Πανεπιστήμιο Πειραιώς

Τμήμα Ψηφιακών Συστημάτων

Π.Μ.Σ. «Ασφάλεια Ψηφιακών Συστημάτων»

[ΙΔΙΩΤΙΚΟΤΗΤΑ ΔΕΔΟΜΕΝΩΝ

ΣΤΟ CLOUD COMPUTING]

Επιβλέπουσα καθηγήτρια: **κ. ΛΑΜΠΡΙΝΟΥΔΑΚΗΣ**

Ονοματεπώνυμο φοιτητή: **Γιαταγάνας Γεώργιος – Ευθύμιος**

Μητρώο: **ΜΤΕ-1205**

Ακαδημαϊκό Έτος 2014-2015

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΕΙΣΑΓΩΓΗ

Αναμφίβολα, με την πάροδο των ετών, η σταδιακή ανάπτυξη και εξέλιξη της τεχνολογίας έχει επιτρέψει, όσον αφορά στην ασφάλεια των υπολογιστικών συστημάτων, τη βελτίωση των πολιτικών και των μεθόδων ασφαλείας, αλλά και την εφεύρεση νέων αποτελεσματικότερων, αποδοτικότερων και καινοτόμων τακτικών ασφαλείας. Μία από αυτές τις τακτικές ασφαλείας που έχει καταστεί ιδαιτέρως γνωστή και ευρέως διαδεδομένη τα τελευταία ιδίως χρόνια, τα χαρακτηριστικά της οποίας θα προσπαθήσουμε να προσεγγίσουμε στην παρούσα διπλωματική εργασία είναι η Υπολογιστική Νέφους, ή αλλιώς, όπως έχει επικρατήσει να λέγεται, το Cloud Computing.

Τα τελευταία χρόνια, το Cloud Computing γίνεται όλο και πιο δημοφιλές. Το Cloud Computing συνίσταται σε ένα σύνολο τεχνολογιών και μοντέλων υπηρεσιών που εστιάζουν στη διαδικτυακή χρήση και παροχή εφαρμογών τεχνολογίας των πληροφοριών, στη δυνατότητα επεξεργασίας δεδομένων, στην παροχή χώρου αποθήκευσης δεδομένων και στην παροχή μνήμης. Έτσι, είναι δυνατή η εύκολη και γρήγορη πρόσβαση στα αποθηκευμένα, στο cloud σύστημα, δεδομένα και εφαρμογές, από οποιοδήποτε σημείο και σε οποιοδήποτε χρόνο, εφόσον ο εκάστοτε χρήστης το επιθυμεί και εφόσον το ζητήσει (on-demand-access). Προφανώς, η παρεχόμενη αυτή δυνατότητα αποτελεί μία πολύ βολική λύση σε πολλές περιπτώσεις, ειδικά μάλιστα, όταν αναφερόμαστε σε έναν οργανισμό, όπου οι χρησιμοποιούμενες υπηρεσίες και τα αποθηκευμένα δεδομένα είναι πάρα πολλά.

Τα οφέλη που προκύπτουν από τη χρήση του Cloud Computing σε έναν οργανισμό είναι πολλαπλά, αφού για παράδειγμα πραγματοποιείται η μείωση των λειτουργικών εξόδων και επιτυγχάνεται η σχεδόν μηδενική επιβάρυνση του πληροφοριακού συστήματος του οργανισμού. Επιπλέον, υπάρχουν οφέλη και σε επίπεδο ασφάλειας, καθώς οι επιχειρήσεις (κυρίως οι μικρομεσαίες) μπορούν να αποκτήσουν, με οριακό κόστος, κορυφαίες τεχνολογίες τις οποίες δεν θα είχαν τη δυνατότητα να αγοράσουν σε άλλη περίπτωση. Ωστόσο, παρά τα πολλά πλεονεκτήματα που προκύπτουν από την ύπαρξη και τη χρήση του Νέφους[1], πρέπει να γνωρίζουμε ότι δεν είναι λίγοι και οι κίνδυνοι που ελλοχεύουν από τη χρήση αυτού. Ιδιαίτερη σημασία δε, αποκτά το ζήτημα της ασφάλειας των δεδομένων που αποθηκεύονται στο Cloud, όταν πρόκειται να αποθηκευτούν ευαίσθητα δεδομένα.

[1] Armbrust M., Fox A., Griffith R., Joseph A., Katz R., Konwinski A., Lee G., Patterson D., Rabkin A., Stoica I., and Zaharia M., "Above the Clouds: A Berkeley View of Cloud Computing", Electrical Engineering and Computer Sciences, University of California at Berkeley, February 10, 2009, http://www.cs.columbia.edu/~roxana/teaching/COMS-E6998-7-Fall-2011/papers/armbrust-tr09.pdflectrical

Όπως είναι γνωστό, κανένα σύστημα ή πολιτική ασφαλείας που αφορά οντότητα που συνδέεται με οποιονδήποτε τρόπο στο Διαδίκτυο δεν μπορεί να εγγυηθεί σε ποσοστό 100% την ασφάλεια και να στερείται ευπαθειών και τρωτότητας, καθώς πάντα οποιαδήποτε υποδομή και αν χρησιμοποιηθεί για το σχεδιασμό και την υλοποίηση μιας νέας πολιτικής ασφαλείας, δεν θα είναι δυνατό εκ των προτέρων να κατορθώσει αφενός να καλύψει και αφετέρου να προβλέψει τις υπάρχουσες απειλές ασφαλείας, εάν προηγουμένως δεν τεθεί στη δοκιμασία του χρόνου. Επιπλέον, γίνεται δεκτό ότι πάντα θα υπάρχουν νέες απειλές και παραλλαγμένοι τρόποι επίθεσης που ευλόγως οι κατασκευαστές αγνοώντας την ύπαρξή τους, δεν τους έχουν λάβει υπόψη τους.

Cloud Computing

Ιστορικά, μέχρι και σήμερα δεν υπάρχει μια σαφής εξήγηση για το πως προέκυψε ο όρος Cloud Computing. Γενικότερα, στις επιστήμες, ο όρος Cloud νοείται ως μια μεγάλη συσσώρευση αντικειμένων, που αν θεαθούν από μακρινή απόσταση φαίνονται σαν ένα νέφος. Χρησιμοποιείται δε για να περιγράψει οποιαδήποτε κατηγορία αντικειμένων, τα οποία δεν ελέγχονται περαιτέρω σε ένα δεδομένο πλαίσιο. Σε αναλογία με την παραπάνω χρήση, η λέξη Cloud χρησιμοποιήθηκε μεταφορικά όταν κάποιος αναφερόταν στο Internet και η χρήση ενός σχήματος που έμοιαζε με νέφος υποδήλωνε το δίκτυο για τις σχηματικές αναπαραστάσεις της τηλεφωνίας και αργότερα για την απεικόνιση του Διαδικτύου σε διαγράμματα δικτύου υπολογιστών. Το σύμβολο του Cloud χρησιμοποιήθηκε το 1994, στο οποίο οι εξυπηρετητές (servers) και λοιπές συσκευές (υπολογιστές, laptops, tablets, κινητά τηλέφωνα) φαίνονται να είναι συνδεδεμένα στο νέφος, αλλά εξωτερικά (βλ. σχήμα 1)[2].

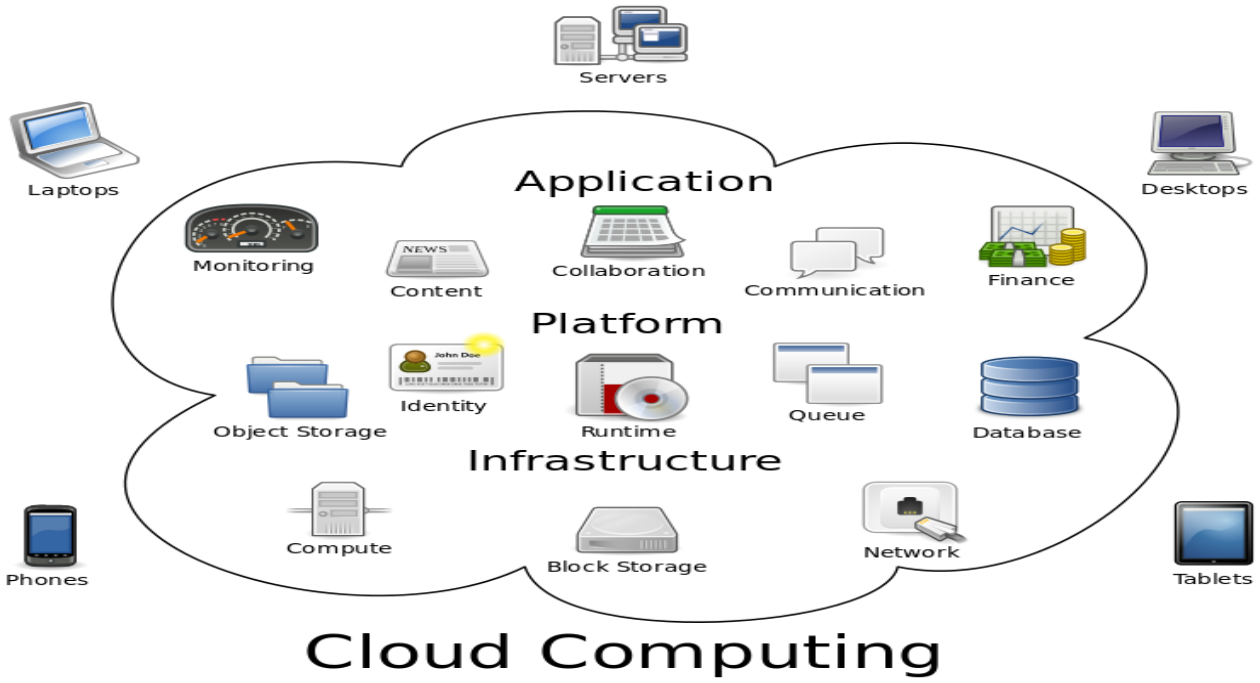
Το Cloud Computing ορίζεται ως «ένα διαδικτυακό υπολογιστικό μοντέλο βάσει του οποίου διαμοιράζονται πόροι, λογισμικό και πληροφορίες σε ηλεκτρονικούς υπολογιστές και λοιπές συσκευές κατά παραγγελία και κατά τα πρότυπα ενός δικτύου ηλεκτρικής ενέργειας»[3], ή ως «ένα μοντέλο που καθιστά εφικτή την άνετη και κατ' απαίτηση δικτυακή πρόσβαση σε μια κοινόχρηστη δεξαμενή

[2] Οι αναφορές πάντως για το Cloud Computing με τη σύγχρονη έννοια του όρου εμφανίζονται ήδη από το 1996, με την παλαιότερη γνωστή αναφορά να εντοπίζεται σε ένα εσωτερικό έγγραφο της Compaq, ενώ η "εκλαΐκευση" του όρου μπορεί να χρονολογηθεί στο έτος 2006 όταν η εταιρεία Amazon.com παρουσίασε την υπηρεσία ιστού (web service) Elastic Compute Cloud (Amazon EC2).

[3] Βλ. Γνωμοδότηση της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής (ΕΟΚΕ) και συγκεκριμένα του ειδικευμένου τμήματος «Μεταφορές, ενέργεια, υποδομές, κοινωνία των πληροφοριών» με θέμα: «Το υπολογιστικό νέφος (cloud computing) στην Ευρώπη», Βρυξέλλες, 12 Οκτωβρίου 2011, http://www.eesc.europa.eu/?i=portal.en.opinions-search.

προσαρμόσιμων υπολογιστικών πόρων (π.χ. δίκτυα, servers, συστήματα αποθήκευσης, εφαρμογές και υπηρεσίες) που μπορεί να αναπτυχθεί και να τεθεί σε χρήση γρήγορα, με ελάχιστη διαχειριστική προσπάθεια και αλληλεπίδραση από τους παρόχους υπηρεσιών»[4].

Το Cloud Computing είναι ένα μοντέλο, το οποίο παρέχει τη δυνατότητα της απανταχού, εύκολης και κατόπιν ζήτησης, πρόσβασης σε ένα κοινόχρηστο σύνολο (shared pool) από υπολογιστικούς πόρους που μπορούν να τροφοδοτηθούν γρήγορα και να αποδεσμευτούν με ελάχιστη προσπάθεια διαχείρισης ή αλληλεπίδρασης των παρόχων υπηρεσιών[5], αποτελείται δε από πέντε ουσιαστικά χαρακτηριστικά, τρία μοντέλα υπηρεσιών και τέσσερα μοντέλα ανάπτυξης[6].



[4] Mell P., Grance T., "The NIST Definition of Cloud Computing", Recommendations of the National Institute of Standards and Technology, National Institute of Standards and Technology, U.S. Department of Commerce, September 2011, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[5] Θα πρέπει να αποσαφηνιστεί ότι το cloud computing είναι ένας νέος τρόπος για την διανομή των υπολογιστικών πόρων και όχι μια νέα μορφή τεχνολογίας.1

[6] Τα βασικά χαρακτηριστικά του Cloud Computing είναι: α) Αυτοεξυπηρέτηση κατόπιν ζήτησης (On-demand Self-service), β) Ευρεία πρόσβαση στο δίκτυο (Broad network access), γ) Συγκέντρωση πόρων (Resource Pooling), δ) Μεγάλη ελαστικότητα (Rapid Elasticity) και ε) Μετρούμενη υπηρεσία (Measured Service).

Σχήμα 1: Απεικόνιση ενός μοντέλου Cloud Computing

Μορφές Cloud με βάση την υποδομή ή τις εφαρμογές

Οι πάροχοι υπηρεσιών Cloud προσφέρουν ένα ευρύ φάσμα υπηρεσιών που κυμαίνεται από συστήματα εικονικής επεξεργασίας (τα οποία αντικαθιστούν ή/και λειτουργούν παράλληλα με τους συμβατικούς διακομιστές υπό τον άμεσο έλεγχο του υπεύθυνου της επεξεργασίας) και υπηρεσίες που υποστηρίζουν την ανάπτυξη εφαρμογών και προηγμένες δυνατότητες φιλοξενίας, έως διαδικτυακές λύσεις λογισμικού, οι οποίες μπορούν να αντικαταστήσουν τις συμβατικές εφαρμογές που εγκαθίστανται συνήθως στους προσωπικούς υπολογιστές των τελικών χρηστών. Σε αυτές περιλαμβάνονται εφαρμογές επεξεργασίας κειμένου, ατζέντες και ημερολόγια, συστήματα αρχειοθέτησης για επιγραμμική αποθήκευση εγγράφων και υπηρεσίες ηλεκτρονικού ταχυδρομείου παρεχόμενες από τρίτους[7].

Ειδικότερα, τα μοντέλα υπηρεσιών του Cloud Computing είναι τα εξής:

i) **Λογισμικό Νέφους ως Υπηρεσία (SaaS)**: Στο συγκεκριμένο μοντέλο, οι χρήστες έχουν τη δυνατότητα να χρησιμοποιούν εφαρμογές που διατίθενται στο Cloud από τους παρόχους. Οι εφαρμογές αυτές είναι προσβάσιμες μέσα από διεπαφές προγραμμάτων ή με τη βοήθεια διεπαφών web browser. Οι χρήστες δεν έχουν το δικαίωμα να ελέγχουν την υποδομή του Cloud ή να αλλάζουν την παραμετροποίηση των παρεχόμενων εφαρμογών[8].

ii) **Πλατφόρμα Νέφους ως Υπηρεσία (PaaS)**: Στην περίπτωση αυτή, οι χρήστες έχουν τη δυνατότητα να αναπτύξουν δικό τους λογισμικό πάνω στην υποδομή του Cloud με τη χρήση γλωσσών

[7] Βλ. την υπ' αριθμ. 05/2012 από 1ης Ιουλίου 2012 Γνώμη της Ομάδας Εργασίας του άρθρου 29 για την προστασία των δεδομένων σχετικά με τη νεφοϋπολογιστική, 01037/12/EL, WP 196, σελ. 5.

[8] Σε αυτήν την περίπτωση την ευθύνη για την προστασία των προσωπικών δεδομένων και πληροφοριών που αποθηκεύονται την έχει ο πάροχος υπηρεσιών υπολογιστικού νέφους.

προγραμματισμού, βιβλιοθηκών και εργαλείων που υποστηρίζει ο πάροχος. Σε αντίθεση με το SaaS, οι χρήστες στο PaaS μπορούν να διαχειρίζονται τις εφαρμογές τους και να παραμετροποιούν το περιβάλλον στο οποίο αυτές βρίσκονται[9].

iii) **Υποδομή Νέφους ως Υπηρεσία (IaaS)**: Εν προκειμένω, οι χρήστες έχουν τη δυνατότητα να επεξεργάζονται τη διάταξη, την αποθήκευση, τα δίκτυα και άλλους βασικούς υπολογιστικούς πόρους. Στο IaaS οι χρήστες μπορούν να αναπτύξουν αυθαίρετο λογισμικό, όπως λειτουργικά συστήματα και εφαρμογές. Μπορεί μεν και πάλι να μην υπάρχει η δυνατότητα ελέγχου της υποδομής του Cloud από τους χρήστες, αλλά οι τελευταίοι μπορούν να αλλάζουν και να παραμετροποιούν το λογισμικό, τον αποθηκευτικό χώρο και να έχουν περιορισμένο έλεγχο βασικών παραμέτρων δικτύων (π.χ. firewalls)[10].

Τα μοντέλα ανάπτυξης του Cloud Computing είναι:

i) **Private**: Η υποδομή του Cloud προορίζεται αποκλειστικά για χρήση από ένα συγκεκριμένο οργανισμό. Αυτό το μοντέλο μπορεί να καταστεί διαχειρίσιμο από τον ίδιο τον οργανισμό, από κάποιον τρίτο ή και από τα δύο αυτά μέρη ταυτόχρονα. Η υποδομή του μπορεί να υπάρχει, είτε εντός, είτε εκτός των κτιριακών εγκαταστάσεων του οργανισμού.

ii) **Public**: Η υποδομή του Cloud προορίζεται για ανοιχτή χρήση και οποιοσδήποτε μπορεί να την χρησιμοποιήσει. Συνήθως ανήκει σε εταιρείες, πανεπιστημιακές κοινότητες ή κυβερνητικούς οργανισμούς, οι οποίοι και τη διαχειρίζονται, η υποδομή δε βρίσκεται εντός των εγκαταστάσεων των παρόχων.

iii) **Community**: Η υποδομή του Cloud προορίζεται για αποκλειστική χρήση από μια συγκεκριμένη κοινότητα οργανώσεων που έχουν κοινά συμφέροντα (π.χ. απαιτήσεις ασφάλειας, πολιτική κ.ά.). Η υποδομή στη συγκεκριμένη περίπτωση καθίσταται διαχειρίσιμη από έναν ή παραπάνω οργανισμούς της κοινότητας ή και από τρίτους και οι εγκαταστάσεις της βρίσκονται εντός ή εκτός των κτιριακών εγκαταστάσεων των οργανισμών.

[9] Εδώ η ευθύνη για την τήρηση των μέτρων ασφαλείας και προστασίας των πληροφοριών είναι κυρίως του παρόχου υπηρεσιών υπολογιστικού νέφους.

[10] Στην προκειμένη περίπτωση την τελική ευθύνη για την ασφάλεια των πληροφοριών που αποθηκεύουν την έχουν αποκλειστικά οι καταναλωτές.

iv) **Hybrid**: Η υποδομή του Cloud είναι ένας συνδυασμός δύο ή περισσότερων διακριτών μοντέλων (private, public ή community) που παραμένουν ξεχωριστές οντότητες, αλλά συνδυασμένα κατάλληλα επιτρέπουν τη φορητότητα δεδομένων και εφαρμογών[11].

Ανάγκη για προστασία της ιδιωτικότητας

Αναφαίρετο δικαίωμα του πολίτη είναι η ιδιωτικότητα και συγκεκριμένα η προστασία της ιδιωτικής ζωής. Η ιδιωτικότητα είναι ένα θεμελιώδες δικαίωμα και εκφράζει την ανάγκη του ατόμου για μια προσωπική ζωή που θα του ανήκει κυριολεκτικά και θα τη διαθέτει κατά το δοκούν. Η ιδιωτικότητα είναι ελευθερία, ένα αγαθό υπέρτατο και πεπερασμένο ταυτόχρονα που συναντά τα όριά του στην ιδιωτικότητα του ατόμου και μόνο σε αυτό. Κατά μια άποψη, θα μπορούσε ακόμα και να ισχυριστεί κανείς ότι η ιδιωτικότητα είναι τόσο σημαντική όσο και η ίδια μας η ζωή.

Το δικαίωμα στην ιδιωτική ζωή είναι καθήκον κάθε πολιτείας να το προστατεύει[12,13]. Η ιδιωτική ζωή είναι τα στοιχεία της ίδιας της προσωπικότητας του ατόμου, τα οποία μπορεί να τα προσβάλλει κάποιος, είτε κατά τη διάρκεια κάποιας έρευνας, είτε κατά τη δημοσιοποίηση αυτής. Το δικαίωμα στην ιδιωτική ζωή οπωσδήποτε αριθμεί πολλαπλούς τρόπους παραβίασης, όπως επί παραδείγματι είναι η συστηματική παρακολούθηση, η υποκλοπή ιδιωτικών συζητήσεων μέσω νέων τεχνολογιών, η μυστική φωτογράφιση σε ιδιωτικούς χώρους ή η αποκάλυψη πραγμάτων και γεγονότων από την ιδιωτική ζωή

[11] Για παράδειγμα ένα νοσοκομείο μπορεί να χρησιμοποιεί δημόσιο νέφος για εφαρμογές που δεν περιέχουν ευαίσθητες πληροφορίες, όπως είναι οι ηλεκτρονικοί φάκελλοι των ασθενών τους, οι οποίοι είναι καλύτερο να είναι διαχειρίσιμοι με εφαρμογές ιδιωτικού νέφους, αφού έτσι εξασφαλίζεται μεγαλύτερος βαθμός εμπιστευτικότητας και ασφάλειας των δεδομένων αυτών.

[12] Ο έλληνας νομοθέτης αντιλαμβανόμενος την ανάγκη για προστασία της ιδιωτικής ζωής, προβλέπει στο άρθρο 5 παρ. 1 του Συντάγματος ότι: «Καθένας έχει δικαίωμα να αναπτύσσει ελεύθερα την προσωπικότητά του και να συμμετέχει στην κοινωνική, οικονομική και πολιτική ζωή της Χώρας, εφόσον δεν προσβάλλει τα δικαιώματα των άλλων και δεν παραβιάζει το Σύνταγμα ή τα χρηστά ήθη».

[13] Εκτός όμως από το Σύνταγμα και στην Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ) προβλέπεται η προστασία της ιδιωτικής ζωής. Ειδικότερα, το άρθρο 8 αυτής ορίζει ότι: «1. Παν πρόσωπον δικαιούται εις σεβασμόν της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και της αλληλογραφίας του. 2. Δεν επιτρέπεται να υπάρξη επέμβασις δημοσίας αρχής εν τη ασκήσει του δικαιώματος τούτου, εκτός εάν η επέμβασις αύτη προβλέπεται υπό του νόμου και αποτελεί μέτρον το οποίον, εις μίαν δημοκρατικήν κοινωνίαν, είναι αναγκαίον δια την εθνικήν ασφάλειαν, την δημοσίαν ασφάλειαν, την οικονομικήν ευημερίαν της χώρας, την προάσπισιν της τάξεως και την πρόληψιν ποινικών παραβάσεων, την προστασίαν της υγείας ή της ηθικής, ή την προστασίαν των δικαιωμάτων και ελευθεριών άλλων». Βλ. επίσης τις αποφάσεις του Ευρωπαϊκού Δικαστηρίου των Δικαιωμάτων του Ανθρώπου (ΕΔΔΑ): *Gaskin v.UK (1989)* και *Botta v. Italy (1998).*

κάποιου προσώπου. Το διαδίκτυο, δυστυχώς, δεν προσφέρει πολλές εναλλακτικές λύσεις για την προστασία από την παραβίαση της ιδιωτικής ζωής του ατόμου, τη στιγμή μάλιστα που το άτομο οικειοθελώς παραθέτει μέσω αυτού στοιχεία και γεγονότα που αφορούν στην ιδιωτική του ζωή[14]. Το παράδειγμα του facebook και των άλλων μέσων κοινωνικής δικτύωσης είναι ένα χαρακτηριστικό παράδειγμα, όπου το άτομο θεωρεί αυτονόητη τη δημοσίευση της ιδιωτικής του ζωής, ξεχνώντας το βασικότατο δικαίωμα της αυτοδιάθεσης.

Οι κίνδυνοι που ελλοχεύουν αναφορικά με την προσβολή της ιδιωτικότητας είναι σοβαροί και πάντα παρόντες όταν γίνεται λόγος για έκθεση των δεδομένων που αφορούν στο άτομο μέσω της χρήσης του διαδικτύου. Ειδικότερα και σχετικά με τα συστήματα Cloud, η παραβίαση της ιδιωτικότητας μπορεί να λάβει χώρα με διάφορες μορφές και να έχει σοβαρό αντίκτυπο στον τρόπο λειτουργίας των επιχειρήσεων ή των ιδιωτών που χρησιμοποιούν το Cloud, εάν δεν ληφθούν υπόψη τα κατάλληλα μέτρα προστασίας[15].

Η παραβίαση των δεδομένων προσωπικού χαρακτήρα μέσω της απώλειας, της καταστροφής ή της διαρροής αυτών αποτελεί μία σοβαρότατη απειλή για το cloud computing, ενώ είναι γεγονός ότι τα μέτρα που μπορεί να τεθούν προκειμένου να αποφευχθεί η παραβίαση αυτών, μπορεί να οδηγήσει μοιραία στην απώλεια αυτών. Αυτό που μπορεί να συμβεί, επί παραδείγματι, είναι ότι μπορούν να κρυπτογραφηθούν τα δεδομένα για να απομειωθεί ο κίνδυνος της παραβίασής τους, αλλά να χαθεί το κλειδί κρυπτογράφησης, με αποτέλεσμα αυτόματα να χαθούν και τα δεδομένα. Αντιστρόφως, μπορούν να κρατηθούν ανεπίσημα αντίγραφα ασφαλείας των δεδομένων για να μειωθούν οι επιπτώσεις μιας καταστροφικής απώλειας δεδομένων[16], αλλά αυτό αυξάνει την έκθεση τους σε παραβιάσεις.

Κίνδυνος για παραβίαση της ιδιωτικότητας μπορεί να προκύψει και μέσα από την παραβίαση λογαριασμών και υπηρεσιών, συνήθως με κλεμμένα διαπιστευτήρια, με τα οποία οι επιτιθέμενοι

---

[14] Citron D., Cyber Civil Rights. Boston University Law Review, Vol. 89, pp. 61-125, 2009, http://www.bu.edu/law/central/jd/organizations/journals/bulr/volume89n1/documents/CITRON.pdf

[15] Top Threats Working Group, The Notorious Nine Cloud Computing Top Threats in 2013, Cloud Security Alliance (CSA), February 2013, (The permanent and official location for Cloud Security Alliance Top Threats research is: https://cloudsecurityalliance.org/research/top-threats/)

[16] Είναι γεγονός ότι πολλές πολιτικές συμμόρφωσης απαιτούν από τους οργανισμούς να διατηρούν αρχεία ελέγχου ή άλλα έγγραφα. Εάν ένας οργανισμός αποθηκεύει τα δεδομένα στο Cloud, απώλεια των δεδομένων θα μπορούσε να επιφέρει κυρώσεις στον οργανισμό, λόγω της θέσης του σε κατάσταση μη συμμόρφωσης με τις υποχρεώσεις του.

μπορούν συχνά να αποκτήσουν πρόσβαση σε κρίσιμες περιοχές των ανεπτυγμένων υπηρεσιών του Cloud Computing, επιτρέποντας τους να θέσουν σε κίνδυνο την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των υπηρεσιών αυτών[17] και επιτάσσοντας από τους διάφορους οργανισμούς την αναγκαιότητα να γνωρίζουν τις τεχνικές και τις στρατηγικές προστασίας σε βάθος, προκειμένου να πετύχουν κατά το δυνατόν, τον περιορισμό της ζημιάς που προκύπτει από την παραβίαση[18].

Τέλος, η παραβίαση των αποθηκευμένων δεδομένων που βρίσκονται σε ένα Cloud σύστημα μπορεί να υλοποιηθεί ακόμη και από ένα κακόβουλο χρήστη εμπιστευτικών πληροφοριών, όπως λόγου χάρη είναι ο διαχειριστής του συστήματος σε ένα σωστά σχεδιασμένο σενάριο Cloud, ο οποίος μπορεί να έχει πρόσβαση σε δυνητικά ευαίσθητες πληροφορίες. Από IaaS σε PaaS και SaaS, ο κακόβουλος χρήστης έχει αυξημένη πρόσβαση σε πιο κρίσιμα συστήματα, και τελικώς στα δεδομένα, με αποτέλεσμα τα συστήματα που εξαρτώνται αποκλειστικά από τον πάροχο υπηρεσιών Cloud (CSP) για την ασφάλεια τους, στην περίπτωση αυτή, να βρίσκονται σε μεγάλο κίνδυνο[19].

Με βάση, επομένως, τα προεκτεθέντα, όπως αναπτύχθηκαν σε αδρές γραμμές, τα ζητήματα που θα μας απασχολήσουν στην παρούσα διπλωματική εργασία είναι αφενός ο εντοπισμός των ωφελειών και αφετέρου των κινδύνων που προκύπτουν από τη χρήση των συστημάτων Cloud και επομένως η συνακόλουθη αναγνώριση της αναγκαιότητας ανάπτυξης πολιτικών ασφαλείας μέσω μιας ηχηρής παρουσίας ενός ολοκληρωμένου συστήματος προστασίας των προσωπικών δεδομένων και της ιδιωτικότητας του ατόμου.

Για το λόγο αυτό, η εργασία διαρθρώνεται, πέραν από τα κεφάλαια της εισαγωγής και του επιλόγου, σε τρία κεφάλαια. Στο πρώτο κεφάλαιο, καταγράφονται οι βασικές αρχές λειτουργίας του Cloud Computing που περιλαμβάνουν, ως επί το πλείστον, τα τεχνικά χαρακτηριστικά του και τις δυνατότητες λειτουργίας του και δίνονται παραδείγματα ευρωπαϊκών παραδειγμάτων ανάπτυξης συστημάτων Cloud. Στο δεύτερο κεφάλαιο παρουσιάζονται τα οφέλη που προκύπτουν από τη χρήση και σωστή αξιοποίηση των συστημάτων Cloud, ενώ παράλληλα αντιπαραβάλλονται οι εγγενείς κίνδυνοι που

[17] Βλ. Poullet Y., Van Gyseghem J., Moiny J., Gérard J. and Gayrel C., «Data Protection in the Clouds» σε Computers, Privacy and Data Protection: an Element of Choice, Springer Netherlands 2011, σελ. 395.

[18] Οι οργανισμοί θα πρέπει να φροντίζουν ιδίως για την απαγόρευση της κατανομής διαπιστευτηρίων λογαριασμών μεταξύ χρηστών και υπηρεσιών, καθώς και για τη μόχλευση ισχυρών τεχνικών ελέγχου ταυτότητας δύο παραγόντων, όπου φυσικά αυτό καθίσταται δυνατόν.

[19] Είναι σαφές ότι ακόμη και αν υλοποιείται κρυπτογράφηση, αν τα κλειδιά δεν βρίσκονται στην κατοχή του πελάτη και είναι διαθέσιμα μόνο σε χρόνο όπου γίνεται χρήση δεδομένων, το σύστημα εξακολουθεί να είναι ευάλωτο σε κακόβουλες επιθέσεις χρηστών.

ενυπάρχουν κατά τη χρήση αυτών, με αποτέλεσμα να αναπτύσσονται οι τρόποι αποτροπής των κινδύνων και να προτάσσεται η ανάγκη για την εκ προοιμίου σκιαγράφηση των απαιτήσεων ασφαλείας που καθίστανται απολύτως αναγκαίες. Τέλος, στο τρίτο κεφάλαιο, γίνεται προσπάθεια να καταδειχτεί το μείζον ζήτημα της χρήσης των συστημάτων Cloud με γνώμονα την προστασία της ιδιωτικότητας των χρηστών, όπου απαριθμούνται τα νομικά ζητήματα που ανακύπτουν και αφορούν ιδίως στον προσδιορισμό του εφαρμοστέου δίκαιου, της αρμοδιότητας για την προστασία των δεδομένων, της ευθύνης για τον έλεγχο και την επεξεργασία τους και τέλος τη διευθέτηση των διαδικασιών μεταφοράς και επεξεργασίας δεδομένων από ή και σε τρίτες χώρες.

ΚΕΦΑΛΑΙΟ 1 – ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΛΕΙΤΟΥΡΓΙΑΣ ΤΟΥ CLOUD COMPUTING

1.1. Τεχνική καταγραφή των δυνατοτήτων και των τρόπων υλοποίησης υποδομών cloud

Το Cloud Computing αναφέρεται, τόσο στις εφαρμογές που παρέχονται ως υπηρεσίες μέσω του Διαδικτύου, όσο και στο υλικό και στα συστήματα λογισμικού στα κέντρα δεδομένων που παρέχουν αυτές τις υπηρεσίες. Οι υπηρεσίες αυτές για καιρό αποδίδονταν με τον όρο *Λογισμικό ως Υπηρεσία (SaaS)*, με αποτέλεσμα να έχει επικρατήσει να χρησιμοποιείται αυτός ο όρος. Επιπλέον, το υλικό κέντρο δεδομένων και το λογισμικό είναι αυτό που αποκαλείται Cloud.

Όταν το Cloud διατίθεται στο κοινό με έναν "pay-as-you-go" τρόπο, αποκαλείται Public Cloud, ενώ η υπηρεσία που πωλείται είναι το Utility Computing[20]. Από την άλλη, χρησιμοποιούμε τον όρο Private Cloud για να αναφερθούμε σε εσωτερικά κέντρα δεδομένων μιας επιχείρησης ή ενός οργανισμού που δεν τίθενται στη διάθεση του κοινού. Έτσι, γίνεται δεκτό ότι το Cloud Computing είναι το άθροισμα των SaaS και Utility Computing, αλλά συνήθως δεν περιλαβάνονται ιδιωτικά Clouds[21].

Τα πλεονεκτήματα του SaaS, τόσο για τους τελικούς χρήστες, όσο και για τους παρόχους υπηρεσιών είναι απολύτως κατανοητά. Ανάμεσα στα πλεονεκτήματα που απολαμβάνουν οι πάροχοι υπηρεσιών είναι η σε μεγάλο βαθμό απλοποιημένη εγκατάσταση και συντήρηση του λογισμικού και ο συγκεντρωτικός έλεγχος εκδόσεων. Οι τελικοί χρήστες μπορούν να έχουν πρόσβαση στην υπηρεσία οποτεδήποτε και από οπουδήποτε, να μοιράζονται δεδομένα, να συνεργάζονται πιο εύκολα και να διατηρούν τα δεδομένα τους αποθηκευμένα με ασφάλεια στην υποδομή.

Το Cloud Computing, όχι μόνο δεν περιορίζεται στα επιχειρήματα αυτά, αλλά δίνει σε περισσότερους παρόχους εφαρμογών την επιλογή της εγκατάστασης του προϊόντος τους ως SaaS χωρίς την τροφοδότηση ενός κέντρου δεδομένων[22]. Αναλόγως με το πώς το SaaS επιτρέπει στο χρήστη να

[20] Τρέχοντα παραδείγματα δημόσιων Utility Computing είναι, μεταξύ άλλων, το Amazon Web Services, το Google AppEngine και το Microsoft Azure.

[21] ό.π., Armbrust M., Fox A., Griffith R., Joseph A., Katz R., Konwinski A., Lee G., Patterson D., Rabkin A., Stoica I., and Zaharia M., “Above the Clouds: A Berkeley View of Cloud Computing”.

[22] Όπως ακριβώς και η εμφάνιση των χυτηρίων ημιαγωγών έδωσε στις εταιρείες κατασκευής chip την ευκαιρία να σχεδιάζουν και να πωλούν chips χωρίς να κατέχουν ένα εργοστάσιο, το cloud computing επιτρέπει την ανάπτυξη SaaS χωρίς την κατασκευή ή την προμήθεια ενός κέντρου δεδομένων.

φορτώσει κάποια προβλήματα στον πάροχο SaaS, ο πάροχος SaaS μπορεί να φορτώσει τώρα μερικά από τα προβλήματά του στον πάροχο Cloud Computing.

Αναγκαία, αλλά όχι επαρκής συνθήκη για να γίνει μια εταιρεία φορέας παροχής Cloud Computing είναι ότι θα πρέπει να έχει υπάρχουσες επενδύσεις, αφενός σε πολύ μεγάλα κέντρα δεδομένων και αφετέρου στην υποδομή λογισμικού μεγάλης κλίμακας, παράλληλα δε απαιτείται σημαντική επιχειρησιακή τεχνογνωσία. Με δεδομένες αυτές τις συνθήκες, που αποτελούν τις ελάχιστες προϋποθέσεις, ώστε μία επιχείρηση να γίνει πάροχος Cloud Computing, μπορεί να υπάρξει επιπλέον και μια ποικιλία άλλων παραγόντων που μπορεί να επηρεάσει το κατά πόσο είναι δυνατή η παροχή υπηρεσιών Cloud computing ή όχι.

Αν και είναι δεδομένο ότι θα υπάρξουν εξ ολοκλήρου νέοι τύποι εφαρμογών που θα ενεργοποιηθούν από το Cloud Computing, εικάζεται ότι αρκετές σημαντικές κατηγορίες των υφιστάμενων εφαρμογών θα γίνουν ακόμη πιο συναρπαστικές με το Cloud Computing και θα συμβάλλουν με τον τρόπο αυτό στην περαιτέρω διάδοσή του. Όταν ο Jim Gray εξέτασε τεχνολογικές τάσεις κατά το έτος 2003[23], κατέληξε στο συμπέρασμα ότι η οικονομική αναγκαιότητα επιτάσσει την τοποθέτηση των δεδομένων κοντά στην εφαρμογή, δεδομένου ότι το κόστος του δικτύου ευρείας περιοχής έχει παρουσιάσει μείωση με πιο αργούς ρυθμούς (και επομένως εξακολουθεί να είναι σχετικά υψηλότερο) σε σχέση με όλα τα άλλα κόστη υλικού πληροφορικής.

Παρά το γεγονός ότι το κόστος του υλικού έχει αλλάξει από την ανάλυση του Gray, η ιδέα του γι’ αυτό το "αναγκαίο σημείο" δεν άλλαξε. Η διορατικότητα του Gray χρησιμοποιείται μέχρι σήμερα για τη διακρίβωση σχετικά με το ποια είδη εφαρμογών αντιπροσωπεύουν ιδιαίτερα καλές ευκαιρίες για το Cloud Computing[24].

[23] Gray J., Distributed Computing Economics, Queue 6, 3 (2008), pp. 63–68. Available from: http://portal.acm.org/ft_gateway.cfm?id=1394131&type=digital%20edition&coll=Portal&dl=GUIDE&CFID=19219697&CFTOKEN=50259492

[24] ό.π., Armbrust M., Fox A., Griffith R., Joseph A., Katz R., Konwinski A., Lee G., Patterson D., Rabkin A., Stoica I., and Zaharia M., “Above the Clouds: A Berkeley View of Cloud Computing”.

1.2. Τεχνολογία Cloud Computing – παραδείγματα από μεγάλες εταιρείες που έχουν αναπτύξει συστήματα Cloud

Google Compute Engine (GCE)

Πρώτο παράδειγμα αποτελεί το Google Compute Engine (GCE), το οποίο είναι ένα IaaS προϊόν που ανακοίνωσε η Google στο Google I/O τον Ιούνιο του 2012 (βλ. Σχήμα 2). Χρησιμοποιεί το KVM, όπως το hypervisor, και υποστηρίζει μόνο guest εικόνες που τρέχουνε σε λειτουργικό σύστημα Linux. Το Google Compute Engine προσφέρει μια ξεκούραστη API για τη διαχείριση των πόρων, όπως τον δίσκο, τις εικόνες και τα instances. Το προεπιλεγμένο λειτουργικό σύστημα που παρέχεται από την Google είναι το Debian 6.0 και 7.0. Εκτός απο το Debian, το μόνο λειτουργικό σύστημα που υποστηρίζεται είναι το CentOS 6.2.

Κάθε Google Compute Engine instance ξεκινά με έναν πόρο δίσκου. Ανάλογα με τον επιλεγμένο τύπο μηχανής, το instance μπορεί να ξεκινήσει με μηδενικό χώρο στο δίσκο (scratch), ή και τα δύο. Scratch χώρος στο δίσκο είναι ο χώρος που συνδέεται με τη ζωή ενός instance. Αν το instance τερματιστεί για οποιονδήποτε λόγο, όλα τα δεδομένα στο scratch δίσκο χάνονται. Αντίθετα, οι persistent δίσκοι έχουν μεγαλύτερη διάρκεια ζωής από ένα instance. Μπορούν να συνδέονται κατά την εκκίνηση, ή να επισυνάπτονται ή να αποκόπτονται από την εκτέλεση ενός instance on demand. Οι persistent δίσκοι μπορούν επίσης να συνδεθούνε σε read-only λειτουργία για να συγχωνεύσουν πολλά instance σε ένα. Οι persistent δίσκοι προσφέρουν επιπλέον χαρακτηριστικά απο τους scratch δίσκους, όπως persistent instances στο δίσκο, booting από έναν persistent δίσκο και μετάβαση των persistent δίσκων σε διαφορετικές ζώνες.

Σχήμα 2: Google Compute Engine (GCE)

Amazon EC2

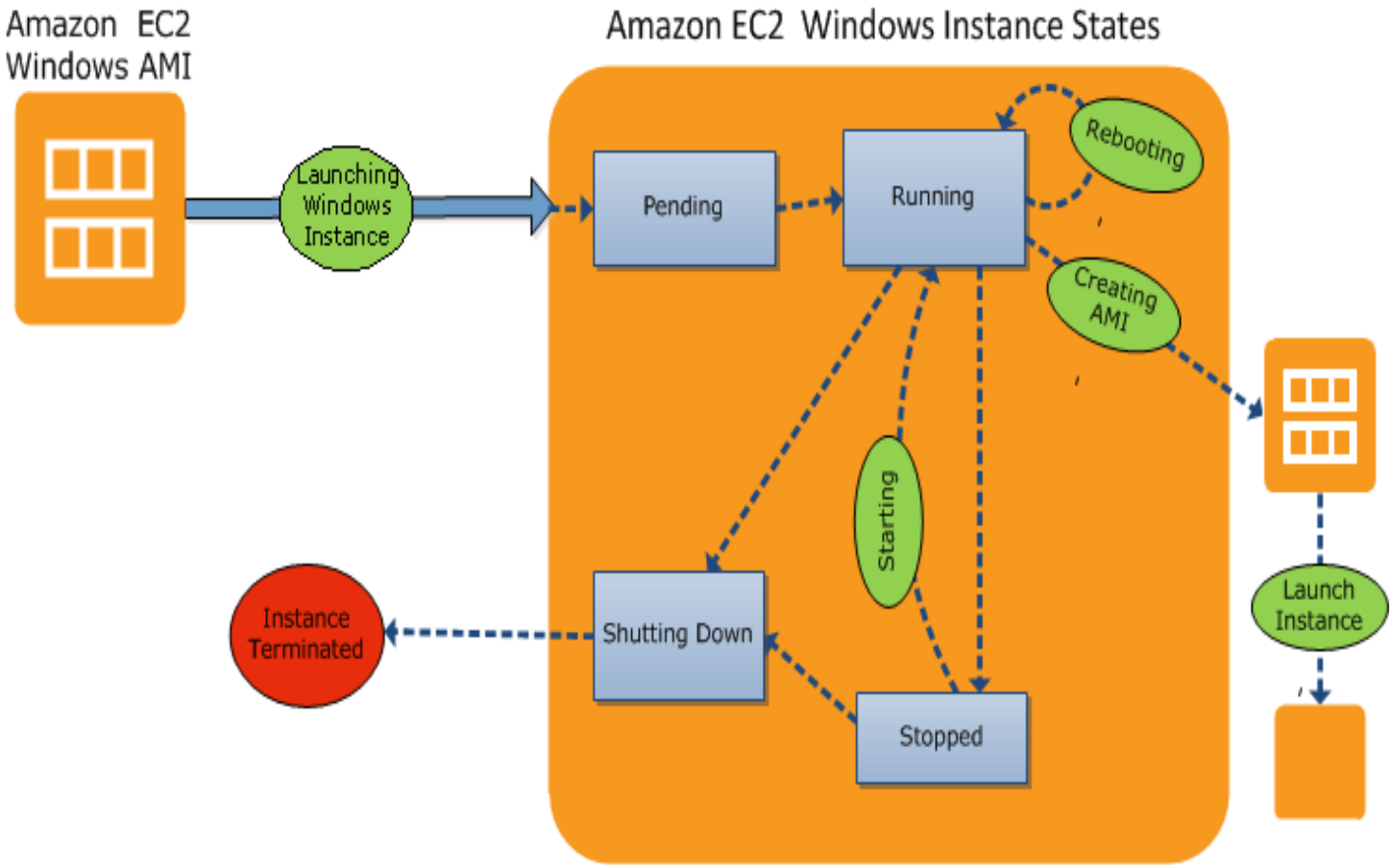
Το Amazon EC2 είναι στο ένα άκρο του φάσματος (βλ. Σχήμα 3). Ένα παράδειγμα EC2 μοιάζει πολύ με φυσικό υλικό και οι χρήστες μπορούν να ελέγχουν σχεδόν ολόκληρη τη στοίβα λογισμικού από τον πυρήνα και προς τα πάνω. Η εκτεθειμένη API είναι “thin” και μερικές δεκάδες API καλούνται να ζητήσουνε και να ρυθμίσουνε το εικονικό υλικό. Δεν υπάρχει όριο στα είδη των εφαρμογών που μπορούν να φιλοξενηθούν. Το χαμηλότερο επίπεδο virtualization-CPU, block-συσκευή αποθήκευσης, σύνδεση σε επίπεδο IP- επιτρέπουνε στους προγραμματιστές να γράψουνε σε όποιον κώδικα θέλουνε. Από την άλλη πλευρά, αυτό είναι δύσκολο για το Amazon, να προσφέρει αυτόματη επεκτασιμότητα και failover, γιατί η σημασιολογία που συνδέεται με την αντιγραφή και άλλα διαχειριστικά του state management είναι άκρως εξαρτημένη από την εφαρμογή.

Το AWS προσφέρει μια σειρά από υψηλού επιπέδου υπηρεσίες διαχείρισης, συμπεριλαμβανομένων πολλών διαφορετικών συσκευών αποθήκευσης σε χρήση, σε συνδυασμό με τον EC2, όπως είναι η SimpleDB. Ωστόσο, αυτές οι προσφορές έχουνε υψηλότερη λανθάνουσα κατάσταση και μη συνηθισμένα API, και αυτό που καταλαβαίνουμε είναι ότι δεν χρησιμοποιούνται τόσο ευρέως ως μέρη ενός AWS.

Στο άλλο άκρο του φάσματος είναι οι domain-specific εφαρμογές, όπως το Google, το AppEngine, το Force.com και το SalesForce που είναι μία πλατφόρμα επιχειρηματικής ανάπτυξης λογισμικού. Το AppEngine απευθύνεται αποκλειστικά σε παραδοσιακές εφαρμογές Web, επιβάλλοντας την υποδομή μιας εφαρμογής να διαχωρίζεται μεταξύ stateless βαθμίδα αποθήκευσης και stateful βαθμίδα αποθήκευσης. Επιπλέον, οι AppEngine εφαρμογές αναμένεται να είναι request-reply based, και ως τέτοιες διαχωρίζονται αυστηρά, ανάλογα με το πόσο χρόνο χρειάζεται να λειτουργήσει η CPU για την εξυπηρέτηση ενός συγκεριμένου αιτήματος. Οι εντυπωσιακοί αυτόματοι μηχανισμοί κλίμακας και υψηλής διαθεσιμότητας του AppEngine, καθώς και το ιδιόκτητο Megastore data storage που είναι διαθέσιμο στις εφαρμογές του AppEngine, στηρίζονται σε αυτούς τους περιορισμούς. Έτσι, το AppEngine δεν είναι κατάλληλο για γενικού σκοπού computing. Ομοίως, το Force.com έχει σχεδιαστεί για να υποστηρίζει τις επιχειρηματικές εφαρμογές που τρέχουν ενάντια στην Salesforce.com βάση δεδομένων.

Το Azure της Microsoft είναι ένα ενδιάμεσο σημείο σε αυτό το φάσμα της ευελιξίας ενάντια στην άνεση του προγραμματιστή. Οι εφαρμογές Azure είναι γραμμένες με .NET βιβλιοθήκες και μετατρέπονται σε Common Language Runtime, με ένα language independent διαχειριζόμενο περιβάλλον. Το σύστημα υποστηρίζει γενικής χρήσης computing και όχι μόνο μία κατηγορία της εφαρμογής. Οι χρήστες έχουνε τη δυνατότητα επιλογής της γλώσσας, αλλά δεν μπορούν να ελέγξουν το

υποκείμενο λειτουργικό σύστημα ή την εκτέλεσή του. Οι βιβλιοθήκες παρέχουν ένα βαθμό αυτόματης ρύθμισης παραμέτρων του διαδικτύου και failover/επεκτασιμότητα, αλλά απαιτούνε από τον προγραμματιστή να προσδιορίζει ορισμένες ιδιότητες της εφαρμογής, προκειμένου να το πράξουνε οι βιβλιοθήκες. Έτσι, το Azure είναι ενδιάμεσο μεταξύ ολοκληρωμένων frameworks των εφαρμογών, όπως το AppEngine από τη μία πλευρά, και hardware εικονικών μηχανών, όπως είναι το EC2 και άλλες, από την άλλη πλευρά.



Σχήμα 3: Amazon EC2

Amazon Elastic Compute Cloud (Amazon EC2)

Το Amazon Elastic Compute Cloud είναι μια διαδυκτιακή υπηρεσία που παρέχει δυνατότητα αλλαγής μεγέθους της υπολογιστικής δυναμικότητας στο Cloud. Έχει σχεδιαστεί για να κάνουν οι προγραμματιστές ευκολότερο web computing. Η απλή υπηρεσία για interface της Amazon EC2 μας δίνει τη δυνατότητα να αποκτήσουμε και να διαμορφώσουμε χωρητικότητα με την ελάχιστη τριβή. Μας παρέχει πλήρη έλεγχο των πόρων του υπολογιστή μας και μας επιτρέπει να εκτελέσουμε το αποδεδειγμένο computing περιβάλλον του Amazon. Το Amazon EC2 μειώνει το χρόνο που απαιτείται για την απόκτηση και την εκκίνηση νέων instances του server σε λεπτά, επιτρέποντάς μας να αναβαθμίσουμε γρήγορα τη χωρητικότητα, πάνω και κάτω, καθώς αλλάζουνε οι πληροφοριακές μας απαιτήσεις. Το Amazon EC2 αλλάζει και τα οικονομικά των servers του Cloud Computing, επιτρέποντας στον πελάτη να πληρώσει μόνο για τη χωρητικότητα που πραγματικά χρησιμοποιεί. Παρέχει, επίσης, στους προγραμματιστές τα εργαλεία για τη δημιουργία ανθεκτικών εφαρμογών, απομονώνοντας τον εαυτό τους από σενάρια αποτυχίας.

Η λειτουργικότητα του Amazon EC2

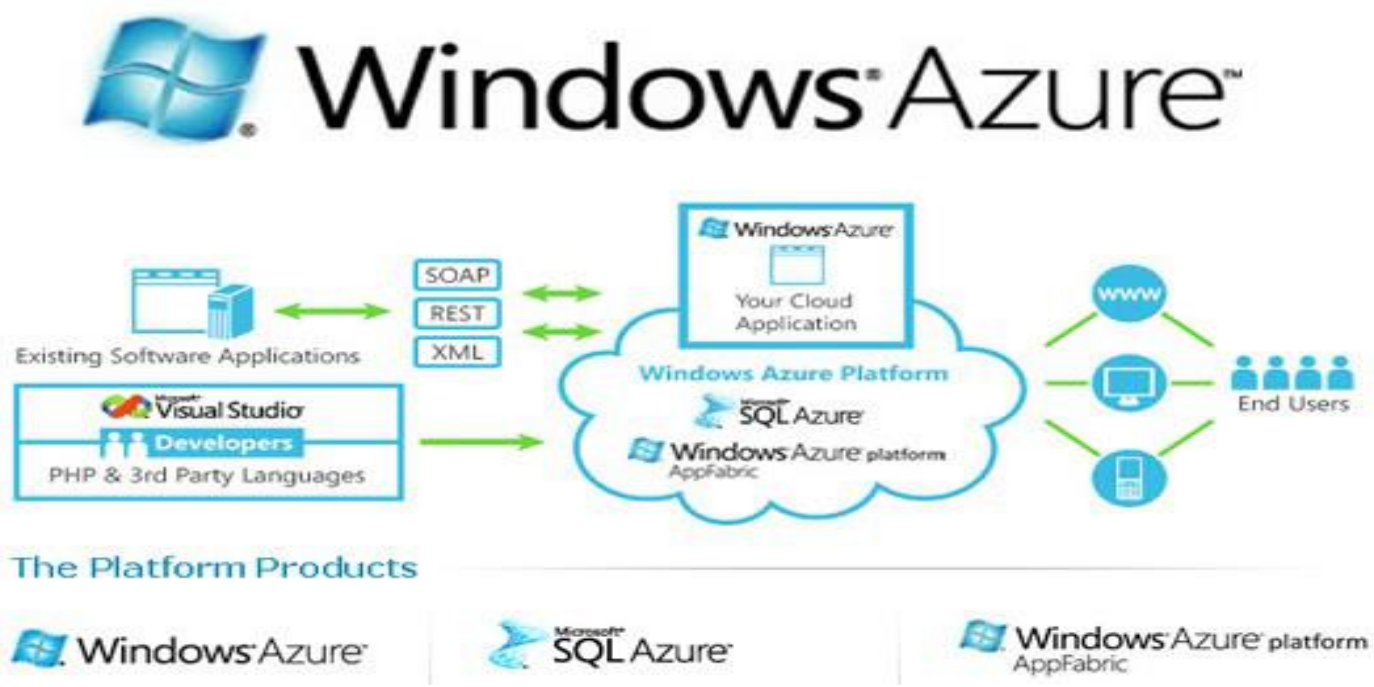
Το Amazon EC2 παρουσιάζει μια πραγματική Cloud Computing υπηρεσία, η οποία μας επιτρέπει να χρησιμοποιούμε διασυνδέσεις web υπηρεσιών για να ξεκινήσουμε instances με μια ποικιλία λειτουργικών συστημάτων. Μπορούμε απλά να χρησιμοποιήσουμε το Amazon EC2 μέσω των κατωτέρω βημάτων:

- Επιλέγουμε ένα pre-configured template Image Machine Amazon (AMI) για να ανέβει και να λειτουργήσει αμέσως, ή μπορούμε να δημιουργήσουμε ένα AMI που να περιέχει τις εφαρμογές μας, τις βιβλιοθήκες, τα δεδομένα και τις συναφείς ρυθμίσεις.
- Διαμορφώνουμε ασφαλή πρόσβαση στο δίκτυο για το Amazon EC2 instance.
- Επιλέγουμε ποια instances θέλουμε, στη συνέχεια ξεκινάμε, καταγράφουμε και τερματίζουμε όσα πιο πολλά instances από το AMI χρειάζονται, χρησιμοποιώντας τη διαδικτυακή υπηρεσία APIs ή την ποικιλία των εργαλείων διαχείρισης που παρέχονται.
- Προσδιορίζουμε, αν θέλουμε να τρέξουμε σε πολλαπλές τοποθεσίες, χρησιμοποιώντας στατικές IP παραμέτρους ή επισυνάπτουμε persistent block αποθηκευτικό χώρο στα instances.
- Πληρώνουμε μόνο για τους πόρους που πραγματικά καταναλώνουμε, όπως τις ώρες ή τη μεταφορά δεδομένων.

Windows Azure

Το Windows Azure είναι μια Cloud Computing πλατφόρμα (βλ. Σχήμα 4) που δημιουργήθηκε από την Microsoft για τη δημιουργία, την ανάπτυξη και τη διαχείρηση εφαρμογών και υπηρεσιών, μέσω ενός παγκόσμιου δικτύου των Microsoft-managed datacenters. Παρέχει την πλατφόρμα ως υπηρεσία (PaaS) και τις υποδομές ως υπηρεσία (IaaS) των υπηρεσιών του και υποστηρίζει πολλές διαφορετικές γλώσσες προγραμματισμού, εργαλεία και frameworks, συμπεριλαμβανομένων της Microsoft ειδικά για third-party λογισμικά ή συστήματα. Το Windows Azure κυκλοφόρησε την 1η Φεβρουαρίου του 2010.

Το Windows Azure είναι η πλατφόρμα εφαρμογής Cloud της Microsoft. Μπορεί να χρησιμοποιηθεί για την κατασκευή μιας web εφαρμογής που τρέχει και αποθηκεύει τα δεδομένα του σε datacenters της Microsoft. Μπορεί να συνδέσει on-premises εφαρμογές μεταξύ τους ή να συνδέσει μεταξύ τους διάφορα σύνολα των πληροφοριών ταυτότητας.



Σχήμα 4: Windows Azure

Τον Ιούνιο του 2012, το Windows Azure κυκλοφόρησε τα εξής νέα χαρακτηριστικά:

- Οι ιστοσελίδες επιτρέπουν στους προγραμματιστές να δημιουργήσουν δικτυακούς πόρους χρησιμοποιώντας ASP.NET, PHP ή Node.js και μπορούν να αναπτυχθούν με τη χρήση FTP, Git ή Team Foundation Server.
- Εικονικές μηχανές επιτρέπουν στους προγραμματιστές να μετεγκαταστήσουν τις εφαρμογές και τις υποδομές τους, χωρίς αλλαγή του υφιστάμενου κώδικα και μπορούν να τρέξουν τα Windows Server και Linux οι εικονικές μηχανές.
- Cloud Services, η πλατφόρμα της Microsoft ως υπηρεσία (PaaS) περιβάλλοντος που χρησιμοποιείται για να δημιουργήσει ολοληρωμένες εφαρμογές και υπηρεσίες.
- Υποστηρίζει σενάρια multi-tier και αυτοματοποιημένες υλοποιήσεις.
- Η διαχείρηση των δεδομένων, με βάση δεδομένων SQL, παλαιότερα γνωστή ως SQL Azure Database, εργάζεται για να δημιουργήσει την κλίμακα και να επεκτείνει τις εφαρμογές στο Cloud χρησιμοποιώντας την τεχνολογία Microsoft SQL Server. Ενσωματώνεται με το Active Directory και το Microsoft System Center και Hadoop.
- Υπηρεσίες οπτικοακουστικών μέσων επικοινωνίας, μια προσφορά PaaS που μπορεί να χρησιμοποιηθεί για την κωδικοποίηση, την προστασία του περιεχομένου, streaming και analytics.

Η Azure Platform των Windows παρέχει ένα API χτισμένο σε REST, HTTP και XML που επιτρέπει στους προγραμματιστές να αλληλεπιδρούν με τις υπηρεσίες που παρέχονται από το Windows Azure. Η Microsoft παρέχει επίσης ένα client-side, το οποίο διαχειρίζεται βιβλιοθήκη κατηγορίας που ενσωματώνει τις λειτουργίες αλληλεπίδρασης με τις υπηρεσίες. Ενσωματώνεται, επίσης, με το Microsoft Visual Studio, Git και Eclipse[25].

Το Windows Azure χρησιμοποιεί ένα εξειδικευμένο λειτουργικό σύστημα που ονομάζεται Windows Azure για να τρέξει το “fabric layer” – ένα σύμπλεγμα που φιλοξενείται σε datacenters της Microsoft που διαχειρίζεται computing πόρους και αποθήκευσης των ηλεκτρονικών υπολογιστών και των διατάξεων των πόρων (ή ένα υποσύνολό τους) σε εφαρμογές που εκτελούνται πάνω από το Windows Azure. Έχει περιγραφεί ως ένα cloud layer στην κορυφή ενός αριθμού συστημάτων του Windows Server, που χρησιμοποιούν Windows Server 2008 και μια προσαρμοσμένη έκδοση του Hyper-V, που είναι γνωστή ως Windows Azure Hypervisor για την παροχή των υπηρεσιών virtualization. Η

[25] Τον Οκτώβριο του 2012, η Microsoft κυκλοφόρησε μια download PDF αφίσα που συνοψίζει τα χαρακτηριστικά του Windows Azure.

κλιμάκωση και η αξιοπιστία ελέγχονται από το Windows Azure Fabric ελεγκτή, ώστε οι υπηρεσίες και το περιβάλλον να μην «κολλάνε», εάν ένας απο τους εξυπηρετητές «κολλάει» μέσα στο datacenter της Microsoft και παρέχει τη διαχείριση της εφαμρογής περιήγησης του χρήστη, όπως πόρους μνήμης και εξισορρόπησης φορτίου.

Yahoo open-source cloud-serving engine

Το Network World – Yahoo αναπτύσσει μια εσωτερική μηχανή cloud-serving για να ενισχύσει την παραγωγικότητά της και σκοπεύει να απελευθερώσει τον κώδικά της ως open source (βλ. Σχήμα 5). Παρόλα αυτά, το εσωτερικό project της Yahoo θα μπορούσε να προωθήσει την ανάπτυξη των δικών του Web ιδιοτήτων για να γίνει πιο αποτελεσματικό και να δώσει στις επιχειρήσεις και στους προγραμματιστές μια πλατφόρμα ελεύθερου λογισμικού για να δημιουργήσουν το δικό τους Cloud.

Η μηχανή του Cloud-serving επιτρέπει στους προγραμματιστές να οικοδομήσουν υπηρεσίες σε containers που βρίσκονται πάνω στο virtual-machine layer, αφήνοντάς τους να αναπτύσσουν γρήγορα εφαρμογές που έχουν ανεβεί και να τρέχουν με μια σειρά από κοινές υπηρεσίες[26]. Ο μηχανισμός cloud-serving είναι γραμμένος σε Java και C++ και υποστηρίζει PHP και Javascript. Πριν από την απελευθέρωσή του σαν open-source, το Yahoo θα αφαιρέσει μερικά στοιχεία που είναι ειδικά για το Yahoo και ως εκ τούτου δεν θα βοηθήσει τους εξωτερικούς χρήστες.

Σχήμα 5: Yahoo open-source cloud-serving engine

1.3. Ελληνική και ευρωπαϊκή περιγραφή της εξάπλωσης και της χρήσης συστημάτων cloud

[26] Είναι κάπου μεταξύ μιας as-a-service υποδομής και της πλατφόρμας platform-as-a-service offering, για παράδειγμα, ένα χαμηλότερο επίπεδο αφαίρεσης από αυτό που προβλέπεται από το Google App Engine, ένα γνήσιο PaaS παιχνίδι.

Το Cloud Computing σύστημα αναδεικνύεται σε ένα δημοφιλές στοιχείο του IT τοπίου στον ελλαδικό χώρο. Εκατοντάδες εκατομμύρια χρήστες βασίζονται σε αυτό προκειμένου να ανταλλάξουν και να αποθηκεύσουν μηνύματα ηλεκτρονικού ταχυδρομείου, φωτογραφίες, βίντεο και άλλου είδους περιεχόμενα. Το Cloud Computing έχει τη δυναμική να γίνει το ανερχόμενο τεχνολογικό επίτευγμα που θα αλλάξει ριζικά τον τρόπο με τον οποίο λειτουργεί η κοινωνία μας, γεγονός το οποίο σαφώς περιλαμβάνει τις τεχνικές παραγωγής της οικονομίας και οδηγεί στην ανταγωνιστικότητα της ελληνικής οικονομίας[27].

Υπολογίζεται ότι το Cloud Computing σύστημα ουσιαστικά ελαττώνει το κόστος, ενισχύει την παραγωγικότητα και δημιουργεί νέες ευκαιρίες επιχειρηματικής ανάπτυξης. Οι έρευνες δείχνουν ότι μέσα στην επόμενη δεκαετία, μάλιστα, θα σωθούν περίπου 5 δισεκατομμύρια από τις ελληνικές επιχειρήσεις, ενώ άλλα 5 δισεκατομμύρια έσοδα θα προστεθούν στην ελληνική οικονομία. Σημαντικός, βέβαια, παράγοντας για την ευεργετική αυτή επίδραση των τεχνολογικών αλλαγών είναι η ταχύτητα ενσωμάτωσης των νέων δεδομένων, αφού αν η πλήρης υιοθέτηση του Cloud συστήματος επιτευχθεί μέσα στην επόμενη πενταετία, τότε τα συνολικά έσοδα μπορούν να αγγίξουν ακόμη και τα 21 δισεκατομμύρια. Επιπρόσθετα, η υιοθέτηση του Cloud Computing συστήματος, πέρα από την αύξηση των εσόδων της ελληνικής οικονομίας, υπολογίζεται ότι θα οδηγήσει στη δημιουργία περίπου 38.000 θέσεων εργασίας μέχρι το τέλος της δεκαετίας 2010-2020[28].

Η υιοθέτηση, βέβαια, του Cloud Compuping συστήματος, προϋποθέτει σε μία πρώτη φάση από τις εταιρείες να αναπτύξουν προωθητικές καμπάνιες αναφορικά με τις χρήσεις του Cloud Computing και των εφαρμογών Cloud, έτσι ώστε να γίνουν ευρέως γνωστά τα οφέλη τους στους καταναλωτές και στις εταιρείες. Σε ένα δεύτερο στάδιο, οι πάροχοι των Cloud Computing συστημάτων θα πρέπει να ανιχνεύουν τις διεθνείς τάσεις και τις ενημερώσεις ασφαλείας στις τεχνολογίες Cloud, ενώ παράλληλα θα πρέπει να υιοθετήσουν κανόνες συμβατούς με τις ανάγκες των επιχειρήσεων αναφορικά με τη διαχείριση και τη μεταφορά των δεδομένων Cloud, κυρίως μέσω της παραμετροποίησης των

[27] Danchev S., Tsakanikas A. and Ventouris N., Cloud Computing: A Driver for Greek Economy Competitiveness, Foundation for Economic and Industrial Research, November 2011, p. 7.

[28] ό.π. Danchev S., Tsakanikas A. and Ventouris N., p. 9.

προτεινόμενων λύσεων[29]. Παράλληλα, στο δημόσιο τομέα, η πολιτεία θα πρέπει να επενδύσει σε μεγάλα κέντρα δεδομένων (G-Data Centres/G-Cloud), τα οποία θα δημιουργήσουν μία κεντρική υπολογιστική υποδομή για την ελληνική κυβέρνηση και η οποία θα λειτουργεί υποστηρικτικά για όλες τις περιοχές του δημόσιου τομέα. Επιπλέον, στο δημόσιο τομέα θα πρέπει πλέον να είναι διαθέσιμες προηγμένες υπηρεσίες ηλεκτρονικής διακυβέρνησης, έτσι ώστε να αποτελεί δέλεαρ για τους πολίτες και τις επιχειρήσεις η υιοθέτηση των τεχνολογιών πληροφορικής, ενώ επιβάλλεται και η υποχρεωτική χρήση των σχετικών εφαρμογών από τους δημοσίους υπαλλήλους για συγκεκριμένες λειτουργίες, έτσι ώστε να διαδοθεί έτι περαιτέρω η υιοθέτησή τους[30].

Σύμφωνα με στοιχεία[31] που συλλέχθησαν κατά το Νοέμβριο του 2014 σε έρευνα της EUROSTAT[32], η χρήση του Cloud Computing από χρήστες εντός της Ευρωπαϊκής Ένωσης είναι ιδαιτέρως ενθαρρυντική. Όπως προκύπτει από την εν λόγω έρευνα, 19 % των επιχειρήσεων της Ευρωπαϊκής Ένωσης χρησιμοποίησαν το Cloud Computing το έτος 2014, κυρίως για να "φιλοξενήσουν" τα συστήματα των e-mail τους και για να αποθηκεύσουν αρχεία σε ηλεκτρονική μορφή. Επιπλέον, 46 % από αυτές τις επιχειρήσεις χρησιμοποίησαν προηγμένες υπηρεσίες Cloud που αφορούν στις οικονομικές και λογιστικές εφαρμογές λογισμικού, στη διαχείριση πελατειακών σχέσεων ή τη χρήση της υπολογιστικής ισχύος για την εκτέλεση επιχειρηματικών εφαρμογών, ενώ σχεδόν διπλάσιος αριθμός επιχειρήσεων χρησιμοποίησε public cloud servers (12 %) αντί για private cloud servers (7 %).

Τέσσερις στις δέκα επιχειρήσεις (39 %) χρησιμοποιώντας το Cloud ανέφεραν τον κίνδυνο παραβίασης της ασφάλειας ως κύριο περιοριστικό παράγοντα στη χρήση των υπηρεσιών Cloud

[29] Η παραμετροποίηση επιτρέπει στους χρήστες να εκμεταλλευτούν τα Cloud χαρακτηριστικά που μπορούν να αναπτυχθούν σε εσωτερικό επίπεδο και βασίζονται στις ιδιαίτερες ανάγκες και στόχους τους, αναθέτοντας παράλληλα άλλες λειτουργίες στους παρόχους Cloud. Η ανωτέρω «φόρμουλα» ίσως αποτελεί μία αρκετά ενδιαφέρουσα προοπτική ιδίως για τα ελληνικά δεδομένα, εξαίτίας του διαφορετικού μεγέθους των ελληνικών εταιρειών, με την έννοια ότι οι μεγαλύτερες εταιρείες ίσως επιθυμούν την ανάπτυξη των δικών τους εσωτερικών Cloud συστημάτων (private clouds), σε αντίθεση με τις μικρότερες εταιρείες, οι οποίες ενδείκνυται να χρησιμοποιούν public clouds.

[30] ό.π. Danchev S., Tsakanikas A. and Ventouris N., p. 10-11.

[31] Τα συγκεκριμένα δεδομένα βασίζονται σε αποτελέσματα έρευνας το έτος 2014 για τη χρήση των ΤΠΕ και του ηλεκτρονικού εμπορίου στις επιχειρήσεις. Τα στατιστικά στοιχεία προέρχονται από έρευνες σε επιχειρήσεις που διεξήχθησαν από τις εθνικές στατιστικές αρχές το 2014. Η μονάδα στατιστικής παρατήρησης είναι η επιχείρηση, όπως ορίζεται στον κανονισμό (ΕΟΚ) αριθ 696/93. Η έρευνα κάλυψε επιχειρήσεις με τουλάχιστον 10 εργαζομένους. Το 2014, 151.000 από τις 1.500.000 επιχειρήσεις στην Ε.Ε. συμμετείχαν στην εν λόγω στατιστική έρευνα. Από τις 1.500.000 επιχειρήσεις, περίπου το 83% ήταν μικρές επιχειρήσεις (10-49 εργαζόμενοι), 14% μεσαίες (50-249 εργαζόμενοι) και 3% μεγάλες (250 εργαζόμενοι και πάνω).

[32] Giannakouris K., Smihili M., Cloud computing - statistics on the use by enterprises, Eurostat, November 2014.

Computing, την ώρα που σχεδόν το ίδιο ποσοστό (42 %) από αυτές που δεν το χρησιμοποιούν ανέφεραν την ανεπαρκή γνώση του Cloud Computing ως τον κύριο αποτρεπτικό παράγοντα για τη χρήση του.

Παρά, επομένως, τα προφανή οφέλη των εταιρειών από τη χρήση του Cloud Computing, που συνίστανται πρωτίστως στην εξασφάλιση κόστους από την κατασκευή ιδίας υποδομής πληροφορικής (η οποία θα περιελάμβανε υλικό και την ανάπτυξη και διατήρηση του λογισμικού εφαρμογών και βάσεων δεδομένων), οι επιχειρήσεις δεν έχουν εξοικειωθεί πλήρως με τη χρήση υπολογιστικών πόρων που φιλοξενούνται από τρίτους στο διαδίκτυο (Cloud)[33].

Όσες, όμως, έχουν εξοικειωθεί με τη χρήση των υπηρεσιών του Cloud Computing πρέπει να έχουν πρόσβαση στο διαδίκτυο, ώστε να είναι σε θέση να τις χρησιμοποιούν, δεδομένου ότι οι υπηρεσίες Cloud Computing μπορεί να διανεμηθούν μόνο μέσω του Διαδικτύου. Το 2014, αυτό εφαρμόστηκε σχεδόν σε όλες τις επιχειρήσεις της Ευρωπαϊκής Ένωσης (97 %) με 10 ή περισσότερους εργαζομένους. Παρά το γεγονός ότι το ποσοστό των επιχειρήσεων με πρόσβαση στο διαδίκτυο ήταν σε παρόμοια επίπεδα κορεσμού στα περισσότερα κράτη μέλη[34], μόνο ένας στους πέντε (19 %) δήλωσε ότι χρησιμοποίησε τις υπηρεσίες υπολογιστικού νέφους.

[33] Εξάλλου, δεν πρέπει να λησμονείται το γεγονός ότι σε τεχνολογικό επίπεδο, το Cloud Computing είναι ένα μοντέλο με το οποίο παρέχεται στις επιχειρήσεις η πρόσβαση με ευέλικτο τρόπο και μέσω του διαδικτύου σε μια κοινόχρηστη δεξαμενή προσαρμόσιμων υπολογιστικών πόρων, συμπεριλαμβανομένων των servers, των βάσεων δεδομένων, των εφαρμογών λογισμικού, της χωρητικότητας αποθήκευσης και της υπολογιστικής ισχύος. Το Cloud Computing μπορεί να θεωρηθεί ως η τεχνολογική εξέλιξη του server-based computing. Οι επιχειρήσεις μπορούν να χρησιμοποιήσουν τις υπηρεσίες του μέσω πρόσβασης στο Internet με τη χρήση συσκευών που κυμαίνονται σε σχετικά χαμηλό κόστος, επιτραπέζιων υπολογιστών (thin clients), αλλά και διάφορων άλλων φορητών συσκευών. Επιπλέον, οι πάροχοι υπηρεσιών μπορούν να παρέχουν υπηρεσίες που σχετίζονται με ΤΠΕ από τους κοινόχρηστους διακομιστές (δημόσιο Cloud) ή από ένα σύννεφο - υποδομή που προβλέπεται για την αποκλειστική χρήση μιας συγκεκριμένης επιχείρησης (private Cloud).

[34] Σημαντικές διαφορές παρατηρούνται μεταξύ των διαφόρων χωρών, όπως για παράδειγμα στη Φινλανδία, την Ισλανδία, την Ιταλία, τη Σουηδία και τη Δανία, όπου πάνω από το 30% των επιχειρήσεων χρησιμοποιούν το Cloud Computing, σε αντίθεση, με την Ουγγαρία, τη Βουλγαρία, την Ελλάδα, την Πολωνία, τη Λετονία και τη Ρουμανία, όπου λιγότερο από το 10% των επιχειρήσεων χρησιμοποιούν τις υπηρεσίες του υπολογιστικού νέφους. Από τις επιχειρήσεις δε που ανέφεραν τη χρήση του Cloud Computing, περίπου το 66% αυτών στηρίχθηκε σε μια λύση "Cloud" για τα e-mail της. Αντί δηλαδή για τη δημιουργία μιας υποδομής server για το σύστημα e-mail τους, πράγμα που θα συνεπαγόταν, μεταξύ άλλων, το κόστος των κεφαλαιουχικών δαπανών και συντήρησης, οι επιχειρήσεις αυτές προτίμησαν μια "Cloud" λύση, όσον αφορά στο λειτουργικό κόστος που βασίζεται ανά χρήστη. Πάνω από το ήμισυ του συνόλου των επιχειρήσεων (53%) χρησιμοποίησαν το «σύννεφο» για την αποθήκευση αρχείων σε ηλεκτρονική μορφή. Επιπλέον, το 39% περίπου το χρησιμοποίησε για να φιλοξενήσει τη βάση δεδομένων τους, ενώ το 34% ανέφερε ότι το χρησιμοποίησε ως λογισμικό γραφείου (π.χ. επεξεργαστές κειμένου, λογιστικά φύλλα, κ.λπ.).

Το πιο σημαντικό, βέβαια, που επιτυγχάνεται μέσω του Cloud, είναι ότι οι επιχειρήσεις έχουν πρόσβαση σε σχετικά πιο προηγμένες εφαρμογές λογισμικού τελικού πελάτη, π.χ. για τα οικονομικά/λογιστικά και τη διαχείριση των πληροφοριών για τους πελάτες τους (διαχείριση πελατειακών σχέσεων – CRM, σε ποσοστό 31% και 21% αντίστοιχα). Επιπλέον, το 17% των επιχειρήσεων ανέφερε τη χρήση (συνήθως υψηλής απόδοσης) πλατφόρμας Cloud Computing για την ύπαρξη υπολογιστικής ισχύος, έτσι ώστε να "τρέξουν" τις δικές τους επιχειρηματικές εφαρμογές λογισμικού. Τέλος, δεν αποτελεί έκπληξη ότι το υψηλότερο ποσοστό των επιχειρήσεων που χρησιμοποιούν τις υπηρεσίες Cloud Computing (45%) δραστηριοποιείται στον τομέα της πληροφόρησης και της επικοινωνίας, ενώ σχεδόν σε όλους τους άλλους τομείς της οικονομίας, το ποσοστό κυμαίνεται από 14% έως 20%. Επαγγελματικές, επιστημονικές και τεχνικές επιχειρήσεις ανέφεραν τη χρήση Cloud σε ποσοστό μόλις 27%.

Όσον αφορά στην εξάρτηση από τις υπηρεσίες Cloud Computing, οι επιχειρήσεις μπορούν να ταξινομηθούν ανάλογα με το βαθμό εξάρτησης σε τρία επίπεδα (κατώτερο-μεσαίο, μεσαίο-ανώτερο και υψηλό) σύμφωνα με τον ακόλουθο πίνακα[35] :

Use of cloud computing services	Medium		High
	Lower-medium	Upper-medium	
(a) e-mail	Yes/No	Yes/No	Yes/No
(b) Office software	Yes/No	Yes/No	Yes/No
(c) Storage of files	Yes/No	Yes/No	Yes/No
(d) Hosting the enterprise's database(s)	**No**	**Yes**	Yes/No
(e) Financial or accounting software applications	**No**	**No**	Yes/No
(f) CRM software application	**No**	**No**	Yes/No
(g) Computing power for enterprise's own software	**No**	**No**	Yes/No

Το 19% των επιχειρήσεων εντός της Ευρωπαϊκής Ένωσης ανέφεραν ότι χρησιμοποιούν το Cloud και ένα σχετικά υψηλό ποσοστό (9% του συνόλου) δήλωσε ότι χρησιμοποιούσε τουλάχιστον μία από τις προηγμένες υπηρεσίες που αναγράφονται στον ανωτέρω πίνακα (e, f και g). Από τα στοιχεία που συνελλέχθησαν καταλήγουμε στο συμπέρασμα ότι το 46% των επιχειρήσεων στην Ευρωπαϊκή Ένωση

[35] Για την ταξινόμηση αυτή, όλες οι πιθανές μεμονωμένες απαντήσεις (με έντονα γράμματα) είναι απαραίτητες προϋποθέσεις. Για παράδειγμα, οι επιχειρήσεις που κατατάσσονται στο "κατώτερο-μεσαίο" επίπεδο χρησιμοποιούν τουλάχιστον μία από τις υπηρεσίες στο (a), (b) ή (c), αλλά καμία από τις υπόλοιπες. Αυτές που κατατάσσονται στο "μεσαίο-ανώτερο" επίπεδο, επιπλέον χρησιμοποιούν ή έχουν χρησιμοποιήσει την υπηρεσία στο (d), αλλά καμία από τις σχετικά προηγμένες υπηρεσίες στα (e), (f) και (g). Επιχειρήσεις που κατατάσσονται στο "υψηλό" επίπεδο έχουν απαντήσει καταφατικά ότι χρησιμοποιούν ή έχουν χρησιμοποιήσει τουλάχιστον μία από τις υπηρεσίες (e), (f) και (g).

που χρησιμοποιεί το υπολογιστικό νέφος είναι «εξαρτώμενο σε μεγάλο βαθμό», ενώ το 49% δεν χρησιμοποιεί καμία από τις προηγμένες υπηρεσίες και ταξινομείται στο «μεσαίο» επίπεδο. Στα δύο άκρα, η πλειοψηφία των επιχειρήσεων στον τομέα της μεταποίησης (58%) ανήκει στην ομάδα μεσαίας εξάρτησης, ενώ η πλειοψηφία των επιχειρήσεων πληροφοριών και επικοινωνιών (63%) αναφέρει τη χρήση προηγμένων υπηρεσιών και ως εκ τούτου, ανήκει στην ομάδα υψηλής εξάρτησης.

Όπως προαναφέρθηκε, οι πάροχοι υπηρεσιών μπορούν να παρέχουν υπηρεσίες Cloud Computing με όλα τα παραπάνω χαρακτηριστικά με δύο βασικούς τρόπους: μέσω των servers του δημόσιου cloud (12% των επιχειρήσεων) ή μέσω ιδιωτικών cloud servers (7% των επιχειρήσεων). Ο δεύτερος τρόπος, εξ ορισμού, περιλαμβάνει το περιβάλλον ενός "ενοικιαστή", όπου το υλικό, η αποθήκευση και το δίκτυο προορίζονται για μία μόνο επιχείρηση. Κατά συνέπεια, η υποδομή εγγυάται υψηλά επίπεδα ασφάλειας, καθώς άλλοι πελάτες του παρόχου υπηρεσιών δεν μπορούν να έχουν πρόσβαση στους ίδιους πόρους. Ένα ποσοστό της τάξης του 7% των μικρο-μεσαίων επιχειρήσεων και ένα ποσοστό 17% των μεγάλων επιχειρήσεων ανέφεραν ότι χρησιμοποιούν private Cloud. Από την άλλη πλευρά, οι υποδομές public Cloud παρέχονται για κοινή χρήση από πολλαπλούς πελάτες. Ουσιαστικά, τείνουν να είναι ιδιαίτερα τυποποιημένοι, με επιλογές περιορισμένης παραμετροποίησης, π.χ. ένα e-mail server μπορεί να προσφέρει σε πολλές επιχειρήσεις την απαραίτητη υποδομή cloud για τη διαχείριση των συστημάτων e-mail τους. Το public Cloud Computing, χρησιμοποιείται από το 24% των μεγάλων επιχειρήσεων και το 12% των μικρο-μεσαίων επιχειρήσεων στην Ευρωπαϊκή Ένωση.

Εντούτοις, οι επιχειρήσεις[36] που χρησιμοποιούν τις υπηρεσίες Cloud Computing ανέφεραν διάφορους παράγοντες που συμβάλλουν στον περιορισμό της χρήσης τους. Ο κίνδυνος παραβίασης της ασφάλειας συγκέντρωσε την υψηλότερη βαθμολογία για τις μεγάλες και τις μικρο-μεσαίες επιχειρήσεις, (57% και 38% αντίστοιχα), γεγονός που καθίσταται απολύτως σαφές, αν αναλογιστεί κανείς τη σημασία που αποδίδουν οι επιχειρήσεις στην προστασία των πληροφοριακών τους συστημάτων[37].

[36] Οι επιχειρήσεις κατανέμονται κατά μέγεθος προσωπικού, σε μικρές (10-49 απασχολούμενοι), μεσαίες (50-249) και μεγάλες (250 και άνω).

[37] Βέβαια, το θέμα θα πρέπει να εξεταστεί στο ευρύτερο πλαίσιο της ανθεκτικότητας σε πιθανές παραβιάσεις ασφαλείας όταν χρησιμοποιείται το Cloud. Οι πάροχοι υπηρεσιών θα πρέπει να είναι σε διαρκή αναμονή, ώστε να λαμβάνουν όλα τα δυνατά μέτρα που σχετίζονται με την καθιέρωση και τη διαφάνεια, καθώς και την εφαρμογή διαδικασιών που σχετίζονται με πιθανές παραβιάσεις της ασφάλειας των συστημάτων και υπηρεσιών που προορίζονται για τους πελάτες τους. Ως εκ τούτου, από την σκοπιά των εταιριών (ανεξάρτητα από το μέγεθος), ο κίνδυνος παραβίασης της ασφάλειας μπορεί να είναι ένα θέμα των παρόχων υπηρεσιών ευθύνης και λογοδοσίας, καθώς και απλώς ένα τεχνικό ζήτημα.

Οι μεγάλες και οι αντίστοιχες μικρο-μεσαίες επιχειρήσεις διέφεραν όμως ως προς τους άλλους περιοριστικούς παράγοντες. Η χρήση των υπηρεσιών του Cloud Computing μπορεί να απαιτεί συγκεκριμένες δεξιότητες διαχείρισης ΤΠΕ, ιδίως για να εκτιμηθούν οι ανάγκες και η χρήση των εργαλείων διαχείρισης για την ακριβή μέτρηση της κατανάλωσης των πόρων πληροφορικής. Ως εκ τούτου, η ανεπαρκής γνώση ή η έλλειψη εξειδίκευσης μπορεί να περιορίσει την "απορρόφηση" του Cloud Computing. Μία στις τρεις μικρο-μεσαίες επιχειρήσεις (32%) που χρησιμοποιούν το Cloud ανέφεραν το ανωτέρω ως περιοριστικό παράγοντα, εν αντιθέσει με κάτι λιγότερο από μία στις πέντε μεγάλες επιχειρήσεις (17%) που ανέφεραν το ίδιο. Παρόμοιο ποσοστό των μικρο-μεσαίων επιχειρήσεων (32%) που χρησιμοποιούν ήδη το Cloud θεωρεί το υψηλό κόστος των υπηρεσιών Cloud Computing ως περιοριστικό παράγοντα.

Οι Cloud υπηρεσίες συχνά φιλοξενούνται σε μία χώρα και χρησιμοποιούνται από άλλες. Οι πάροχοι υπηρεσιών μπορούν να χρησιμοποιούν κέντρα δεδομένων τα οποία είναι διάσπαρτα σε όλο τον κόσμο και ως εκ τούτου επιχειρήσεις που χρησιμοποιούν το Cloud μπορεί να αισθάνονται αβέβαιες για τη θέση των δεδομένων τους. Επιπλέον, ενδέχεται να υπάρχουν προβλήματα νομικής δικαιοδοσίας σε περίπτωση διαφοράς και αβεβαιότητας σχετικά με το εφαρμοστέο δίκαιο. Οι δύο αυτοί παράγοντες έχουν αναφερθεί ως κύριος περιοριστικός παράγοντας στη χρήση του Cloud Computing, ιδιαίτερα για τις μεγάλες επιχειρήσεις, οι οποίες χρησιμοποιούν ήδη το Cloud.

Εκτός, όμως, από τους περιοριστικούς παράγοντες για τη χρήση των υπηρεσιών Cloud, τα στοιχεία της έρευνας της EUROSTAT, ανέδειξαν και το ζήτημα της ύπαρξης περιοριστικών παραγόντων για την άρνηση αγοράς υπηρεσιών Cloud. Έτσι, η πλειοψηφία των επιχειρήσεων διαφόρων τομέων της Ευρωπαϊκής Ένωσης[38] δεν αγόρασε υπηρεσίες Cloud Computing με το αιτιολογικό ότι η ανεπαρκής γνώση του Cloud Computing τους απέτρεψε από μία ενδεχόμενη αγορά. Είναι γεγονός ότι η εμπειρογνωμοσύνη και η επαρκής γνώση των συμβατικών και νομικών πτυχών, καθώς και οι λεπτομέρειες της τεχνικής εφαρμογής είναι απαραίτητες προϋποθέσεις για μια επιχείρηση, ώστε να αποφασίσει να αγοράσει τις υπηρεσίες Cloud Computing (αυτό ισχύει επίσης για τις επιχειρήσεις που χρησιμοποιούν ήδη το Cloud).

[38] Οι τομείς οικονομικής δραστηριότητας που αναφέρονται καλύπτουν τις κατασκευαστικές εταιρίες, την ηλεκτρική ενέργεια, το φυσικό αέριο και τον ατμό, την ύδρευση, το χονδρικό και λιανικό εμπόριο, την επισκευή μηχανοκίνητων οχημάτων και μοτοσυκλετών, τη μεταφορά και αποθήκευση, τη στέγαση και τις δραστηριότητες υπηρεσιών εστίασης, τις πληροφορίες και τις επικοινωνίες, τα ακίνητα, τις επαγγελματικές, επιστημονικές και τεχνικές δραστηριότητες, τις διοικητικές και υποστηρικτικές δραστηριότητες και την επισκευή των ηλεκτρονικών υπολογιστών και εξοπλισμού επικοινωνίας.

ΚΕΦΑΛΑΙΟ 2 – Οφέλη και δυνατότητες του Cloud Computing

2.1. Οφέλη που προκύπτουν από τη σωστή αξιοποίηση των τεχνολογιών Cloud Computing

Όπως σε κάθε πτυχή των τεχνολογικών επιτευγμάτων, έτσι και στις τεχνολογίες των Cloud Computing συστημάτων, τα οφέλη που προκύπτουν είναι άμεσα σχετιζόμενα με τη σωστή χρήση και αξιοποίηση των τεχνολογιών Cloud. Είναι γεγονός ότι πολλές νεοσύστατες επιχειρήσεις πιθανότατα δεν θα υπήρχαν χωρίς τις υπηρεσίες Cloud[39].

Σε σχετική έρευνα που έλαβε χώρα[40] σχετικά με τη μεταφορά των πληροφοριακών συστημάτων μιας επιχείρησης σε ένα μοντέλο Iaas (Δομή νέφους σαν Υπηρεσία), αυτά αναφέρονται σε μία δομή Cloud διαχειριζόμενη από τρίτους. Σύμφωνα με τους ερευνητές, αν αυτή η δομή χρησιμοποιηθεί από την επιχείρηση, τότε η τελευταία επωφελείται με πολλούς τρόπους δυνάμενη να βελτιώσει τη διαχείριση των εσόδων και των εξόδων της, καθώς επίσης και τα εσωτερικά οικονομικά της, αλλά και τις συνδιαλλαγές της με τους πελάτες. Επιπλέον, η προαναφερθείσα δομή ευνοεί τη διαχείριση της ροής κεφαλαίου στα εσωτερικά οικονομικά ζητήματα της επιχείρησης, καθώς το μοντέλο τιμολόγησης των υπηρεσιών Cloud έχει ελάχιστο αρχικό κόστος και μηνιαία τιμολόγηση, ενώ παράλληλα μειώνεται η μεταβλητότητα στις ανάγκες ηλεκτρισμού.

Τα ανωτέρω είναι τα οφέλη από τη χρήση της δομής Cloud, συγκρινόμενα με ένα κέντρο επεξεργασίας δεδομένων εντός της επιχείρησης, καθώς κάτι τέτοιο αφενός μπορεί να είναι πολυέξοδο λόγω της ανάγκης αναβάθμισης των μηχανημάτων και του λογισμικού της, αφετέρου ενδέχεται η ροή

[39] Παραδείγματα τέτοιων επιχειρήσεων είναι η Animoto, που παρέχει υπηρεσίες που επιτρέπουν στο χρήστη να μετατρέψει φωτογραφίες σε καλλιτεχνικά μουσικά βίντεο κάνοντας χρήση λογισμικού τεχνητής νοημοσύνης. Όταν λανσαρίστηκε αυτή η υπηρεσία στο Facebook, ένα κοινωνικό δίκτυο, η ζήτηση ήταν τέτοια που έπρεπε η επιχείρηση να αυξήσει τις εικονικές της μηχανές στο AWS από 50 σε 3.500 εντός τριών ημερών. Επρόκειτο δηλαδή για ένα αδύνατο σενάριο επίτευξης, ακόμη και με παροχή τεράστιων κεφαλαίων από την ίδια την επιχείρηση. Το AWS δεν αντιμετώπισε πρόβλημα να ανταπεξέλθει σε αυτή την κορύφωση της ζήτησης και κάλυψε επαρκώς τις ανάγκες της επιχείρησης (The Economist, 2008).

[40] Khajeh-Hosseini A., Greenwood D. and Sommerville I., (2010 a), Cloud Migration: A Case Study of Migrating an Enterprise IT System to IaaS, 3rd IEEE International conference on Cloud Computing, Cloud 2010, 5-10 July, Miami, USA.

του κεφαλαίου να καθυστερεί ή να δυσχεραίνεται από τους client υπολογιστές[41]. Παράλληλα, η εταιρεία πρέπει να αντιμετωπίσει και το κόστος της ενέργειας την οποία χρησιμοποιεί. Η δομή του Cloud είναι εξόχως επιβοηθητική για το οικονομικό τμήμα μιας επιχείρησης, καθώς μειώνει το διοικητικό φόρτο εργασίας. Η μεταβίβαση σε τρίτους όλων αυτών των διοικητικής φύσεως διαδικασιών, παρέχει λύσεις με νέα μοντέλα κοστολόγησης, τα οποία βοηθούν στη διαχείριση των εσόδων από πελάτες, από πωλήσεις και από το μάρκετινγκ.

Οι ερευνητές κατέληξαν στο συμπέρασμα ότι το Cloud Computing είναι μια αποδιοργανωτική διαδικασία, της οποίας σκοπός είναι να αλλάξει ο τρόπος λειτουργίας των πληροφοριακών συστημάτων σε μία επιχείρηση. Περαιτέρω, ιδιαίτερη έμφαση δίνεται στην ανάπτυξη των πληροφοριακών συστημάτων εντός μιας εταιρείας, επειδή αυτά είναι φτηνά, απλά στη χρήση και χαρακτηρίζονται από δυνατότητες επεκτασιμότητας. Το Cloud Computing μπορεί να είναι σημαντικά φθηνότερο συγκριτικά με την αγορά και συντήρηση ενός εσωτερικού κέντρου επεξεργασίας πληροφοριών, καθώς εξαλείφει πλήρως την ανάγκη υποστήριξης αυτού, αφού ουσιαστικά δεν υπάρχει κάποια φυσικής μορφής δομή για να συντηρηθεί.

Σε πολλές επιχειρήσεις, ένα εκτιμώμενο ως χαμηλό διοικητικό κόστος, μπορεί να είναι αρκετά υψηλό, όταν τα τμήματα της επιχείρησης είναι διάσπαρτα σε ένα κτίριο, συχνά δε πολύ υψηλότερο από τη διατήρηση και συντήρηση του μηχανικού εξοπλισμού που συμβάλει στη διοίκηση. Με τη συμβολή του Cloud Computing οι επιχειρήσεις μπορούν να υποσκελίσουν το διοικητικό κόστος με τρεις τρόπους. Πρώτον, η δομή του συστήματος, η οποία αποτελείται από το μηχανικό εξοπλισμό και τη συντήρησή του, την αναβάθμισή του, αλλά και τις συνεχείς αναβαθμίσεις λογισμικού αναλαμβάνονται από το Cloud. Δεύτερον, αφού η εταιρεία έχει κατασταλάξει στο πρωτόκολλο διαδικασιών για backup, το Cloud διασφαλίζει τη συνεχή διεκπεραίωση και διαχείρισή του. Τέλος, η εγκατάσταση μιας λογισμικής εφαρμογής λαμβάνει χώρα μια φορά και γίνεται διαθέσιμη σε όλους τους χρήστες[42]. Είναι σημαντικό,

[41] Με τον όρο client υπολογιστές εννοούνται οι περιφερειακοί υπολογιστές.

[42] Βέβαια, η διαχείριση της εφαρμογής, λ.χ. η υποστήριξή της, οι αναβαθμίσεις της ή η διαχείρισή της από τους χρήστες, δε συμπεριλαμβάνεται κατά τη μεταφορά στο Cloud, με αποτέλεσμα να μην είναι ο καθοριστικός λόγος για να κάνει χρήση του Cloud Computing μια επιχείρηση, αλλά αποτελεί έναν, έστω και ελάσσονος σημασίας, λόγο.

επομένως, να γίνει αντιληπτό ότι αυτά που θεωρούνται χαμηλά διοικητικά κόστη, μπορούν πριν τη μεταφορά τους σε λειτουργίες Cloud να είναι αρκετά υψηλότερα από το κόστος χρήσης του Cloud[43].

Στα συμβατικά συστήματα, η χρήση των πόρων είναι γενικά χαμηλή. Εκτιμάται ότι κυμαίνεται στο 15-20% για τα κέντρα πληροφοριών, ενώ άλλοι εκτιμούν ότι είναι ακόμη χαμηλότερη[44]. Υπάρχουν πολλοί λόγοι που είναι χαμηλή η χρήση των πόρων, καθώς τα στελέχη συνήθως επενδύουν στην απόκτηση πόρων, προκειμένου να αντιμετωπίσουν τις περιόδους υψηλής ζήτησης αυτών. Αυτό, βέβαια, συνεπάγεται ότι, πέραν αυτών των περιόδων, οι υπολογιστικοί πόροι παραμένουν ανεκμετάλλευτοι. Η συμβολή του Cloud Computing σε αυτό το ζήτημα είναι ότι ουσιαστικά εξομαλύνει την παροχή των πόρων, ανάλογα με τη ζήτηση, δίνοντας τη δυνατότητα στους χρήστες να διατηρούν περίπου το 40% των διαθέσιμων πόρων σε διαρκή χρήση[45].

Ένα άλλο στοιχείο που αξίζει να εξετάσουμε είναι ότι η ισχύς του server είναι ανάλογη του κόστους λειτουργίας του, δεδομένων των απαιτούμεων διαδικασιών ψύξης και κατανάλωσης ενέργειας. Το Cloud Computing μειώνει αυτό το κόστος μέσω των οικονομιών κλίμακας, καθώς διαχειρίζεται καλύτερα τις ανάγκες σε ενέργεια, σε διαδικασίες ψύξης και σε κόστος κιλοβατώρας. Αυτό προκύπτει από μία καλύτερη διαχείριση των ανωτέρω παραγόντων κόστους, δεδομένου ότι είναι από τους κυριότερους πόρους μιας εταιρείας παροχής υπηρεσιών Cloud. Στα δεδομένα αυτά προστίθεται και το γεγονός ότι οι πάροχοι Cloud Computing επιλέγουν να εγκατασταθούν σε περιοχές με χαμηλές αντικειμενικές αξίες, με αποτέλεσμα ακόμη μεγαλύτερη μείωση των λειτουργικών εξόδων.

Με λίγα λόγια τα τρία κύρια κόστη μίας επιχείρησης που επηρεάζονται από το Cloud Computing είναι τα ακόλουθα: α) η διοίκηση του συστήματος, καθώς η γενική διάθεση οικονομικών και ανθρώπινων πόρων για τη διαχείριση και συντήρηση ενός κέντρου πληροφοριών εντός της επιχείρησης πολλές φορές κοστίζει περισσότερο από την καταβολή αντιτίμου για τις υπηρεσίες Νέφους, β) η ιδανική χρήση υπολογιστικών πόρων χωρίς σπατάλη αυτών επιτυγχάνεται ευχερέστερα μέσω του Cloud και γ) οι

[43] Rosenthal A., Mork P., Li M.H., Stanford J., Koester D. and Reynolds P., (2010), Cloud Computing: A New Business Paradigm for Biomedical Information Sharing, Journal of Biomedical Informatics, Vol. 43, Issue 2, April, p.p. 342–353.

[44] Evdemon J., Liptaak C., (2007), Internet Scale Computing: MSDN Blog, Oct 17, 2007, διαθέσιμο στο: http://blogs.msdn.com/jevdemon/archive/2007/10/24/internetscale-computing.aspx

[45] Βλ. ό.π. Rosenthal A., Mork P., Li M.H., Stanford J., Koester D. and Reynolds P., p.p. 342–353.

υπηρεσίες του Cloud Computing καταφέρνουν μέσω των οικονομιών κλίμακας να μειώσουν τις απαιτήσεις σε ενέργεια και άρα το συνολικό κόστος για τη διαχείριση πληροφοριών.

2.2. Τρόποι, πρακτικές και αποτελέσματα χρήσης τεχνολογιών Cloud Computing

Τα τελευταία χρόνια, με τη χρήση του Cloud Computing και ανάλογα με τους τρόπους και τις πρακτικές που αυτό χρησιμοποιείται ανά περίπτωση, έχουν προκύψει αρκετά οφέλη τόσο αναφορικά με την ασφάλεια των επιχειρήσεων, όσο και την ασφάλεια των ιδιωτών-πελατών. Κάποια από αυτά έχουν άμεσες συνέπειες και αποτελέσματα, ενώ άλλα εμφανίζονται σε βάθος χρόνου. Οι πάροχοι υπηρεσιών Cloud ωφελούν ιδιαιτέρως τους ιδιώτες και τις μικρο-μεσαίες επιχειρήσεις και καλύπτουν τις αδυναμίες σε περιορισμένους ή ανύπαρκτους πόρους και προϋπολογισμούς. Μερικά σημεία με βάση τις πρακτικές και τα αποτελέσματα που απορρέουν από τη χρήση των τεχνολογιών Cloud Computing περιγράφονται παρακάτω[46]:

1. Κεντρική διαχείριση δεδομένων:

Μία τακτική που συνηθίζεται στο Cloud Computing είναι η κεντρική διαχείριση δεδομένων με αποτέλεσμα να υπάρχει μειωμένη διαρροή πληροφοριών και καλύτερος έλεγχος. Η μειωμένη διαρροή είναι το πιο πολυσυζητημένο και δημοφιλές όφελος του Cloud Computing και ειδικά για τις επιχειρήσεις. Πολλές εξ' αυτών αποθηκεύουν τα δεδομένα τους σε δίσκους ή σε φορητούς υπολογιστές, αλλά αυτό δεν εξασφαλίζει την ασφάλεια των δεδομένων. Είναι πιο ασφαλές να μεταφέρεις δεδομένα σε προσωρινές συσκευές αποθήκευσης ή σε φορητές συσκευές από ότι να μεταφέρεις από φορητό σε φορητό υπολογιστή. Επίσης, δεν δύνανται όλες οι μικρές επιχειρήσεις να χρησιμοποιούν τεχνικές κρυπτογράφησης, με αποτέλεσμα η ασφάλεια των δεδομένων να μπορεί να εξασφαλιστεί μόνο από την τεχνολογία του Cloud Computing. Όσον αφορά στον καλύτερο έλεγχο, είναι ευκολότερο να ελέγχεις και να παρακολουθείς τα δεδομένα, όταν αυτά βρίσκονται συγκεντρωμένα.

Παρόλα αυτά, η άλλη όψη του νομίσματος είναι ότι η κεντρική διαχείριση των δεδομένων είναι εξίσου ριψοκίνδυνη, αν λάβει χώρα μια κλοπή, οπότε θα χαθούν όλα. Ωστόσο, και πάλι είναι προτιμότερη, δεδομένου ότι είναι προτιμότερο να ξοδέψεις χρόνο να σχεδιάσεις την ασφάλεια για ένα

[46] Balding C., (2008), Assessing the Security Benefits of Cloud Computing, July 21, 2008, διαθέσιμο στο: http://cloudsecurity.org/blog/2008/07/21/assessing-the-security-benefits-of-cloud-computing.html

κεντρικό μέρος αποθήκευσης, παρά για να βρεις τρόπο να εξασφαλίσεις την ασφάλεια σε όλα τα μέρη που οι εταιρίες διατηρούν τα αρχεία τους.

2. Αντιμετώπιση περιστατικών παραβίασης ασφάλειας

Από τη χρήση του IaaS είναι πιθανό να ανατεθεί σε έναν ξεχωριστό διακομιστή του Νέφους η ευθύνη της αντιμετώπισης περιστατικών "διάρρηξης" και να βρίσκεται σε κατάσταση offline, έτοιμος για χρήση ανά πάσα στιγμή. Ο χρήστης πληρώνει μόνο για τις υπηρεσίες αποθήκευσης και αν συμβεί κάποιο περιστατικό παραβίασης, τότε τον θέτει σε λειτουργία online από το διαδικτυακό περιβάλλον του παρόχου, χωρίς να μεσολαβήσει κάποιος τρίτος για να το θέσει σε λειτουργία.

Ο χρόνος απόκτησης στοιχείων λόγω παραβίασης της ασφαλείας μειώνεται δραστικά, όταν η επιχείρηση αποφασίζει να υιοθετήσει το Cloud Computing. Για παράδειγμα, αν διακυβεύεται ένας διακομιστής στο Cloud, τότε δημιουργείται ένα αντίγραφό του και γίνεται διαθέσιμο στο διακομιστή που είναι υπεύθυνος για τον εντοπισμό της παραβίασης, ώστε ο μεν πρώτος να συνεχίσει να είναι διαθέσιμος στο χρήστη, το δε αντίγραφό του να ελέγχεται παράλληλα για τη διαρροή του.

Το Cloud Computing, επομένως, ωφελεί από την άποψη ότι μειώνει, αν όχι εξαλείφει, τους νεκρούς χρόνους. Όπως προαναφέρθηκε, το εικονικό αντίγραφο του hardware που παρέχουν οι υπηρεσίες του Cloud λειτουργεί σαν μέσο προκειμένου να μην τεθεί όλο το σύστημα της επιχείρησης offline για έλεγχο. Επομένως, με λίγα λόγια, το εικονικό αντίγραφο του hardware απομακρύνει το εμπόδιο για να γίνει έλεγχος για διαρροές.

3. Έλεγχος αξιοπιστίας κωδικού (cracking)

Οι επιχειρήσεις συχνά τεστάρουν την ισχύ ενός κωδικού κάνοντας χρήση προγραμμάτων που λειτουργούν για αυτόν ακριβώς το σκοπό, γεγονός το οποίο συνίσταται σε μια εξαιρετικά χρονοβόρα διαδικασία. Παρόλα αυτά, ο χρόνος ελέγχου της αξιοπιστίας του κωδικού μειώνεται δραστικά με τη χρήση του Cloud Computing, καθώς οι πάροχοι των υπηρεσιών Νέφους προβαίνουν σε αυτήν την ενέργεια αυτοβούλως. Ένα επιπλέον όφελος χρήσης του Νέφους είναι ότι οι διαδικασίες cracking απασχολούν εξειδικευμένες μηχανές ή λογισμικά. Συνήθως, οι επιχειρήσεις χρησιμοποιούν λογιστικά cracking διανεμημένα σε πολλές μηχανές, όταν αυτές δεν λειτουργούν, για να μειώσουν το φορτίο

εργασίας, ενώ με τις υπηρεσίες Νέφους η εργασία αυτή μεταβιβάζεται σε ξεχωριστές μηχανές, με αποτέλεσμα να είναι προφανή τα ωφέλη που προκύπτουν.

4. Καταγραφή αρχείων

Το Cloud Computing παρέχει ένα ακόμη όφελος στις επιχειρήσεις με τη μορφή της απεριόριστης αποθήκευσης αρχείων. Με τη συμβολή αυτής της λειτουργίας του Νέφους, οι επιχειρήσεις μπορούν να αξιοποιήσουν τις υπολογιστικές υπηρεσίες για να αναζητήσουν οποιοδήποτε από αυτά τα αρχεία σε πραγματικό χρόνο και να πετύχουν τα καλύτερα και γρηγορότερα δυνατά αποτελέσματα.

5. Βελτίωση της κατάστασης των λογισμικών ασφαλείας – δοκιμές ασφαλείας

Το Cloud Computing οδηγεί τους παρόχους στην κατασκευή πιο αποδοτικών λογισμικών ασφαλείας. Επιπλέον, οι επιχειρήσεις προτιμούν να δοκιμάζουν τις αλλαγές στις δομές ασφαλείας κάνοντας χρήση του Νέφους: δημιουργούν ένα αντίγραφο του παραγωγικού περιβάλλοντός τους, εφαρμόζουν τις αλλαγές στην ασφάλεια και τεστάρουν τις επιδράσεις με χαμηλό κόστος και σε ελάχιστο χρόνο. Αυτό απομακρύνει το κύριο πρόσκομμα της δοκιμής διαφορετικών συστημάτων ασφαλείας σε παραγωγικά περιβάλλοντα, ενώ επιπλέον το Cloud Computing παρέχει χαμηλό κόστος δοκιμών ασφαλείας.

Εν κατακλείδι, οι τεχνολογίες Cloud Computing, ιδίως στις επιχειρήσεις, έχουν επικρατήσει τόσο για τεχνολογικούς, όσο και για οικονομικούς λόγους. Όσον αφορά στην πρώτη κατηγορία, κατ' αρχάς η ψευδαίσθηση της ύπαρξης άπειρων υπολογιστικών πόρων διαθέσιμων σε πρώτη ζήτηση, με αποτέλεσμα να εξαλείφεται η ανάγκη στους χρήστες του Cloud Computing να σχεδιάζουν μία μελλοντική τροφοδότηση είναι ο πλέον καθοριστικός παράγοντας. Δευτερευόντως, σημαντικό ρόλο παίζει και η κατάργηση της εκ των προτέρων δέσμευσης από τους χρήστες Cloud, επιτρέποντας έτσι στις εταιρείες να αυξάνουν τους πόρους του hardware, μόνο όταν υπάρχει αύξηση στις ανάγκες τους. Τέλος, οι διάφορες επιχειρήσεις υπολογίζουν ιδιαιτέρως στη δυνατότητα πληρωμής για τη χρήση των υπολογιστικών πόρων σε βραχυπρόθεσμη βάση (π.χ. επεξεργαστές με την ώρα και αποθήκευση με την ημέρα), απελευθερώνοντας κατ' αυτόν τον τρόπο τις μηχανές και την αποθήκευση, όταν πλέον δεν τις χρειάζονται.

Όσον αφορά στους οικονομικούς λόγους, πρόκειται πρωτίστως για τη διαπίστωση που εξετάσαμε και σε προηγούμενη παράγραφο, σύμφωνα με την οποία, η γενική διάθεση οικονομικών και ανθρώπινων πόρων για τη συντήρηση και τη διαχείριση ενός κέντρου πληροφοριών εντός της επιχείρησης πολλές φορές κοστίζει περισσότερο από την καταβολή ενός αντίτιμου για τις υπηρεσίες Νέφους. Επιπλέον, η χρήση των υπολογιστικών πόρων γίνεται ορθότερα με τη χρήση του Cloud Computing, χωρίς να γίνεται σπατάλη αυτών, ενώ τέλος, οι υπηρεσίες Νέφους καταφέρνουν μέσα από τις οικονομίες κλίμακας να μειώσουν τις απαιτήσεις σε ενέργεια, άρα και το συνολικό κόστος, για τη διαχείριση των πληροφοριών.

2.3. Περιγραφή των κινδύνων του Cloud Computing και τρόπων αποτροπής αυτών

Είναι δεδομένο ότι πέρα από από τα πολυάριθμα οφέλη της χρήσης των υπηρεσιών του Cloud Computing, υπάρχει πλήθος κινδύνων από τη χρήση αυτού. Οι κίνδυνοι αυτοί διακρίνονται στην πλειονότητα τους σε δύο μεγάλες κατηγορίες: στην έλλειψη ελέγχου επί των δεδομένων και στην ανεπάρκεια πληροφοριών σχετικά με την ίδια την επεξεργασία (έλλειψη διαφάνειας).

Πάντα επί παραδείγματι, ελλοχεύει ο κίνδυνος της πρόσβασης τρίτων οντοτήτων σε κρίσιμες πληροφορίες με αποτέλεσμα να υπάρχει μη εξουσιοδοτημένη αποκάλυψη πληροφοριών προς βλάβη των συμφερόντων της εκάστοτε εταιρείας ή οργανισμού που χρησιμοποιεί το Cloud σύστημα για τις πληροφορίες και τις εφαρμογές της. Εκτός από την ασφάλεια των δεδομένων τους, οι χρήστες θα πρέπει επίσης να ανησυχούν και για τα δεδομένα που συλλέγει ο πάροχος, αλλά και για τον τρόπο στον οποίο αυτός κατεφεύγει για να προστατεύει τα συγκεκριμένα αυτά δεδομένα. Επιπλέον, θα πρέπει να ανησυχούν για τα στοιχεία των πελατών, για το ποια metadata έχει ο πάροχος για τα δεδομένα του, πώς τα έχει ασφαλισμένα, και τι πρόσβαση έχουμε εμείς σαν πελάτες σε αυτά τα metadata. Όσο αυξάνεται ο όγκος των δεδομένων που μοιραζόμαστε με έναν πάροχο, τόσο αυξάνεται και η αξία αυτών των metadata.

Επιπλέον, ο πάροχός μας συλλέγει και πρέπει να προστατεύει ένα τεράστιο όγκο από security-related δεδομένα. Για παράδειγμα, σε επίπεδο δικτύου, ο φορέας θα πρέπει να συλλέγει, να παρακολουθεί και να προστατεύει το firewall, το σύστημα αποτροπής εισβολών (IPS), περιστατικά ασφάλειας και διαχειριστικά instances (SIEM), καθώς και τα δεδομένα ροής του router. Στο επίπεδο του host, ο πάροχος θα πρέπει να συλλέγει αρχεία καταγραφής του συστήματος και σε επίπεδο εφαρμογής SaaS παρόχων θα πρέπει να συλλέγει το σχετικό αρχείο των δεδομένων των εφαρμογών, συμπεριλαμβανομένων των πληροφοριών πιστοποίησης και εξουσιοδότησης.

Όταν πρόκειται για την προστασία του απορρήτου των δεδομένων που αποθηκεύονται σε ένα δημόσιο Cloud, υπάρχουν δύο πιθανές ανησυχίες[47]. Πρώτον, το είδος του ελέγχου προστασίας που υπάρχει στην πρόσβαση των δεδομένων. Ο έλεγχος πρόσβασης χωρίζεται σε δύο βήματα, στην

[47] Catteddu D. and Hogben G., (2009), Cloud Computing: benefits, risks and recommendations for information security. Technical Report. European Network and Information Security Agency, pp 3-125.

ταυτότητα και την αδειοδότηση. Οι πάροχοι υπηρεσιών Cloud χρησιμοποιούν συνήθως ανεπαρκείς μηχανισμούς πιστοποίησης (π.χ. username και password) και οι έλεγχοι άδειας (access) που διατίθενται στους χρήστες τείνουν να είναι αρκετά «χοντροκομμένοι» για μεγάλους οργανισμούς, με αποτέλεσμα αυτή η «χοντροκομμένη» έγκριση να παρουσιάζει σημαντικά μειονεκτήματα ως προς την προσωπική ασφάλεια. Συχνά, τα μόνα επίπεδα εξουσιοδότησης που παρέχουν οι cloud πάροχοι είναι η άδεια διαχειριστή (δλδ. ο ίδιος ο ιδιοκτήτης του λογαριασμού) και η άδεια χρήστη (δλδ. όλοι οι υπόλοιποι εξουσιοδοτημένοι χρήστες), χωρίς επίπεδα στο ενδιάμεσο (π.χ. διαχειριστές επιχειρησιακών μονάδων να εγκρίνουν την πρόσβαση για το ποιοι είναι εξουσιοδοτημένοι για πρόσβαση από το προσωπικό).

Η δεύτερη πιθανή ανησυχία είναι πώς τα δεδομένα που είναι αποθηκευμένα στο Cloud προστατεύονται στην πραγματικότητα. Για την προστασία των δεδομένων που είναι αποθηκευμένα στο Cloud περιλαμβάνεται η χρήση κρυπτογράφησης. Είναι όμως τα στοιχεία του πελάτη πραγματικά κρυπτογραφημένα όταν αποθηκεύονται στο Cloud? Και αν ναι, με ποιό αλγόριθμο κρυπτογράφησης, καθώς και με τι κλειδί? Η απάντηση στα ανωτέρω ερωτήματα εξαρτάται, και συγκεκριμένα εξαρτάται από το ποιοι CSP χρησιμοποιούνται[48].

Περαιτέρω, εάν ένας CSP κρυπτογραφεί τα δεδομένα ενός πελάτη, ο επόμενος προβληματισμός μας είναι ποιόν αλγόριθμο κρυπτογράφησης χρησιμοποιεί. Δεν είναι όλοι οι αλγόριθμοι κρυπτογράφησης ίδιοι. Κρυπτογραφικά, πολλοί αλγόριθμοι παρέχουν επαρκή ασφάλεια. Ωστόσο, μόνο αλγόριθμοι που έχουν ελεγχθεί από έναν επίσημο πρότυπο οργανισμό (π.χ. NIST) ή που τουλάχιστον είναι γνωστοί ανεπίσημα από την κρυπτογραφική κοινότητα θα πρέπει να χρησιμοποιούνται[49]. Επιπλέον, εδώ μιλάμε για συμμετρικούς αλγόριθμους κρυπτογράφησης, καθώς μόνο η συμμετρική κρυπτογράφηση[50] έχει την ταχύτητα και την υπολογιστική αποδοτικότητα για να χειριστεί την κρυπτογράφηση μεγάλου όγκου δεδομένων. Η συμμετρική κρυπτογράφηση περιλαμβάνει τη χρήση ενός ενιαίου μυστικού κλειδιού, τόσο για την κρυπτογράφηση, όσο και για την αποκρυπτογράφηση των δεδομένων.

[48] Για παράδειγμα, η Mozy Enterprise της EMC κάνει κρυπτογράφηση των δεδομένων του πελάτη. Ωστόσο, η AWS δεν κρυπτογραφεί τα δεδομένα των πελατών. Οι πελάτες έχουν τη δυνατότητα να κρυπτογραφήσουν τα δεδομένα τους μόνοι τους πριν από το ανέβασμα στο Cloud, αλλά το S3 δεν παρέχει κρυπτογράφηση.

[49] Θα πρέπει οπωσδήποτε να αποφεύγεται οποιοσδήποτε αλγόριθμος είναι ιδιόκτητος.

[50] Θα ήταν εξαιρετικά ασυνήθιστο να χρησιμοποιήσουμε έναν ασύμετρο αλγόριθμο για κρυπτογράφηση.

Η επόμενή μας ανησυχία είναι το μήκος του κλειδιού που χρησιμοποιείται. Με συμμετρική κρυπτογράφηση, όσο μεγαλύτερο είναι το κλειδί (π.χ. ο μεγαλύτερος αριθμός των bits του κλειδιού), τόσο ισχυρότερη είναι η κρυπτογράφηση. Αν και μεγάλα σε μήκος κλειδιά παρέχουν μεγαλύτερη προστασία, είναι επίσης και πιο υπολογιστικά ευαίσθητα, και επομένως μπορούν να καταπονήσουν τις δυνατότητες των επεξεργαστών των ηλεκτρονικών υπολογιστών. Αυτό που μπορούμε να πούμε με βεβαιότητα είναι πως το μήκος του κλειδιού θα πρέπει να είναι τουλάχιστον 112 bits για το Triple DES (Data Encryption Standard) και 128 bits για το AES (Advanced Encryption Standard) και τα δύο με έγκριση από το NIST.

Ένα επόμενο ζήτημα εμπιστευτικότητας αναφορικά με την κρυπτογράφηση είναι η διαχείριση των κλειδιών. Πώς είναι τα κλειδιά που χρησιμοποιούνται, πώς θα αντιμετωπιστούν και από ποιόν; Μπορούμε εμείς να διαχειριστούμε τα δικά μας κλειδιά; Η απάντηση είναι ναι. Δεν συνίσταται να αναθέσουμε σε έναν πάροχο να διαχειριστεί τα δικά μας κλειδιά, τουλάχιστον όχι τον ίδιο πάροχο που διαχειρίζεται τα δεδομένα μας. Αυτό σημαίνει επιπλέον πόρους, επιπλέον δυνατότητες, αλλά και δεξιότητες που είναι απαραίτητες, καθώς η σωστή διαχείριση κλειδιών είναι ένα εξαιρετικά δύσκολο και πολυσύνθετο έργο[51]. Και αφού η διαχείριση των κλειδιών είναι μία εξαιρετικά δύσκολη και πολυσύνθετη υπόθεση για έναν πελάτη, είναι ακόμη πιο δύσκολη και σύνθετη για τους CSP όταν καλούνται να προσπαθήσουν να διαχειριστούν σωστά τα κλειδιά των πελατών τους[52].

Εκτός όμως από την εμπιστευτικότητα των δεδομένων μας, θα πρέπει επίσης να ανησυχούμε και για την ακεραιότητα των δεδομένων μας. Τα δεδομένα μπορεί μεν να κρυπτογραφούνται για λόγους εμπιστευτικότητας, και όμως μπορεί να μην υπάρχει ένας τρόπος που να επαληθεύει την ακεραιότητά τους[53]. Η κρυπτογράφηση μπορεί από μόνη της να είναι επαρκής για τη διατήρηση της εμπιστευτικότητας, αλλά για την εξασφάλιση της ακεραιότητας απαιτείται επίσης η χρήση του μηνύματος κωδικού ταυτότητας (MAC). Ο απλούστερος τρόπος για να χρησιμοποιήσουμε τις MAC για κρυπτογραφημένα δεδομένα είναι να χρησιμοποιήσουμε έναν block συμμετρικό αλγόριθμο (σε

[51] Ο πελάτης θα πρέπει τουλάχιστον να συμβουλεύεται και τα τρία μέρη του NIST 800-57, “Recommendation for Key Management”.

[52] Για παράδειγμα, είναι σύνηθες για έναν πάροχο να κρυπτογραφεί όλα τα δεδομένα ενός πελάτη με ένα μόνο κλειδί. Ακόμα χειρότερα, είναι πιθανό ένας πάροχος Cloud αποθήκευσης να χρησιμοποιεί ένα μόνο κλειδί κρυπτογράφησης για όλους τους πελάτες του.

[53] ό.π. Catteddu D. and Hogben G., (2009), Cloud Computing: benefits, risks and recommendations for information security.

αντίθεση με έναν streaming συμμετρικό αλγόριθμο) σε block chaining (CBC) θέση λειτουργίας και να περιλάβουμε μια one-way hash συνάρτηση[54].

Είναι αυτονόητο ότι οι ανωτέρω διαδικασίες δεν είναι εύχρηστες για άτομα που δεν είναι εξοικειωμένα με την κρυπτογράφηση και αυτός είναι ένας λόγος που η αποτελεσματική διαχείριση των κλειδιών είναι δύσκολη. Οι πελάτες θα πρέπει, λοιπόν, αναγκαστικά να ζητάνε βοήθεια από τους παρόχους τους για ζητήματα που αφορούν στην αποτελεσματική διαχείριση των κλειδιών. Αυτό είναι σημαντικό, όχι μόνο για την ακεραιότητα των δεδομένων του πελάτη, αλλά και για την παροχή πληροφοριών σχετικά με το πόσο περίπλοκο είναι το πρόγραμμα ασφαλείας του παρόχου[55].

Πολύ σημαντική είναι και μια άλλη πτυχή της ακεραιότητας των δεδομένων που αφορά στην αποθήκευση μεγάλου όγκου δεδομένων χρησιμοποιώντας IaaS. Μόλις ένας πελάτης έχει αρκετά gigabytes ανεβασμένα στο Cloud για αποθήκευση, πώς αυτός μπορεί να διασφαλιστεί ότι ελέγχει την ακεραιότητα των δεδομένων του που είναι αποθηκευμένα εκεί; Υπάρχουν έξοδα μεταβίβασης στο IaaS που συνδέονται με τη μετακίνηση των δεδομένων προς και πίσω από το Cloud. Αυτό που θέλει πραγματικά να κάνει ο πελάτης είναι να επαληθεύσει την ακεραιότητα των δεδομένων του, ενώ τα δεδομένα παραμένουν στο Cloud χωρίς να έχουνε κατέβει ή ανέβει.

Η εργασία αυτή καθίσταται ακόμα πιο δύσκολη, γιατί πρέπει να γίνει στο Cloud με τη ρητή γνώση ολόκληρου του συνόλου των δεδομένων. Οι πελάτες γενικά δεν ξέρουνε σε ποιές φυσικές μηχανές αποθηκεύονται τα δεδομένα τους, ή που βρίσκονται τα συστήματα αυτά. Επιπλέον, όπως είναι γνωστό το σύνολο των δεδομένων είναι δυναμικό και αλλάζει συχνά. Αυτές οι συχνές αλλαγές καθιστούν περιττή την παραδοσιακή αποτελεσματικότητα των τεχνικών ασφάλειας της ακεραιότητας. Αυτό που χρειάζεται, αντιθέτως, είναι μια απόδειξη της ανάκτησης, δηλαδή ένας μαθηματικός τρόπος για να βεβαιωνόμαστε ανά πάσα ώρα και στιγμή για την ακεραιότητα των δεδομένων που είναι αποθηκευμένα δυναμικά στο Cloud.

Υποθέτοντας τώρα ότι τα στοιχεία ενός πελάτη έχουνε διατηρήσει τόσο την εμπιστευτικότητα, όσο και την ακεραιότητά τους, θα πρέπει να ανησυχούμε επιπλέον και για τη διαθεσιμότητα αυτών,

[54] ό.π., Armbrust M., Fox A., Griffith R., Joseph A., Katz R., Konwinski A., Lee G., Patterson D., Rabkin A., Stoica I., and Zaharia M., “Above the Clouds: A Berkeley View of Cloud Computing”.

[55] Αυτό που πρέπει να θυμόμαστε είναι ότι δεν κρυπτογραφούν όλοι οι πάροχοι τα δεδομένα των πελατών τους, ειδικά όταν πρόκειται για PaaS και SaaS υπηρεσίες.

καθώς υπάρχουν τρείς μεγάλες απειλές –καμία από τις οποίες δεν είναι καινούργια στην πληροφορική– αλλά όλες λαμβάνουν χώρα λόγω του αυξημένου κινδύνου που είναι σύμφυτος με τη χρήση των υπηρεσιών του Cloud Computing.

Η πρώτη απειλή που αφορά στη διαθεσιμότητα των δεδομένων που είναι αποθηκευμένα στο Cloud είναι οι network-based επιθέσεις. Η δεύτερη απειλή αφορά στη διαθεσιμότητα του ίδιου του CSP, ενώ η τρίτη απειλή συνίσταται στο ότι οι υποψήφιοι πελάτες του Cloud θα πρέπει να είναι σε θέση να εξακριβώσουν τι είδους υπηρεσίες τους προσφέρει πραγματικά ο πάροχος. Ο αποθηκευτικός χώρος του Cloud δεν σημαίνει ότι τα αποθηκευμένα δεδομένα είναι απαραίτητα και backed up. Κάποιοι πάροχοι Cloud αποθήκευσης έχουν αντίγραφα ασφαλείας των δεδομένων των πελατών, ή προβαίνουν στην ενέργεια αυτή παρέχοντάς την σαν πρόσθετη επί πληρωμή υπηρεσία[56].

Συνοψίζοντας, αξίζει να αναφερθεί ότι και οι τρείς απο αυτές τις εκτιμήσεις (εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα) θα πρέπει να είναι έγκλειστες σε μια συμφωνία επιπέδου υπηρεσιών ενός SLA. Ωστόσο, αυτή τη στιγμή, τα SLAs των CSP είναι εξαιρετικά αδύναμα, στην πραγματικότητα δε, και για πρακτικούς σκοπούς, είναι ουσιαστικά άνευ αξίας. Ακόμη και όταν ένας CSP φαίνεται να έχει τουλάχιστον ένα επαρκή SLA, το πώς στην πραγματικότητα μετριέται το SLA είναι ένα μάλλον προβληματικό ζήτημα.

Ζήτημα, μπορεί επίσης να προκύψει σε περίπτωση υποβολής αιτημάτων για σκοπούς επιβολής του νόμου απευθείας σε παρόχους υπηρεσιών νεφοϋπολογιστικής, αφού οι αρχές επιβολής του νόμου των κρατών μελών της ΕΕ και τρίτων χωρών δύνανται να υποβάλλουν αιτήματα επιβολής του νόμου ζητώντας την κοινοποίηση δεδομένων προσωπικού χαρακτήρα που υφίστανται επεξεργασία εντός του υπολογιστικού νέφους. Ελλοχεύει έτσι ο κίνδυνος κοινοποίησης δεδομένων προσωπικού χαρακτήρα σε (ξένες) αρχές επιβολής του νόμου χωρίς έγκυρη ενωσιακή νομική βάση, με αποτέλεσμα να παραβιάζεται η νομοθεσία της ΕΕ περί προστασίας των δεδομένων[57].

Τέλος, οι πάροχοι υπηρεσιών Cloud είναι πιθανό να μην παρέχουν στον υπεύθυνο της επεξεργασίας τα μέτρα και τα εργαλεία που χρειάζεται για να διαχειρίζεται ευκολότερα τα δεδομένα,

[56] Για παράδειγμα τα δεδομένα που αποθηκεύονται στο Amazon S3, στο Amazon SimpleDB ή στο Amazon Elastic Block Store αποθηκεύονται σε πολλαπλές φυσικές τοποθεσίες ως ένα κανονικό μέρος των υπηρεσιών αυτών και χωρίς επιπλέον χρέωση.

[57] Βλ. την υπ' αριθμ. 05/2012 από 1ης Ιουλίου 2012 Γνώμη της Ομάδας Εργασίας του άρθρου 29 για την προστασία των δεδομένων σχετικά με τη νεφοϋπολογιστική, 01037/12/EL, WP 196, σελ. 7.

ενώ συχνά είναι πιθανό να εκμεταλλεύονται το φυσικό έλεγχο που ασκούν επί δεδομένων που προέρχονται από διαφορετικούς πελάτες με σκοπό τη σύνδεση των δεδομένων προσωπικού χαρακτήρα μεταξύ τους.

Εκτός, όμως, από τους κινδύνους που προκύπτουν και αφορούν στην επιλογή του ίδιου του παρόχου, υπάρχουν και κίνδυνοι που αφορούν στο ίδιο το υπολογιστικό νέφος και χωρίζονται σε δύο κατηγορίες, αφενός στις απειλές και επιθέσεις εντός και αφετέρου σε αυτές εκτός του Cloud συστήματος.

Στην πρώτη κατηγορία, οπωσδήποτε ανήκει το ζήτημα της εξάντλησης των πόρων. Η ανακριβής κατανομή των πόρων χρήσης προκαλεί τη μη διαθεσιμότητα των υπηρεσιών και του ελέγχου πρόσβασης με αποτέλεσμα να υπάρξει ρήξη ασφάλειας στο ηλεκτρονικό σύστημα της εκάστοτε υπηρεσίας ή οργανισμού. Η πιο συχνή επίθεση είναι η κατανεμημένη άρνηση εξυπηρέτησης (DDOS attack) με συνέπεια την παραβίαση της ακεραιότητας και της εμπιστευτικότητας των δεδομένων.

Ένας επιπλέον κίνδυνος που μπορεί να αντιμετωπιστεί εντός του Cloud είναι η αποτυχία της δομής. Ο κίνδυνος που εμφανίζεται από την αποτυχία των μηχανισμών που χωρίζουν την αποθήκευση, τη μνήμη και τη δρομολόγηση μεταξύ των οργανισμών-πελατών της κοινής υποδομής μπορεί να οδηγήσει σε επιθέσεις SQL injection και side channel επιθέσεις[58].

Εξίσου σημαντικός είναι και ο κίνδυνος της παρακολούθησης των δεδομένων κατά τη μεταφορά. Το Cloud Computing είναι ένα σύστημα με κατανεμημένη αρχιτεκτονική που επιτρέπει τη μεταφορά περισσότερων δεδομένων σε σύγκριση με τις παραδοσιακές υποδομές. Για παράδειγμα, τα δεδομένα μεταφέρονται με τέτοιο τρόπο, ώστε να συγχρονίζονται πολλαπλές εικόνες μηχανών και εν συνεχεία, οι εικόνες αυτές διανέμονται σε πολλαπλές φυσικές μηχανές του Cloud και των απομακρυσμένων υπολογιστών-πελατών. Η μη ασφαλής μετάδοση δεδομένων μπορεί να οδηγήσει σε επιθέσεις πλαστογράφησης δεδομένων (spoofing), σε επιθέσεις ενδιάμεσου στο κανάλι (man-in-the-middle) και σε επιθέσεις καταγραφής ανταλλαγής μηνυμάτων (replay).

Συναφώς με τον ανωτέρω, ενυπάρχει και ο κίνδυνος της μη ασφαλούς ή αναποτελεσματικής διαγραφής δεδομένων. Ο κίνδυνος σε αυτήν την περίπτωση είναι πως τα δεδομένα διαγράφονται πλήρως μόνο με την καταστροφή ενός δίσκου, οπότε οποιοσδήποτε κακόβουλος χρήστης μπορεί να

[58] Άλλη επίθεση μπορεί να είναι η κοινωνική μηχανική (social engineering), όπου ο επιτιθέμενος μπορεί να προσποιηθεί τον πελάτη, πλην όμως ο κίνδυνος αυτός είναι μέτριας επικινδυνότητας.

χρησιμοποιήσει τα δεδομένα αυτά[59]. Επιπλέον, γίνεται δεκτό ότι μπορεί να υπάρξει απώλεια των κλειδιών κρυπτογράφησης. Η κακή διαχείριση των κλειδιών έχει ως αποτέλεσμα τη διαρροή πληροφοριών (Data Leakage), επειδή διευκολύνεται η παράκαμψη των κωδικών ασφαλείας του συστήματος και έτσι οι επιτιθέμενοι μπορούν να εισβάλλουν στο σύστημα και να προκαλέσουν ζημιά.

Επιπλέον, σημειώνεται ότι η έκθεση στον κίνδυνο της μηχανής υπηρεσιών δεν είναι άμοιρη συνεπειών. Πιο συγκεκριμένα, πάνω από τους υλικούς πόρους των πελατών βρίσκεται μια μηχανή υπηρεσιών (service engine) που τους διαχειρίζεται. Μία τέτοια μηχανή μπορεί να είναι ο hypervisor και μπορεί να τεθεί σε κίνδυνο, είτε μέσα από hacking εικονικών μηχανών, είτε επηρεάζοντας το runtime περιβάλλον. Αποτέλεσμα αυτών είναι η ανεξέλεγκτη πρόσβαση στα δεδομένα των χρηστών, τα οποία μπορεί να αλλοιωθούν με διαφανή τρόπο και να μειωθούν οι εικονικοί πόροι της εταιρείας, γεγονός που συνεπάγεται αδιαμφισβήτητα την απώλεια της φήμης της εταιρείας και την "άρνηση" παροχής ηλεκτρονικών υπηρεσιών από αυτή.

Στη δεύτερη κατηγορία, δηλαδή, όσον αφορά στις απειλές και επιθέσεις εκτός του Cloud Computing, σημαντικότερος εμφανίζεται ο κίνδυνος της έλλειψης εκπαίδευσης του εταιρικού προσωπικού στον τομέα της ασφάλειας. Είναι λογικό, αν το προσωπικό δεν γνωρίζει να χειρίζεται σωστά τις τεχνολογίες του Cloud Computing, περιστατικά όπως η είσοδος σε μολυσμένες σελίδες ή η κακή διαχείριση πιστοποιητικών ταυτοποίησης, μπορούν να είναι μοιραία για το ηλεκτρονικό σύστημα της εταιρείας δημιουργώντας παράλληλα κινδύνους για την εμπιστευτικότητα και την ακεραιότητα των δεδομένων.

Στην έλλειψη εκπαίδευσης του εταιρικού προσωπικού προστίθεται και η έλλειψη ισχυρής αυθεντικοποίησης του ασύρματου δικτύου. Η συγκεκριμένη αβλεψία μπορεί να προκαλέσει σημαντική ρήξη ασφάλειας, αφού κάποιος μπορεί εκμεταλλευόμενός την να εισβάλλει στο διαδίκτυο εξαπολύοντας επιθέσεις πλαστογράφησης δεδομένων (spoofing), ενδιάμεσου στο κανάλι (man-in-the-middle) και καταγραφής ανταλλαγής μηνυμάτων (replay).

[59] Δημοφιλής κίνδυνος είναι η απώλεια ή η κλοπή αντιγράφου ασφαλείας, αλλά η πιθανότητα να συμβεί κάτι τέτοιο είναι εξαιρετικά χαμηλή, ενώ η επικινδυνότητα μάλλον κατατάσσεται στη μεσσαία βαθμίδα.

2.4. Απαιτήσεις ασφαλείας

Προκειμένου να αποφευχθούν οι κίνδυνοι που ενυπάρχουν από τη χρήση των υπηρεσιών του Cloud Computing και ιδίως προκειμένου να αποφευχθεί η παραβίαση του Cloud συστήματος θα πρέπει οι πάροχοι των Cloud συστημάτων να ανταποκρίνονται σε ένα μίνιμουμ κριτηρίων που οι εκάστοτε επιχειρήσεις – πελάτες ή ακόμα και κυβερνήσεις απαιτούν από τους παρόχους. Πιο συγκεκριμένα, ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) έχει προβεί στην κατάρτιση ενός Πλαισίου Διασφάλισης Πληροφοριών (INFORMATION ASSURANCE FRAMEWORK) το οποίο, κατά βάση, προβλέπει μια σειρά από ερωτήσεις που ένας οργανισμός μπορεί να ζητήσει από τον πάροχο υπηρεσιών Cloud για να διαβεβαιωθεί ότι προστατεύονται επαρκώς οι πληροφορίες που του έχουν ανατεθεί[60].

Οι πελάτες προκειμένου να εξασφαλίσουν ότι οι κίνδυνοι από τη χρήση του Cloud Computing ισοσκελίζονται σε σχέση με τα αποκτώμενα οφέλη πρέπει να διασφαλίσουν ότι έχει τηρηθεί μια σειρά προϋποθέσεων. Ειδικότερα, θα πρέπει να έχουν καταγραφεί ρητά και αδιαμφισβήτητα οι υποχρεώσεις και οι ευθύνες που επιμερίζονται μεταξύ αυτών των ίδιων και των παρόχων, να έχει διασφαλιστεί ότι το προσωπικό είναι αξιόπιστο, σωστά εκπαιδευμένο και ότι αξιολογείται τακτικά αναφορικά με τα καθήκοντα που του έχουν ανατεθεί, να γίνεται έλεγχος σχετικά με τον τρόπο με τον οποίο ο αρχικός πάροχος συμβάλλεται με τρίτους προκειμένου να τον υποβοηθούν σε ορισμένες λειτουργίες και να εξασφαλίζεται ότι ο πάροχος χρησιμοποιεί τους κατάλληλους ελέγχους για τον περιορισμό της παραβίασης της ασφάλειας. Επιπλέον, οι πελάτες θα πρέπει να τσεκάρουν με σχετικές ερωτήσεις τους τα συστήματα διαχείρισης ταυτότητας, εξουσιοδότησης, πιστοποίησης και πρόσβασης των παρόχων, τον τρόπο διαχείρισης των προσωπικών δεδομένων, την ύπαρξη κρυπτογράφησης και τέλος τον τρόπο αποθήκευσης των δεδομένων και τη διαδικασία που απαιτείται για τη μετάφορά τους[61].

Σε κάθε περίπτωση, το μεγάλο διακύβευμα συνίσταται στο ότι ο πάροχος ενδέχεται να παρουσιάσει αδυναμία εκπλήρωσης των υπηρεσιών στις οποίες υποχρεούται, η οποία αδυναμία με τη

[60] Βλ. σχετικώς το Cloud Computing Security Risk Assessment δημοσιευμένο στο διαδικτυακό τόπο: https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment/

[61] Για τις συγκεκριμένες ερωτήσεις που πρέπει να απευθύνονται από τους πελάτες στους παρόχους προκειμένου να διαπιστώνεται το αν αυτοί ανταποκρίνονται στις προσδοκίες τους βλ. ειδικότερα, Cloud Computing, Information Assurance Framework, ENISA, November 2009, σελ. 6-24.

σειρά της, μπορεί να έχει επιπτώσεις στην εμπιστευτικότητα και τη διαθεσιμότητα των πληροφοριών. Παρακάτω παρατίθενται κατηγοριοποιημένες οι βασικές προϋποθέσεις που πρέπει να πληρούνται και που συνίστανται στις εξής :

- **Εμπιστευτικότητα δεδομένων**: Μόνο εξουσιοδοτημένα άτομα πρέπει να έχουν πρόσβαση στις υπηρεσίες και στα αποθηκευμένα δεδομένα.
- **Ακεραιότητα δεδομένων**: Λόγω του γεγονότος ότι ένα Cloud σύστημα αποτελείται από επιμερισμένα συστήματα και υποδομές, οι πάροχοι υπηρεσιών Cloud είναι φυσικό να επεξεργάζονται δεδομένα προσωπικού χαρακτήρα τα οποία προέρχονται από ευρύ φάσμα πηγών, τόσο από πρόσωπα στα οποία αναφέρονται τα δεδομένα όσο και από οργανισμούς, με επακόλουθο την πιθανότητα ύπαρξης αντικρουόμενων συμφερόντων ή/και διαφορετικών στόχων. Για το λόγο αυτό είναι αναγκαία η ύπαρξη δικλείδων ασφαλείας, ώστε να μην υπάρχει τροποποίηση ή αλλοίωση προσωπικών, εταιρικών ή ευαίσθητων δεδομένων.
- **Διαθεσιμότητα δεδομένων**: Στην περίπτωση που ο πάροχος υπηρεσιών Cloud χρησιμοποιεί ιδιόκτητη τεχνολογία, ο πελάτης ενδέχεται να δυσκολευτεί να μεταφέρει τα δεδομένα και τα έγγραφά του από ένα σύστημα σε άλλο (φορητότητα δεδομένων) ή να ανταλλάξει πληροφορίες με οντότητες που χρησιμοποιούν υπηρεσίες Cloud οι οποίες τελούν υπό τη διαχείριση διαφορετικών παρόχων (διαλειτουργικότητα). Απαραίτητη προϋπόθεση, λοιπόν, καθίσταται η διασφάλιση της διαθεσιμότητας των δεδομένων, τα οποία θα πρέπει να προσφέρονται άμα τη αιτήσει ορισμένου χρήστη.
- **Αυθεντικοποίηση (Access control)**: Η πρόσβαση στα δεδομένα και τις εφαρμογές του Cloud Computing προϋποθέτει την εξασφάλιση της απόδειξης της ταυτότητας ενός ατόμου, ενέργεια που επιτυγχάνεται με τη χρήση πρωτοκόλλων κρυπτογράφησης.
- **Εξουσιοδότηση**: Πέρα όμως από την αυθεντικοποίηση, απαραίτητη κρίνεται και η εξουσιοδότηση, ώστε να παρέχονται δικαιώματα πρόσβασης σε τρίτους, βασισμένα πάντοτε στην εκάστοτε πολιτική ασφάλειας του συστήματος.
- **Εφαρμογή κρυπτογράφησης των πληροφοριών:** Η εφαρμογή κρυπτογραφικών μοντέλων δεν απαιτείται μόνο για τη διαδικασία access control, αλλά και για τη μεταφορά και την αποθήκευση των επιθυμούμενων πληροφοριών στο Cloud.
- **Χρήση του τοίχους προστασίας (Firewall)**

- **Δημιουργία αντιγράφων ασφάλειας (Back up)**: Για να λειτουργήσει αποτελεσματικά το Cloud Computing σύστημα απαιτείται η εξασφάλιση αντιγράφων ασφαλείας για την άμεση ανάκτηση των πληροφοριών σε περίπτωση έκτακτης ανάγκης και την άμεση επαναλειτουργία του συστήματος.
- **Ασφαλής αποθήκευση δεδομένων**: Η αποθήκευση των δεδομένων και οποιωνδήποτε άλλων χρήσιμων και σημαντικών στοιχείων σε μια κρυπτογραφημένη βάση δεδομένων, αποτελεί βασική προϋπόθεση για την όλη λειτουργία του συστήματος.
- **Χρονική ακολουθία ελέγχου δεδομένων (audit trail)**: Οπωσδήποτε, εξίσου σημαντική καθίσταται και η ανάγκη τήρησης αρχείων καταγραφής των εκάστοτε εκτελούμενων δραστηριοτήτων.
- **Σχέδιο αποκατάστασης καταστροφής (Disaster Recovery Plan)**: Σε περιπτώσεις φυσικών καταστροφών, ο διαχειριστής του συστήματος πρέπει να ξεκινήσει τα instances των εικονικών εξυπηρετητών και να χρησιμοποιήσει IP διευθύνσεις για τη μετάβαση των δεδομένων από τον ένα εξυπηρετητή στον άλλον.

ΚΕΦΑΛΑΙΟ 3 – ΠΡΟΫΠΟΘΕΣΕΙΣ ΧΡΗΣΗΣ CLOUD COMPUTING ΠΡΟΣ ΟΦΕΛΟΣ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΤΩΝ ΧΡΗΣΤΩΝ

3.1. Περιγραφή της σημερινής κατάστασης και των προβλημάτων που υπάρχουν σε σχέση με την ιδιωτικότητα των χρηστών Cloud Computing και πιθανοί τρόποι αντιμετώπισης φαινομένων παραβατικότητας

Για την Ευρωπαϊκή Ένωση, η ανάπτυξη του Cloud Computing είναι μέρος των δράσεων της Ψηφιακής Ατζέντας για την Ευρώπη 2010-2020, καθώς θεωρείται ότι η υιοθέτηση των σχετικών εφαρμογών θα αποτελέσει μοχλό ανάπτυξης της ευρωπαϊκής οικονομίας[62]. Έχει γίνει αποδεκτό ότι πλέον σταδιακά οδηγούμαστε «σε ένα παγκόσμιο περιβάλλον διάχυτου υπολογισμού, όπου η επεξεργασία δεδομένων πραγματοποιείται σε υπολογιστές που βρίσκονται οπουδήποτε στον κόσμο, χωρίς ο χρήστης της υπηρεσίας να γνωρίζει τον τόπο αποθήκευσης των δεδομένων»[63].

Ειδικότερα, στις μέρες μας, τόσο οι υπάρχουσες δικτυακές υποδομές, όσο και η ραγδαία εξάπλωση του Διαδικτύου επιτρέπουν αφενός το «ανέβασμα» (upload) και αφετέρου το «κατέβασμα» (download), αλλά και τη συλλογή πληθώρας πληροφοριών με εύκολο και ταχύτατο τρόπο. Ωστόσο, πολλές από αυτές τις άμεσα διαθέσιμες, προς όλους τους διαδικτυακούς χρήστες, πληροφορίες μπορεί να αποτελούν προσωπικά δεδομένα ή διαβαθμισμένο υλικό, γεγονός που σε πολλές περιπτώσεις συγκρούεται με το δικαίωμα της ιδιωτικότητας των υπό κρίση ατόμων[64]. Η παραβίαση της ιδιωτικότητας, από διαδικτυακή πάντα άποψη, μπορεί να λάβει χώρα τόσο με άμεσο όσο με έμμεσο τρόπο[65].

Επιπλέον, η ιδιωτικότητα του χρήστη μπορεί να παραβιάζεται και από τον ίδιο τον τρόπο λειτουργίας του διαδικτύου, καθώς όταν ένας χρήστης συνδέεται σε αυτό, χρησιμοποιεί συγκεκριμένη

---

[62] Towards a European Cloud Strategy στο http://ec.europa.eu/information_society/activities/cloudcomputing/index_en.htm

[63] Γεράρης Χ., Τα προσωπικά δεδομένα και οι νέες προκλήσεις, ΔιΜΕΕ 2010, σελ. 43 επ.

[64] Βλ. σχετικά με τη διακινδύνευση των προσωπικών δεδομένων στο περιβάλλον του Web 2.0 σε Μήτρου Λ., Η ιδιωτικότητα στο web 2.0, ΔιΜΕΕ 2010, σελ. 319 επ.

[65] Για παράδειγμα, οι διαδικτυακοί χρήστες που επιθυμούν να κάνουν μια διαδικτυακή (online) αγορά έχουν εξαρχής λιγότερες επιλογές και περιθώρια για να προστατεύσουν τα προσωπικά τους δεδομένα. Και αυτό γιατί, για να τελεσφορήσει μια τέτοια αγορά απαιτείται η παροχή προσωπικών δεδομένων από την πλευρά των χρηστών, είτε για τη δημιουργία ενός λογαριασμού ή ενός προσωπικού προφίλ, είτε ως «αντάλλαγμα» για την πρόσβαση στην αντίστοιχη υπηρεσία με την οποία ρυθμίζεται η αγορά.

και μοναδική διεύθυνση IP, ενώ ταυτόχρονα κατά τη διαδικτυακή του περιήγηση διατηρούνται cookies. Το σημαντικότερο είναι ότι αυτή η μορφή παραβίασης της ιδιωτικότητας του χρήστη γίνεται πάντα χωρίς τη συναίνεση του χρήστη και σε πολλές περιπτώσεις εν αγνοία του, καθώς πολλοί χρήστες δεν ξέρουν πως λειτουργούν τα υπολογιστικά δίκτυα[66].

Κατά καιρούς, οι διάφοροι χρήστες έχουν αναρωτηθεί πώς είναι δυνατόν κατά τη διαδικτυακή περιήγησή τους, σε διαφορετικές ιστοσελίδες, να εμφανίζονται διαφημίσεις, όπου μάλιστα το προϊόν ή η υπηρεσία που διαφημίζεται είναι στενά συνδεδεμένα με την επαγγελματική τους δραστηριότητα ή τα προσωπικά τους ενδιαφέροντα. Το φαινόμενο αυτό δεν είναι όμως και τόσο παράδοξο. Και αυτό γιατί έχουν επινοηθεί προηγμένες τεχνικές εξόρυξης δεδομένων (data mining) που επιτρέπουν την παραγωγή νέας πληροφορίας, χρήσιμης στους τομείς της έρευνας της αγοράς και των διαφημίσεων[67]. Εν συνεχεία η πληροφορία αυτή αξιολογείται και χρησιμοποιείται στοχευμένα από την εκάστοτε εταιρεία ως διαφημιστική τακτική για την προσέλκυση των υποψήφιων καταναλωτών[68].

Ειδικότερα, όσον αφορά στο περιβάλλον του Cloud Computing, είναι γεγονός ότι το εικονικό αυτό περιβάλλον με τις τόσες ιδιαιτερότητες, θέτει πραγματικά πολλά ερωτήματα σχετικά με την ασφάλεια και την προστασία των προσωπικών δεδομένων των χρηστών, αφού στην ουσία οι χρήστες παραδίδουν σε τρίτους το σύνολο των προσωπικών τους δεδομένων (στα οποία μπορεί να περιλαμβάνονται και τα ευαίσθητα[69]) που μέχρι τώρα κρατούσαν στους υπολογιστές τους[70].

---

[66] Ακόμα, όμως, και αν κάποιος ξέρει πως να περιορίσει τα cookies, δεν μπορεί να εισέλθει στις ιστοσελίδες κορυφαίας ζήτησης, μια εκ των οποίων είναι και αυτή της Google.

[67] Πρακτικές, όπως το λεγόμενο behavioural targeting ή άλλες εξατομικευμένες υπηρεσίες δείχνουν τη χρησιμότητα που έχουν τα ευαίσθητα και μη, προσωπικά δεδομένα στον οικονομικό αντίκτυπο των εταιρειών που τα χρησιμοποιούν. Σε καμία περίπτωση, βέβαια, οι επιχειρήσεις αυτές δεν αναγνωρίζουν τα επίμαχα δεδομένα ως προσωπικά, αλλά ως "εταιρικά", τονίζοντας σε κάθε περίπτωση ότι η συλλογή τους και η επεξεργασία τους γίνεται πάντα προς όφελος του καταναλωτή.

[68] Άξιο λόγου είναι και ένα άλλο κομβικό σημείο το οποίο παρουσιάζει αφενός ενδιαφέρον, αλλά αφετέρου εγκυμονεί και κινδύνους. Αυτό είναι η εξαγορά της εταιρείας Double Click, που είναι η μεγαλύτερη διαφημιστική εταιρεία στον κόσμο από την Google. Επίσης, έχει γίνει ιδιαιτέρως πολύπλοκη η οργάνωση των εταιρειών-φορέων που ασχολούνται με την επεξεργασία των εν λόγω δεδομένων, με τακτικές όπως το outsourcing ή το off-shoring, ενώ ακόμα πιο πολύπλοκες καθίστανται οι σχέσεις μεταξύ αυτών που συλλέγουν, επεξεργάζονται ή χρησιμοποιούν τις προσωπικές πληροφορίες. Τα ανωτέρω ζητήματα φαντάζουν εξαιρετικά πολύπλοκα και γίνονται πιο έντονα, ιδίως στην περίπτωση των πολυεθνικών εταιριών, όπου η επεξεργασία των επίμαχων δεδομένων-πληροφοριών λαμβάνει χώρα σε πολλές και διαφορετικές, ως προς το επίπεδο προστασίας, χώρες.

[69] Ευαίσθητα δεδομένα, είναι ιδίως αυτά που αφορούν π.χ. στην υγεία, σε στοιχεία απογραφής κ.λπ.

[70] Κίτσος Π. και Παππά Π., Η προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής στις υπηρεσίες του υπολογιστικού νέφους. Εννοιολογικά προβλήματα και ρυθμιστικές προσεγγίσεις της Ευρωπαϊκής νομοθεσίας, Εισήγηση στο 4ο διεθνές

Επομένως, τα προσωπικά δεδομένα υπό τη μορφή των πληροφοριών που ενυπάρχουν στο ηλεκτρονικό ταχυδρομείο, στα έγγραφα, τα υπολογιστικά φύλλα, τα βίντεο, τα αρχεία υγείας, τις φωτογραφίες, καθώς επίσης και οι φορολογικές ή άλλες χρηματοοικονομικές πληροφορίες, τα επιχειρηματικά σχέδια, οι παρουσιάσεις PowerPoint, τα λογιστικά στοιχεία, οι διαφημιστικές εκστρατείες, οι πωλήσεις, τα ημερολόγια, τα βιβλία διευθύνσεων, τα οποία αποθηκεύονται τοπικά σε έναν υπολογιστή, με το υπολογιστικό νέφος αποθηκεύονται πια σε ξένους υπολογιστές, σε τεράστια κέντρα δεδομένων (data centers), τα οποία μπορεί να βρίσκονται οπουδήποτε στον κόσμο[71].

Το σύνολο του περιεχομένου της συσκευής αποθήκευσης ενός χρήστη μπορεί να αποθηκευτεί από ένα και μόνο πάροχο, ή από πολλούς παρόχους υπηρεσιών «υπολογιστικού νέφους», πλην όμως συχνά προκύπτουν θέματα σχετικά με το απόρρητο ή την εμπιστευτικότητα και ιδίως ως προς τη δυνατότητα και τις προϋποθέσεις πρόσβασης και χρήσης των δεδομένων από ένα άτομο, μια επιχείρηση, μια κυβερνητική υπηρεσία, ή άλλη οντότητα η οποία δύναται να μοιράζεται τις πληροφορίες στο υπολογιστικό νέφος[72].

Οι εκάστοτε κακόβουλοι χρήστες που θέλουν να παραβιάσουν την ιδιωτικότητα των άλλων χρηστών[73] μπορούν να το κάνουν, είτε θέτοντας σε εφαρμογή κάποια δική τους τακτική, είτε εκμεταλλευόμενοι κάποια "κενά" ασφαλείας που μπορούν να διαπιστωθούν ακόμα και από το λιγότερο

συνέδριο Δικαίου της Πληροφορικής με θέμα: "Values and Freedoms in Modern Information Law and Ethics", Θεσσαλονίκη, 20-21 Μαΐου 2011.

[71] ό.π., Κίτσος Π. και Παππά Π., Η προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής στις υπηρεσίες του υπολογιστικού νέφους. Εννοιολογικά προβλήματα και ρυθμιστικές προσεγγίσεις της Ευρωπαϊκής νομοθεσίας.

[72] Gellman R. «Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing», World Privacy Forum, February 23, 2009 στο http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf βλ. επίσης σχετικά με το ανωτέρω θέμα και Wildstrom S., «Cloud Computing: Understand the Risks», διαθέσιμο στο http://www.businessweek.com/magazine/content/09_14/b4125000676483.htm

[73] Μεγάλη προσβολή της ιδιωτικότητας λαμβάνει χώρα και στις λεγόμενες ιστοσελίδες κοινωνικής δικτύωσης (social media). Την πρωτιά στα μέσα κοινωνικής δικτύωσης, αναφορικά με την παραβίαση των προσωπικών δεδομένων, κατέχει η ιστοσελίδα www.facebook.com. Η ιστοσελίδα αυτή έχει μεγάλη απήχηση σχεδόν σε όλους τους διαδικτυακούς χρήστες και ιδίως στις νεαρές ηλικίες. Μάλιστα, στις περιπτώσεις αυτές, πολλές φορές οι ίδιοι οι χρήστες παραβιάζουν την ίδια τους την ιδιωτικότητα με αναρτήσεις προσωπικών δεδομένων (στοιχεία ταυτότητας, σχέσεις κ.λπ.), καθώς και με αναρτήσεις γεωγραφικής θέσης (check-in) γεγονός που μερικές φορές έχει οδηγήσει ακόμα και στη διάρρηξη της οικίας του διαδικτυακού χρήστη, ο οποίος είχε αναρτήσει ότι βρισκόταν για διακοπές σε γνωστό νησί και έτσι οι κακόβουλοι χρήστες που παρατηρούσαν τη δραστηριότητα του έδρασαν ανενόχλητοι. Επιπλέον, από τις εν λόγω ιστοσελίδες και από κάθε προφίλ που υπάρχει, μπορούμε να αποθηκεύσουμε τοπικά στον υπολογιστή μας τις φωτογραφίες άλλων διαδικτυακών χρηστών. Η λήψη τέτοιων προσωπικών δεδομένων, έχει σκοπό, κατά κύριο λόγο, τη δημιουργία νέων ψεύτικων προφίλ με τα οποία οι κακόβουλοι χρήστες έχουν σκοπό να διασύρουν, να συκοφαντήσουν και να δημιουργήσουν προβλήματα στο πραγματικό πρόσωπο που απεικονίζεται.

καταρτισμένο τεχνικά διαδικτυακό χρήστη. 'Ετσι, από τη μία πλευρά η διακινδύνευση της ιδιωτικότητας στο Cloud οφείλεται στην αποτυχία των μηχανισμών για το διαχωρισμό του αποθηκευτικού χώρου, της μνήμης, της δρομολόγησης, ακόμα και της υπόληψης ανάμεσα στα διάφορα τμήματα της διαμοιραζόμενης υποδομής. Η κεντρικοποιημένη αποθήκευση και η διαμοιραζόμενη κατοχή του αποθηκευτικού χώρου έχει ως συνέπεια οι χρήστες του Cloud να είναι σε μεγαλύτερο κίνδυνο αποκάλυψης των ευαίσθητων δεδομένων που τους αφορούν (π.χ. αρχεία υγείας) σε ανεπιθύμητους χρήστες.

Γενικότερα, όσον αφορά στην παραβατικότητα κατά τη χρήση των υπηρεσιών Cloud Computing, προκειμένου αυτή να αντιμετωπιστεί σε έναν ικανοποιητικό βαθμό, θα πρέπει να ληφθούν εξαρχής υπόψη, κάποιοι αρκετά σημαντικοί παράγοντες. Κατ' αρχάς, είναι ζήτημα ζωτικής σημασίας, προτού μεταφερθούν τα δεδομένα και οι διάφορες εφαρμογές στο Cloud, να ορίσουμε την πολιτική ασφαλείας του συστήματος και να λάβουμε υπόψη το νομοθετικό πλαίσιο που αφορά στην προστασία των προσωπικών και ευαίσθητων δεδομένων. Πρόκειται για μια βασική προϋπόθεση, κατά την οποία πρέπει να καθοριστεί αυστηρά ο τρόπος με τον οποίο θα λειτουργεί ο οργανισμός/εταιρεία και πως θα πρέπει να αντιδράσει σε περίπτωση επίθεσης. Έτσι, λοιπόν, είναι δόκιμο να οριστεί το αν θα πρέπει να διεξάγονται δικαστικές διαδικασίες, έρευνες από τη μεριά της κυβέρνησης, αν θα πρέπει να διακόπτεται η λειτουργία του οργανισμού, καθώς και τι έξοδα αποκατάστασης και απαιτήσεις προκύπτουν από τέτοιες περιπτώσεις.

Επιπλέον, είναι συνετό, πριν τη μεταφορά των δεδομένων και εφαρμογών, να επιλέξουμε τα μοντέλα ανάπτυξης και τα μοντέλα υπηρεσιών που μας βολεύουν καλύτερα και μας δίνουν τη δυνατότητα να ελέγχουμε στο μέγιστο την προστασία των δεδομένων μας. Αν πρόκειται για ένα private cloud, στην περίπτωση αυτή, χρειαζόμαστε τα μοντέλα εκείνα που μας επιτρέπουν να έχουμε αποκλειστικά και μόνο δικά μας δεδομένα αποθηκευμένα στους εξυπηρετητές του Cloud, καθώς αυτά τα μοντέλα μας επιτρέπουν να κάνουμε αποκλειστική χρήση του Cloud. Ακόμη, η επιτυχημένη ασφαλής διαχείριση του Cloud, εξασφαλίζοντας την ιδιωτικότητα των χρηστών, συσχετίζεται άμεσα με τη Διαχείριση Κρυπτογραφικού Κλειδιού (Cryptography Key Management). Η χρήση κρυπτογράφησης απαιτεί τη διαχείριση των κλειδιών κρυπτογραφίας, την προσωποποίηση και το διαμοιρασμό έξυπνων καρτών στους χρήστες[74].

[74] Κατά συνέπεια γεννώνται διάφορα ερωτήματα, όπως ποιος ελέγχει τα κλειδιά κρυπτογραφίας και ποιος διαχειρίζεται τις χαμένες/κλεμμένες κάρτες με την απώλεια των κλειδιών κρυπτογραφίας.

Ανάλογα, βέβαια, με το πόσο ευαίσθητα είναι τα διαχειρίσιμα δεδομένα, θα πρέπει να εξετάσουμε κατά πόσο αυτά είναι ασφαλή στο Cloud. Η στοιχειώδης επιδεικνυόμενη επιμέλεια, μπορεί να περιλαμβάνει ερωτηματολόγια, επιτόπιους ελέγχους, επιβεβαιώσεις ή ακόμα και αναλύσεις εκ μέρους του παρόχου. Ένα ζήτημα εξίσου υψηλής σημασίας για τη διασφάλιση των δεδομένων είναι η επιλογή αυτή καθ' εαυτή του παρόχου. Θα πρέπει να δοθεί αρκετή προσοχή στο εάν ο πάροχος που επιλέγουμε δίνει εγγυήσεις προστασίας, αν μας παρέχει τη δυνατότητα να περιορίσουμε τα δεδομένα μας σε μια συγκεκριμένη γεωγραφική περιοχή και το αν θέλουμε ή όχι να μοιραζόμαστε υπολογιστικούς πόρους με άλλους οργανισμούς, επιχειρήσεις ή και απλούς χρήστες υπηρεσιών Cloud.

Σαφώς, για την προστασία των ευαίσθητων δεδομένων έχουν προταθεί διάφορες μέθοδοι. Μία από αυτές[75] προτείνει για την προστασία του PHR, κρυπτογράφηση δεδομένων με τη βοήθεια του αλγορίθμου AES (Attribute-Based Encryption) και κρυπτογράφηση συνθηματικών με τον αλγόριθμο MD5, όπως επίσης την οργάνωση του PHR σε επίπεδα. Αυτοί είναι δύο κρυπταλγόριθμοι που εξασφαλίζουν υψηλή προστασία δεδομένων και η διαφοροποίηση των δεδομένων σε επίπεδα προσθέτει προστασία σε δεδομένα υψηλής ευαισθησίας. Αντίστοιχα, άλλη μέθοδος προτείνει[76] ένα αρκετά αναλυτικό πλαίσιο ασφάλειας του PHR στηριζόμενο και αυτό σε Attribute-Based Encryption Key, αλλά στο μοντέλο MA-ABE, όπου πάνω από ένας χρήστης θα έχει πρόσβαση στα δεδομένα, ανάλογα με την εξουσιοδότηση που του έχει δοθεί.

Υπάρχουν ερευνητές[77], ωστόσο, που υποστηρίζουν ότι η κρυπτογράφηση των δεδομένων μπορεί να είναι μια πολύ χρήσιμη μέθοδος προστασίας από διάφορες απειλές, μερικές από τις οποίες αναφέραμε προηγουμένως, όμως δεν προστατεύει στο μέγιστο από κακόβουλο λογισμικό και κακοπροαίρετους χρήστες ή ακόμα και από εσωτερικές απειλές. Έτσι, οι ερευνητές αυτοί προτείνουν μια νέα αρχιτεκτονική, την Iris, η οποία εξασφαλίζει διαρκή επιβεβαίωση της ακεραιότητας και της εγκυρότητας των δεδομένων. Πέρα από την αρχιτεκτονική αυτή, η οποία περιλαμβάνει και τμήματα αρχείων MAC (Message Authentication Codes) για την κρυπτογράφηση δεδομένων, προτείνεται η χρήση του HAIL. Το HAIL είναι μια τεχνική που βοηθάει στην ενίσχυση της διαθεσιμότητας των δεδομένων. Οι

[75] Korde P., Panwar V. and Kalse S., Securing Personal Health Records in Cloud using Attribute Based Encryption, International Journal of Engineering and Advanced Technology (IJEAT), Volume 2, Issue 4, April 2013, p.p. 95-97.

[76] Ming Li, Matti Siekkinen, Sasu Tarkoma, Antti Ylä-Jääski and Yong Cui. Segment Level Authentication: Combating Internet Source Spoofing. In the Proceedings of the 15th IEEE Symposium on Computers and Communications (ISCC'10), June 2010.

[77] Bowers K.D., Juels A., Oprea A., (2009), Proofs of retrievability: Theory and implementation, Proceedings of the 2009 ACM workshop on Cloud computing security, p.p. 43-54.

τεχνικές αυτές, όχι μόνο εξασφαλίζουν σε πολύ μεγάλο βαθμό την ακεραιότητα, την εμπιστευτικότητα και τη διαθεσιμότητα των δεδομένων, αλλά προστατεύουν σε εξαιρετικό βαθμό τους πελάτες από εσωτερικές και εξωτερικές απειλές, καθώς και από περιπτώσεις όπου χρησιμοποιούμε κοινόχρηστους και μη έμπιστους υπολογιστικούς πόρους στο Cloud[78].

[78] Πέραν των τεχνικών που αναφέραμε, μπορούμε να εφαρμόσουμε και άλλες τεχνικές προκειμένου να αυξήσουμε την ασφάλεια και να περιορίσουμε όσο το δυνατόν περισσότερο τις απειλές. Τέτοιες τεχνικές μπορεί να είναι η τοποθέτηση firewalls στα σημεία του δικτύου και στα σημεία σύνδεσης με το Cloud, η εφαρμογή συμμετρικών (SKC) ή ασύμμετρων κλειδιών κρυπτογράφησης και τεχνικές που προσθέτουν ασφάλεια σε επίπεδο αυθεντικοποίησης και εξουσιοδότησης, όπως τα μοντέλα MAC (Mandatory Access Control), DAC (Discretionary Access Control) και RBAC (Role based Access Control).

3.2. Σκιαγράφηση του νομικού πλαισίου ως προς την ιδιωτικότητα

Είναι αξιοσημείωτο ότι στο πεδίο της προστασίας των προσωπικών δεδομένων οι πρώτες κανονιστικές αντιδράσεις καταγράφονται σε διεθνές και όχι σε κρατικό επίπεδο[79]. Η ανάγκη προστασίας της ιδιωτικότητας[80] διατυπώνεται ήδη στη Σύμβαση της Ρώμης της 4ης Νοεμβρίου 1950 για την προστασία των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών, ενώ στα πρώτα σχετικά κείμενα κατατάσσεται και η απόφαση 2450/19.12.1968 της Γ.Σ. των Ηνωμένων Εθνών, η οποία αφορά στα προβλήματα που ανακύπτουν σχετικά με τα ανθρώπινα δικαιώματα από την ανάπτυξη της επιστήμης και της τεχνολογίας και ειδικότερα από τη χρήση των ηλεκτρονικών μέσων[81].

Ακολούθως, ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ) εξέδωσε τις «Κατευθυντήριες Αρχές[82] που διέπουν την προστασία της ιδιωτικότητας και τις διασυνοριακές ροές προσωπικών δεδομένων» (1980)[83]. Εν συνεχεία, η Σύμβαση 108/28.01.1981 «για την προστασία των ατόμων από την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα» του Συμβουλίου της Ευρώπης αποτέλεσε το πρώτο διεθνές δεσμευτικό κείμενο, χωρίς όμως να είναι αμέσου εφαρμογής. Σταθμό για την προστασία δεδομένων προσωπικού χαρακτήρα αποτέλεσε η κοινοτική Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 «για την προστασία των

[79] Ήδη, από τα τέλη της δεκαετίας του ΄60 καταγράφεται η ανάγκη νομοθετικής προστασίας της ιδιωτικότητας. Το προβάδισμα της διεθνούς κοινότητας οφείλεται στη διασυνοριακή ροή των προσωπικών πληροφοριών, δηλαδή στην ανταλλαγή και διαβίβαση πληροφοριών από χώρα σε χώρα και την ανάγκη της προστασίας της νόμιμης διασυνοριακής κυκλοφορίας των προσωπικών πληροφοριών.

[80] Η έννοια γένους της ιδιωτικότητας εμπλουτίστηκε σταδιακά με επιμέρους έννοιες, όπως το δικαίωμα στην ιδιωτική ζωή, τον περιορισμό της προσβασιμότητας, την ελαχιστοποίηση των "παρεμβάσεων" (intrusiveness), το δικαίωμα στο απόρρητο, την –υπό στενή έννοια- ιδιωτικότητα (intimacy), την ανωνυμία, την απόσυρση (reserve) κ.ά.

[81] Γέροντα Απ., Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία προσωπικών δεδομένων, εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 2002.

[82] Οι αρχές αυτές περιλαμβάνουν την αρχή της περιορισμένης συγκέντρωσης και συλλογής των δεδομένων (collection limitation principle), την αρχή της ποιότητας των δεδομένων (data quality principle), την αρχή του προσδιορισμένου σκοπού (purpose specification principle), την αρχή της περιορισμένης χρήσης των προσωπικών δεδομένων (use limitation principle), την αρχή μέτρων ασφαλείας των προσωπικών δεδομένων (security safeguards principle), την αρχή της διαφάνειας (openness principle), την αρχή της συμμετοχής του ατόμου (individual participation principle) και τέλος την αρχή της ευθύνης (accountability principle).

[83] Αραβαντινό Β., Η προστασία των στοιχείων προσωπικού χαρακτήρα από την αθέμιτη επεξεργασία τους με ηλεκτρονικό υπολογιστή, εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 1997.

φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών», με την οποία επιδιώχθηκε για πρώτη φορά η εναρμόνιση των ευρωπαϊκών νομοθεσιών σε ένα υψηλό επίπεδο προστασίας[84]. Προσωπικά δεδομένα σύμφωνα με την ανωτέρω Οδηγία «είναι 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 δε 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». Από την άλλη ως επεξεργασία προσωπικών δεδομένων ορίζεται «κάθε εργασία ή σειρά εργασιών που πραγματοποιούνται με ή χωρίς τη βοήθεια αυτοματοποιημένων διαδικασιών και εφαρμόζονται σε δεδομένα προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώρηση, η οργάνωση, η αποθήκευση, η προσαρμογή ή η τροποποίηση, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η ανακοίνωση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η εναρμόνιση ή ο συνδυασμός, καθώς και το κλείδωμα, η διαγραφή ή η καταστροφή».

Τελικώς, το κοινοτικό κανονιστικό πλαίσιο για την προστασία των προσωπικών δεδομένων συμπληρώθηκε με την Οδηγία 97/66/ΕΚ για την προστασία του ατόμου έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα, η οποία στη συνέχεια αντικαταστάθηκε με την Οδηγία 2002/58/ΕΚ για την προστασία δεδομένων προσωπικού χαρακτήρα στον τομέα των ηλεκτρονικών επικοινωνιών, όπως αναθεωρήθηκε με την οδηγία 2009/136/ΕΚ.

Ωστόσο, η βαρύτητα που απέδιδε η Ευρωπαϊκή Ένωση στο ζήτημα της προστασίας προσωπικών δεδομένων αποτυπώθηκε περαιτέρω στη Συνθήκη του Άμστερνταμ (1997), με το άρθρο 286, προβλέποντας, μεταξύ άλλων, την ίδρυση ενός *ανεξάρτητου εποπτικού οργάνου*[85] με αντικείμενο τον έλεγχο της τήρησης των ουσιαστικών ρυθμίσεων, ενώ η ένταξη του δικαιώματος της προστασίας των προσωπικών δεδομένων στο Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης αποδεικνύει περίτρανα τη σημασία που αποδίδεται στην προστασία του θεμελιώδους αυτού δικαιώματος. Σημειώνεται ότι ήδη το δικαίωμα προστασίας των προσωπικών δεδομένων περιλαμβάνεται και στη

[84] Γκρίτζαλη Δ., Γκρίτζαλη Στ., Ηλιάδη Γ., Καμπουράκη Κ., Καρύδα Μ., Κάτσικα Σ., Κιουντούζη Ευ., Κοκολάκη Σπ., Λαμπρινουδάκη Κ., Λέκκα Δ., Μήτρου Λ., Μουλίνο Κ., Μπαλόπουλο Θ. και Τσούμα Β., Ασφάλεια Πληροφοριακών Συστημάτων, εκδόσεις Νέων Τεχνολογιών, Αθήνα 2004, σελ. 455 επ.

[85] Πρόκειται για τον Ευρωπαίο Επόπτη Προστασίας Προσωπικών Δεδομένων, στις αρμοδιότητες του οποίου υπάγεται η διατύπωση γνώμης για την προτεινόμενη ευρωπαϊκή νομοθεσία και ο έλεγχος της τήρησης των κανόνων προστασίας προσωπικών δεδομένων από τα όργανα της Ευρωπαϊκής Ένωσης.

Συνθήκη της Λισαβόνας και συγκεκριμένα στο άρθρο 16 της Συνθήκης για τη Λειτουργία της Ευρωπαϊκής Ένωσης.

Το ελληνικό κανονιστικό πλαίσιο έχει ανταποκριθεί θετικά στο ζήτημα της προστασίας των προσωπικών δεδομένων. Η Ελλάδα δεν άργησε[86] να εφαρμόσει τις πρέπουσες, κατά την Ευρώπη, πολιτικές αναφορικά με την προστασία του δικαιώματος της ιδιωτικότητας και συγκεκριμένα υπήρξε από τις πρώτες χώρες που μετέφεραν την κοινοτική Οδηγία στο εσωτερικό δίκαιο. Στο Σύνταγμα, μετά την αναθεώρηση του 2001, προβλέπεται με το άρθρο 9Α[87] το δικαίωμα προστασίας των προσωπικών δεδομένων[88], ενώ το βασικό ελληνικό νομοθέτημα για την προστασία των προσωπικών δεδομένων είναι ο ν. 2472/1997 (Α' 50) «Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα», ο οποίος τροποποιήθηκε αρκετές φορές με μεταγενέστερα νομοθετήματα[89]. Η δε Αρχή που προβλέπεται στο άρθρο 9Α του Συντάγματος είναι η Ανεξάρτητη Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ). Επιπλέον, τα προσωπικά δεδομένα μπορούμε να υποστηρίξουμε ότι προστατεύονται και από άλλες διάσπαρτες διατάξεις, όπως τα άρθρα 57-59 του Αστικού Κώδικα (Α.Κ.)[90]

[86] Η πρώτη προσπάθεια να νομοθετηθεί το ζήτημα χρονολογείται στο 1985, όμως το αποτέλεσμα δεν ήταν ιδιαιτέρως θετικό.

[87] «Καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, όπως νόμος ορίζει».

[88] Βλ. σχετικά με την αναγκαιότητα πρόβλεψης του δικαιώματος προστασίας των προσωπικών δεδομένων στο αναθεωρημένο Σύνταγμα του 2001 σε Μήτρου Λ., Προστασία Προσωπικών Δεδομένων: ένα νέο δικαίωμα/Τσάτσο Δ., Βενιζέλο Ευ. και Κοντιάδη Ξ. (επιμ.), Το Νέο Σύνταγμα – Πρακτικά συνεδρίου για το αναθεωρημένο Σύνταγμα 1975/1986/2001, Αθήνα – Κομοτηνή, 2001, σελ. 83 επ.

[89] Ο ν. 2472/1997, τροποποιήθηκε με τους ν. 2623/1998 (Α΄ 139), 2703/1999 (Α΄ 72), 2721/1999 (Α΄ 112), 2819/2000 (Α΄ 84), 2915/2001 (Α΄ 109), 3051/2002 (Α΄ 220), 3068/2002 (Α΄ 274), 3090/2002 (Α΄ 329), 3144/2003 (Α΄ 111), 3156/2003 (Α΄ 157), 3471/ 2006 (Α΄ 133), 3625/2007 (Α΄ 290), 3783/2009 (Α΄ 136), 3917/2011 (Α΄ 22), 3994/2011 (Α΄ 165), 4024/2011 (Α΄ 226), 4139/2013 (Α΄ 74) και 4152/2013 (Α΄ 107).

[90] Άρθρο 57: «Όποιος προσβάλλεται παράνομα στην προσωπικότητά του έχει δικαίωμα να απαιτήσει να αρθεί η προσβολή και να μην επαναληφθεί στο μέλλον. Αν η προσβολή αναφέρεται στην προσωπικότητα προσώπου που έχει πεθάνει, το δικαίωμα αυτό έχουν ο σύζυγος, οι κατιόντες, οι ανιόντες, οι αδελφοί και οι κληρονόμοι του από διαθήκη. Αξίωση αποζημίωσης σύμφωνα με τις διατάξεις για τις αδικοπραξίες δεν αποκλείεται».

Άρθρο 58: «Αν σ' αυτόν που δικαιούται να φέρει ένα όνομα αμφισβητείται από άλλον το δικαίωμα αυτό, ή αν κάποιος χρησιμοποιεί παράνομα ορισμένο όνομα, ο δικαιούχος ή εκείνος που βλάπτεται, μπορεί να ζητήσει να αρθεί η προσβολή και να μην επαναληφθεί στο μέλλον. Αξίωση αποζημίωσης σύμφωνα και με τις διατάξεις για τις αδικοπραξίες δεν αποκλείεται».

Άρθρο 59: «Στις περιπτώσεις των δύο προηγούμενων άρθρων το δικαστήριο με την απόφασή του, ύστερα από αίτηση αυτού που έχει προσβληθεί και αφού λάβει υπόψη το είδος της προσβολής, μπορεί επιπλέον να καταδικάσει τον υπαίτιο να

για την προστασία της προσωπικότητας, αλλά και τα άρθρα 370^{A}, 370^{B} και 370^{Γ} του Ποινικού Κώδικα (Π.Κ.)[91].

Το ανωτέρω, βέβαια, νομοθετικό πλαίσιο δεν αφορά συγκεκριμένα στην επεξεργασία των προσωπικών δεδομένων στο Cloud Computing, αλλά στην προστασία των προσωπικών δεδομένων εν

ικανοποιήσει την ηθική βλάβη αυτού που έχει προσβληθεί. Η ικανοποίηση συνίσταται σε πληρωμή χρηματικού ποσού, σε δημοσίευμα, ή σε οτιδήποτε επιβάλλεται από τις περιστάσεις».

[91] Άρθρο 370^{A}: «1. Όποιος αθέμιτα παγιδεύει ή με οποιονδήποτε άλλον τρόπο παρεμβαίνει σε συσκευή, σύνδεση ή δίκτυο παροχής υπηρεσιών τηλεφωνίας ή σε σύστημα υλικού ή λογισμικού, που χρησιμοποιείται για την παροχή τέτοιων υπηρεσιών, με σκοπό ο ίδιος ή άλλος να πληροφορηθεί ή να αποτυπώσει σε υλικό φορέα το περιεχόμενο τηλεφωνικής συνδιάλεξης μεταξύ τρίτων ή τα στοιχεία της θέσης και κίνησης της εν λόγω επικοινωνίας, τιμωρείται με κάθειρξη μέχρι δέκα ετών. Με την ίδια ποινή τιμωρείται η πράξη του προηγούμενου εδαφίου και όταν ο δράστης αποτυπώσει σε υλικό φορέα το περιεχόμενο της τηλεφωνικής επικοινωνίας του με άλλον χωρίς τη ρητή συναίνεση του τελευταίου. 2. Όποιος αθέμιτα παρακολουθεί με ειδικά τεχνικά μέσα ή αποτυπώνει σε υλικό φορέα προφορική συνομιλία μεταξύ τρίτων ή αποτυπώνει σε υλικό φορέα μη δημόσια πράξη άλλου, τιμωρείται με κάθειρξη μέχρι δέκα ετών. Με την ίδια ποινή τιμωρείται η πράξη του προηγούμενου εδαφίου και όταν ο δράστης αποτυπώσει σε υλικό φορέα το περιεχόμενο της συνομιλίας του με άλλον χωρίς τη ρητή συναίνεση του τελευταίου. 3. Με κάθειρξη μέχρι δέκα ετών τιμωρείται όποιος κάνει χρήση της πληροφορίας ή του υλικού φορέα επί του οποίου αυτή έχει αποτυπωθεί με τους τρόπους που προβλέπονται στις παραγράφους 1 και 2 αυτού του άρθρου. 4. Αν ο δράστης των πράξεων των παραγράφων 1, 2 και 3 αυτού του άρθρου είναι πάροχος υπηρεσιών τηλεφωνίας ή νόμιμος εκπρόσωπος αυτού ή μέλος της διοίκησης ή υπεύθυνος διασφάλισης του απορρήτου ή εργαζόμενος ή συνεργάτης του παρόχου ή ενεργεί ιδιωτικές έρευνες ή τελεί τις πράξεις αυτές κατ' επάγγελμα ή κατά συνήθεια ή απέβλεπε στην είσπραξη αμοιβής, επιβάλλεται κάθειρξη μέχρι δέκα ετών και χρηματική ποινή από πενήντα πέντε χιλιάδες (55.000) μέχρι διακόσιες χιλιάδες (200.000) ευρώ. 5. Αν οι πράξεις των παραγράφων 1 και 3 αυτού του άρθρου συνεπάγονται παραβίαση στρατιωτικού ή διπλωματικού απορρήτου ή αφορούν απόρρητο που αναφέρεται στην ασφάλεια του κράτους ή την ασφάλεια εγκαταστάσεων κοινής ωφέλειας, τιμωρούνται κατά τα άρθρα 146 και 147 του Ποινικού Κώδικα».

Άρθρο 370^{B}: «1. Όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτον ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα υπολογιστών, τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα, τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Ως απόρρητα θεωρούνται και εκείνα που ο νόμιμος κάτοχός τους, από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι να λάβουν γνώση τους. 2. Αν ο δράστης είναι στην υπηρεσία του κατόχου των στοιχείων, καθώς και αν το απόρρητο είναι ιδιαίτερα μεγάλης οικονομικής σημασίας, επιβάλλεται φυλάκιση τουλάχιστον ενός έτους. 3. Αν πρόκειται για στρατιωτικό ή διπλωματικό απόρρητο ή για απόρρητο που αναφέρεται στην ασφάλεια του κράτους, η κατά την παράγραφο 1 πράξη τιμωρείται κατά τα άρθρα 146 και 147. 4. Οι πράξεις που προβλέπονται στις παραγράφους 1 και 2 διώκονται ύστερα από έγκληση».

Άρθρο 370^{Γ}: «1. Όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με φυλάκιση μέχρι έξι μήνες και με χρηματική ποινή διακοσίων ενενήντα (290) ΕΥΡΩ έως πέντε χιλιάδων εννιακοσίων (5.900) ΕΥΡΩ. 2. Όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών, εφόσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα, ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφάλειας που είχε λάβει ο νόμιμος κάτοχός τους, τιμωρείται με φυλάκιση μέχρι τρεις μήνες ή με χρηματική ποινή τουλάχιστον είκοσι εννέα (29) ΕΥΡΩ. Αν η πράξη αναφέρεται στις διεθνείς σχέσεις ή στην ασφάλεια του κράτους, τιμωρείται κατά το άρθρο 148. 3. Αν ο δράστης είναι στην υπηρεσία του νόμιμου κατόχου των στοιχείων, η πράξη της προηγούμενης παραγράφου τιμωρείται μόνο αν απαγορεύεται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου ή αρμόδιου υπαλλήλου του. 4. Οι πράξεις των παραγράφων 1 έως 3 διώκονται ύστερα από έγκληση».

γένει, σε οποιοδήποτε περιβάλλον, πραγματικό ή ψηφιακό ενδέχεται να υπάρξει περίπτωση παραβίασής τους από την επεξεργασία τους. Έτσι, επί παραδείγματι, η Οδηγία 95/46/ΕΚ εφαρμόζεται για τις περιπτώσεις προστασίας των προσωπικών δεδομένων στο υπολογιστικό νέφος, δεν εφαρμόζεται, όμως, σε οικιακές δραστηριότητες που γίνονται μέσω υπηρεσιών υπολογιστικού νέφους δηλ. όταν η επεξεργασία δεδομένων προσωπικού χαρακτήρα πραγματοποιείται από φυσικό πρόσωπο στο πλαίσιο αποκλειστικά προσωπικών ή οικιακών δραστηριοτήτων, όπως οι επεξεργασίες οι σχετικές με την αλληλογραφία και την τήρηση καταλόγων διευθύνσεων.

3.3. Νομικές προκλήσεις που αφορούν στο κανονιστικό πλαίσιο για την προστασία των δεδομένων, όπως:

3.3.1. Ο προσδιορισμός του εφαρμοστέου δίκαιου και της δικαιοδοσίας

Πρέπει να γίνει δεκτό ότι ως δίκαιο προστασίας των προσωπικών δεδομένων νοείται το σύνολο των κανόνων, προϋποθέσεων, όρων, εξουσιών και απαγορεύσεων που αφορούν ως επί το πλείστον στην καταγραφή, συλλογή, αξιολόγηση και επεξεργασία προσωπικών δεδομένων, καθώς και οι ρυθμίσεις που αφορούν σε διαδικασίες, θεσμικούς ελέγχους, εγγυήσεις και αντίβαρα των περιορισμών των δικαιωμάτων προστασίας των προσωπικών δεδομένων των προσώπων.

Ειδικότερα, και αναφορικά με τα συστήματα Cloud Computing, όπως αντιλαμβάνεται κανείς, η διαμόρφωση των ιδιαίτερων αναγκών των πελατών, συνεπάγεται και την ανάλογη απαίτηση για διαμόρφωση του ιδιαίτερου τρόπου λειτουργίας των υπηρεσιών του Cloud Computing, πλην όμως, όπως είναι λογικό, κάτι τέτοιο, θα καθίστατο εξαιρετικά περίπλοκο και χρονοβόρο για τους παρόχους των Υπηρεσιών Cloud Computing. Έτσι, αφού ο κάθε πελάτης δεν μπορεί να εξασφαλίσει τους ατομικούς όρους διαπραγμάτευσης με τον πάροχο υπηρεσιών Cloud Computing, θα πρέπει να αρκεστεί στις παρεχόμενες από αυτόν υπηρεσίες, εκτιμώντας, βέβαια, εκ των προτέρων, εάν οι λειτουργίες του Cloud ανταποκρίνονται στις ανάγκες του, κατανοώντας παράλληλα τις διαδικασίες και τους διενεργούμενους ελέγχους του[92].

Τα κριτήρια βάσει των οποίων προσδιορίζεται το εκάστοτε εφαρμοστέο δίκαιο παρατίθενται στο άρθρο 4 της οδηγίας 95/46/ΕΚ, το οποίο αναφέρεται στη νομοθεσία που διέπει τους εγκατεστημένους σε ένα ή περισσότερα σημεία εντός του ΕΟΧ υπεύθυνους της επεξεργασίας, καθώς επίσης και στη νομοθεσία που διέπει τους εγκατεστημένους εκτός του ΕΟΧ υπεύθυνους της επεξεργασίας, οι οποίοι

[92] Αρκετοί μεγάλοι πάροχοι Υπηρεσιών Cloud Computing συμμορφώνονται με πρότυπα και πιστοποιήσεις ως απόδειξη των δυνατοτήτων των Υπηρεσιών Cloud Computing που παρέχουν και οι υποψήφιοι πελάτες θα πρέπει να ζητούν αυτές τις πιστοποιήσεις ως μέσο επαλήθευσης.

όμως χρησιμοποιούν για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα μέσα εγκατεστημένα εντός του ΕΟΧ[93].

Στην πρώτη περίπτωση, το κριτήριο για την εφαρμογή ή όχι της νομοθεσίας της ΕΕ στον υπεύθυνο της επεξεργασίας είναι η τοποθεσία όπου είναι εγκατεστημένος και οι δραστηριότητες που επιτελεί, ενώ κανέναν ρόλο δεν παίζει το μοντέλο παροχής υπηρεσιών νεφοϋπολογιστικής. Στην περίπτωση αυτή, εφαρμόζεται το δίκαιο της χώρας στην οποία είναι εγκατεστημένος ο υπεύθυνος της επεξεργασίας[94] που έχει συνάψει σύμβαση για την παροχή υπηρεσιών Cloud και όχι το δίκαιο της χώρας στην οποία είναι εγκατεστημένοι οι πάροχοι. 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. Εάν, τέλος, κάποιος πελάτης υπηρεσιών Cloud είναι εγκατεστημένος εκτός του ΕΟΧ, αλλά έχει προσλάβει πάροχο υπηρεσιών Cloud εγκατεστημένο εντός του ΕΟΧ, η νομοθεσία περί προστασίας των δεδομένων που διέπει τον πάροχο επεκτείνεται και στον πελάτη[95].

Το ρυθμιστικό βάρος και οι επιταγές της προστασίας της πληροφοριακής ιδιωτικότητας παραμένουν, λοιπόν, αναπόφευκτα, σημαντικά προσανατολισμένες σε εδαφικούς όρους. Αυτό, αναπόφευκτα περιέχει κάποιες εγγενείς δυσκολίες. Ένα πρώτο ζήτημα που τίθεται αφορά στη δυσχέρεια προσδιορισμού και εφαρμογής του δικαίου ή/και των δικαστικών αποφάσεων, καθώς το δίκαιο και οι υποχρεώσεις που επιβάλλει συνδέονται άρρηκτα με την έννοια της εδαφικά προσδιορισμένης επικράτειας. Ποιο ρυθμιστικό πλαίσιο εφαρμόζεται αλήθεια, στην περίπτωση μιας γερμανικής πολυεθνικής εταιρείας, η οποία διεκπεραιώνει τα λογιστικά της στην Ινδία, διατηρεί τη βάση δεδομένων

[93] Η ομάδα εργασίας του άρθρου 29 έχει εξετάσει το ζήτημα αυτό στη γνώμη 8/2010 που έχει εκδώσει για το εφαρμοστέο δίκαιο.

[94] Ο πρώτος και βασικός ρόλος του υπεύθυνου της επεξεργασίας είναι να καθορίζει ποιος είναι υπεύθυνος για τη συμμόρφωση προς τους κανόνες προστασίας των δεδομένων, και με ποιον τρόπο τα πρόσωπα στα οποία αναφέρονται τα δεδομένα μπορούν να ασκήσουν τα δικαιώματά τους στην πράξη, με άλλα λόγια πρόκειται για μία κατανομή αρμοδιοτήτων, Βλ. σχετικώς την υπ' αριθμ. 01/2010 Γνώμη της Ομάδας Εργασίας του άρθρου 29 για την προστασία των δεδομένων σχετικά με τη νεφοϋπολογιστική.

[95] Βλ. ό.π. την υπ' αριθμ. 05/2012 από 1ης Ιουλίου 2012 Γνώμη της Ομάδας Εργασίας του άρθρου 29 για την προστασία των δεδομένων σχετικά με τη νεφοϋπολογιστική, 01037/12/EL, WP 196, σελ. 9.

όλων των εργαζομένων στη Σιγκαπούρη, ενώ ο εξυπηρετητής του ηλεκτρονικού ταχυδρομείου (e-mail server) διατηρείται στο San Francisco[96];

Μία δεύτερη επίπτωση του ρυθμιστικού προσανατολισμού στα γεωγραφικά όρια είναι ακριβώς ότι αγνοούνται οι νέες μορφές δεδομένων και οι νέες μορφές επεξεργασίας τους. Η Ευρωπαϊκή Ένωση επέβαλε αυστηρούς κανόνες ως προς τη διασυνοριακή ροή δεδομένων σε τρίτες χώρες, καθώς η νομιμότητά της εξαρτάται από το εάν η χώρα υποδοχής των προσωπικών δεδομένων (κρίνεται ότι) παρέχει «ικανοποιητικό επίπεδο» προστασίας των δεδομένων αυτών. Η εφαρμογή τους, όμως, εξαρτάται σε μεγάλο βαθμό από το αίσθημα υποχρέωσης συμμόρφωσης που έχουν οι αποδέκτες των ρυθμίσεων, καθώς οι μηχανισμοί επιβολής του δικαίου δοκιμάζονται από την τεχνική ευκολία με την οποία, με ένα mouse-click, μία βάση δεδομένων μπορεί να διαβιβαστεί σε μία τρίτη χώρα.

Ο τόπος τήρησης των δεδομένων είναι ένα πολυσυζητημένο θέμα, με τους υπερασπιστές της προστασίας της ιδιωτικότητας και τις ρυθμιστικές αρχές να διατυπώνουν ανησυχίες σχετικά με τους κινδύνους από τη μεταφορά των δεδομένων σε νέες δικαιοδοσίες, ειδικά όταν οι υποδομές που χρησιμοποιούνται είναι εκτός της Ευρωπαϊκής Ένωσης, αλλά και σχετικά με την αβεβαιότητα ως προς το εφαρμοστέο δίκαιο. Είναι γεγονός ότι έως τώρα, δεν υπάρχουν εμπειρικές αποδείξεις ότι τα δεδομένα είναι ασφαλέστερα σε μια γεωγραφική θέση σε σύγκριση με κάποια άλλη.

Εντούτοις, η οικονομία του Cloud Computing απαιτεί κλίμακα, πράγμα που σημαίνει ότι οι περισσότεροι πελάτες εξυπηρετούνται από γεωγραφικώς διεσπαρμένα κέντρα δεδομένων. Επιπλέον, σημαίνει ότι εκτός εάν ο πελάτης τυχαίνει να δραστηριοποιείται στη δικαιοδοσία όπου βρίσκεται το κέντρο δεδομένων, κατά πάσα πιθανότητα, ο πελάτης θα εξυπηρετείται από κέντρο δεδομένων σε απομακρυσμένη τοποθεσία. Ακόμη και αν ο πελάτης βρίσκεται στην ίδια δικαιοδοσία με το κέντρο δεδομένων, τα δεδομένα του πελάτη πιθανότατα διαβιβάζονται σε άλλους τόπους για λόγους λήψης αντιγράφων ασφαλείας (backup) και αποκατάστασης καταστροφών (disaster recovery), υποστήριξης και για άλλους τεχνικούς και λειτουργικούς λόγους.

[96] Βλ. Λαμπρινουδάκης Κ., Μήτρου Λ., Γκρίτζαλης Στ. και Κάτσικας Σ., Προστασία της Ιδιωτικότητας και Τεχνολογίες Πληροφορικής και Επικοινωνιών, Τεχνικά και Νομικά Θέματα, εκδόσεις Παπασωτηρίου, Αθήνα 2010, σελ. 536 επ. με την εκεί παραπομπή, σύμφωνα με την οποία, το παράδειγμα που μνημονεύεται, παρατίθεται από το Schaar για να υπογραμμίσει την ιδιαίτερη δυσκολία εφαρμογής των αυστηρών κανόνων προστασίας προσωπικών δεδομένων που ισχύουν στη Γερμανία σε πολυεθνικές επιχειρήσεις που δραστηριοποιούνται και σε χώρες με ανύπαρκτη ή ελάσσονος έναντι του ευρωπαϊκού επιπέδου προστασίας των προσωπικών δεδομένων.

Επομένως, είναι λογικό, αυτό που έχει σημασία να είναι όχι η εξασφάλιση ενός συγκεκριμένου τόπου για το κέντρο δεδομένων, αλλά η απαίτηση διαφάνειας, από μέρους των πελατών, σχετικά με τον τόπο αποθήκευσης των βασικών τους δεδομένων, τις σχετικές ροές των δεδομένων και τις δικλείδες ασφαλείας, την ταυτοποίηση των πιθανών περαιτέρω εκτελούντων την επεξεργασία, αλλά και σχετικά με την απόδοση ευθυνών και τη συνεχή τήρηση της τεκμηρίωσης που τηρεί ο πάροχος για τις διαδικασίες επεξεργασίας[97].

[97] Shahab Α. και Παπανικολάου Α., Υπολογιστικό Νέφος (cloud computing): Θέματα σύναψης συμβάσεων και συμμόρφωσης για νομικούς συμβούλους, Δίκαιο Επιχειρήσεων και Εταιρειών 6/2014, σελ. 570-576.

3.3.2. Ο προσδιορισμός της αρμοδιότητας για την προστασία των δεδομένων

Η προστασία και η ασφάλεια των προσωπικών δεδομένων αποτελεί κορυφαίο πεδίο προβληματισμού στον κλάδο του Cloud Computing, καθώς υπάρχουν ανησυχίες για το πώς μπορεί να αντλούνται τα δεδομένα (data mining) των πελατών[98]. Οι πελάτες, επομένως, δικαιολογημένα ανησυχούν για τις πολιτικές προστασίας και ασφάλειας των δεδομένων που εφαρμόζουν οι πάροχοι Cloud Computing.

Συχνά και προκειμένου να διασφαλιστεί η προστασία των δεδομένων, καταρτίζονται λεπτομερείς συμφωνίες[99] ανάμεσα στους πελάτες και τους παρόχους σχετικά με την ανάθεση της επεξεργασίας των δεδομένων (data processing agreement), προκειμένου να διασφαλίζεται η ορθή αντιμετώπιση της προστασίας, της ασφάλειας και της εμπιστευτικότητας των δεδομένων και η τήρηση τόσο των γενικών συμβατικών δικαιωμάτων, όσο και των ειδικών δικαιωμάτων των υποκειμένων, τα δεδομένα των οποίων, κατέχει ο πελάτης ως υπεύθυνος επεξεργασίας, καθώς και για σκοπούς κανονιστικής συμμόρφωσης[100].

Στις ανωτέρω συμφωνίες θα πρέπει να περιέχονται σαφείς όροι αναφορικά με το πώς οι πάροχοι θα χρησιμοποιούν τα δεδομένα των πελατών και να διασφαλίζεται ότι η χρήση των εν λόγω δεδομένων περιορίζεται για το σκοπό της παροχής των υπηρεσιών Cloud Computing στον πελάτη και όχι για άλλους σκοπούς επεξεργασίας, όπως π.χ. για την υποστήριξη των υπηρεσιών του καταναλωτή (διαφήμιση κ.λπ.)[101].

---

[98] Η πιο συχνή περίπτωση άντλησης των δεδομένων των πελατών είναι οι περιπτώσεις παροχής στοχευμένης διαφήμισης.

[99] Εκτός από τις συμφωνίες ανάθεσης της επεξεργασίας των δεδομένων, συνάπτονται και συμφωνίες επιπέδου υπηρεσιών (service level agreements) προκειμένου να καθοριστούν οι προσδοκίες όσον αφορά στις διαδικασίες των υπηρεσιών και τους χρόνους λειτουργίας. Σε αυτές προβλέπονται ακόμη και οικονομικές επιπτώσεις, γεγονός που διασφαλίζει έτι περαιτέρω τους πελάτες αναφορικά με την τήρηση από μέρους του παρόχου της συναφθείσας συμφωνίας.

[100] Βλ. Mantelero A., Cloud computing, trans-border data flows and the European Directive 95/46/EC: applicable law and task distribution, European Journal of Law and Technology, Vol 3, Issue 2, 2012

[101] ό.π., Shahab A. και Παπανικολάου Α., Υπολογιστικό Νέφος (cloud computing): Θέματα σύναψης συμβάσεων και συμμόρφωσης για νομικούς συμβούλους.

3.3.3. Ο προσδιορισμός της ευθύνης για τον έλεγχο και την επεξεργασία των δεδομένων

Όπως είναι γνωστό, ο πελάτης των υπηρεσιών Cloud καθορίζει τον τελικό σκοπό της επεξεργασίας και αποφασίζει ή όχι να αναθέσει την επεξεργασία και την εκχώρηση του συνόλου ή μέρους των δραστηριοτήτων επεξεργασίας σε εξωτερικό τρίτο οργανισμό, ενεργεί, επομένως, ως υπεύθυνος της επεξεργασίας δεδομένων[102]. Επιπλέον, ως υπεύθυνος της επεξεργασίας[103], πρέπει να αποδέχεται την ευθύνη της συμμόρφωσης προς τη νομοθεσία περί προστασίας των δεδομένων, είναι δε υπεύθυνος για όλες τις νομικές υποχρεώσεις που αναφέρονται στην οδηγία 95/46/ΕΚ. Σε κάθε περίπτωση, δύναται να αναθέτει στον πάροχο υπηρεσιών Cloud το καθήκον να επιλέγει τις μεθόδους και τα τεχνικά ή οργανωτικά μέσα που θα χρησιμοποιήσει για να επιτύχει τους σκοπούς του υπευθύνου της επεξεργασίας[104].

Στον αντίποδα του υπευθύνου της επεξεργασίας, έχουμε τον εκτελούντα την επεξεργασία[105], δηλαδή τον πάροχο υπηρεσιών Cloud, ο οποίος παρέχει τα μέσα και την πλατφόρμα, ενεργώντας εξ ονόματος του πελάτη. Είναι σύνηθες φαινόμενο οι εκτελούντες την επεξεργασία να προσλαμβάνουν με υπεργολαβία πρόσθετους (υπό)εκτελούντες την επεξεργασία[106], οι οποίοι αποκτούν με τη σειρά τους πρόσβαση στα δεδομένα προσωπικού χαρακτήρα. Εάν οι εκτελούντες την επεξεργασία αναθέτουν με

---

[102] Σύμφωνα με την Οδηγία 95/46/ΕΚ, ως υπεύθυνος της επεξεργασίας νοείται *«το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή οποιοσδήποτε άλλος φορέας που μόνος ή από κοινού με άλλους καθορίζει τους στόχους και τον τρόπο της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα».*

[103] Είναι, βέβαια, γνωστό ότι μπορεί να υπάρχουν και περιπτώσεις στις οποίες ο πάροχος υπηρεσιών Cloud δύναται να θεωρείται είτε ως υπεύθυνος της επεξεργασίας από κοινού με άλλους είτε ως μόνος υπεύθυνος της επεξεργασίας, αναλόγως των πραγματικών περιστάσεων.

[104] Βλ. ό.π. την υπ' αριθμ. 05/2012 από 1ης Ιουλίου 2012 Γνώμη της Ομάδας Εργασίας του άρθρου 29 για την προστασία των δεδομένων σχετικά με τη νεφοϋπολογιστική, 01037/12/EL, WP 196, σελ. 10.

[105] Σύμφωνα με την Οδηγία 95/46/ΕΚ, ως εκτελών της επεξεργασίας νοείται *«το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή οποιοσδήποτε άλλος φορέας που επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας».*

[106] Κατά την άποψη της ομάδας εργασίας του άρθρου 29, ο εκτελών την επεξεργασία μπορεί να αναθέτει με υπεργολαβία τις δραστηριότητές του, μόνο εφόσον έχει τη συγκατάθεση του υπευθύνου της επεξεργασίας, η οποία δύναται να δίδεται γενικώς κατά την έναρξη της παροχής της υπηρεσίας με τη σαφή υποχρέωση του εκτελούντος την επεξεργασία να ενημερώνει τον υπεύθυνο της επεξεργασίας για τυχόν σκοπούμενες αλλαγές που αφορούν την προσθήκη ή την αντικατάσταση υπεργολάβων, με τον υπεύθυνο δε της επεξεργασίας να διατηρεί πάντοτε τη δυνατότητα να αντιταχθεί στις αλλαγές αυτές ή να τερματίσει τη σύμβαση.

υπεργολαβία υπηρεσίες σε (υπό)εκτελούντες την επεξεργασία, υποχρεούνται να κοινοποιούν τις συναφείς πληροφορίες στον πελάτη, αναφέροντας αναλυτικά το είδος των υπηρεσιών που έχουν ανατεθεί με υπεργολαβία, τα χαρακτηριστικά των τρεχόντων ή δυνητικών υπεργολάβων και τις εγγυήσεις συμμόρφωσης προς την οδηγία 95/46/ΕΚ που παρέχουν οι τελευταίοι στον πάροχο υπηρεσιών Cloud[107].

Οπωσδήποτε πάντως, ο υπεύθυνος επεξεργασίας των δεδομένων που πρόκειται να χρησιμοποιήσει, οφείλει εκ των προτέρων να γνωστοποιήσει αφενός τους σκοπούς του στο υποκείμενο των δεδομένων, είτε κατά τη φάση συλλογής, είτε κατά τη φάση της πρώτης διαβίβασης των δεδομένων που το αφορούν σε τρίτους και αφετέρου τους αποδέκτες των δεδομένων, αλλά και άλλα δικαιώματα του υποκειμένου των δεδομένων. Επισημαίνεται ότι οι υποχρεώσεις συμμόρφωσης προς τους κανόνες προστασίας των δεδομένων και οι ευθύνες σε περίπτωση πιθανής παραβίασής τους πρέπει να κατανέμονται με σαφήνεια, ακόμη και σε περίπλοκα περιβάλλοντα επεξεργασίας δεδομένων, όπως κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα όπου εμπλέκονται διάφοροι υπεύθυνοι της επεξεργασίας, ώστε να αποφεύγεται το ενδεχόμενο υποβάθμισης του επιπέδου προστασίας των δεδομένων προσωπικού χαρακτήρα ή «αρνητικής σύγκρουσης αρμοδιοτήτων» και εμφάνισης κενών που θα είχαν ως αποτέλεσμα τη μη διασφάλιση από κανέναν συμβαλλόμενο ορισμένων υποχρεώσεων ή δικαιωμάτων που απορρέουν από την Οδηγία[108].

Σημαντικό ρόλο, βέβαια, αναφορικά με τον έλεγχο της προστασίας των προσωπικών δεδομένων παίζουν οι διάφορες ανεξάρτητες αρχές, ως δημόσιες αρχές ελέγχου, με πλήρη ανεξαρτησία, επιφορτισμένες με τον έλεγχο και την άσκηση καθηκόντων που αφορούν στον έλεγχο της προστασίας των προσωπικών δεδομένων[109].

---

[107] Βλ. ό.π. την υπ' αριθμ. 05/2012 από 1ης Ιουλίου 2012 Γνώμη της Ομάδας Εργασίας του άρθρου 29 για την προστασία των δεδομένων σχετικά με τη νεφοϋπολογιστική, 01037/12/EL, WP 196, σελ. 12. Φυσικό επακόλουθο είναι ότι όλες οι υποχρεώσεις που ισχύουν για τον πάροχο, πρέπει, να ισχύουν και για τους (υπό)εκτελούντες την επεξεργασία μέσω συμβάσεων μεταξύ του παρόχου και του υπεργολάβου.

[108] Βλ. ό.π. την υπ' αριθμ. 05/2012 από 1ης Ιουλίου 2012 Γνώμη της Ομάδας Εργασίας του άρθρου 29 για την προστασία των δεδομένων σχετικά με τη νεφοϋπολογιστική, 01037/12/EL, WP 196, σελ. 11.

[109] Βλ. ό.π. Γκρίτζαλη Δ., Γκρίτζαλη Στ., Ηλιάδη Γ., Καμπουράκη Κ., Καρύδα Μ., Κάτσικα Σ., Κιουντούζη Ευ., Κοκολάκη Σπ., Λαμπρινουδάκη Κ., Λέκκα Δ., Μήτρου Λ., Μουλίνο Κ., Μπαλόπουλο Θ. και Τσούμα Β., Ασφάλεια Πληροφοριακών Συστημάτων, σελ. 467 επ.

Οι πελάτες υπηρεσιών Cloud είναι πιθανό να μην έχουν περιθώρια διαπραγμάτευσης των συμβατικών όρων χρήσης των παρεχόμενων υπηρεσιών, καθώς οι περισσότερες παρέχονται βάσει τυποποιημένων συμβάσεων. Ο πελάτης είναι, εντούτοις, αυτός που αποφασίζει τελικά να εκχωρήσει ή όχι μέρος ή το σύνολο των διαδικασιών επεξεργασίας σε υπηρεσίες νεφοϋπολογιστικής για συγκεκριμένους σκοπούς, με αποτέλεσμα ο πάροχος υπηρεσιών νεφοϋπολογιστικής να αναλαμβάνει ρόλο εργολάβου έναντι του πελάτη, ο οποίος πρέπει αφενός να διασφαλίζει το απόρρητο και αφετέρου να συμμορφώνεται προς τη νομοθεσία περί προστασίας των δεδομένων. Οι εκτελούντες την επεξεργασία οφείλουν να λαμβάνουν μέτρα ασφαλείας αντίστοιχα με εκείνα που προβλέπονται στη νομοθεσία της ΕΕ, όπως εφαρμόζονται στις δικαιοδοσίες του υπεύθυνου της επεξεργασίας και του εκτελούντος την επεξεργασία. Πρέπει, ακόμη, να στηρίζουν και να συνδράμουν τον υπεύθυνο της επεξεργασίας στο καθήκον της συμμόρφωσής του προς τα (ασκούμενα) δικαιώματα των προσώπων στα οποία αναφέρονται τα δεδομένα[110].

Ομοίως, σε περιπτώσεις ανάθεσης των υπηρεσιών Cloud με υπεργολαβία μέσω μιας συμφωνίας εξωτερικής ανάθεσης, ο πελάτης μπορεί να ασκεί έλεγχο με τη διαπραγμάτευση δικαιωμάτων εξέτασης και ελέγχου, ώστε να διασφαλίζεται η τήρηση της δέουσας τεκμηρίωσης και το σύννομο των διαδικασιών. Είναι πολύ δύσκολο για έναν πάροχο υπηρεσιών Cloud Computing να παραχωρεί τέτοια δικαιώματα, δεδομένου ότι δεν είναι δυνατόν να έχει εκατομμύρια πελάτες να εξετάζουν τα κέντρα δεδομένων του ή τις άλλες λειτουργίες του. Οι άμεσοι έλεγχοι από τους πελάτες δεν θα είχαν μόνο απαγορευτικό κόστος, αλλά θα ήταν και εξαιρετικά διασπαστικοί για τη συνοχή των λειτουργιών, θέτοντας ενδεχομένως σε κίνδυνο τα δεδομένα και τις λειτουργίες άλλων πελατών, των οποίων τα δεδομένα υποβάλλονται σε επεξεργασία στον ίδιο τόπο. Η τήρηση της ασφάλειας είναι ένας βασικός λόγος για τον οποίο οι πάροχοι υπηρεσιών Cloud Computing γενικά αποφεύγουν να παρέχουν στους πελάτες πρόσβαση στα κέντρα δεδομένων[111].

[110] Βλ. ό.π. την υπ' αριθμ. 05/2012 από 1ης Ιουλίου 2012 Γνώμη της Ομάδας Εργασίας του άρθρου 29 για την προστασία των δεδομένων σχετικά με τη νεφοϋπολογιστική, 01037/12/EL, WP 196, σελ. 12.

[111] Οι πάροχοι υπηρεσιών Cloud Computing που προσφέρουν υπηρεσίες σε επιχειρηματικούς πελάτες έχουν αναγνωρίσει αυτό το ζήτημα και παρέχουν συνοπτικά αποτελέσματα ελέγχων από ανεξάρτητους τρίτους φορείς και πιστοποιήσεις, π.χ. την πιστοποίηση ISO 27001, προκειμένου να καλύψουν τις ανάγκες των πελατών. Αυτή η προσέγγιση ικανοποιεί την ανάγκη των πελατών να μπορούν να είναι βέβαιοι ότι ο πάροχος υπηρεσιών Cloud Computing τηρεί υψηλού επιπέδου πρότυπα ασφαλείας, ενώ είναι και λιγότερο διασπαστική για την παροχή των υπηρεσιών Cloud Computing. Βλ. σχετικώς και Trustworthy Computing, Privacy in the Public Cloud: The Office 365 Approach, December 2011.

3.3.4. Διαδικασίες μεταφοράς/επεξεργασίας δεδομένων από/και σε τρίτες χώρες

Η διασυνοριακή ροή δεδομένων προσωπικού χαρακτήρα, δηλαδή η διαβίβαση ή μετάδοση δεδομένων σε άλλες χώρες ενέχει πολλούς κινδύνους για την προστασία των δεδομένων και εν γένει των δικαιωμάτων των προσώπων, καθώς τα δεδομένα διαφεύγουν και αποξενώνονται από το αρχικό νομικό πλαίσιο, υπό τους κανόνες και τον έλεγχο του οποίου έχουν συλλεχθεί και υποστεί επεξεργασία. Από την άλλη πλευρά, η διασυνοριακή ροή δεδομένων[112], αφενός είναι, από τεχνολογικής απόψεως, εξαιρετικά ευχερής, και αφετέρου εξυπηρετεί τις ανάγκες της οικονομίας, της διακρατικής συνεργασίας, αλλά και τα συμφέροντα του ατόμου[113].

Η Ευρωπαϊκή Ένωση εφαρμόζει συγκεκριμένους κανόνες σχετικά με τη διαβίβαση προσωπικών δεδομένων εκτός του Ευρωπαϊκού Οικονομικού Χώρου και της Ελλάδας, αντιστοίχως[114]. Δεδομένου ότι πολλοί μεγάλοι πάροχοι υπηρεσιών Cloud Computing εδρεύουν στις Ηνωμένες Πολιτείες, υπάρχει συχνά ανάγκη για μεταφορά δεδομένων στις Ηνωμένες Πολιτείες, για διάφορους λόγους. Πολλοί αξιόλογοι πάροχοι υπηρεσιών Cloud Computing έχουν λάβει σχετική πιστοποίηση[115], σύμφωνα με την οποία τους

[112] Για την έννοια της διασυνοριακής διαβίβασης δεδομένων μπορούν να λεχθούν πάρα πολλά. Το ποιες περιπτώσεις συνιστούν περιπτώσεις διασυνοριακής διαβίβασης δεδομένων έχει κριθεί και από το Δικαστήριο των Ευρωπαϊκών Κοινοτήτων, το οποίο, μεταξύ άλλων, έκρινε ότι η ανάρτηση δεδομένων σε ιστοσελίδα, στην οποία υπάρχει δυνατότητα πρόσβασης από οπουδήποτε δεν συνιστά καθεαυτή διασυνοριακή διαβίβαση. Η ως άνω κρίση, δεν είναι βέβαιο ότι συνιστά μία στέρεη νομική θέση ή μία πραγματιστική λύση, καθώς στην αντίθετη περίπτωση θα οδηγούμασταν στο άτοπο να υπάρχει υποχρέωση εφαρμογής των κανόνων για τη διασυνοριακή ροή σε κάθε δημοσιοποίηση δεδομένων στο Διαδίκτυο.

[113] Βλ. ό.π. Γκρίτζαλη Δ., Γκρίτζαλη Στ., Ηλιάδη Γ., Καμπουράκη Κ., Καρύδα Μ., Κάτσικα Σ., Κιουντούζη Ευ., Κοκολάκη Σπ., Λαμπρινουδάκη Κ., Λέκκα Δ., Μήτρου Λ., Μουλίνο Κ., Μπαλόπουλο Θ. και Τσούμα Β., Ασφάλεια Πληροφοριακών Συστημάτων, σελ. 484 επ.

[114] Απεναντίας, η διασυνοριακή διαβίβαση δεδομένων εντός της Ευρωπαϊκής Ένωσης, λόγω της μεταφοράς της Οδηγίας 95/46/ΕΚ οδηγεί μοιραία στο συμπέρασμα, ότι όλες οι χώρες της Ευρωπαϊκής Ένωσης εξασφαλίζουν ισοδύναμο επίπεδο προστασίας και κατά συνέπεια η διαβίβαση δεν υπόκειται σε κανένα περιορισμό ή διαδικασία.

[115] Η πιστοποίηση αφορά στο καθεστώς «ασφαλούς λιμένα Η.Π.Α. – Ε.Ε.» (Safe Harbor Framework).

επιτρέπεται να μεταφέρουν δεδομένα στις Ηνωμένες Πολιτείες, σύμφωνα όμως με τους κανόνες της Ευρωπαϊκής Ένωσης[116].

Επιπλέον, οι πάροχοι που εστιάζουν το ενδιαφέρον τους στην ικανοποίηση των αναγκών των επιχειρηματικών πελατών τους για την προστασία των δεδομένων τους, ενδέχεται να παρέχουν και τις τυποποιημένες συμβατικές ρήτρες της Ευρωπαϊκής Ένωσης (EU Standard Contractual Clauses)[117]. Οι τυποποιημένες συμβατικές ρήτρες της Ευρωπαϊκής Ένωσης, που δημοσιεύονται από την Ευρωπαϊκή Επιτροπή είναι ένας στέρεος και νομικά έγκυρος τρόπος για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα εκτός του ΕΟΧ, με τρόπο που προσφέρει ικανοποιητικό επίπεδο προστασίας[118].

Τα άρθρα 25 και 26 της Οδηγίας 95/46/ΕΚ προβλέπουν την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα σε χώρες εκτός του ΕΟΧ μόνο εάν οι χώρες αυτές ή ο αποδέκτης παρέχουν επαρκές επίπεδο προστασίας των δεδομένων[119]. Σε αντίθετη περίπτωση, ο υπεύθυνος και οι συνυπεύθυνοι της επεξεργασίας ή/και οι εκτελούντες την επεξεργασία πρέπει να προβλέπουν ειδικές εγγυήσεις[120]. Οι διαπιστώσεις επαρκούς προστασίας των δεδομένων έχουν περιορισμένο γεωγραφικό πεδίο εφαρμογής, με αποτέλεσμα να μην καλύπτουν όλες τις διαδικασίες διαβίβασης εντός του υπολογιστικού νέφους. Σύμφωνα με τη νομοθεσία της ΕΕ, η διαβίβαση δεδομένων σε οργανισμούς των Η.Π.Α. που εφαρμόζουν τις αρχές είναι σύννομη εφόσον οι οργανισμοί-αποδέκτες θεωρείται ότι

[116] Οι πελάτες επιβάλλεται να ελέγχουν την κατάσταση της σχετικής πιστοποίησης των παρόχων στο σχετικό μητρώο που υπάρχει στον ιστότοπο του Υπουργείου Εμπορίου των Η.Π.Α. (US Department of Commerce), βλ. https://safeharbor.export.gov/list.aspx

[117] Βλ. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EL:PDF, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp161_el.pdf

[118] Πρόσφατα ενεκρίθησαν, επί παραδείγματι, τροποποιήσεις της Microsoft, στην τυποποιημένη σύμβαση επεξεργασίας δεδομένων που προτείνει σε ευρωπαϊκές επιχειρήσεις/πελάτες της για υπηρεσίες Cloud Computing για τη διασυνοριακή διαβίβαση δεδομένων κρίνοντάς τις ως συμβατές με τις προαναφερόμενες τυποποιημένες συμβατικές ρήτρες.

[119] Η επάρκεια της προστασίας που παρέχεται από τρίτη χώρα σταθμίζεται ανάλογα λαμβανομένων υπόψη όλων των περιστάσεων που επηρεάζουν μια διαβίβαση ή κατηγορία διαβιβάσεων δεδομένων. Ειδικότερα, εξετάζονται η φύση των δεδομένων, οι σκοποί και η διάρκεια των προβλεπομένων επεξεργασιών, η χώρα προέλευσης και τελικού προορισμού, οι γενικοί ή τομεακοί κανόνες δικαίου, οι επαγγελματικοί κανόνες και τα μέτρα ασφαλείας που ισχύουν στην εν λόγω τρίτη χώρα.

[120] Η ομάδα εργασίας του άρθρου 29 έχει εγκρίνει, ωστόσο, γνώμη στην οποία διατυπώνει την άποψη ότι εξαιρέσεις θα πρέπει να ισχύουν μόνο σε περίπτωση που οι διαδικασίες διαβίβασης δεν είναι ούτε επαναλαμβανόμενες, ούτε μαζικές ούτε διαρθρωτικές.

παρέχουν επαρκές επίπεδο προστασίας στα διαβιβασθέντα δεδομένα[121]. Οι διάφορες, βέβαια, εθνικές νομοθεσίες και αρμόδιες αρχές προστασίας δεδομένων δύνανται να προβλέπουν πρόσθετες απαιτήσεις.

Οι τυποποιημένες συμβατικές ρήτρες[122] που έχει θεσπίσει η Ευρωπαϊκή Επιτροπή για το 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 Cloud 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[123].

Όταν ο πάροχος υπηρεσιών νεφοϋπολογιστικής που ενεργεί ως εκτελών την επεξεργασία είναι εγκατεστημένος στην ΕΕ, η κατάσταση περιπλέκεται ακόμη περισσότερο, καθώς οι τυποποιημένες ρήτρες ισχύουν γενικώς μόνο σε περίπτωση διαβίβασης δεδομένων από υπεύθυνο της επεξεργασίας εγκατεστημένο στην ΕΕ σε εκτελούντα την επεξεργασία εγκατεστημένο εκτός ΕΕ (βλ. αιτιολογική σκέψη 23 της απόφασης 2010/87/ΕΕ της Επιτροπής σχετικά με τις τυποποιημένες ρήτρες και έγγραφο WP 176).

Είναι, επομένως, κάτι παραπάνω από δεδομένο ότι οι πελάτες πρέπει γενικά να ασκούν πιέσεις στους παρόχους των υπηρεσιών Cloud Computing, ώστε να επιτυγχάνεται σαφήνεια σχετικά με τους νομικούς μηχανισμούς που χρησιμοποιούν οι τελευταίοι για τη διαβίβαση δεδομένων εκτός Ευρώπης και ως εκ τούτου και εκτός Ελλάδος, ώστε να διασφαλίζεται η συμμόρφωση με τους αντίστοιχους ελληνικούς και κοινοτικούς κανόνες. Ιδίως δε, είναι πολύ σημαντική η ενσωμάτωση στο πλαίσιο της σύμβασης των τυποποιημένων συμβατικών ρητρών της Ευρωπαϊκής Ένωσης, καθώς αποτελεί έναν ασφαλή τρόπο για την παροχή πρόσθετης διασφάλισης ότι τα δεδομένα μπορούν να μεταφέρονται νομίμως στο Cloud.

---

[121] Βλ. ό.π. την υπ' αριθμ. 05/2012 από 1ης Ιουλίου 2012 Γνώμη της Ομάδας Εργασίας του άρθρου 29 για την προστασία των δεδομένων σχετικά με τη νεφοϋπολογιστική, 01037/12/EL, WP 196, σελ. 23.

[122] Εκτός από τις τυποποιημένες συμβατικές ρήτρες, η Ομάδα Εργασίας εκτιμά ότι οι πάροχοι υπηρεσιών Cloud θα μπορούσαν να προτείνουν στους πελάτες τους διατάξεις βάσει των πραγματικών εμπειριών τους, εφόσον βεβαίως οι τελευταίες δεν αντιβαίνουν, άμεσα ή έμμεσα, στις τυποποιημένες συμβατικές ρήτρες που έχει εγκρίνει η Επιτροπή ή δεν θίγουν τα θεμελιώδη δικαιώματα ή τις θεμελιώδεις ελευθερίες των προσώπων στα οποία αναφέρονται τα δεδομένα.

[123] Βλ. ό.π. την υπ' αριθμ. 05/2012 από 1ης Ιουλίου 2012 Γνώμη της Ομάδας Εργασίας του άρθρου 29 για την προστασία των δεδομένων σχετικά με τη νεφοϋπολογιστική, 01037/12/EL, WP 196, σελ. 25.

Η ελληνική έννομη τάξη, μεταφέροντας τις αντίστοιχες ρυθμίσεις της Οδηγίας 95/46/ΕΚ, επιτρέπει τη διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες, η οποία επιτρέπεται εφόσον εξασφαλίζεται ικανοποιητικό επίπεδο προστασίας, ενώ προβλέπονται και παρεκκλίσεις από τη ρύθμιση αυτή[124], η δε διαπίστωση της εξασφάλισης ενός ικανοποιητικού επιπέδου προστασίας προέρχεται από την Αρχή Προστασίας Δεδομένων Προστασίας Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), η οποία εκδίδει τη σχετική άδεια[125].

Η διαβίβαση δεδομένων προσωπικού χαρακτήρα προς χώρα που δεν εξασφαλίζει ικανοποιητικό επίπεδο προστασίας, επιτρέπεται, κατ' εξαίρεση, με άδεια της Αρχής, εφόσον υπάρχει συγκατάθεση του υποκειμένου των δεδομένων, εκτός αν η συγκατάθεση έχει αποσπασθεί με τρόπο που να αντίκειται στο νόμο ή τα χρηστά ήθη. Σε περίπτωση που δεν υπάρχει συγκατάθεση, η διαβίβαση κρίνεται νόμιμη, εφόσον είναι απαραίτητη για τη διασφάλιση ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή για τη συνομολόγηση και την εκτέλεση σύμβασης μεταξύ αυτού και του υπεύθυνου επεξεργασίας ή μεταξύ του υπεύθυνου επεξεργασίας και τρίτου προς το συμφέρον του υποκειμένου των δεδομένων. Τα ανωτέρω ισχύουν και στην περίπτωση, όπου η διαβίβαση είναι αναγκαία για την αναγνώριση, άσκηση ή υπεράσπιση δικαιώματος ενώπιον του δικαστηρίου. Τέλος, η αντιμετώπιση εξαιρετικής ανάγκης, η διαφύλαξη υπέρτερου δημόσιου συμφέροντος, ιδίως για την εκτέλεση συμβάσεων συνεργασίας με δημόσιες αρχές άλλης χώρας, συνιστά έναν άλλο λόγο για να επιτραπεί η διαβίβαση, εφόσον ο υπεύθυνος επεξεργασίας παρέχει επαρκείς εγγυήσεις για την προστασία της ιδιωτικής ζωής και των θεμελιωδών ελευθεριών και την άσκηση των σχετικών δικαιωμάτων.

Με βάση τα προεκτεθέντα, πρέπει να αναγνωριστεί ότι η ραγδαία ανάπτυξη της τεχνολογίας και το πλήθος των κινδύνων που αυτή συνεπάγεται, ιδίως αναφορικά με την προστασία του ατόμου δεν είναι δυνατόν, όπως θα ήταν αναμενόμενο, να αντιμετωπίζονται με τον ίδιο τρόπο από τις διάφορες έννομες τάξεις. Η κανονιστική αντιμετώπιση, όπως και η επιλογή της μη αντιμετώπισης ή της αντιμετώπισης με προϋφιστάμενα δικαιικά εργαλεία αντικατοπτρίζουν τις διαφορετικές προσεγγίσεις

[124] Βλ. σχετικά Γιαννόπουλο Γ., Προστασία προσωπικών δεδομένων και διασυνοριακή ροή πληροφοριών. Το πρόβλημα του «ικανοποιητικού επιπέδου προστασίας», ΔτΑ 2001, σελ. 733 επ.

[125] Κατά τη διαδικασία αυτή λαμβάνονται υπόψη ιδίως η φύση των δεδομένων, ο σκοπός και η διάρκεια της επεξεργασίας, οι σχετικοί και ειδικοί κανόνες δικαίου, οι κώδικες δεοντολογίας, τα μέτρα ασφαλείας για την προστασία δεδομένων προσωπικού χαρακτήρα, καθώς και το επίπεδο προστασίας των χωρών προέλευσης, διέλευσης και τελικού προορισμού των δεδομένων.

της πληροφοριακής ιδιωτικότητας και τη θέση αυτής στην εκάστοτε κλίμακα συνταγματικών αξιών και δημόσιων αγαθών.

Η προστασία της ιδιωτικότητας διαμέσου του διαδικτύου ποικίλλει ανάλογα με το νομικό πολιτισμό μιας χώρας, τις κυρίαρχες αντιλήψεις για τη σχέση ιδιωτικής – δημόσιας σφαίρας, το γενικότερο πολιτικο – οικονομικό υπόβαθρο, αλλά και την επιδίωξη των μερικότερων δικαιωμάτων και συμφερόντων που καλούνται να εκπληρωθούν σε κάθε δικαιικό σύστημα. Επιπλέον, σε κάθε έννομη τάξη το επίπεδο προστασίας της ιδιωτικότητας εξαρτάται από το ρυθμό ανάπτυξης της τεχνολογίας, την αλλαγή των αντιλήψεων του κοινωνικού συνόλου και των θεσμών αναφορικά με το εν λόγω φαινόμενο, αλλά και τις εν γένει κοινωνικές αντιλήψεις του ατόμου σχετικά με την ανάγκη προστασίας του και τα μέσα που απαιτούνται για το σκοπό αυτό.

Αν και ο αριθμός των νομοθετημάτων αυξάνεται, η προστασία των προσωπικών δεδομένων παραμένει μάλλον η εξαίρεση στο διεθνές περιβάλλον, καθώς ουσιαστικά εκτός Ευρώπης, λίγες μόνο χώρες έχουν εισαγάγει δεσμευτικούς κανόνες προστασίας των προσωπικών δεδομένων. Όσον αφορά στις χώρες που διαθέτουν πλαίσιο προστασίας των προσωπικών δεδομένων, τα κανονιστικά μοντέλα θα μπορούσαν σχηματικά να διαχωριστούν σε δύο μείζονες κατηγορίες: α) σε εκείνες που προάγουν μία ολιστική ρύθμιση όλων των τομέων κρατικής και ιδιωτικής δραστηριότητας και β) σε εκείνες που επιλέγουν ή/και αρκούνται σε ρύθμιση ορισμένων τομέων και πεδίων κρατικής και ιδιωτικής δραστηριότητας επενδύοντας, κυρίως ή ταυτόχρονα, στη λύση της αυτορρύθμισης, δηλ. της διατύπωσης και εφαρμογής κανόνων δεοντολογίας και συμπεριφοράς χωρίς την κρατική παρέμβαση –συμμετοχή. Η ίδια η εξέλιξη της ηλεκτρονικής επεξεργασίας και του Διαδικτύου συνοδεύεται από τη συζήτηση για την αυτορρύθμιση ως μία εναλλακτική λύση, πιο ευέλικτη και πιο προσαρμοσμένη στις ανάγκες των «δικτυακών» επικοινωνιών και συναλλαγών[126].

Στην Ευρώπη, ήδη από τη δεκαετία του 1970, εμφαίνονται οι βασικές διαφορές ανάμεσα αφενός στα σκανδιναβικά κράτη και αφετέρου στη Γερμανία και τη Γαλλία. Η Γαλλία και οι διάφορες σκανδιναβικές χώρες εισήγαγαν συστήματα αδειοδότησης, ως μορφής προληπτικού ελέγχου της επεξεργασίας των προσωπικών δεδομένων και προαπαιτούμενο όρο της νομιμότητας της επεξεργασίας αυτής, ενώ στις χώρες αυτές η ανεξάρτητη αρχή έχει πέρα από τον ελεγκτικό της ρόλο και το ρόλο της

[126] Βλ. ό.π. Λαμπρινουδάκη Κ., Μήτρου Λ., Γκρίτζαλη Στ. και Κάτσικα Σ., Προστασία της Ιδιωτικότητας και Τεχνολογίες Πληροφορικής και Επικοινωνιών, σελ. 520 επ. με τις εκεί παραπομπές.

στάθμισης των εκάστοτε δικαιωμάτων και συμφερόντων. Αντίθετα, στη Γερμανία και στην Αυστρία εισήχθησαν εκτενείς ουσιαστικές προϋποθέσεις, ως προς τις οποίες έχουν υποχρέωση συμμόρφωσης όσοι επεξεργάζονται προσωπικά δεδομένα με την αντίστοιχη ανεξάρτητη αρχή να εστιάζει στην ελεγκτική της λειτουργία και στην πρόκληση, κατά βάση, δημόσιας συζήτησης.

Τόσο η ενωσιακή, όσο και η ελληνική νομοθεσία για την προστασία των προσωπικών δεδομένων ενδιαφέρονται, πλην των άλλων, για την ασφάλεια των πληροφοριών και των δεδομένων που διαχέονται διαμέσου των εκάστοτε πληροφοριακών συστημάτων, γι' αυτό άλλωστε και προβλέπουν τη λήψη των αναγκαίων μέτρων ασφάλειας, ώστε να προστατεύονται τα δεδομένα αυτά από τυχαία, θεμιτή ή αθέμιτη καταστροφή, απώλεια, απαγορευμένη ή μη διάδοση και πρόσβαση και γενικά από κάθε άλλης μορφής αθέμιτη επεξεργασία. Τα επίπεδα, μάλιστα, ασφάλειας που απαιτούνται πρέπει να είναι ανάλογα των κινδύνων που ελλοχεύουν από τη συλλογή και επεξεργασία των εκάστοτε προσωπικών δεδομένων.

Επιπλέον, φαίνεται πως η ιδιωτικότητα προσεγγίζεται με διαφορετικό τρόπο ανάμεσα στην αμερικανική και την ευρωπαϊκή θεωρία και νομολογία. Το Ευρωπαϊκό Δικαστήριο Δικαιωμάτων του Ανθρώπου (ΕΔΔΑ) έχει συμβάλει σημαντικά στην εξέλιξη της έννοιας της ιδιωτικότητας, όπως άλλωστε και σε πλήθος άλλων εννοιών που χρησιμοποιούνται, κατά καιρούς, από τα δικαστήρια των κρατών – μελών, προσδίδοντας στην έννοια της ιδιωτικότητας μια κοινωνική διάσταση και επεκτείνοντάς την πέρα από την κλασική στενή προσωπική σφαίρα, με αποτέλεσμα να αναγνωρίζει την ύπαρξη της ιδιωτικότητας και στο δημόσιο χώρο[127]. Σε αντίθεση με την Ευρώπη, στις Η.Π.Α., δεν εμφανίζεται η ανάγκη για προστασία της ιδιωτικότητας στο χώρο εργασίας ή εν γένει στο δημόσιο χώρο, με αποτέλεσμα να αντιμετώπιζονται με αρκετά διαφορετικό τρόπο φαινόμενα ενδεχόμενης παραβίασης της ιδιωτικότητας στους χώρους αυτούς[128].

Περαιτέρω, ενώ σύμφωνα με τη διαμορφωθείσα από το ΕΔΔΑ νομολογία, το δικαίωμα του ιδιωτικού βίου περιλαμβάνει τόσο μία αρνητική, όσο και μία θετική διάσταση, δηλαδή αφενός το δικαίωμα κάποιου να μην υφίσταται παρεμβάσεις και αφετέρου την υποχρέωση του κράτους να

[127] Η προσέγγιση επομένως αυτή, όπως είναι αναμενόμενο, δημιουργεί μια διαφορετική διάσταση στην αντιμετώπιση των προβλημάτων που αφορούν στην προσβολή της ιδιωτικότητας στο πλαίσιο των εργασιακών σχέσεων ή σε σχέση με τη χρήση κλειστών κυκλωμάτων τηλεόρασης στο δημόσιο χώρο. Βλ. σχετικά τις αποφάσεις του ΕΔΔΑ: *Niemitz v. Germany* (1992) και *Peck v. UK (2003)*.

[128] Αντίστοιχα, με την ως άνω περίπτωση, το Supreme Court έκρινε ότι ένα άτομο δεν μπορεί να προσδοκά την προστασία της ιδιωτικότητάς του όταν αποκαλύπτει πληροφορίες σε τρίτα άτομα ή οργανισμούς και στη συνέχεια διαβιβάστηκαν από αυτούς σε μία δημόσια αρχή (βλ. US v. Miller, Smith v. Maryland).

λαμβάνει μέτρα για την προστασία της ιδιωτικότητας[129], η νομολογία των δικαστηρίων των Η.Π.Α. αναγνωρίζει μόνο το δικαίωμα του πολίτη στην ιδιωτικότητα έναντι του κράτους, το οποίο φυσικά δεν έχει καμία υποχρέωση να λάβει οιαδήποτε μέτρα ως προς τους ιδιώτες.

Οι ανωτέρω διαφορές φαίνεται πως εδράζονται στο γεγονός ότι σε γενικές γραμμές στις Η.Π.Α. και αναφορικά με το πλαίσιο προστασίας των προσωπικών δεδομένων ισχύει ένα φάσμα γενικών αρχών, που όμως συχνά, αν όχι κατά κόρον, στερείται δεσμευτικού περιεχομένου, γεγονός που μάλλον λειτουργεί πιο αποτρεπτικά, σε συνδυασμό με την έλλειψη ολοκληρωμένου νομοθετικού πλαισίου, σε σύγκριση με τα όσα ισχύουν σε ευρωπαϊκό επίπεδο για το σύστημα προστασίας των δεδομένων προσωπικού χαρακτήρα.

Βέβαια, πρέπει να σημειωθεί ότι σημαντικό ρόλο παίζουν και οι αντιλήψεις των πολιτών τόσο της Ευρωπαϊκής Ένωσης, όσο και των Ηνωμένων Πολιτειών της Αμερικής αναφορικά με το επίπεδο και την έκταση της προστασίας που δικαιούνται να προσδοκούν. Η *«εύλογη προσδοκία για ιδιωτικότητα»* ή αλλιώς «*reasonable expectation of privacy»*, κεντρική έννοια του αμερικανικού δικαίου[130], αλλά και ερμηνευτικό εργαλείο στη νομολογία του Ευρωπαϊκού Δικαστηρίου των Δικαιωμάτων του Ανθρώπου, είναι μια έννοια ευέλικτη, το περιεχόμενο της οποίας συμπροσδιορίζεται από τις τεχνολογικές ή/και κοινωνικές αλλαγές. Ωστόσο, σε κάθε περίπτωση πρέπει να γίνει δεκτό ότι ο βαθμός προσδοκίας της ιδιωτικότητας δεν μένει ανεπηρέαστος από την έκταση και την ένταση της επεξεργασίας πληροφορίας και επιτήρησης που ασκείται σε μία κοινωνία[131].

[129] Βλ. σχετικά την απόφαση του ΕΔΔΑ: *Guerra and others v. Italy (1998).*

[130] Η αρχή, βέβαια, της *εύλογης προστασίας για ιδιωτικότητα* δεν εμποδίζει τη νομοθεσία των Ηνωμένων Πολιτειών της Αμερικής να επιτρέπει την παροχή σε αμερικανικές δημόσιες αρχές online πρόσβασης στα δεδομένα των επιβατών σε πτήσεις από ή προς τις Η.Π.Α., ή την παροχή της δυνατότητας σε αμερικανικές δημόσιες αρχές να έχουν πρόσβαση στα δεδομένα συναλλαγών που τηρούσε η εγκατεστημένη στο Βέλγιο Society for Worldwide Interbank Financial Telecommunication (SWIFT), φαινόμενα τα οποία για τα ευρωπαϊκά δεδομένα είναι μάλλον πρωτόγνωρα. Βλ. σχετικά την κριτική που ασκήθηκε από τις ευρωπαϊκές αρχές προστασίας προσωπικών δεδομένων, Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT).

[131] Βλ. ό.π. Λαμπρινουδάκη Κ., Μήτρου Λ., Γκρίτζαλη Στ. και Κάτσικα Σ., Προστασία της Ιδιωτικότητας και Τεχνολογίες Πληροφορικής και Επικοινωνιών, σελ. 540.

3.3.5. Κανονισμοί που πρέπει να διέπουν τους οργανισμούς αναφορικά με τον έλεγχο της ιδιωτικότητας των χρηστών

Η νομιμότητα της επεξεργασίας δεδομένων προσωπικού χαρακτήρα εντός του υπολογιστικού νέφους εξαρτάται από τη συμμόρφωση προς τις βασικές αρχές της νομοθεσίας της ΕΕ που διέπει την προστασία των δεδομένων. Συγκεκριμένα, πρέπει να διασφαλίζεται η διαφάνεια έναντι του προσώπου στο οποίο αναφέρονται τα δεδομένα, πρέπει να τηρείται η αρχή του προσδιορισμού και του περιορισμού του σκοπού, καθώς και να διαγράφονται τα δεδομένα προσωπικού χαρακτήρα μόλις πάψει να είναι πλέον απαραίτητη η διατήρησή τους. Πρέπει, επιπλέον, να εφαρμόζονται και τα κατάλληλα τεχνικά και οργανωτικά μέτρα, ώστε να διασφαλίζεται ένα επαρκές επίπεδο προστασίας και ασφάλειας των δεδομένων[132].

Είναι δεδομένο ότι όταν ο υπεύθυνος της επεξεργασίας αποφασίζει να συνάψει σύμβαση παροχής υπηρεσιών νεφοϋπολογιστικής για λογαριασμό του, οφείλει να επιλέγει προς εκτέλεση της επεξεργασίας πρόσωπο το οποίο παρέχει επαρκείς εγγυήσεις όσον αφορά τα μέτρα τεχνικής ασφάλειας και οργάνωσης της επεξεργασίας[133] και να εξασφαλίζει την τήρηση των μέτρων αυτών. Υποχρεούται, ακόμη, από τον νόμο να υπογράφει επίσημη σύμβαση με τον πάροχο υπηρεσιών νεφοϋπολογιστικής, η οποία πρέπει, κατ' ελάχιστον, να προβλέπει συγκεκριμένα ότι ο εκτελών την επεξεργασία οφείλει να τηρεί τις οδηγίες του υπεύθυνου της επεξεργασίας και να εφαρμόζει τεχνικά και οργανωτικά μέτρα με γνώμονα την επαρκή προστασία των δεδομένων προσωπικού χαρακτήρα.

Είναι γεγονός ότι τα ζητήματα κανονιστικής συμμόρφωσης των υπηρεσιών Cloud Computing αποτελούν ένα φλέγον ζήτημα συζήτησης σε όλον τον κόσμο. Οι περισσότεροι μεγάλοι και αξιόπιστοι πάροχοι υπηρεσιών Cloud Computing διεξάγουν αυστηρές αναλύσεις για να διασφαλίζουν τη

[132] Βλ. ό.π. την υπ' αριθμ. 05/2012 από 1ης Ιουλίου 2012 Γνώμη της Ομάδας Εργασίας του άρθρου 29 για την προστασία των δεδομένων σχετικά με τη νεφοϋπολογιστική, 01037/12/EL, WP 196, σελ. 14.

[133] Το NIST εξέδωσε οδηγίες για τη λήψη μέτρων ασφαλείας κατά τη χρήση του υπολογιστικού νέφους από δημόσιους οργανισμούς. Συγκεκριμένα κάνει λόγο για τη χρησιμοποίηση βέλτιστων πρακτικών για την ασφάλεια των web browser και αποφυγή περιηγήσεων σε κακόβουλες ιστοσελίδες, την ισχυρή κρυπτογράφηση, τη φυσική ασφάλεια των εγκαταστάσεων, για μηχανισμούς ελέγχου της ταυτότητας και πρόσβασης. Βλ. σχετικά, Jansen W., Grance T., «Guidelines on Security and Privacy in Public Cloud Computing" σε: http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf.

συμμόρφωσή τους με τη γενικά ισχύουσα νομοθεσία. Ειδικότερα, στην Ελλάδα, οι πάροχοι υπηρεσιών Cloud Computing μπορεί να χαρακτηριστούν ως εκτελούντες την επεξεργασία δεδομένων, αφού επεξεργάζονται δεδομένα προσωπικού χαρακτήρα για λογαριασμό των πελατών τους[134]. Ωστόσο, πρέπει να γίνει κατανοητό ότι την τελική ευθύνη για τη συμμόρφωση με τις ισχύουσες νομοθετικές και κανονιστικές διατάξεις την έχει ο ίδιος ο πελάτης, καθώς αυτός είναι ο υπεύθυνος επεξεργασίας των εν λόγω δεδομένων[135].

Στις περιπτώσεις κανονισμών που ισχύουν για επιχειρήσεις σε συγκεκριμένους κλάδους (sectorial regulations) και όχι κατ' αρχάς απ' ευθείας για τους παρόχους υπηρεσιών Cloud, οι τελευταίοι πρέπει να παρέχουν λεπτομερή πληροφόρηση στους υποψήφιους πελάτες σχετικά με το πώς το Cloud μπορεί να τους βοηθήσει να συμμορφώνονται με τις απαιτήσεις αυτές. Με λίγα λόγια, οι πάροχοι οφείλουν να εξηγούν στους ενδιαφερόμενους πελάτες το πώς οι υποκείμενες παρεχόμενες υπηρεσίες και οι λειτουργίες τους μπορούν να συμβάλλουν στη στρατηγική κανονιστικής συμμόρφωσης του πελάτη.

Επιπλέον, οι υπηρεσίες Cloud μπορεί να περιλαμβάνουν βασικά δεδομένα των πελατών και σε περίπτωση καταγγελίας της σύμβασης ή σε περίπτωση πτώχευσης του παρόχου, είναι σημαντικό ο πελάτης να μπορεί να πάρει πίσω τα δεδομένα του. Παρόλο που θα υπάρχει κόστος για τις εν λόγω ανταλλαγές, οι πελάτες πρέπει να διαπραγματεύονται τους όρους που επιτρέπουν τη «μετανάστευση» των δεδομένων (data migration) και θα πρέπει να διασφαλίζουν ότι ο πάροχος δεν αποκτά κανένα δικαίωμα ιδιοκτησίας επί των δεδομένων των πελατών του. Τέλος, εξίσου σημαντικό είναι να διασφαλιστεί ότι ο πάροχος θα διαγράφει μόνιμα τα δεδομένα του πελάτη του, κατόπιν αιτήματός του, μέσα σε εύλογο χρονικό διάστημα για την πρόληψη ζητημάτων εμπιστευτικότητας[136].

---

[134] Η επεξεργασία αυτή των δεδομένων προσωπικού χαρακτήρα γίνεται με την έννοια του ν. 2472/1997 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, με τον οποίο ενσωματώθηκε στο ελληνικό δίκαιο η Οδηγία 95/46/ΕΚ για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.

[135] Σε μία περίπτωση, επί παραδείγματι, όπου πάροχος υπηρεσιών Cloud Computing υπέβαλε ερώτημα αναφορικά με την υπηρεσία διαχείρισης και αποθήκευσης ιατρικής απεικόνισης (Picture Archiving and Communication Systems Hosting - PACS) που παρέχεται από υποδομή που φιλοξενείται σε κέντρο δεδομένων του παρόχου στην Ελλάδα, η ελληνική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα διευκρίνισε ότι ο πάροχος λειτουργεί ως εκτελών την επεξεργασία, καθώς ενεργεί για λογαριασμό του εκάστοτε πελάτη, ο οποίος καθορίζει το σκοπό και τον τρόπο της επεξεργασίας και συνεπώς βαρύνεται με τις υποχρεώσεις του υπεύθυνου επεξεργασίας.

[136] ό.π., Shahab Α. και Παπανικολάου Α., Υπολογιστικό Νέφος (cloud computing): Θέματα σύναψης συμβάσεων και συμμόρφωσης για νομικούς συμβούλους.

ΕΠΙΛΟΓΟΣ

Είναι γεγονός ότι η ανάπτυξη της τεχνολογίας δημιούργησε την ανάγκη για κατοχύρωση σε νομικό επίπεδο της προστασίας της ιδιωτικότητας και των προσωπικών δεδομένων. Τα πράγματα, βέβαια, στην πορεία, συνέχισαν προς την ίδια κατεύθυνση. Όσο, δηλαδή, η τεχνολογία σημείωνε πρόοδο και εξέλιξη, τόσο ενισχυόταν η ανάγκη για δημιουργία ενός πιο στέρεου, εξελιγμένου και ολοκληρωμένου μοντέλου προστασίας των προσωπικών πληροφοριών του ατόμου.

Το δίκαιο, όμως, ως ένα δυναμικό σύστημα που ρυθμίζει τις διάφορες έννομες σχέσεις μέσα σε μία κοινωνία, πρέπει να βρίσκεται σε ένα διαρκή αγώνα εξέλιξης και ανάπτυξης, ώστε να μπορεί, αν όχι να προλαμβάνει, τουλάχιστον να συστοιχίζεται με τις εξελίξεις στον τομέα της τεχνολογίας. Ο νομοθέτης, όπως συνήθως συμβαίνει για όλες τις έννομες σχέσεις, προσπαθεί να συμβαδίσει με τις ταχύτατες τεχνολογικές εξελίξεις και τις συνακόλουθες εξελίξεις σε επίπεδο εννόμων σχέσεων και άλλοτε προλαβαίνει, άλλοτε όμως φτάνει αρκετά καθυστερημένα, ώστε απαιτείται συχνά πολύ γρήγορα εκ νέου νέα αλλαγή στο νομοθετικό πλαίσιο, πριν καλά καλά προλάβει να ολοκληρωθεί η προηγούμενη αλλαγή.

Είναι γεγονός ότι, κατά τη διάρκεια των τελευταίων χρόνων, ο νομοθέτης έχει επιχειρήσει να αντιμετωπίσει το ζήτημα με σημειακές παρεμβάσεις, είτε ρυθμίζοντας τις ηλεκτρονικές επικοινωνίες και συναλλαγές, είτε επεκτείνοντας συμπεριφορές που εκδηλώνονται στον δικτυακό κόσμο, είτε τέλος επιχειρώντας, σε αρκετές πλέον περιπτώσεις, την άρση των τυχόν προβλημάτων μέσω της προσέγγισης της «τεχνολογικής ουδετερότητας». Ωστόσο, η λύση αυτή εγείρει ουσιαστικά προβλήματα προκατανόησης της τεχνολογίας, καθώς όσο τεχνολογικά ουδέτερη και αν είναι μία διατύπωση, οι αντιλήψεις και επιλογές του νομοθέτη αναπόφευκτα διαμορφώνονται υπό το πρίσμα της «τεχνολογίας του καιρού» του[137]. Ενίοτε μάλιστα, διαπιστώνεται ότι επιχειρείται η συσταλτική τροποποίηση τεχνολογικά ουδέτερων διατυπώσεων, προκειμένου να εξυπηρετηθούν πολιτικοοικονομικές επιδιώξεις[138].

[137] Βλ. ό.π. Λαμπρινουδάκη Κ., Μήτρου Λ., Γκρίτζαλη Στ. και Κάτσικα Σ., Προστασία της Ιδιωτικότητας και Τεχνολογίες Πληροφορικής και Επικοινωνιών, σελ. 546.

[138] Χαρακτηριστικό παράδειγμα, εν προκειμένω, αποτελεί η προσπάθεια να αποσυνδεθεί ο ορισμός των διευθύνσεων IP ως προσωπικό δεδομένο από το γενικό κριτήριο της δυνατότητας προσδιορισμού ενός προσώπου και να υπάρξει κανονιστική διάκριση μεταξύ στατικών και δυναμικών διευθύνσεων IP.

Εξίσου σοβαρό ζήτημα είναι και ο προσδιορισμός του ρυθμιστέου αντικειμένου, καθώς οι διάφορες πράξεις, ενέργειες, συμπεριφορές και σχέσεις που αναπτύσσονται σε ψηφιακά περιβάλλοντα, ακριβώς επειδή είναι σύμφυτες με τη δυναμική της τεχνολογίας, απαιτούν διαφορετική νομική αντιμετώπιση από αυτές που αναπτύσσονται στο συμβατικό περιβάλλον. Το γεγονός αυτό, μοιραία οδηγεί στο συμπέρασμα, ότι συχνά το δίκαιο με την παραδοσιακή του μορφή δεν μπορεί να καλύψει την ευρεία γκάμα των δικτυακών συναλλαγών και των αντίστοιχων πληροφοριακών ροών, ούτε τις καινοφανείς και απρόβλεπτες στο νομοθέτη μορφές δραστηριότητας και επικοινωνίας που αναπτύσσονται στον εικονικό κόσμο.

Δεν είναι, λοιπόν, παράδοξο να υποστηρίζεται ότι η προστασία της ιδιωτικότητας είναι ζήτημα που θα πρέπει να επιλυθεί με τεχνολογικά μέσα. Η τεχνολογική προστασία, δηλαδή η σχεδίαση και εφαρμογή τεχνολογικών προϊόντων και υπηρεσιών με τρόπο ώστε να γίνεται σεβαστή και να προωθείται η ιδιωτικότητα είναι αναγκαίος, αν όχι συστατικός, όρος αποτελεσματικής προστασίας. Ωστόσο, η επιλογή των ρυθμιστικών επιταγών που θα μετουσιωθούν σε τεχνολογία δεν είναι τεχνοκρατικό, αλλά πρωτίστως θεσμικό ζήτημα και απαιτεί αντίστοιχη αντιμετώπιση[139]. Η υποστήριξη, άλλωστε, των Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας, ή αλλιώς, *Privacy Enhancing Technologies, (PETs*) εκφράζεται πλέον και σε κοινοτικό επίπεδο, χωρίς ωστόσο να προσλαμβάνει την ποιότητα κανονιστικής επιταγής[140], ενώ πρέπει να σημειωθεί ότι δεν καταγράφεται η αναμενόμενη διάδοση των Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας[141].

Σε κάθε περίπτωση, αυτό που πρέπει να γίνει αντιληπτό είναι ότι η επίλυση των προβλημάτων καθίσταται ευχερέστερη αν καταφέρουμε να εισάγουμε τους ρυθμιστικούς κανόνες δικαίου, με τη δυναμική που αυτοί περικλείουν, στην τεχνολογία και να μην οδηγηθούμε στο άτοπο να αφήσουμε την

[139] Βλ. ό.π. Λαμπρινουδάκη Κ., Μήτρου Λ., Γκρίτζαλη Στ. και Κάτσικα Σ., Προστασία της Ιδιωτικότητας και Τεχνολογίες Πληροφορικής και Επικοινωνιών, σελ. 547.

[140] Η Ευρωπαϊκή Επιτροπή με μία δημόσια ανακοίνωση της 2ας Μαΐου 2007 δήλωσε την άμεση υποστήριξή της στις Τεχνολογίες αυτές, ώστε να ενισχυθεί η ιδιωτικότητα και να υποβοηθηθεί η εφαρμογή των κανόνων προστασίας προσωπικών δεδομένων. Η Επιτροπή αντιλαμβάνεται, άλλωστε, τις τεχνολογίες αυτές ως συμπλήρωμα του νομοθετικού πλαισίου, διευκρινίζοντας μάλιστα ότι η εφαρμογή των ως άνω τεχνολογιών δεν απαλλάσσει τους υπεύθυνους επεξεργασίας από τις νομικές υποχρεώσεις τους.

[141] Αφού ο νομοθέτης δεν απαιτεί την υιοθέτηση των PETs από τις εταιρίες, οι τελευταίες δεν μπαίνουν στη διαδικασία να τις χρησιμοποιήσουν. Ο νομοθέτης δε δεν απαιτεί την υιοθέτησή τους, καθώς διαπιστώνει τη μη ύπαρξη προσφοράς τέτοιων τεχνολογιών, προσφορά όμως που δεν αναπτύσσεται, επειδή οι επιχειρήσεις δεν είναι υποχρεωμένες να τις εισάγουν (φαύλος κύκλος των PETs).

τεχνολογία να ρυθμίζει μόνη της τα κάθε φορά ανακύπτοντα ζητήματα. Αντίστοιχα, ιδιαίτερη προσοχή πρέπει να σημειωθεί και στο φαινόμενο της παραγωγής κανόνων από τους ενδιαφερόμενους φορείς και την αυτοδέσμευσή τους ως προς την τήρησή τους. Τόσο η κοινοτική Οδηγία για την προστασία προσωπικών δεδομένων, όσο και οι νομοθεσίες των ευρωπαϊκών κρατών ευνοούν μεν την υιοθέτηση κωδίκων δεοντολογίας, πλην όμως ως συμπλήρωμα των νομικών κανόνων[142].

Εξάλλου, το κοινό σημείο αναφοράς μεταξύ των κανόνων αυτορρύθμισης[143] και των κανόνων δικαίου είναι η εξουσιαστική υφή αυτών. Η ποιοτική διαφορά είναι ο φορέας που τους επιβάλλει. Στην πρώτη περίπτωση είναι οι ιδιωτικοί φορείς, ενώ στη δεύτερη η κρατική εξουσία. Έτσι, σε μια προσπάθεια συγκερασμού των πλεονεκτημάτων και μειονεκτημάτων των δύο αυτών διαφορετικών ροών ρυθμίσεων και σε μία προσπάθεια υπέρβασης των αδυναμιών της παραδοσιακής νομοθετικής ρύθμισης, αλλά και εξισορρόπησης του έλλειμματος δημοκρατικής νομιμοποίησης της αυτορρύθμισης καταλήγουμε μοιραία στα μοντέλα της συρρύθμισης (*co-regulation)*[144] ή ρυθμιζόμενης αυτορρύθμισης[145].

Πάντως, είναι γεγονός ότι η αυτορρύθμιση προτάσσεται συχνά ως λύση για την αντιμετώπιση του παγκοσμιοποιημένου χαρακτήρα των πληροφοριακών ροών, καθώς οι εκάστοτε ρυθμιστικές προσεγγίσεις, εφόσον και όπου υφίστανται, παρουσιάζουν σημαντικές αποκλίσεις μεταξύ τους[146]. Η επιθυμία για την υιοθέτηση ενός παγκόσμιας εμβέλειας ρυθμιστικού εργαλείου είναι τόσο προφανής, πλην όμως καθίσταται εξαιρετικά δυσχερής η υλοποίηση της εν λόγω ιδέας. Και αυτό γιατί αφενός υφίσταται πραγματική αδυναμία επίτευξης συναίνεσης ως προς τις κανονιστικές επιλογές, αφετέρου δε,

---

[142] Είναι αυτονόητο ότι η αυτορρυθμιστική προσέγγιση είναι πιο ισχυρή σε χώρες που αξιολογούν τη νομοθεσία για την προστασία των δεδομένων ως οικονομικό και διοικητικό βάρος/επιβάρυνση για τον ιδιωτικό τομέα και περιορίζονται σε ειδικές, τομεακές νομοθετικές παρεμβάσεις.

[143] Γενικά για την αυτορρύθμιση στο διαδίκτυο, βλ. Μήτρου Λ., (Αυτορ)ρύθμιση στον Κυβερνοχώρο στο συλλογικό τόμο Αυτορρύθμιση Γ. Παπαδημητρίου (επιμ.), Αθήνα – Θεσσαλονίκη, 2005, σελ. 75 επ.

[144] Στο μοντέλο της συρρύθμισης η έμφαση δίνεται στην εισαγωγή και υιοθέτηση διαδικασιών διαβούλευσης με τους ενδιαφερομένους, αλλά και με ειδικούς.

[145] Στο μοντέλο της ρυθμιζόμενης αυτορρύθμισης η κρατική/διακρατική ρύθμιση περιορίζεται σε στρατηγικά σημεία, ορίζοντας τις βασικές αρχές και τις προδιαγραφές που χρησιμεύουν ως βάσεις για την ανάπτυξη της αυτορρύθμισης και των κανονιστικών τεχνικών που συνδέονται με αυτή.

[146] Αξίζει πάντως να επισημανθεί ότι η βασική διακήρυξη της τελευταίας Παγκόσμιας Διάσκεψης των Επιτρόπων και Αρχών Προστασίας Προσωπικών Δεδομένων (2008) αναφέρεται ακριβώς στην *ανάγκη «να εκπονηθεί μία κοινή πρόταση για τη θέσπιση διεθνών προδιαγραφών για την προστασία της ιδιωτικότητας και των προσωπικών δεδομένων».* Εύλογα μπορεί κανείς να αντιληφθεί το λόγο και τη χρησιμότητα ενός τέτοιου εγχειρήματος.

ακόμη και αν επιτευχθεί μία παγκόσμια συναίνεση, δεν μπορεί ευκρινώς να καθοριστεί το επίπεδο στο οποίο αυτή θα επιτευχθεί[147].

Σε κάθε περίπτωση αυτό που δεν πρέπει να ξεχνάμε είναι ότι η ανάπτυξη και η εξέλιξη της τεχνολογίας καθιστά τον καθένα από εμάς εν δυνάμει φορέα της δυνατότητας επεξεργασίας της πληροφορίας και συνακόλουθα παραβίασης των δικαιωμάτων της ιδιωτικότητας. Οι σελίδες κοινωνικής δικτύωσης δίνουν τη δυνατότητα σε άλλους χρήστες να «καρπώνονται» τα προσωπικά δεδομένα των προσώπων με περαιτέρω συνέπεια την ύπαρξη σοβαρής πιθανότητας προσβολής των δικαιωμάτων τους.

Ακριβώς λόγω των μεταλλαγών ως προς τις επικοινωνιακές σχέσεις και τη διάχυση της επεξεργασίας προσωπικών πληροφοριών, προβάλλεται το τελευταίο διάστημα, εκ νέου και με έμφαση, το μοντέλο του «αυτοπροστατευόμενου ατόμου-χρήστη»[148]. Η προστασία των δεδομένων είναι το ύψιστο διακύβευμα, ειδικά σε μία δημοκρατική κοινωνία, και επομένως, η συγκατάθεση του ατόμου ή η αυτοδιαχείριση της δικτυακής του εικόνας και παρουσίας είναι όντως μία πρωταρχική έκφραση του δικαιώματος του πληροφοριακού αυτοκαθορισμού, με αποτέλεσμα να καθίσταται αδήριτη ανάγκη να μπορεί το άτομο να καθιστά δυνατή την επιθυμητή επεξεργασία και να παρεμποδίζει την ανεπίτρεπτη, πλην όμως, φαίνεται πως η τεχνολογία ίσως δεν παρέχει τις κατάλληλες αντικειμενικές προϋποθέσεις ώστε να εξασφαλίζεται η ελεύθερη επιλογή των ατόμων.

Οι λεγόμενες τεχνολογίες βελτίωσης της ιδιωτικότητας θα ήταν, επίσης, μία ηχηρή απάντηση στην επιτυχή διασυνοριακή διαβίβαση των προσωπικών δεδομένων. Με την από 2.5.2007 Ανακοίνωσή της, η Ευρωπαϊκή Επιτροπή, στο πλαίσιο της ανάγκης ελαχιστοποίησης της επεξεργασίας προσωπικών δεδομένων και της μη χρησιμοποίησης ανώνυμων ή ψευδώνυμων δεδομένων μέσω των τεχνολογιών για τη βελτίωση της προστασίας της ιδιωτικότητας (TBI), εξέτασε και τις «σφραγίδες ιδιωτικότητας», δηλαδή ένα σύστημα πιστοποίησης των προϊόντων ότι είναι συμβατά με πρότυπα που αντιστοιχούν σε κανόνες προστασίας δεδομένων. Η ευρεία χρήση των σφραγίδων ιδιωτικότητας θα μπορούσε να

[147] Τεκμαίρεται ότι το επίπεδο αυτό θα είναι η συνισταμένη ή ο ελάχιστος κοινός παρονομαστής των διαφόρων προσεγγίσεων για την προστασία της ιδιωτικότητας, πλην όμως σίγουρα θα έχουν υιοθετηθεί σημαντικές αποκλίσεις.

[148] Ακριβέστερα, η προσέγγιση αυτή συντίθεται αφενός από την παροχή της δυνατότητας στο άτομο να προσδιορίσει με τον μηχανισμό της συγκατάθεσης το εύρος των πληροφοριών που οι άλλοι θα επεξεργάζονται για αυτό και αφετέρου από τη χρήση τεχνικών εργαλείων για να θωρακίσει την ιδιωτικότητά του. Υποστηρίζεται ότι είναι προτιμότερη η παροχή προϋποθέσεων εξατομικευμένης αυτοπροστασίας από την γενικευμένη επιταγή που «εξαναγκάζει» σε προστασία.

βοηθήσει και τους πολίτες που κάνουν χρήση τέτοιων τεχνολογιών, προϊόντων και υπηρεσιών, αλλά και τους παρόχους υπηρεσιών και εφαρμογών «υπολογιστικού νέφους», αφού έτσι μπορεί να ενισχυθεί τελικώς η ευθύνη των υπευθύνων επεξεργασίας δεδομένων[149].

Χαρακτηριστικό παράδειγμα μιας τέτοιας πιστοποίησης είναι το νέο πρότυπο ISO/IEC 27018 (ISO 27018)[150], το οποίο ενισχύει την προστασία των προσωπικών δεδομένων με την προσθήκη κλειδιών προστασίας για τις ευαίσθητες πληροφορίες των πελατών που αποθηκεύονται στο Cloud. Σημειωτέον ότι πριν το ISO 27018 δεν υπήρχε ένα ισχυρό, διεθνώς αναγνωρισμένο σημείο αναφοράς για την προστασία των αποθηκευμένων PII στο Cloud. Έτσι, μετά την καθιέρωση του προτύπου ISO 27001: 2013, ενός δηλαδή διεθνούς προτύπου με το οποίο παρείχετο ένα ευέλικτο σύστημα για τον εντοπισμό των κινδύνων για την ασφάλεια των πληροφοριών και την επιλογή των ελέγχων για την αντιμετώπισή τους, προέκυψε ως προσθήκη το πρότυπο ISO 27018: 2014 με το οποίο παρέχονται συγκεκριμένες οδηγίες στους παρόχους υπηρεσιών Cloud για την αξιολόγηση των κινδύνων και την εφαρμογή των ελέγχων για την προστασία των PII που είναι αποθηκευμένες στο Cloud.

Μια υπηρεσία Cloud σύμφυτη με το πρότυπο ISO 27018 αποτελεί για τους πελάτες έναν εύκολο τρόπο, ώστε να επιβεβαιώσουν ότι τα προσωπικά στοιχεία που αναθέτουν στους παρόχους θα χρησιμοποιηθούν μόνο όπως αυτοί εγκρίνουν και ότι οπωσδήποτε θα παραμένουν ασφαλή. Επιπλέον, το ISO 27018 υποστηρίζει τους κανονισμούς που ορίζονται από τις αρχές προστασίας των δεδομένων σε όλο τον κόσμο[151]. Έτσι, εξασφαλίζεται ένας σημαντικός βαθμός ομοιομορφίας στη βιομηχανία, ενισχύεται η ασφάλεια των αναγνωρίσιμων προσωπικών πληροφοριών και εξασφαλίζεται η συμμόρφωση σε ένα περιβάλλον που βασίζεται στην αποθήκευση και επεξεργασία των πληροφοριών που βρίσκονται σε Cloud συστήματα. Τέλος, το πρότυπο αυτό δίνει νέες, σαφείς οδηγίες βασισμένες στις αρχές προστασίας δεδομένων της ΕΕ, ιδίως αναφορικά με το πώς ένας επεξεργαστής δεδομένων θα

[149] ό.π., Κίτσος Π. και Παππά Π., Η προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής στις υπηρεσίες του υπολογιστικού νέφους. Εννοιολογικά προβλήματα και ρυθμιστικές προσεγγίσεις της Ευρωπαϊκής νομοθεσίας.

[150] Το ISO 27018 δημοσιεύθηκε στις 30 Ιουλίου 2014 από τον Διεθνή Οργανισμό Τυποποίησης (ISO) και θέτει τις κατευθυντήριες γραμμές για τους παρόχους υπηρεσιών Cloud σχετικά με τις αναγνωρίσιμες προσωπικές πληροφορίες (PII). Το πρότυπο αυτό αναπτύχθηκε σε συνεργασία με εισηγητές από 14 χώρες και 5 διεθνείς οργανισμούς.

[151] International Standard ISO/IEC 27018, Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.

πρέπει να προστατεύει τα δεδομένα των πελατών, συμπεριλαμβανομένης της απαίτησης οι πάροχοι να μη χρησιμοποιούν τα δεδομένα των πελατών για διαφημιστικούς σκοπούς.

Με λίγα λόγια, οι πελάτες θα γνωρίζουν πάντα που μπορούν να αποθηκευτούν τα δεδομένα τους και ποιος τα επεξεργάζεται, χωρίς να υφίσταται λόγος ανησυχίας ότι οι πάροχοι θα χρησιμοποιήσουν τις πληροφορίες τους για λόγους μάρκετινγκ και διαφήμισης χωρίς τη συγκατάθεσή τους. Επιπλέον, οι πελάτες μπορούν να είναι βέβαιοι ότι οι πάροχοι θα μπορούν να επιστρέψουν, μεταφέρουν ή να διαθέσουν ασφαλώς τα προσωπικά τους δεδομένα κατόπιν αιτήσεώς τους. Τέλος, χρησιμοποιώντας ένα πρότυπο ISO 27018 εξασφαλίζεται ότι θα υπάρχει συμμόρφωση μόνο με τις νομικά δεσμευτικές αιτήσεις για την αποκάλυψη των δεδομένων τους.

Σε κάθε περίπτωση και πιο συγκεκριμένα αναφορικά με το υπάρχον θεσμικό πλαίσιο στο επίπεδο των υπηρεσιών νεφοϋπολογιστικής, αυτό που προκύπτει είναι ότι δεν καθίσταται επαρκές για την αντιμετώπιση των προβλημάτων που σχετίζονται με την ανάπτυξη των υπηρεσιών και εφαρμογών του υπολογιστικού νέφους[152]. Για την αντιμετώπιση των προβλημάτων που σχετίζονται με τη μεταβίβαση και επεξεργασία προσωπικών δεδομένων στο υπολογιστικό νέφος χρειάζεται οπωσδήποτε μία νέα προσέγγιση σε έννοιες όπως της «επεξεργασίας» των προσωπικών δεδομένων και των συναρτημένων με αυτή εννοιών του «υπεύθυνου επεξεργασίας» και του «εκτελούντος την επεξεργασία». Είναι, επίσης, αναγκαίος ο εντοπισμός της εφαρμοστέας νομοθεσίας, η λεπτομερής ρύθμιση των υποχρεώσεων των παρόχων για την ασφάλεια των δεδομένων και η αντιμετώπιση των προβλημάτων που προκύπτουν από τη διασυνοριακή μεταβίβαση των προσωπικών δεδομένων.

Για το λόγο αυτό, η Ευρωπαϊκή Επιτροπή ανταποκρινόμενη στην ανάγκη αναθεώρησης του θεσμικού πλαισίου για την προστασία των προσωπικών δεδομένων, δημοσίευσε ήδη το προσχέδιο του Κανονισμού που θα αντικαταστήσει την Οδηγία 95/46/ΕΚ και θα αποτελέσει το νέο νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων σε όλον τον Ευρωπαϊκό Οικονομικό Χώρο. Η πρόταση για την υιοθέτηση ενός νέου Κανονισμού που θα ενισχύσει την προστασία των προσωπικών δεδομένων με διατάξεις που απαντούν στα σύγχρονα προβλήματα φαίνεται ότι κινείται προς την κατεύθυνση της ομοιόμορφης τήρησης των κανόνων για την προστασία των προσωπικών δεδομένων, αλλά και της δημιουργίας ενός πλαισίου, όπου διακρίνονται καθαρά τα δικαιώματα των καταναλωτών, οι

[152] Οι νέες πιστοποιήσεις όπως η ISO/IEC 27018 (ISO 27018), οπωσδήποτε ενισχύουν την ιδιωτικότητα των δεδομένων προσθέτοντας κλειδιά προστασίας για τις ευαίσθητες πληροφορίες των πελατών που αποθηκεύονται στο Cloud.

υποχρεώσεις των παρόχων και των εκτελούντων την επεξεργασία των προσωπικών δεδομένων, καθώς και ο ρόλος των ανεξάρτητων αρχών.

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΞΕΝΟΓΛΩΣΣΗ

- Armbrust M., Fox A., Griffith R., Joseph A., Katz R., Konwinski A., Lee G., Patterson D., Rabkin A., Stoica I., and Zaharia M., "Above the Clouds: A Berkeley View of Cloud Computing", Electrical Engineering and Computer Sciences, University of California at Berkeley, February 10, 2009
- Balding C., Assessing the Security Benefits of Cloud Computing, July 21, 2008
- Bowers K.D., Juels A., Oprea A., Proofs of retrievability: Theory and implementation, Proceedings of the 2009 ACM workshop on Cloud computing security, 2009
- Catteddu D. and Hogben G., Cloud Computing: benefits, risks and recommendations for information security. Technical Report. European Network and Information Security Agency, 2009
- Citron D., Cyber Civil Rights. Boston University Law Review, Vol. 89, pp. 61-125, 2009
- Danchev S., Tsakanikas A. and Ventouris N., Cloud Computing: A Driver for Greek Economy Competitiveness, Foundation for Economic and Industrial Research, November 2011
- Evdemon J., Liptaak C., Internet Scale Computing: MSDN Blog, Oct 17, 2007
- European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions, Unleashing the Potential of Cloud Computing in Europe (Text with EEA relevance), {SWD(2012) 271 final}, Brussels, 27.9.2012, COM(2012) 529 final
- Gellman R., «Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing», World Privacy Forum, February 23, 2009
- Giannakouris K., Smihili M., Cloud computing - statistics on the use by enterprises, Eurostat, November 2014
- Gray J., Distributed Computing Economics, Queue 6, 3, 2008
- International Standard ISO/IEC 27018, Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

- Khajeh-Hosseini A., Greenwood D. and Sommerville I., Cloud Migration: A Case Study of Migrating an Enterprise IT System to IaaS, 3rd IEEE International conference on Cloud Computing, Cloud 2010, 5-10 July, Miami, USA
- Korde P., Panwar V. and Kalse S., Securing Personal Health Records in Cloud using Attribute Based Encryption, International Journal of Engineering and Advanced Technology (IJEAT), Volume 2, Issue 4, April 2013
- Mantelero A., Cloud computing, trans-border data flows and the European Directive 95/46/EC: applicable law and task distribution, European Journal of Law and Technology, Vol 3, Issue 2, 2012
- Mell P., Grance T., "The NIST Definition of Cloud Computing", Recommendations of the National Institute of Standards and Technology, National Institute of Standards and Technology, U.S. Department of Commerce, September 2011
- Ming Li, Matti Siekkinen, Sasu Tarkoma, Antti Ylä-Jääski and Yong Cui, Segment Level Authentication: Combating Internet Source Spoofing. In the Proceedings of the 15th IEEE Symposium on Computers and Communications (ISCC'10), June 2010
- Poullet Y., Van Gyseghem J., Moiny J., Gérard J. and Gayrel C., «Data Protection in the Clouds», Computers, Privacy and Data Protection: an Element of Choice, Springer Netherlands 2011
- Rosenthal A., Mork P., Li M.H., Stanford J., Koester D. and Reynolds P., Cloud Computing: A New Business Paradigm for Biomedical Information Sharing, Journal of Biomedical Informatics, Vol. 43, Issue 2, April, 2010
- Schwartz P., Information Privacy in the cloud, University of Pennsylvania Law Review, vol. 161: 1623-1662
- Top Threats Working Group, The Notorious Nine Cloud Computing Top Threats in 2013, Cloud Security Alliance (CSA), February 2013

ΕΛΛΗΝΙΚΗ

- Αραβαντινός Β., Η προστασία των στοιχείων προσωπικού χαρακτήρα από την αθέμιτη επεξεργασία τους με ηλεκτρονικό υπολογιστή, εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 1997

- Γεράρης Χ., Τα προσωπικά δεδομένα και οι νέες προκλήσεις, ΔιΜΕΕ 2010

- Γέροντας Απ., Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία προσωπικών δεδομένων, εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 2002

- Γιαννόπουλος Γ., Προστασία προσωπικών δεδομένων και διασυνοριακή ροή πληροφοριών. Το πρόβλημα του «ικανοποιητικού επιπέδου προστασίας», ΔτΑ 2001

- Γκρίτζαλης Δ., Γκρίτζαλης Στ., Ηλιάδης Γ., Καμπουράκη Κ., Καρύδα Μ., Κάτσικας Σ., Κιουντούζης Ευ., Κοκολάκης Σπ., Λαμπρινουδάκης Κ., Λέκκας Δ., Μήτρου Λ., Μουλίνος Κ., Μπαλόπουλος Θ. και Τσούμας Β., Ασφάλεια Πληροφοριακών Συστημάτων, εκδόσεις Νέων Τεχνολογιών, Αθήνα 2004

- Κίτσος Π. και Παππά Π., Η προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής στις υπηρεσίες του υπολογιστικού νέφους. Εννοιολογικά προβλήματα και ρυθμιστικές προσεγγίσεις της Ευρωπαϊκής νομοθεσίας, Εισήγηση στο 4ο διεθνές συνέδριο Δικαίου της Πληροφορικής με θέμα: "Values and Freedoms in Modern Information Law and Ethics", Θεσσαλονίκη, 20-21 Μαΐου 2011

- Λαμπρινουδάκης Κ., Μήτρου Λ., Γκρίτζαλης Στ. και Κάτσικας Σ., Προστασία της Ιδιωτικότητας και Τεχνολογίες Πληροφορικής και Επικοινωνιών, Τεχνικά και Νομικά Θέματα, εκδόσεις Παπασωτηρίου, Αθήνα 2010

- Μήτρου Λ., Προστασία Προσωπικών Δεδομένων: ένα νέο δικαίωμα/Τσάτσο Δ., Βενιζέλο Ευ. και Κοντιάδη Ξ. (επιμ.), Το Νέο Σύνταγμα – Πρακτικά συνεδρίου για το αναθεωρημένο Σύνταγμα 1975/1986/2001, Αθήνα – Κομοτηνή, 2001

- Μήτρου Λ., Η ιδιωτικότητα στο web 2.0, ΔιΜΕΕ 2010

- Μήτρου Λ., Προστασία Προσωπικών Δεδομένων και Ασφάλεια σε Τιμητικό Τόμο για τα 125 Χρόνια του Νομικού Συμβουλίου του Κράτους, Αθήνα – Κομοτηνή 2008

- Shahab Α. και Παπανικολάου Α., Υπολογιστικό Νέφος (cloud computing): Θέματα σύναψης συμβάσεων και συμμόρφωσης για νομικούς συμβούλους, Δίκαιο Επιχειρήσεων και Εταιρειών 6/2014