/2014]
15. European Commission (2013) *Analysis of cloud best practices and pilots for the public sector*. Διαθέσιμο*:* http://ec.europa.eu/digital-agenda/en/news/analysis-cloud-best-practices-and-pilots-public-sector [Προσπελάστηκε 20/1/2014]
16. CloudStore. Διαθέσιμο: http://gcloud.civilservice.gov.uk/cloudstore/ [Προσπελάστηκε 1/3/2014]
17. Nemhandel. Διαθέσιμο: http://www.nemhandel.dk (Προσπελάστηκε 1/3/2014)
18. BSA(2012). *Cloud Computing in the Europe Union 2012* Διαθέσιμο: http://www.bsa.org/~/media/Files/Policy/SoftwareInnovation/cloud/EUIpsos_EN.ashx [Προσπελάστηκε 10/2/2014]
19. ΕΣΠΑ(2007).*Επιχειρησιακό Πρόγραμμα «Ψηφιακή Σύγκλιση» (2007-2013)* Διαθέσιμο:http://www.espa.gr/elibrary/Episimo_Keimeno_EP_Psifiaki_Sygklisi.pdf [Προσπελάστηκε 10/03/14]
20. Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. *Αποστολή της Αρχής* Διαθέσιμο:http://www.dpa.gr/portal/page?_pageid=33,14970&_dad=portal&_schema=PORTAL [Προσπελάστηκε 1/3/2014]
21. Εφημερίδα της Κυβερνήσεως (2003). *Αρ. Φύλλου 47 27/02/2003* Διαθέσιμο: http://www.adae.gr/fileadmin/docs/nomoi/N.3115-2003.pdf [Προσπελάστηκε 01/04/2014]
22. Βουλή των Ελλήνων (1997), νόμος υπ'αριθμ. 2472/97 (ΦΕΚ 133 Α΄/24.07.1997)
23. Βουλή των Ελλήνων (1997), νόμος υπ'αριθμ. 2774/97 (ΦΕΚ 163 Α΄/24.07.1997)
24. European Parliament, Council. (2002) Council Directive 2002/58/EC of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), O.J. L 201, 31.7.2002
25. European Parliament, Council. (2009) Council Directive 2009/136/EC of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive

2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L 337, 18.12.2009

26. Βουλή των Ελλήνων (2007), νόμος υπ'αριθμ. 3625/07 (ΦΕΚ 290 Α΄/24.12.2007)
27. Κοινωνία της Πληροφορίας (2012). *Διαγωνισμοί / Κεντρικές Υπολογιστικές Υποδομές ΚτΠ ΑΕ - Κόμβος G-Cloud της ΓΓΠΣ*. Διαθέσιμο: http://www.ktpae.gr/index.php?option=com_ktpcontests&task=Details&id=367&Itemid=13 [Προσπελάστηκε 20/03/2014]
28. Datatilsynet (3/2/2011). *Processing of sensitive personal data in a cloud solution* Διαθέσιμο:http://www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution/ [Προσπελάστηκε 18/02/2014]
29. Warwick Ashford (07/03/2014). *ICO fines charity £200,000 for data breach* Διαθέσιμο:http://www.computerweekly.com/news/2240215767/ICO-fines-charity-200000-for-data-breach [Προσπελάστηκε 15/04/2014]
30. ICO (24/01/2014).*Sony fined £250,000 after millions of UK gamers' details compromised.*Διαθέσιμο:http://ico.org.uk/news/latest_news/2013/ico-news-release-2013 [Προσπελάστηκε 15/02/2014]
31. W Kuan Hon (2012). *Data Protection Jurisdiction and Cloud Computing – When are Cloud Users and Providers Subject to EU Data Protection Law?*, International Review of Law, Computers and Technology, Vol. 26, Issue 2-3, 2012.
32. ΑΠΔΠΧ (2013). *Ετήσια έκθεση 2012* Διαθέσιμο: http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ANNUALREPORTS/AR2012/ARXH%20PROSTASIAS%20APOLOGISMOS%202012_%20WEBUSE.PDF [Προσπελάστηκε 10/04/2014]
33. ΟΛΜΕ (11/03/2014). *Δελτίο Τύπου: Προσφυγή στην Αρχή Προστασίας Προσωπικών Δεδομένων για το "myschool"*. Διαθέσιμο: http://olme-attik.att.sch.gr/new/?p=7369 [Προσπελάστηκε στις 15/04/2014]
34. RT. *Head of Russia's largest social network VKontakte leaves his post.* Διαθέσιμο:http://rt.com/news/durov-resigns-vkontakte-social-904/ [Προσπελάστηκε 1/5/2014]
35. Kevin Rawlinson (21/3/2014).*Turkey blocks use of Twitter after prime minister attacks social media site* Διαθέσιμο:

http://www.theguardian.com/world/2014/mar/21/turkey-blocks-twitter-prime-minister [Προσπελάστηκε 1/4/2014]

36. Job Timmermans, Bernd Carsten Stahl (2010) *The Ethics of Cloud Computing*, CloudCom , 2010 IEEE Second International Conference
37. Siavash Moshiri , Peter Lake, Laurie Hirsch, Richard Hill(2013). *Social, Economic and Political Aspects of the Cloud*. Guide to Cloud Computing Principles and Practice, Springer. pp. 43-61
38. Wikipedia. *Edward Snowden*. Διαθέσιμο: http://en.wikipedia.org/wiki/Edward_Snowden [Προσπελάστηκε 1/4/2014]
39. TACD (2013) , *50/13 Resolution on Data Flows in the TransAtlantic Trade and Investment Partnership*, INFOSOC