ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ
ΤΜΗΜΑ ΝΟΜΙΚΗΣ

ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

Η ΑΠΟΣΤΟΛΗ ΥΒΡΙΣΤΙΚΩΝ (CYBER BULLING), ΡΑΤΣΙΣΤΙΚΩΝ – ΞΕΝΟΦΟΒΙΚΩΝ, ΕΚΒΙΑΣΤΙΚΩΝ ΜΗΝΥΜΑΤΩΝ ΣΤΑ ΜΕΣΑ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ (ΟΠΩΣ FACEBOOK, INSTAGRAM, TWITTER) ΚΑΙ Η ΑΠΟΘΗΚΕΥΣΗ ΤΩΝ ΜΗΝΥΜΑΤΩΝ ΑΥΤΩΝ ΣΤΟ CLOUD ΤΟΥ ΘΥΤΗ. ΖΗΤΗΜΑΤΑ - ΠΡΟΕΚΤΑΣΕΙΣ- ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΤΟΥ ΘΥΜΑΤΟΣ

Διπλωματική Εργασία

της

Κωνσταντίνας Α. Κεχαγιά

Θεσσαλονίκη, Ιούλιος, 2020

Η ΑΠΟΣΤΟΛΗ ΥΒΡΙΣΤΙΚΩΝ (CYBER BULLING), ΡΑΤΣΙΣΤΙΚΩΝ – ΞΕΝΟΦΟΒΙΚΩΝ, ΕΚΒΙΑΣΤΙΚΩΝ ΜΗΝΥΜΑΤΩΝ ΣΤΑ ΜΕΣΑ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ (ΟΠΩΣ FACEBOOK, INSTAGRAM, TWITTER) ΚΑΙ Η ΑΠΟΘΗΚΕΥΣΗ ΤΩΝ ΜΗΝΥΜΑΤΩΝ ΑΥΤΩΝ ΣΤΟ CLOUD ΤΟΥ ΘΥΤΗ. ΖΗΤΗΜΑΤΑ - ΠΡΟΕΚΤΑΣΕΙΣ-ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΤΟΥ ΘΥΜΑΤΟΣ

Κωνσταντίνα Α. Κεχαγιά

Πτυχίο Νομικής, ΑΠΘ, 2015

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΟ ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέποντες Καθηγητές:
Θεοχάρης Δαλακούρας
Κωνσταντίνος Ψάννης

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 14η Ιουλίου 2020

Θεοχάρης Δαλακούρας Κωνσταντίνος Ψάννης Χρήστος Μαστροκώστας

Κωνσταντίνα Α. Κεχαγιά

ΠΕΡΙΛΗΨΗ

Η παρούσα διπλωματική εργασία πραγματεύεται στο πρώτο της μέρος το ζήτημα της αποστολής υβριστικών (cyber bulling), ρατσιστικών, ξενοφοβικών, εκβιαστικών μηνυμάτων στα μέσα κοινωνικής δικτύωσης, στις γνωστές σε όλους μας ιστοσελίδες του Facebook, του Instagram, του Twitter ενώ στο δεύτερο, αυτό της αποθήκευσης των μηνυμάτων αυτών στο cloud του θύτη καθώς και των ζητημάτων που προκύπτουν από τις ενέργειες αυτές. Αρχικά, γίνεται αναφορά στην ελευθερία της έκφρασης και στο πώς η ίδια κατοχυρώνεται στο Σύνταγμά μας αλλά και στην Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου καθώς και στο ποιοί είναι οι φορείς και οι αποδέκτες του δικαιώματος αυτού. Εν συνεχεία, παρατίθενται οι εθνικές διατάξεις που απαγορεύουν τον προσβλητικό, μισαλλόδοξο και εκβιαστικό λόγο στο διαδίκτυο. Φυσικά, δεν θα μπορούσε να μην γίνει αναφορά στο διαδίκτυο και συγκεκριμένα στα μέσα κοινωνικής δικτύωσης με μια αναδρομή στο πότε έκαναν την εμφάνιση τους καθώς και στα ιδιαίτερα χαρακτηριστικά τους. Ο συνδετικός κρίκος μεταξύ των μέσων κοινωνικής δικτύωσης και του προσβλητικού, εκβιαστικού λόγου είναι οι αποφάσεις των Ελληνικών Δικαστηρίων που ρίχνουν φώς στο πώς η Ελληνική Δικαιοσύνη αντιμετωπίζει τις υποθέσεις ρατσιστικού και εκβιαστικού λόγου που διατυπώνεται μέσω των μέσων κοινωνικής δικτύωσης. Και όταν τα μηνύματα αυτά αποθηκεύονται στο cloud του εκφραστή του προσβλητικού, ρατσιστικού αυτού λόγου τι συμβαίνει; Στο δεύτερο και τελευταίο μέρος της παρούσας διπλωματικής εργασίας, γίνεται προσπάθεια μέσω της παράθεσης του ορισμού του cloud computing, των χαρακτηριστικών του, των υπηρεσιών που προσφέρει καθώς και των ζητημάτων που σχετίζονται γύρω από την ασφάλεια των δεδομένων στο σύννεφο (cloud), να δοθεί απάντηση στο ερώτημα αυτό. Αρωγοί αυτής της προσπάθειας, ο Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων, διάφορα αλλά νομοθετήματα της Ευρωπαϊκής Ένωσης και φυσικά η Ελληνική Δικαιοσύνη. Τέλος, όπως κάθε έρευνα, έτσι και αυτή που συντελείται με την παρούσα διπλωματική εργασία, ολοκληρώνεται με την παράθεση σε κάθε μέρος της τελευταίας ξεχωριστά συμπερασμάτων πάνω στα ζητήματα που εξετάστηκαν.

Λέξεις κλειδιά: ελευθερία της έκφρασης, προσβλητικός λόγος, εκβιαστικός λόγος, μέσα κοινωνικής δικτύωσης (social media), cloud computing

ABSTRACT

This thesis deals in the first part with the issue of sending cyber bullies, racist, xenophobic, blackmail on social media, the well-known websites of Facebook, Instagram, Twitter and at the second part the storage of these messages in the cloud of the victim and the issues that arise from these actions. Initially, there is a reference to freedom of expression and how it is enshrined in our Constitution and in the European Convention on Human Rights, as well as who are the beneficiaries and recipients of this right. Then, there are the national provisions, who are banning offensive, intolerant and blackmailing speech on the Internet. Of course, there could be no mention of the internet and in particular at the social media with a look back at when they appeared and their particular features. The link between social media and the offensive, blackmailing discourse is the judgments of the Greek Courts that shed light on how Greek Justice treats the cases of racist and blackmailing expressed through social media. And what happens when these messages are stored in the cloud of the exponent of the offensive and racist word? In the second and final part of this thesis, an attempt is made to answer this question with the definition of cloud computing, its features, the services it offers, and issues related to cloud data security. Supporters of this endeavor, the General Regulation on the Protection of Personal Data, various other legislation of the European Union and of course the Greek Justice. Finally, as with any research, as with the present diplomatic work, it concludes with a presentation of each of the last separate conclusions on the issues discussed.

Keywords: freedom of expression, offensive speech, blackmail, social media, cloud computing

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω τους εποπτεύοντες καθηγητές μου, κ.κ. Θεοχάρη Δαλακούρα και Κωνσταντίνο Ψάννη, για την συνεργασία και επικοινωνία, καθώς και για τις χρήσιμες παρατηρήσεις και συμβουλές που μου έδωσαν κατά την συγγραφή της παρούσας διπλωματικής εργασίας.

Επίσης, θα ήθελα να ευχαριστήσω την οικογένεια και τους φίλους μου για την πολύτιμη βοήθεια και στήριξη που μου έδειξαν όλο αυτό το χρονικό διάστημα έρευνας και συγγραφής της παρούσας διπλωματικής εργασίας.

ΠΕΡΙΕΧΟΜΕΝΑ **ΣΕΛΙΔΕΣ**

ΛΙΣΤΑ ΣΧΗΜΑΤΩΝ

ΕΙΣΑΓΩΓΗ

Οι ιστοσελίδες κοινωνικής δικτύωσης χρονολογούνται ήδη από τις αρχές της δεκαετίας του ’90. Πρόσφατα τα ψηφιακά κοινωνικά δίκτυα έχουν εξελιχθεί σημαντικά σε ό,τι αφορά την επέκταση, την πολυπλοκότητα και την απήχησή τους. Ήταν ωστόσο η γεωμετρική αύξηση του αριθμού των χρηστών του Facebook αρχικά – αργότερα των άλλων μέσων κοινωνικής δικτύωσης (Instagram, Twitter, κ.ά), που κατέστησε τα δίκτυα αυτά κοινωνικό φαινόμενο και έδωσε νέα διάσταση στη δημόσια και νομική συζήτηση για την ιδιωτικότητα και την επικοινωνία στο διαδίκτυο. Το Facebook είναι ίσως ο πλέον γνωστός και δημοφιλής σε παγκόσμια κλίμακα ιστότοπος κοινωνικής δικτύωσης. Μια βασική παράμετρος της επιτυχίας, όχι μόνο αυτού αλλά και των υπολοίπων μέσων κοινωνικής δικτύωσης που ακολούθησαν μετά από αυτό, έγκειται καταρχήν στη δυνατότητα που προσφέρει στους χρήστες να συνδυάσουν σε ένα μέσο την επικοινωνία, τη δημιουργία διαδικτυακών επαφών και σχέσεων, την έκφραση, την ψυχαγωγία αλλά και πλέον ποικίλλες δραστηριότητες επαγγελματικού, οικονομικού ή και πολιτικού χαρακτήρα.

Παράλληλα, τα μέσα κοινωνικής δικτύωσης, εκτός των ανωτέρων δυνατοτήτων που προσφέρουν, χρησιμοποιούνται ως μέσα και πεδία για τη διάδοση πληροφοριών που δεν αφορούν απαραιτήτως χρήστες ή μέλη του δικτύου. Μάλιστα ο δημόσιος και επιστημονικός διάλογος για τα δίκτυα αυτά επικεντρώνεται συνήθως στην αυτό-έκθεση των χρηστών ή στην χρήση των πληροφοριών (που αναρτούν οι ίδιοι οι χρήστες) από τα μέσα κοινωνικής δικτύωσης ή τρίτους. Φυσικά, δεν πρέπει να διαφεύγει της προσοχής μας ότι η ανάρτηση πληροφορίας μπορεί να έχει επιπτώσεις σε τρίτους, «μη φίλους» και «μη χρήστες»: εκτός από την προσβολή δικαιωμάτων τρίτων που ενέχει για παράδειγμα η ανάρτηση ειδήσεων ή φωτογραφιών που αφορούν και περιλαμβάνουν και πρόσωπα πέραν του χρήστη, η ανάρτηση πληροφορίας στο Facebook, στο Instagram, στο Twitter, ενδέχεται να περιλαμβάνει και άλλο, ενίοτε προσβλητικό και δυσφημιστικό υλικό.

Ένα πάντως είναι σίγουρο: το Διαδίκτυο συγκροτεί ένα νέο πεδίο επικοινωνίας και δραστηριότητας αλλά και ταυτόχρονα ρέπλικα του εξωδικτυακού, του «πραγματικού» κόσμου και κατά συνέπεια πεδίο, και μάλιστα πρόσφορο, παραβατικότητας και προσβολής δικαιωμάτων. Το Διαδίκτυο μεταλλάσσει τον τρόπο και την ταχύτητα διάδοσης της πληροφορίας αλλά ταυτόχρονα η ευχέρια διανομής πληροφοριών και πρόσβασης στις πληροφορίες αυτές περιορίζει δραστικά τον έλεγχο που έχουν τα άτομα επί της φήμης τους. Και όπως πολύ εύστοχα αναφέρει ο J. Blocher στο Reputation as Property in Virtual Economies, « *εάν η φήμη κάποιου καταστρέφεται ενδοδικτυακά*

καταστρέφεται και εξωδικτυακά», καθώς ο online κόσμος και ο offline κόσμος είναι προφανώς και αναπόφευκτα, συγκοινωνούντα περιβάλλοντα.

Μέσα από την παρούσα διπλωματική εργασία γίνεται μία προσπάθεια στο να αναδειχθούν ζητήματα που σχετίζονται με την εποχή και τον κόσμο στον οποίο ζούμε. Δυστυχώς στις μέρες μας, οι άνθρωποι φαίνεται να έχουν μπερδέψει τα όρια ανάμεσα στο δικαίωμα της ελευθερία της έκφρασης της γνώμης τους και στο δικαίωμα της προστασίας της προσωπικότητας του κάθε ανθρώπου στον οποίον άμεσα ή έμμεσα απευθύνουν την γνώμη τους. Με «όπλο» τα μέσα κοινωνικής δικτύωσης και την ανωνυμία που αυτά μπορούν να προσφέρουν, με προσβλητικό, υβριστικό ακόμη και εκβιαστικό τρόπο στρέφονται κατά του συνανθρώπου τους αδιαφορώντας για τις συνέπειες που μπορούν να προκληθούν από τον λόγο τους, ανάμεσα στις οποίες είναι και η στο διηνεκές ύπαρξη των εκβιαστικών, ρατσιστικών, εκβιαστικών αυτών μηνυμάτων στο γνωστό σε όλους μας σύννεφο.

Η παρούσα διπλωματική εργασία διαρθρώνεται σε δύο μέρη. Αρχικά, στο πρώτο μέρος και στο πρώτο κεφάλαιο αυτής, αναπτύσσεται το ζήτημα της ελευθερίας και συγκεκριμένα της ελευθερίας της έκφρασης και στο πώς η ίδια κατοχυρώνεται στο Σύνταγμά μας αλλά και στην Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου καθώς και στο ποιοι είναι οι φορείς και οι αποδέκτες του δικαιώματος αυτού. Στο δεύτερο κεφάλαιο, γίνεται αναφορά στις εθνικές διατάξεις που απαγορεύουν τον προσβλητικό, μισαλλόδοξο και εκβιαστικό λόγο στο διαδίκτυο, ενώ στο τρίτο αναλύεται το ζήτημα των μέσων κοινωνικής δικτύωσης. Στο τέταρτο κεφάλαιο παρουσιάζεται νομολογία που σχετίζεται με την ποινική αντιμετώπιση εκδηλώσεων ρατσισμού ξενοφοβίας, εξύβρισης, και εκβιασμού στο διαδίκτυο. Τέλος, το πρώτο μέρος ολοκληρώνεται με την παράθεση στατιστικών στοιχείων της ελληνικής αστυνομίας αναφορικά με την δίωξη των εγκλημάτων που διαπράττονται μέσω διαδικτύου ή με τη χρήση αυτού στο πέμπτο κεφάλαιο, ενώ στο έκτο παραθέτονται συμπεράσματα που προέκυψαν από τα παραπάνω κεφάλαια.

Στο δεύτερο μέρος, η παρούσα διπλωματική εργασία αποκτά τεχνολογική χροιά καθώς πραγματεύεται το ζήτημα του cloud computing. Ειδικότερα, στο πρώτο κεφάλαιο γίνεται αναφορά στο cloud computing και συγκεκριμένα στα ιδιαίτερα χαρακτηριστικά του που προκύπτουν από τον ορισμό του που παρατίθεται καθώς και από τα είδη των υπηρεσιών, άλλως cloud models, που προσφέρει. Στο δεύτερο κεφάλαιο, γίνεται λόγος για ένα από τα μοντέλα του cloud computing, αυτό του Storage as a service (StaaS), ενώ στο τρίτο αναφερόμαστε στα ζητήματα ασφαλείας που προκύπτουν στο σύννεφο (cloud). Στο τέταρτο κεφάλαιο συντελείται σύμπραξη του νόμου με την τεχνολογία καθώς αναπτύσσονται ζητήματα και ταυτόχρονα ερωτήματα που σχετίζονται με την

ύπαρξη των προσωπικών δεδομένων στο σύννεφο και τους κινδύνους που επιφυλάσσει η ύπαρξη αυτή, στα οποία δίνονται απαντήσεις με την αρωγή πρωτίστως του Γενικού Κανονισμού για την Προστασία των Προσωπικών Δεδομένων καθώς και άλλων νομοθετημάτων. Τέλος, το δεύτερο μέρος ολοκληρώνεται με την παράθεση στοιχείων της Ελληνικής Δικαιοσύνης που σχετίζονται με το Cloud Computing στο πέμπτο κεφάλαιο, ενώ στο έκτο παραθέτονται συμπεράσματα που προέκυψαν από τα παραπάνω κεφάλαια.

Α' ΜΕΡΟΣ

Α. Η ΕΛΕΥΘΕΡΙΑ ΤΗΣ ΕΚΦΡΑΣΗΣ ΓΕΝΙΚΑ

Η ελευθερία της έκφρασης αποτελεί χωρίς αμφιβολία ένα από τα κύρια θεμέλια μιας δημοκρατικής κοινωνίας. Αυτό ίσχυε ανέκαθεν (πρβλ. άρθρο 1 της γαλλικής διακήρυξης των Δικαιωμάτων του ανθρώπου και του Πολίτη του 1789 «Η ελεύθερη διάδοση των σκέψεων και των γνωμών είναι ένα από τα πολυτιμότερα δικαιώματα του ανθρώπου»), ισχύει όμως σε αυξημένο βαθμό και σήμερα στη μεταβιομηχανική κοινωνία.

Στο παρόν κεφάλαιο θα γίνει μια σύντομη αναφορά στις κυριότερες διεθνείς συμβάσεις, που έχουν κυρωθεί από την Ελλάδα και έχουν δεσμευτική ισχύ και κατοχυρώνουν την ελευθερία έκφρασης, δίνοντας έμφαση στην Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου και στο Ελληνικό Σύνταγμα

1. Έννοια και ratio της συνταγματικής κατοχύρωσης της ελευθερίας της έκφρασης κατά το εθνικό Σύνταγμα και περιορισμοί αυτής.

Σύμφωνα με το άρθρο 14 παρ. 1 του Συντάγματος «1. *Καθένας μπορεί να εκφράζει και να διαδίδει προφορικά, γραπτά και δια του τύπου τους στοχασμούς του τηρώντας τους νόμους του Κράτους*». Στο άρθρο αυτό εμπεριέχεται η αντικειμενική αρχή της ελευθερίας των ιδεών. Το Σύνταγμα, με την κατοχύρωση της ελευθερίας των ιδεών ως αντικειμενική αρχή, προσδίδει σε αυτή ιδιαίτερα μεγάλη σημασία για το όλο δικαιοπολιτικό μας σύστημα αλλά και για τον έκαστο φορέα αυτής. Όπως αναφέρει και ο Δημητρόπουλος, στο βιβλίο του «Συνταγματικά Δικαιώματα, Γενικό Μέρος-Ειδικό Μέρος: Μητρικά Δικαιώματα- Φυσική Υπόσταση- Πνευματική Υπόσταση, Σύστημα Συνταγματικού Δικαίου», η ελευθερία των ιδεών μπορεί να αναλυθεί σε τρεις μερικότερες ελευθερίες, α) την ελευθερία πίστης, δηλαδή την ελευθερία συνείδησης, ύπαρξης και «κατοχής» ιδεών, β) την ελευθερία παραγωγής ιδεών, δηλαδή την ελευθερία σκέψης, στοχασμών, και γ) την ελευθερία έκφρασης των ιδεών, δηλαδή την ελευθερία κυκλοφορίας και διάδοσης των ιδεών. Αν μπορούσαμε να αναλύσουμε τον όρο «ιδέα», (με την ευρύτατη έννοια του όρου), θα τον ορίζαμε ως οποιαδήποτε αναφορά του ανθρώπινου πνεύματος. Ιδέα συνεπώς, είναι οποιαδήποτε αντίληψη, οποιαδήποτε σκέψη, οποιαδήποτε κρίση. Αν θέλαμε βέβαια να αποδώσουμε στον παραπάνω όρο τον ακριβή εννοιολογικό προσδιορισμός του, θα παρατηρούσαμε ότι έχει απασχολήσει ιδιαίτερως τόσο την φιλοσοφία όσο και άλλους χώρους της επιστήμης. Οι όροι «ιδέα» και «στοχασμός» συνδέονται πολύ στενά. Στοχασμός, είναι η πνευματική λειτουργία του ανθρώπινου εγκεφάλου της οποίας αποτέλεσμα είναι η ιδέα. Προηγείται δηλαδή η σκέψη και έπεται η ιδέα. Ο όρος «στοχασμός» χρησιμοποιείται επίσης διττά. Δηλώνει την εγκεφαλική λειτουργία αλλά και το

αποτέλεσμά της, χρησιμοποιείται δηλαδή και ως συνώνυμο της ιδέας. Ο όρος «στοχασμός» χρησιμοποιείται από τον συντακτικό νομοθέτη στο άρθρο 14 παρ. 1 ως συνώνυμο της ιδέας.

Από την άλλη πλευρά, **η έκφραση** αναφέρεται κυρίως στην εξωτερίκευση της ιδέας, της συνείδησης του ανθρώπου. Εν αντιθέσει με την συνείδηση που είναι εσωτερική, η έκφραση έχει εξωτερική υπόσταση, και αφορά κυρίως την προς τα έξω εμφάνιση της συνείδησης. Συνώνυμος προς την έκφραση είναι και ο λόγος με την ευρύτερη έννοια του όρου.

Την ελευθερία της έκφρασης μπορούμε να την διακρίνουμε με δύο έννοιες.: α) την θετική ελευθερία έκφρασης και β) την αρνητική ελευθερία της έκφρασης. Όταν μιλάμε για θετική ελευθερία της έκφρασης, μιλάμε για το δικαίωμα να έχεις, να εκφράζεις, να λαμβάνεις, να διαμορφώνεις, και να διαδίδεις γνώμες αλλά ως ένα σημείο και πληροφορίες χωρίς όμως να υφίσταται καμία παρεμπόδιση, παρενόχληση ή δυσμενή έννομη συνέπεια. Και αυτό γιατί η αλήθεια της γνώμης δεν έχει καμία νομική σημασία, αφού δεν προστατεύεται μόνον η «ορθή» αλλά και η «λανθασμένη» γνώμη. Με άλλα λόγια, δεν προστατεύεται μόνο η κρατούσα, αλλά και η μη κρατούσα, η μειοψηφούσα γνώμη, η οποία μάλιστα έχει και ιδιαίτερη ανάγκη προστασίας. Φυσικά, αξίζει να αναφέρουμε ότι η θετική ελευθερία της έκφρασης περιλαμβάνει και την ελευθερία να εκφράζεται κανείς με όποιον τρόπο, όχι απαραίτητα γλωσσικό (π.χ νοήματα, ενδυμασίες κ.λ.π) και πάντως σε όποια γλώσσα αυτός επιθυμεί. Κάτι τέτοιο όμως δεν ισχύει, όταν δεν πρόκειται για άσκηση της ελευθερίας της έκφρασης, αλλά για επιτέλεση νόμιμου καθήκοντος, όπως για παράδειγμα η σύνταξη δημοσίου εγγράφου. Εκεί ισχύει άλλη αρχή: η αρχή, να μπορεί ο πολίτης να επικοινωνεί στη γλώσσα του με τη δημόσια εξουσία στην οποία υπόκειται. Και αυτό γιατί, σύμφωνα με την αρχή της λαϊκής κυριαρχίας, «*όλες οι εξουσίες πηγάζουν από το λαό και επομένως γλώσσα στην οποία εκφράζεται δημόσια εξουσία δεν μπορεί να είναι άλλη από τη γλώσσα του λαού»,* όπως αναφέρει και στην Εισήγησή του επί της με αριθ. 5148/1987 απόφασης του ΣτΕ ο δικαστικός Βασίλειος Μποτόπουλος.

Επιπλέον, στο άρθρο 14 παρ. 1 του Συντάγματος, κατοχυρώνεται, από την άλλη πλευρά, και η αρνητική ελευθερία της έκφρασης. Με την χρήση του δυνητικού *«καθένας μπορεί»* συνάγεται εξ αντιδιαστολής το συμπέρασμα, ότι καθένας δεν υποχρεούται να εκφράσει τις γνώμες του. Παρ' όλα αυτά, μπορεί να επιβληθεί υποχρέωση παροχής πληροφοριών, στοιχείων, όπως για παράδειγμα για ανακριτικούς, φορολογικούς ή στατιστικούς σκοπούς, μέσα όμως στα όρια που διαγράφονται, κατοχυρώνονται και περιγράφονται στο άρθρο 5 παρ. 1 του Συντάγματος, με την προστασία της προσωπικότητας.

Στο σημείο αυτό, αξίζει να αναφέρουμε ότι η χρήση του δικαιώματος της ελευθερίας της έκφρασης δεν είναι απεριόριστη, αλλά τελεί υπό τη γενική επιφύλαξη του νόμου «τηρώντας τους

νόμους του Κράτους». Και αυτό συμβαίνει, όταν η άσκησή της υπάγεται σε καθεστώς προηγούμενης διοικητικής άδειας. Στην έννοια βέβαια των κατά το άρθρο 14 του Συντάγματος *«νόμων του κράτους»* γίνεται δεκτό, ότι συμπεριλαμβάνονται και οι ουσιαστικοί νόμοι. Η νομολογία ερμηνεύει τη ρήτρα αυτή με την έννοια ότι αναφέρεται στους γενικούς νόμους. Τέτοιοι δεν είναι όσοι επιδιώκουν την με οποιοδήποτε τρόπο παρεμπόδιση της έκφρασης και διάδοσης γνώμης ή ιδέας ή πληροφορίας ή του ελέγχου των πράξεων ή παραλείψεων των κρατικών οργάνων στην άσκηση των καθηκόντων τους, διότι θα παραβίαζαν το άρθρο 14 του Συντάγματος. Αντίθετα, θεωρούνται θεμιτοί όσοι νόμοι συμβάλλουν στην προστασία τόσο του ατόμου όσο και του κοινωνικού συνόλου από την καταχρηστική άσκηση του δικαιώματος της ελεύθερης έκφρασης γνώμης ή διάδοσης πληροφοριών. Η αναφορά άλλωστε στην καταχρηστική άσκηση δικαιώματος μάλλον δυσχεραίνει το πρόβλημα, χωρίς να προσφέρει τίποτα ουσιαστικό στο δικανικό συλλογισμό.

Περιορισμό της ελευθερίας της έκφρασης, θα υποστήριζε κανείς, ότι θεσπίζουν οι διατάξεις του Ποινικού Κώδικα, οι οποίες κατοχυρώνουν και επιβάλλουν ποινές στα εγκλήματα κατά της τιμής. Περιορισμός ο οποίος είναι αυτονόητος, αν αναλογιστεί κανείς, ότι το άρθρο 5 παρ. 2 του Συντάγματος επιτάσσει την απόλυτη προστασία της τιμής όλων όσοι βρίσκονται στην Ελληνική Επικράτεια, χωρίς βέβαια να παύει να είναι απαραίτητη και εδώ μια εναρμόνιση μεταξύ της προστασίας αυτής αφενός και του δικαιώματος για άσκηση κριτικής αφετέρου.

Παράλληλα, περιορισμοί στην ελευθερία της έκφρασης γίνεται δεκτό εξάλλου ότι μπορούν να θεσπιστούν για λόγους που αφορούν την προστασία της ξένης ιδιοκτησίας, της υγείας, της προστασίας του φυσικού και πολιτιστικού περιβάλλοντος. Επομένως, η απαγόρευση της αναγραφής λέξεων ή φράσεων ή συμβόλων σε τείχους ή σε άλλες επιφάνειες ιστορικών ιδίως μνημείων, δημοσίων κτιρίων, που δεν ανήκουν στην ιδιοκτησία όποιου γράφει τα παραπάνω, είναι συνταγματικά κατοχυρωμένη.

Επιπλέον, ειδική μνεία πρέπει να γίνει και στο άρθρο 5Α παρ. 1 του Συντάγματος όπου κατοχυρώνεται ένα γενικότερο δικαίωμα στην πληροφόρηση. Ειδικότερα, σύμφωνα με το άρθρο αυτό: *«Καθένας έχει δικαίωμα στην πληροφόρηση, όπως νόμος ορίζει. Περιορισμοί στο δικαίωμα αυτό είναι δυνατόν να επιβληθούν με νόμο εφόσον είναι απολύτως αναγκαίοι και δικαιολογούνται για λόγους εθνικής ασφάλειας, καταπολέμησης του εγκλήματος ή προστασίας των δικαιωμάτων και συμφερόντων τρίτων».*

Περιεχόμενο του δικαιώματος αυτού είναι τόσο η κατοχύρωση του πληροφορείν, όσο και η κατοχύρωση του πληροφορείσθαι. Οι ελευθερίες αυτές βέβαια προστατεύονταν μέσω των

υπαρχουσών και πριν την αναθεώρηση διατάξεων, όπως αναπτύχθηκε ανωτέρω. Η αυξανόμενη όμως παρουσία και επιρροή των μέσων μαζικής ενημέρωσης οδήγησε στην ρητή καθιέρωσή τους από τον αναθεωρητικό νομοθέτη.

Σημαντικοί είναι οι περιορισμοί που προβλέπει για το δικαίωμα αυτό η πρώτη παράγραφος του άρθρου 5Α του Συντάγματος. Περιορισμοί, που πρέπει να πληρούν τους όρους που θέτει η αρχή της αναλογικότητας, η οποία υπονοείται μέσω της φράσης «*απολύτως αναγκαίοι*». Οι θεμιτοί λόγοι περιορισμού συνεπώς πρέπει να ερμηνεύονται στενά. Έτσι, η εθνική ασφάλεια περιλαμβάνει μόνο την εξωτερική απειλή για το κράτος και κυρίως θέματα που αφορούν την εθνική άμυνα. Η καταπολέμηση του εγκλήματος αναφέρεται σε σοβαρά εγκλήματα, κυρίως κακουργηματικού χαρακτήρα. Τέλος, η προστασία των δικαιωμάτων των τρίτων αποτελεί έτσι κι αλλιώς το όριο όλων των δικαιωμάτων προκειμένου να είναι δυνατή η εναρμονισμένη άσκησή τους.

2. Η έννοια της ελευθερίας της έκφρασης κατά την ΕΣΔΑ

Στο άρθρο 10 της Ευρωπαϊκής Σύμβασης των Δικαιωμάτων του Ανθρώπου κατοχυρώνεται το δικαίωμα στην έκφραση της γνώμης. Ειδικότερα, σύμφωνα με τον άρθρο αυτό: «*1. Παν πρόσωπον έχει δικαίωμα εις την ελευθερία εκφράσεως. Το δικαίωμα τούτο περιλαμβάνει την ελευθερία γνώμης ως και την ελευθερία λήψεως ή μεταδόσεως πληροφοριών ή ιδεών, άνευ επεμβάσεως δημοσίων αρχών και ασχέτως συνόρων. Το παρόν άρθρο δεν κωλύει τα Κράτη από του να υποβάλωσι τας επιχειρήσεις ραδιοφωνίας, κινηματογράφου ή τηλεοράσεως εις κανονισμούς εκδόσεως αδειών λειτουργίας. 2. Η άσκηση των ελευθεριών τούτων, συνεπαγόμενων καθήκοντα και ευθύνες δύναται να υπαχθεί εις ορισμένες διατυπώσεις, όρους, περιορισμούς ή κυρώσεις, προβλεπόμενους υπό του νόμου και αποτελούντες αναγκαία μέτρα εν δημοκρατική κοινωνία δια την εθνική ασφάλειαν, την εδαφική ακεραιότητα ή δημοσία ασφάλεια, την προάσπιση της τάξεως και πρόληψη του εγκλήματος, την προστασία της υπολήψεως ή των δικαιωμάτων των τρίτων, την παρεμπόδιση της κοινολογήσεως εμπιστευτικών πληροφοριών ή την διασφάλιση του κύρους και αμεροληψίας της δικαστικής εξουσίας».*

Στο άρθρο 10 φανερώνεται ρητώς ότι στο δικαίωμα της ελευθερίας της έκφρασης, περιλαμβάνεται η ελευθερία της γνώμης και η ελευθερία λήψης ή μετάδοσης πληροφοριών χωρίς παρέμβαση από τις αρχές και χωρίς συνοριακούς περιορισμούς. Η ελευθερία της γνώμης αποτελεί ουσιώδες στοιχείο της ελευθερίας της έκφρασης και περιλαμβάνει την ελευθερία του ατόμου να διαμορφώνει την γνώμη μου, να την αλλάζει πάντα με τη βούλησή του και φυσικά να την αποσιωπά. Η ελευθερία της πληροφορίας συμβάλλει σημαντικά στην διαμόρφωση και την έκφραση γνώμης. Η ελευθερία της γνώμης είναι στενά συνδεδεμένη αλλά ευρύτερη από την ελευθερία της σκέψης, την οποία κατοχυρώνει το άρθρο 9 της ως άνω Σύμβασης.

Το ΕΔΔΑ ερμηνεύει διασταλτικά τις έννοιες «πληροφορίες» και «ιδέες». Η έννοια της πληροφορίας δεν καλύπτει μόνο γεγονότα και ειδήσεις, ή ζητήματα τα οποία απασχολούν το ευρύ σύνολο και συζητούνται στον Τύπο. Πληροφορία συνιστά και η διαφήμιση στον τύπο, τα περιοδικά, οι φωτογραφίες, η τηλεοπτική διαφήμιση, η διατύπωση κριτικής. Αβίαστα επομένως προκύπτει το συμπέρασμα ότι, η προστασία της ελευθερίας της έκφρασης δεν περιορίζεται στο σύνηθες πεδίο ανταλλαγής πολιτικών, θρησκευτικών, φιλοσοφικών, ιστορικών απόψεων και δεν προσδιορίζεται από τη σημασία της πληροφορίας, το περιεχόμενο και την ποιότητά της. Εξάλλου, σύμφωνα με το ΕΔΔΑ, το άρθρο 10 βρίσκει εφαρμογής ακόμη και σε πληροφορίες και ιδέες, οι οποίες δύνανται να γίνουν προσβλητικές, σοκαριστικές ή ενοχλητικές. Και αυτό γιατί το άρθρο 10 δεν προστατεύει μόνο την ουσία και το περιεχόμενο των απόψεων, αλλά και τον τρόπο έκφρασης ή το μέσο διάδοσης αυτών.

Στη δεύτερη παράγραφο γίνεται αναφορά στους περιορισμούς που μπορούν να επιβληθούν στο δικαίωμα έκφρασης. Η διατύπωση, μπορεί να είναι παρόμοια με αυτή του Συμφώνου, αλλά στην ΕΣΔΑ γίνεται ειδικότερη και πιο σαφής αναφορά στα συμφέροντα της κοινωνίας υπέρ των οποίων δύναται να καμφθεί η ελευθερία έκφρασης, όπως η εδαφική ακεραιότητα, η δημόσια ασφάλεια, και η πρόληψη του εγκλήματος (αντί του όρου δημόσια τάξη), η παρεμπόδιση αποκάλυψης και διάδοσης εμπιστευτικών πληροφοριών και η διασφάλιση του κύρους και της αμεροληψίας της δικαιοσύνης. Οι περιορισμοί βέβαια σε κάθε περίπτωση πρέπει να προβλέπονται από το νόμο, να εξυπηρετούν ένα θεμιτό σκοπό και φυσικά να είναι αναγκαίοι σε μια δημοκρατική κοινωνία. Η φράση *«να προβλέπονται από το νόμο»* δεν έχει μόνο την έννοια της αρχής nullum crimen sine lege, δηλαδή την έννοια να έχει θεσπιστεί συγκεκριμένη διάταξη ή συγκεκριμένος νόμος. Έχει πολύ περισσότερο την έννοια η διάταξη που προβλέπει τον περιορισμό να είναι σαφής και ακριβής, ώστε να μπορεί ο καθένας να ρυθμίζει εκ των προτέρων τη συμπεριφορά του και έτσι να μην προβαίνει σε παράνομες πράξεις. Θα πρέπει δηλαδή να μπορεί να προβλέψει ότι μια συμπεριφορά του θα μπορούσε να αποτελεί μέρος αυτής που περιορίζεται βάσει νόμου, ώστε να την αποφύγει. Πρόκειται για τη σαφήνεια και την προβλεψιμότητα του νόμου.

Παράλληλα, η φράση *«να εξυπηρετούν ένα θεμιτό σκοπό»* αναφέρεται στα έννομα αγαθά και συμφέροντα, των οποίων όμως η προστασία δικαιολογεί τον περιορισμό της ελευθερίας της έκφρασης σε ορισμένες περιπτώσεις. Αυτά θα μπορούσαν να χωριστούν σε δυο κατηγορίες: α) η πρώτη κατηγορία αφορά τα συμφέροντα της κοινωνίας ως συνόλου, όπως η δημόσια τάξη και ασφάλεια, η εδαφική ακεραιότητα και η πρόληψη του εγκλήματος και β) η δεύτερη κατηγορία αφορά τα δικαιώματα των τρίτων που μπορεί να θίγονται από μια συμπεριφορά ή έκφραση. Αξίζει

να αναφέρουμε ότι σύμφωνα με το Δικαστήριο η αναφορά των συμφερόντων αυτών στο άρθρο 10 είναι εξαντλητική.

Κλείνοντας, η φράση «*να είναι αναγκαίοι σε μια δημοκρατική κοινωνία»* έχει την έννοια ότι οι περιορισμοί θα πρέπει να είναι απαραίτητοι και κατάλληλοι να εξυπηρετήσουν τους θεμιτούς σκοπούς που τίθενται ανάλογα με τις ανάγκες της δημοκρατικής κοινωνίας. Θα πρέπει δηλαδή να επιλέγονται εκείνοι που εξυπηρετούν καλύτερα τα συμφέροντά της. Εξετάζοντας το ΕΔΔΑ τη ρήτρα αυτή αναζητεί την ύπαρξη μιας «επιτακτικής κοινωνικής ανάγκης», που επιβάλλει τον περιορισμό της ελευθερίας έκφρασης της γνώμης και προχωρά σε στάθμιση ανάμεσα στο δικαίωμα έκφρασης και τον επιδιωκόμενο νόμιμο σκοπό. Σε κάθε περίπτωση, η αρχή της αναλογικότητας, αν και δεν αναφέρεται ρητά στο άρθρο 10, είναι ένα σημαντικό εργαλείο για να εξετάσει το Δικαστήριο, αν τα μέτρα περιορισμού της έκφρασης ήταν κατάλληλα και για την προστασία του θεμιτού σκοπού. Ειδικότερα, ο περιορισμός πρέπει – όπως επιτάσει η αρχή της αναλογικότητας - να είναι α) πρόσφορος για την επίτευξη του αποτελέσματος, β) ο λιγότερο επαχθής και επώδυνος για το δικαίωμα έκφρασης και γ) ανάλογος προς το θεμιτό σκοπό που επιδιώκεται.

3. Φορείς και Αποδέκτες

Φορείς του δικαιώματος ελεύθερης έκφρασης είναι χωρίς διάκριση οι Έλληνες αλλά και οι αλλοδαποί, όπως καθίσταται σαφές από την ίδια τη διατύπωση του άρθρου 14 παρ. 1 του Συντάγματος. Φυσικά, φορείς είναι και τα νομικά πρόσωπα ιδιωτικού δικαίου, αφού συχνά με την έκφραση της συλλογικής γνώμη προωθούνται αποτελεσματικά οι σκοποί τους (π.χ ψήφισμα της γενικής συνέλευσης σωματείου ή έκδοση ανακοίνωσης από τη διοίκησή του), αλλά και ενώσεις προσώπων χωρίς νομική προσωπικότητα, όπως ιδίως τα πολιτικά κόμματα. Επίσης, τα νομικά πρόσωπα δημοσίου δικαίου υπό προϋποθέσεις, δύνανται να είναι φορείς του δικαιώματος αυτού. Έτσι για παράδειγμα τα αρμόδια όργανα των Α.Ε.Ι μπορούν να εκφέρουν τη γνώμη τους, ως εκφραστές των αντίστοιχων ιδρυμάτων, για μεταρρυθμίσεις ή μέτρα που σχεδιάζει το Υπουργείο Παιδείας να επιβάλλει στην ανώτατη εκπαίδευση.

Αποδέκτης, από την άλλη πλευρά, δεν είναι μόνο η κρατική εξουσία, αλλά και οι ιδιώτες. Και αυτό γιατί το άρθρο 14 παρ. 1 του Συντάγματος δεν φαίνεται να διαφοροποιεί ανάλογα με την κατεύθυνση από την οποία προέρχεται η κατά της ελευθερίας απειλή, αφετέρου διότι η τελευταία μπορεί να προκύψει ακριβώς από αυτούς. Το ΕΔΔΑ εξάλλου δέχεται ότι φορείς της ελευθερίας της έκφρασης είναι φυσικά και νομικά πρόσωπα. Το ΕΔΔΑ συγκεκριμένα έχει δεχθεί προσφυγές στις οποίες εταιρείες, ενώσεις προσώπων, καθώς και πολιτικά κόμματα επικαλέστηκαν το άρθρο 10. Το

άρθρο 10 εφαρμόζεται ανεξαρτήτως της ιδιότητας του φυσικού προσώπου ή της φύσης των δραστηριοτήτων του νομικού προσώπου.

Κλείνοντας, στο σημείο αυτό, μετά και την ως άνω λεπτομερή αναφορά στην έννοια αλλά και στην ratio της συνταγματικής κατοχύρωσης της ελευθερίας της έκφρασης κατά το εθνικό μας Σύνταγμα, στους περιορισμούς που θέτει αυτό, αλλά και στην ερμηνεία που δίνει η Ευρωπαϊκή Σύμβαση των Δικαιωμάτων των Ανθρώπων στην έννοια της ελευθερίας της έκφρασης καθώς και στους φορείς και του αποδέκτες αυτής, κρίνεται σκόπιμο να αναφέρουμε πως η «χρήση» του δικαιώματος αυτού πρέπει πάντοτε να γίνεται στα πλαίσια που προστάζει ο νόμος, να μην προσβάλλεται η ανθρώπινη αξιοπρέπεια και φυσικά πάντα σύμφωνα με την αρχή της αναλογικότητας που κατοχυρώνεται στο άρθρο 25 του Συντάγματος.

Η αξία του ανθρώπου πρέπει να διαφυλάσσεται από οποιαδήποτε έκφραση και με οποιονδήποτε τρόπο ή μέσο αυτή εκδηλώνεται και αυτό μάλιστα συντελείται όχι μόνο με τις ως άνω γενικές διατάξεις που κατοχυρώνουν το δικαίωμα στην ελευθερία της έκφρασης αλλά και με ειδικότερες διατάξεις που απαγορεύουν τον ρατσιστικό, εκβιαστικό, προσβλητικό και μισαλλόδοξο λόγο, για τις οποίες θα γίνει αναφορά στο κεφάλαιο που ακολουθεί με εξειδικεύσεις όσον αφορά τον τρόπο που διατυπώνονται τα «είδη» αυτά λόγου (ήτοι ρατσιστικός προσβλητικός, εκβιαστικός) και συγκεκριμένα την αναφορά τους στα social media.

Β. ΕΘΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΠΟΥ ΑΠΑΓΟΡΕΥΟΥΝ ΤΟΝ ΠΡΟΣΒΛΗΤΙΚΟ, ΜΙΣΑΛΛΟΔΟΞΟ ΚΑΙ ΕΚΒΙΑΣΤΙΚΟ ΛΟΓΟ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

1. Η Ελληνική Νομοθεσία για την Ποινική Αντιμετώπιση Εκδηλώσεων Ρατσισμού, Ξενοφοβίας, Εξύβρισης, και Εκβιασμού στο διαδίκτυο.

1.1.Νομοθεσία για την Ποινική Αντιμετώπιση Εκδηλώσεων Ρατσισμού και Ξενοφοβίας

1.1.1. Ο προηγούμενος Ν. 927/1979 «*περί κολασμού πράξεων ή ενεργειών αποσκοπουσών εις φυλετικάς διακρίσεις*»

Σκόπιμο κρίνεται, προκειμένου να γίνει μια διεύρυνση των νομικών ζητημάτων που αφορούν την αντιρατσιστική νομοθεσία γενικότερα, να γίνει μία αναφορά στον προηγούμενο Ν.927/1979, που αν και υπήρξε για πάνω από 40 χρόνια, εφαρμόστηκε ελάχιστες φορές.

- Οι ρυθμίσεις του (παλαιού) νόμου

Ο Ν. 927/1979 τυποποιούσε τέσσερα αδικήματα δόλου με στόχο την αποτροπή διακρίσεων σε βάρος προσώπου ή ομάδας προσώπων λόγω της φυλετικής ή εθνικής τους καταγωγής, ή λόγω

του θρησκεύματός τους. Στο πρώτο του άρθρο και συγκεκριμένα στην πρώτη παράγραφο αυτού, υπήρχε η τυποποίηση ενός εγκλήματος προτροπής σε πράξεις ή ενέργειες που μπορούν να προκαλέσουν διακρίσεις σε πράξεις ή ενέργειες που μπορούν να προκαλέσουν διακρίσεις, μίσος ή βία εναντίον προσώπου ή ομάδας προσώπων εξ αιτίας και μόνον της φυλετικής ή εθνικής καταγωγής ή του θρησκεύματός τους. Στην παράγραφο 2 του άρθρου 1 του Ν. 927/1979 προβλεπόταν το έγκλημα της σύστασης ή συμμετοχής σε οργάνωση που προωθεί τις συγκεκριμένες διακρίσεις. Η έννοια της οργάνωσης έχει ερμηνευθεί ως κάθε σύνολο ή ένωση προσώπων, νόμιμο ή παράνομο, εφόσον διακρίνεται από στοιχειώδη στοιχεία οργάνωσης όπως διοίκηση, ιεραρχία, συντονισμό και κοινό σκοπό.

Στο δεύτερο άρθρο του Ν. 927/1979 προβλεπόταν το έγκλημα της έκφρασης προσβλητικών ιδεών λόγω φυλετικής ή εθνικής καταγωγής ή λόγω θρησκεύματος. Το έγκλημα αυτό απαιτούσε μόνο την δημόσια έκφραση προσβλητικών απόψεων, χωρίς κάποια προτροπή για πράξεις εις βάρος των προσώπων αυτόν, παρουσιαζόμενο έτσι ως μια διακεκριμένη μορφή της εξύβρισης του άρθρου 361ΠΚ. Τέλος, στο τρίτο άρθρο του Ν. 927/1979 τυποποιούνταν η άρνηση προμήθειας αγαθών ή προσφοράς υπηρεσιών λόγω καταγωγής ή θρησκεύματος, ένα υπαλλακτικά μικτό έγκλημα που τελείται από κατ' επάγγελμα προμηθευτές αγαθών ή προσφέροντες κάποια υπηρεσία που αρνούνται να το κάνουν αυτό για το μέλος μιας ομάδας λόγω των προηγούμενων κριτηρίων.

- Κριτική στον παλιό Ν. 927/1979

Ο νόμος παρέμεινε σχεδόν ανεφάρμοστος, και αυτό όχι γιατί στην χώρα μας δεν υπήρξαν περιστατικά ρατσιστικής βίας ή λόγου, αλλά επειδή η νομοτεχνική του διατύπωση παρουσίαζε σημαντικά προβλήματα που δημιούργησαν τόσο θεωρητικές αμφιβολίες όσο και πρακτικές δυσχέρειες στην εφαρμογή του. Κεντρικό ζήτημα αποτέλεσε η ένσταση για την αναγκαιότητα της αντιρατσιστικής νομοθεσίας λόγω του ιδιαίτερου χαρακτήρα της και των διχογνωμιών ως προς το προστατευόμενο από αυτήν έννομο αγαθό.

1.1.2. Οι τροποποιήσεις των Ν. 4285/2014 και Ν.4491/2017 στον Ν. 927/1979

Η ενωσιακή υποχρέωση, μετά την απόφαση πλαίσιο 2008/913/ΔΕΥ, για τροποποίηση της αντιρατσιστικής νομοθεσίας, έτσι ώστε η Ελλάδα να προσαρμοστεί στις νέες επιταγές του ενωσιακού δικαίου συνδυαστικά πάντα και με τις νέες και ραγδαίες κοινωνικές και νομοθετικές εξελίξεις, οδήγησαν στην συζήτηση για την ψήφιση ενός νέου αντιρατσιστικού νομοσχεδίου. Μετά από πολλές αντιδράσεις, ενστάσεις και τροποποιήσεις έχουμε την ψήφιση του **Ν. 4285/2014** με τίτλο «Τροποποίηση του ν. 927/1979 (Α' 139) και προσαρμογή του στην απόφαση – πλαίσιο

2008/913/ΔΕΥ της 28ης Νοεμβρίου 2008 για την καταπολέμηση ορισμένων μορφών και εκδηλώσεων ρατσισμού και ξενοφοβίας μέσω του ποινικού δικαίου (L 328) και άλλες διατάξεις». Το 2017 βέβαια, έχουμε και την ψήφιση του **Ν.4491/2017**, διατάξεις του οποίου τροποποίησαν διατάξεις του Ν.4285/2014.

- Άρθρο 1 παρ.1 του Ν.4285/2014

Σύμφωνα με το άρθρο 1 παρ.1 του Ν.4285/2014: «*Όποιος με πρόθεση, δημόσια, προφορικά ή δια του τύπου, μέσω του διαδικτύου ή με οποιοδήποτε άλλο μέσο ή τρόπο, υποκινεί, προκαλεί, διεγείρει ή προτρέπει σε πράξεις ή ενέργειες που μπορούν να προκαλέσουν διακρίσεις, μίσος ή βία κατά προσώπου ή ομάδας προσώπων, που προσδιορίζονται με βάση τη φυλή, το χρώμα, τη θρησκεία, τις γενεαλογικές καταβολές, την εθνική ή εθνοτική καταγωγή, το σεξουαλικό προσανατολισμό, την ταυτότητα φύλου «χαρακτηριστικά φύλου» ή την αναπηρία, κατά τρόπο που εκθέτει σε κίνδυνο τη δημόσια τάξη ή ενέχει απειλή για τη ζωή, την ελευθερία ή τη σωματική ακεραιότητα των ως άνω προσώπων, τιμωρείται με φυλάκιση τριών (3) μηνών έως τριών (3) ετών και με χρηματική ποινή πέντε έως είκοσι χιλιάδων (5.000 - 20.000) ευρώ.*»

Στην διάταξη αυτή, τυποποιείται το έγκλημα της δημόσιας υποκίνησης βίας ή μίσους: υπαλλακτικά μικτό έγκλημα ως προς τα αποτελέσματά του.

- Άρθρο 7 παρ.1 του Ν.4491/2017

Σύμφωνα με το άρθρο 7 παρ. 1 του Ν.4491/2017, «1. *Οποιος με πρόθεση, δημόσια, προφορικά ή δια του τύπου, μέσω του διαδικτύου ή με οποιοδήποτε άλλο μέσο ή τρόπο, επιδοκιμάζει, ευτελίζει ή κακόβουλα αρνείται την ύπαρξη ή τη σοβαρότητα εγκλημάτων γενοκτονιών, εγκλημάτων πολέμου, εγκλημάτων κατά της ανθρωπότητας, του Ολοκαυτώματος και των εγκλημάτων του ναζισμού που έχουν αναγνωριστεί με αποφάσεις διεθνών δικαστηρίων ή της Βουλής των Ελλήνων και η συμπεριφορά αυτή στρέφεται κατά ομάδας προσώπων ή μέλους της που προσδιορίζεται με βάση τη φυλή, το χρώμα, τη θρησκεία, τις γενεαλογικές καταβολές, την εθνική ή εθνοτική καταγωγή, το σεξουαλικό προσανατολισμό, την ταυτότητα φύλου «χαρακτηριστικά φύλου» ή την αναπηρία, όταν η συμπεριφορά αυτή εκδηλώνεται κατά τρόπο που μπορεί να υποκινήσει βία ή μίσος ή ενέχει απειλητικό ή υβριστικό χαρακτήρα κατά μίας τέτοιας ομάδας ή μέλους της, τιμωρείται με τις ποινές της παραγράφου 1 του προηγούμενου άρθρου.*».

Στην διάταξη αυτή, το έγκλημα που τυποποιείται είναι αφηρημένα συγκεκριμένης διακινδύνευσης.

- Άρθρο 3 του Ν.4285/2014

Σύμφωνα με το άρθρο 3 του Ν.4285/2014, «*Όταν οι πράξεις των προηγουμένων άρθρων τελούνται μέσω διαδικτύου ή άλλου μέσου επικοινωνίας, τόπος τέλεσης θεωρείται και η Ελληνική Επικράτεια, εφόσον στο έδαφος της παρέχεται πρόσβαση στα συγκεκριμένα μέσα, ανεξάρτητα από τον τόπο εγκατάστασής τους.».*

Στο άρθρο αυτό, αξίζει να σταθούμε στο γεγονός ότι τόπος τέλεσης των εγκλημάτων αυτών, ήτοι των εγκλημάτων που τελούνται μέσω του διαδικτύου είναι και **η Ελληνική Επικράτεια,** με τους όρους όμως και τις προϋποθέσεις που θέτει η διάταξη αυτή.

- Άρθρο 4 του Ν.4285/2014

Σύμφωνα με το άρθρο 4 του Ν.4258/2014, «*Αν κάποια από τις αξιόποινες πράξεις του παρόντος νόμου τελέσθηκε προς όφελος ή για λογαριασμό νομικού προσώπου ή ενώσεως προσώπων, από φυσικό πρόσωπο που ενεργεί είτε ατομικά είτε ως μέλος οργάνου του νομικού προσώπου ή της ενώσεως προσώπων και που καθ οιονδήποτε τρόπο το εκπροσωπεί, επιβάλλονται στο νομικό πρόσωπο ή στην ένωση προσώπων, με κοινή απόφαση του Υπουργού Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων και του κατά περίπτωση αρμόδιου Υπουργού, σωρευτικά ή διαζευκτικά, μετά από αμετάκλητη παραπομπή του φυσικού προσώπου σε δίκη, οι ακόλουθες διοικητικές κυρώσεις: α) πρόστιμο από δέκα χιλιάδες (10.000) έως εκατό χιλιάδες (100.000) ευρώ, β) αποκλεισμός από δημόσιες παροχές, επιχορηγήσεις, ενισχύσεις, επιδοτήσεις ή αναθέσεις έργων και υπηρεσιών, προμήθειες, διαφημίσεις και διαγωνισμούς του δημοσίου ή των νομικών προσώπων του δημόσιου τομέα από έναν έως έξι μήνες. Η διοικητική κύρωση του στοιχείου α επιβάλλεται πάντοτε, ανεξαρτήτως της επιβολής άλλων κυρώσεων. Σε περίπτωση υποτροπής οι κυρώσεις του στοιχείου β μπορεί να προσαυξηθούν μέχρι του διπλασίου του ανωτάτου ορίου.»*

Στην διάταξη αυτή, προβλέπεται ένα πλέγμα προβλέψεων για την ευθύνη νομικών προσώπων που συνδέονται με το ρατσιστικό έγκλημα και τις πιθανές διοικητικές κυρώσεις εις βάρος τους.

- Άρθρο 5 του Ν.4285/2014

Σύμφωνα με το άρθρο 5 του Ν.4258/2014, «*Οι πράξεις που περιγράφονται στον παρόντα νόμο, καθώς και τα εγκλήματα που τελούνται συνεπεία αυτών, διώκονται αυτεπαγγέλτως. Ο παθών, κατά την υποβολή της έγκλησης, όπως και όταν παρίσταται ως πολιτικώς ενάγων, δεν καταβάλλει το σχετικό παράβολο υπέρ του Δημοσίου.»*

Με το άρθρο αυτό, προβλέπεται το αυτεπάγγελτο της δίωξης των εγκλημάτων του νόμου αυτού.

1.1.3. Άρθρο 82^{A} νΠΚ

Σύμφωνα με το άρθρο 82^{A} νΠΚ, « *Εάν έχει τελεστεί έγκλημα κατά παθόντος, η επιλογή του οποίου έγινε λόγω των χαρακτηριστικών φυλής, χρώματος, εθνικής ή εθνοτικής καταγωγής, γενεαλογικών καταβολών, θρησκείας, αναπηρίας, γενετήσιου προσανατολισμού, ταυτότητας ή χαρακτηριστικών φύλου, το πλαίσιο ποινής διαμορφώνεται ως εξής: α) Στην περίπτωση πλημμελήματος, που τιμωρείται με φυλάκιση έως ένα έτος, το ελάχιστο όριο της ποινής αυξάνεται κατά έξι μήνες. Στις λοιπές περιπτώσεις πλημμελημάτων, το ελάχιστο όριο αυτής αυξάνεται κατά ένα έτος. β) Στην περίπτωση κακουργήματος το ελάχιστο όριο ποινής αυξάνεται κατά δύο έτη*.»

Το άρθρο αυτό το συναντάμε στον Νέο Ποινικό Κώδικα που ψηφίστηκε με τον Ν.4619/2019 και τροποποίησε τις μέχρι τότε ισχύουσες διατάξεις. Στο προηγούμενο νομοθετικό καθεστώτος, ο «προκάτοχος» του άρθρου του, το άρθρο 81^{A} όριζε: «*Εάν από τις περιστάσεις προκύπτει ότι έχει τελεστεί έγκλημα κατά παθόντος, η επιλογή του οποίου έγινε λόγω των χαρακτηριστικών φυλής, χρώματος, εθνικής ή εθνοτικής καταγωγής γενεαλογικών καταβολών, θρησκείας, αναπηρίας, σεξουαλικού προσανατολισμού, ταυτότητας ή χαρακτηριστικών φύλου το πλαίσιο ποινής διαμορφώνεται ως εξής: α) Στην περίπτωση πλημμελήματος, που τιμωρείται με φυλάκιση έως ένα (1) έτος, το κατώτερο όριο της ποινής αυξάνεται στους έξι (6) μήνες και το ανώτερο όριο αυτής στα δύο (2) έτη. Στις λοιπές περιπτώσεις πλημμελημάτων το κατώτερο όριο ποινής αυξάνεται κατά ένα (1) έτος. β) Στην περίπτωση κακουργήματος, που το προβλεπόμενο πλαίσιο ποινής ορίζεται σε πέντε (5) έως δέκα (10) έτη, το κατώτερο όριο ποινής αυξάνεται κατά δύο (2) έτη. Στις λοιπές περιπτώσεις κακουργημάτων το κατώτερο όριο ποινής αυξάνεται κατά τρία (3) έτη. γ) Στην περίπτωση εγκλήματος, που τιμωρείται με χρηματική ποινή, το κατώτερο όριο αυτής διπλασιάζεται. Σε περίπτωση μετατροπής της ποινής φυλάκισης που έχει επιβληθεί κατά τα παραπάνω, το ποσό της μετατροπής δεν μπορεί να είναι κατώτερο από το διπλάσιο του κατώτατου ορίου του προβλεπόμενου ποσού μετατροπής*.»

Αν κάναμε μία σύγκριση μεταξύ του παλαιού με το νέο καθεστώς, αυτό που θα λέγαμε είναι ότι αλλάζουν τα πλαίσια της ποινής και μόνο καθώς και ότι στο νέο άρθρο δεν γίνεται αναφορά αναφορικά με τις περιπτώσεις εγκλημάτων για τα οποία έχει επιβληθεί χρηματική ποινή. Ο νομοθέτης και στα δύο άρθρα, προγενέστερο και μεταγενέστερο, είναι ιδιαίτερα προστατευτικός απέναντι στον παθόντα, φροντίζοντας να καλύψει κάθε κίνητρο του δράστη που στρέφεται κατά του θύματος και αφορά χαρακτηριστικά του τελευταίου που σχετίζονται με την φυλή, το χρώμα, την εθνική ή εθνοτική του καταγωγή, τις γενεαλογικές καταβολές, την θρησκεία, την αναπηρία, τον γενετήσιο προσανατολισμό του.

1.2.Νομοθεσία για την Ποινική Αντιμετώπιση Εκδηλώσεων Εξύβρισης

1.2.1 Άρθρα 361, 362 και 363 ΠΚ

Σύμφωνα με το άρθρο 361 παρ.1 του νέου Ποινικού Κώδικα, «*Όποιος, εκτός από τις περιπτώσεις της δυσφήμησης (άρθρα 362 και 363), προσβάλλει την τιμή άλλου με λόγο ή με έργο ή με οποιονδήποτε άλλο τρόπο τιμωρείται με φυλάκιση έως έξι μήνες ή χρηματική ποινή. Αν τελεί την πράξη δημόσια με οποιονδήποτε τρόπο ή μέσω διαδικτύου, επιβάλλεται φυλάκιση έως ένα έτος ή χρηματική ποινή.»*

Σύμφωνα με το άρθρο 362 του νέου Ποινικού Κώδικα, «*Όποιος με οποιονδήποτε τρόπο ενώπιον τρίτου ισχυρίζεται ή διαδίδει για κάποιον άλλον γεγονός που μπορεί να βλάψει την τιμή ή την υπόληψή του τιμωρείται με φυλάκιση έως ένα έτος ή χρηματική ποινή. Αν η πράξη τελέστηκε δημόσια με οποιονδήποτε τρόπο ή μέσω διαδικτύου, επιβάλλεται φυλάκιση έως τρία έτη ή χρηματική ποινή.»*

Σύμφωνα με το άρθρο 363 του νέου Ποινικού Κώδικα, «*Αν στην περίπτωση του προηγούμενου άρθρου, το γεγονός είναι ψευδές και ο υπαίτιος γνώριζε ότι αυτό είναι ψευδές τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών και χρηματική ποινή και αν τελεί την πράξη δημόσια με οποιονδήποτε τρόπο ή μέσω του διαδικτύου, με φυλάκιση τουλάχιστον έξι μηνών και χρηματική ποινή.»*

Με τον νέο Ποινικό Κώδικα προστέθηκε στις ως άνω διατάξεις και το διαδίκτυο ως τρόπος εκτέλεσης, δια μέσου του οποίου μπορούν να τελεστούν τα ως άνω εγκλήματα που στρέφονται κατά της τιμής του ανθρώπου. Όπως δε αναφέρεται και στην Αιτιολογική Έκθεση του νέου Ποινικού Κώδικα, *«…..προβλέπεται επιβαρυντική περίσταση στα εγκλήματα των άρθρων 361, 362 και 363 Π.Κ. αν η πράξη τελείται δημόσια με οποιονδήποτε τρόπο ή μέσω του διαδικτύου λόγω επίτασης της προσβολής του προστατευόμενου αγαθού».*

1.3.Νομοθεσία για την Ποινική Αντιμετώπιση Εκδηλώσεων Εκφοβισμού – Εκβιασμού

Η αλήθεια είναι πως παρά την ψήφιση νέου Ποινικού Κώδικα και παρά την ολοένα και αυξανόμενη εμφάνιση κρουσμάτων εκφοβισμού στο διαδίκτυο, το γνωστό σε όλους μας πλέον **Cyberbullying,** δεν υπάρχει κάποια ρητή νομοθετική διάταξη που να τιμωρεί τον δράστη τέλεσης τέτοιων εγκλημάτων. Τι είναι όμως το cyberbulling και πώς εκδηλώνεται;

1.3.1.Cyberbulling: Έννοια – Μέσα και Τρόποι εκδήλωσης αυτού

1.3.1.1. Ορισμός Cyberbulling

Αν μπορούσαμε να δώσουμε ένα ορισμό για την έννοια του εκφοβισμού μέσω διαδικτύου, θα λέγαμε πως, εκφοβισμός μέσω διαδικτύου (cyberbullying) είναι οποιαδήποτε επαναλαμβανόμενη πράξη εκφοβισμού, επιθετικότητας, παρενόχλησης, τρομοκρατικής ή αυταρχικής συμπεριφοράς που πραγματοποιείται μέσω της χρήσης ψηφιακών συσκευών (Η/Υ, Tablets, κινητών τηλεφώνων). Ο ψηφιακός εκφοβισμός μοιάζει πολύ με τον απλό εκφοβισμό, αφού υπάρχει θύτης, θύμα και παρατηρητές. Έχει όμως και μερικές σημαντικές διαφορές. Αρχικά, ο θύτης μπορεί να παραμείνει ανώνυμος και φυσικά δεν υπάρχει προσωπική επαφή με το θύμα, γεγονός που κάνει τον δράστη σκληρότερο. Το θύμα πλήττεται στο σπίτι του και στον προσωπικό του χώρου, αφού όλα γίνονται δια μέσου του ηλεκτρονικού υπολογιστή και μπορεί μάλιστα να μην είναι το αποκλειστικό θύμα του δράστη, αφού τα εκβιαστικά μηνύματα του τελευταίου μπορούν να έχουν πολλούς παραλήπτες.

1.3.1.2. Μέσα άσκησης Cyberbulling

Αναφορικά με τα μέσα που χρησιμοποιούνται για την παρενόχληση μέσω διαδικτύου, αυτά είναι:

- το ηλεκτρονικό ταχυδρομείο (e-mail),
- τα γραπτά μηνύματα (sms),
- τα μέσα κοινωνικής δικτύωσης (social media),
- τα δωμάτια επικοινωνίας (chat rooms),
- τα ιστολόγια (blogs),
- τα διαδικτυακά παιχνίδια (internet games)

1.3.1.3. Τρόποι εκδήλωσης Cyberbulling

Επιπλέον, σχετικά με τον τρόπο εκδήλωσης αυτού, αρχικά αυτό που λέγαμε πως τα άτομα που ασκούν εκφοβισμό, χρησιμοποιούν τις νέες τεχνολογίες για να παρενοχλήσουν, να απειλήσουν, να εκφοβίσουν, να εκβιάσουν, να δυσφημήσουν και, σε μερικές περιπτώσεις, να υποδυθούν τρίτους ή να υποκλέψουν την ταυτότητά τους. Μερικές από τις πιο κοινές μεθόδους είναι οι εξής:

- Αποστολή κειμένων, e-mail, ή άμεσων μηνυμάτων με προσβλητικό περιεχόμενο (σε instant messengers ή chatrooms),
- Η κακόβουλη δημοσίευση φωτογραφιών σε μέσα κοινωνικής δικτύωσης (social networks), ιστολόγια (blogs) ή άλλες ιστοσελίδες με μοναδικό σκοπό την παρενόχληση,

- Διάδοση φημών και ψευδών γεγονότων με σκοπό την δυσφήμιση σε τρίτους σε μέσα κοινωνικής δικτύωσης, ιστολόγια, ιστοσελίδες κ.λπ.,
- Ανώνυμες κλήσεις και μηνύματα με σκοπό τον φόβο και την ταραχή,
- Χρήση του ονόματος ξένου χρήστη με σκοπό τη διάδοση φημών για κάποιον τρίτο (κλοπή ταυτότητας),
- Η δημιουργία ιστοσελίδων που στοχοποιούν συγκεκριμένα άτομα καλώντας άλλους να δημοσιεύσουν μηνύματα μίσους,
- Η αποστολή ειδικών προγραμμάτων trojan horses (δούρειοι ίπποι) σκόπιμα για να δημιουργήσουν πρόβλημα, με την υποκλοπή κωδικών,
- Εκφοβισμός στη διάρκεια ενός διαδραστικού online παιχνιδιού.

1.3.2. Άρθρο 312 Ν.4332/2015

Σύμφωνα με το άρθρο 312 παρ.1. του Ν.4332/2015, το οποίο και προβλέπονταν στον παλαιό Ποινικό Κώδικα, «*Αν δεν συντρέχει περίπτωση βαρύτερης αξιόποινης πράξης, τιμωρείται με φυλάκιση, όποιος με συνεχή σκληρή συμπεριφορά προξενεί σε τρίτον σωματική κάκωση ή άλλη βλάβη της σωματικής ή ψυχικής υγείας. Αν η πράξη τελείται μεταξύ ανηλίκων δεν τιμωρείται εκτός αν η μεταξύ τους διαφορά ηλικίας είναι μεγαλύτερη από τρία (3) έτη, οπότε επιβάλλονται μόνο αναμορφωτικά ή θεραπευτικά μέτρα.».*

Στην διάταξη αυτή, την οποίας το περιεχόμενο έχει αλλάξει με τον νέο Ποινικό Κώδικα (θα γίνει αναφορά κατωτέρο), με την αναφορά στην βλάβη της ψυχικής αλλά και σωματικής υγείας, εκτός βέβαια από την πρόκληση σωματικών κακώσεων που αναφέρει η διάταξη, ποινικοποιείται ξεκάθαρα ο εκφοβισμός, άλλως το γνωστό σε όλους πλέον **bulling**. Το bulling με το cyberbulling που περιγράψαμε ανωτέρω, όσον αφορά τα βασικά τους στοιχεία είναι ίδια με την μόνη διαφορά πως στην περίπτωση του cyberbulling, ο εκφοβισμός, η παρενόχληση γίνονται δια μέσω της χρήσης ψηφιακών συσκευών (Η/Υ, Tablets, κινητών τηλεφώνων).

Σήμερα με τον νόμο 4619/2019, ο οποίος τροποποίησε τον Ποινικό Κώδικα, η ως άνω διάταξη έχει τροποποιηθεί ως εξής: «*Όποιος προκαλεί σωματική κάκωση ή βλάβη της υγείας σε ανήλικο ή σε πρόσωπο που δεν μπορεί να υπερασπίσει τον εαυτό του, εφόσον τα πρόσωπα αυτά βρίσκονται υπό την επιμέλεια ή την προστασία του δράστη βάσει νόμου, δικαστικής απόφασης ή πραγματικής κατάστασης, συνοικούν με τον δράστη ή έχουν μαζί του σχέση εργασίας ή υπηρεσίας, τιμωρείται: α) για την πράξη του άρθρου 308 παρ. 1 εδάφιο α`, με φυλάκιση τουλάχιστον ενός έτους, β) για την πράξη του άρθρου 309, με φυλάκιση τουλάχιστον δύο ετών, γ) για την πράξη του άρθρου 310 παρ. 1 εδ. α`, με φυλάκιση τουλάχιστον τριών ετών και αν επεδίωκε την πρόκληση βαριάς σωματικής βλάβης, με κάθειρξη και δ) για την πράξη του άρθρου 311, με κάθειρξη*».

Η καινοτομία της διάταξης αυτής, έχει να κάνει με το γεγονός πως το θύμα είναι είτε ανήλικος, είτε πρόσωπο που δεν μπορεί να υπερασπιστεί τον εαυτό του και μάλιστα αυτό (ήτοι το θύμα) βρίσκεται υπό την εποπτεία ή προστασία του δράστη, ή μένουν μαζί ή υπάρχει μεταξύ τους εργασιακή σχέση. Όλα αυτά τα στοιχεία που συνθέτουν την αντικειμενική υπόσταση του εγκλήματος που περιγράφεται στην διάταξη του άρθρου 312 του νΠΚ, περιορίζουν θα λέγαμε τις περιπτώσεις που μπορεί να συντρέξει εφαρμογή της ως άνω διάταξης, καθότι το θύμα πρέπει να βρίσκεται σε μία σχέση «εξάρτησης» με τον δράστη κάτι που ο νομοθέτης δεν απαιτούσε στην προηγούμενη μορφή του άρθρου.

Συμπερασματικά, τα ως άνω νομοθετήματα και οι διατάξεις αυτών, σκοπό έχουν, ως αναφέρθηκε και ανωτέρω, να διαφυλάξουν όσο το δυνατό περισσότερο το υποκείμενο των δικαιωμάτων από οποιαδήποτε προσβολή της προσωπικότητας του. Οι προσβολές κατά του υποκειμένου μπορούν να γίνουν με οποιοδήποτε τρόπο. Συγκεκριμένα μπορεί να είναι λεκτικές, έγγραφες, εικονικές και φυσικά μέσω των διαδεδομένων πλέον μέσων κοινωνικής δικτύωσης, τα γνωστά σε όλους μας **social media.**

Είναι γεγονός πως τα τελευταία χρόνια, εκατομμύρια άνθρωποι από κάθε μεριά του πλανήτη είναι χρήστες των μέσων κοινωνικής δικτύωσης, τα οποία και διαδραματίζουν τεράστιο ρόλο στην καθημερινότητα αυτών. Παρ' όλα αυτά, όπως καθετί καινούργιο στις ζωές μας, εκτός από τα οφέλη του έχει και τα τρωτά του σημεία, τα οποία στην περίπτωση μας έχουν να κάνουν με την χρήση των social media ως μέσω έκφρασης ρατσιστικών, ξενοφοβικών, υβριστικών και εκβιαστικών μηνυμάτων με αποδέκτες χρήστες ανεξαρτήτως ηλικίας, φύλου, χρώματος, χώρα προέλευσης.

Στα κεφάλαια που ακολουθούν θα γίνει αρχικά μια αναδρομή στην ιστορία των μέσων κοινωνικής δικτύωσης, στις κατηγορίες και τα χαρακτηριστικά αυτών, θα παρατεθούν αποφάσεις των δικαστηρίων που σχετίζονται με τα μέσα κοινωνικής δικτύωσης και τις προσβολές που διατυπώνονται μέσω αυτών, ενώ τέλος θα γίνει αναφορά και σε στατιστικά στοιχεία της ελληνικής αστυνομίας αναφορικά με την δίωξη των εγκλημάτων που διαπράττονται μέσω διαδικτύου ή με τη χρήση αυτού.

1.3.3. Το cyberbulling σε παγκόσμιο επίπεδο

Ασία

Η Κίνα έχει αυστηρούς νόμους κατά του εκφοβισμού και είναι ιδιαίτερα επιθετική στις προσπάθειές της να αντιμετωπίσει τον κυβερνο-εκφοβισμό. Η χώρα ψήφισε πρόσφατα ένα νόμο που απαιτεί από τους πολίτες της να καταχωρούν τα πραγματικά τους ονόματα σε «online» συνδέσεις στο διαδίκτυο. Αυτό επιτρέπει στην κυβέρνηση να εντοπίζει τα άτομα πιο εύκολα,

αναγκάζοντας έτσι τη λογοδοσία σε ό, τι οι άνθρωποι δημοσιεύουν στο διαδίκτυο. Οι εταιρείες υποχρεούνται να παρέχουν ένα υγιές περιβάλλον για τους εργαζομένους και τα άτομα υποχρεούνται να λαμβάνουν μέτρα όταν υποφέρουν από πράξεις εκφοβισμού εντός μιας επιχείρησης.

Το 2013, η Ιαπωνία εισήγαγε νόμο που απαιτεί από τα σχολεία να αντιμετωπίζουν τον εκφοβισμό, συμπεριλαμβανομένης της παρενόχλησης στον κυβερνοχώρο. Τα σχολεία ήταν υποχρεωμένα να ενεργούν για την πρόληψη των περιστατικών εκφοβισμού και να αναφέρουν επίσης περιστατικά που προκύπτουν. Η Ιαπωνία όμως δεν έχει συγκεκριμένους νόμους για τον εκφοβισμό στο εργατικό δυναμικό. Ωστόσο, οι ισχύοντες νόμοι σχετικά με την παρενόχληση, την επίθεση και παρόμοια συμβάντα μπορούν επίσης να εφαρμοστούν σε περιπτώσεις εκφοβισμού.

Οι Φιλιππίνες έχουν προωθήσει την νομοθεσία κατά των εκφοβισμών στα σχολεία, με ευρείες διατάξεις για την προστασία των παιδιών από σωματική και ψυχολογική κακοποίηση. Αυτοί οι νόμοι περιλαμβάνουν διατάξεις για την αντιμετώπιση του εκφοβισμού στον κυβερνοχώρο, καθώς και για τον εκφοβισμό που συμβαίνει μακριά από το σχολείο, αλλά στις δραστηριότητες που χρηματοδοτούνται από το σχολείο. Ο νόμος ορίζει ότι όλα τα ιδιωτικά και δημόσια σχολεία υιοθετούν ολοκληρωμένα προγράμματα πρόληψης για τον εκφοβισμό που αφορούν το προσωπικό και τους σπουδαστές σε όλα τα επίπεδα. Ωστόσο, οι νόμοι περί εκφοβισμού στο χώρο εργασίας είναι πολύ λιγότερο ανεπτυγμένοι. Η νομοθεσία για την απαγόρευση του εκφοβισμού στο χώρο εργασίας δεν έχει ακόμη εγκριθεί και πολλές περιπτώσεις δείχνουν ότι ο εκφοβισμός στο χώρο εργασίας είναι έντονος και δεν γίνεται τίποτε για την καταπολέμηση του προβλήματος.

Το 2014, η Σιγκαπούρη καταδίκασε τον εκφοβισμό στον κυβερνοχώρο ως μέρος μιας σαρωτικής σειράς νόμων που στοχεύουν στην αντικοινωνική συμπεριφορά που καλύπτει τόσο τον χώρο εργασίας όσο και τις σχολικές αίθουσες. Η παρενόχληση στον κυβερνοχώρο, ο εκφοβισμός των παιδιών, η σεξουαλική παρενόχληση στο χώρο εργασίας και η καταδίωξη είναι παράνομες, με το αδίκημα να τιμωρείται για πρώτη φορά, με πρόστιμο έως 5.000 δολάρια ή ένα χρόνο φυλάκισης. Οι επανειλημμένοι παραβάτες αντιμετωπίζουν πρόστιμα ύψους 10.000 δολαρίων και /ή φυλάκιση δύο ετών.

Αφρική

Η Κένυα έχει νόμους που εμποδίζουν όλες τις μορφές σεξουαλικής παρενόχλησης, τις οποίες ορίζει ως άμεσες ή έμμεσες από κάποιον για σεξουαλική επαφή, ή οποιαδήποτε άλλη μορφή σεξουαλικής δραστηριότητας που περιέχει σιωπηρή ή ρητή υπόσχεση μεταχείρισης στην απασχόληση ή εναλλακτικά, απειλή καταχρηστικής μεταχείρισης γενικότερα. Ωστόσο, ο νόμος είναι ασαφής για άλλες μορφές παρενόχλησης. Η Κένυα έχει νόμους απαγόρευσης για τις διακρίσεις σε βάρος οποιουδήποτε προσώπου λόγω φυλής, φύλου, εγκυμοσύνης, οικογενειακής

κατάστασης, υγειονομικής κατάστασης, εθνοτικού ή κοινωνικού περιβάλλοντος, ηλικίας, θρησκείας, ή γλώσσας. Δεν υπάρχουν συγκεκριμένοι νόμοι που να αντιτίθενται στον εκφοβισμό στα σχολεία της Κένυας, παρά το γεγονός ότι η χώρα έχει μερικά από τα υψηλότερα ποσοστά εκφοβισμού στην Αφρική. Υπάρχουν όμως νόμοι που απαγορεύουν ρητά την παρενόχληση των μαθητών από τους εκπαιδευτικούς.

Στη Νότια Αφρική τα παιδιά ηλικίας κάτω των 18 ετών μπορούν επίσης να απευθύνονται στα δικαστήρια χωρίς τη γνώση των γονέων τους. Το 2013, η χώρα δημοσίευσε ευρεία νομοθεσία για την καταπολέμηση της παρενόχλησης στο χώρο εργασίας. Μεταξύ άλλων, ο νόμος για την προστασία από την παρενόχληση επιτρέπει σε έναν υπάλληλο να λάβει μια μορφή προστασίας έναντι μιας καταχρηστικής συμπεριφοράς εργοδότη ή συναδέλφου.

Αυστραλία

Η Αυστραλία διαθέτει εκτεταμένες διατάξεις για την αντιμετώπιση του εκφοβισμού, τόσο στα σχολεία όσο και στον εργασιακό χώρο. Στο χώρο εργασίας, τα άτομα ενθαρρύνονται να επιλύουν ζητήματα εκφοβισμού μέσω του εσωτερικού κανονισμού της επιχείρησης. Αν όμως αυτό δεν επιλύσει το πρόβλημα, είναι πιθανό να ζητηθεί περαιτέρω βοήθεια, μεταβιβάζοντας το ζήτημα στην Επιτροπή Εργασίας. Σε περίπτωση που ο εκφοβισμός είναι βίαιος ή αλλιώς απειλητικός, η αστυνομία είναι επίσης αρμόδια από το νόμο να χειρίζεται τις καταγγελίες. Στα σχολεία, κάθε κράτος ή τοπική κοινότητα διαμορφώνει το δικό του/της σύνολο αντι-εκφοβιστικών πολιτικών και εφαρμόζει αυτές τις πολιτικές στα δημόσια σχολεία.

ΗΠΑ

Ο εκφοβισμός αντιμετωπίζεται στις ΗΠΑ από ομοσπονδιακούς και τοπικούς νόμους. Σε σύνολο 41 από τις 50 πολιτείες των ΗΠΑ έχουν νόμους και πολιτικές για την αντιμετώπιση του εκφοβισμού στα σχολεία και σε ορισμένες πολιτείες ο εκφοβισμός εμφανίζεται στον ποινικό κώδικα και μπορεί να εφαρμοστεί σε ανηλίκους. Οι νόμοι για τον εκφοβισμό στο χώρο εργασίας, εν τω μεταξύ, εμπίπτουν στους νόμους περί παρενόχλησης των ΗΠΑ. Η παρενόχληση ορίζεται ως παράνομη όταν α) η συνέχιση της προσβλητικής συμπεριφοράς γίνεται προϋπόθεση για συνεχιζόμενη απασχόληση ή β) η συμπεριφορά είναι αρκετά σοβαρή ή διεισδυτική ώστε να δημιουργήσει ένα εργασιακό περιβάλλον που ένας λογικός άνθρωπος θα θεωρούσε εκφοβιστικό, εχθρικό ή καταχρηστικό. Η επιθετική συμπεριφορά μπορεί να συνιστά, αλλά δεν περιορίζεται σε προσβλητικά λόγια, κακοποιήσεις, φυσική επίθεση ή απειλές, εκφοβισμό, κοροϊδία, χρήση επιθετικών εικόνων και παρεμβολή στην απόδοση της εργασίας. Η παρενόχληση είναι επίσης παράνομη όταν χρησιμοποιείται σε αντίποινα για την κατάθεση κατηγορίας διακρίσεων, τη μαρτυρία ή τη συμμετοχή σε έρευνα, διαδικασία ή αγωγή σύμφωνα με αυτούς τους νόμους.

Σύμφωνα με το αμερικανικό δίκαιο, ο εργοδότης είναι αυτομάτως υπεύθυνος για κάθε παρενόχληση που μπορεί να προκληθεί στο εργασιακό περιβάλλον.

Ευρώπη

Το 2014, το Βέλγιο έθεσε σε εφαρμογή νέους νόμους κατά του «bullying», ως μέρος μιας μεταρρύθμισης που αποσκοπούσε στην αντιμετώπιση όλων των ψυχοκοινωνικών κινδύνων στο χώρο εργασίας. Αυτός ο σαρωτικός νόμος καλύπτει τη βία, τον εκφοβισμό και την ανεπιθύμητη σεξουαλική συμπεριφορά στο χώρο εργασίας. Σύμφωνα με αυτούς τους νόμους, οι εργοδότες υποχρεούνται να γνωρίζουν και να διαχειρίζονται όλους τους κινδύνους που θα μπορούσαν να βλάψουν την ψυχολογική υγεία των εργαζομένων ή να οδηγήσουν σε άγχος, εξάντληση ή απαράδεκτη συμπεριφορά. Οι επιχειρήσεις υποχρεούνται να διαθέτουν επίσημες πολιτικές σε αυτούς τους τομείς και να αναθέτουν σε ένα υπεύθυνο άτομο να επιβλέπει αυτόν τον τομέα. Το Βέλγιο έχει επίσης θεσπίσει προηγμένους νόμους κατά της επιθετικής συμπεριφοράς για τον εκφοβισμό στα σχολεία και αντιμετωπίζει ενεργά το πρόβλημα της αύξησης του εκφοβισμού στον κυβερνοχώρο σε ολόκληρη τη χώρα.

Ο εκφοβισμός αναφέρεται στη Γαλλία ως «ηθική παρενόχληση» και η χώρα έχει νόμους για την απαγόρευση τέτοιων πράξεων. Η ηθική παρενόχληση ορίζεται ως «επαναλαμβανόμενες πράξεις που οδηγούν σε επιδείνωση των συνθηκών εργασίας που ενδέχεται να βλάψουν την αξιοπρέπεια, τη σωματική ή ψυχολογική υγεία του θύματος ή τη σταδιοδρομία του». Αυτοί οι νόμοι επιτρέπουν τόσο την αστική όσο και την ποινική δίωξη εναντίον του θύτη. Οι μέγιστες ποινές μπορούν να είναι τόσο υψηλές δηλαδή δύο χρόνια φυλάκιση και πρόστιμο 30.000 Ευρώ. Κάθε εκφοβισμός που συμβαίνει μέσα στα στενά όρια του εργασιακού περιβάλλοντος, φέρει την ευθύνη ο εργοδότης και ένας εκφοβισμένος εργαζόμενος είναι σε θέση να κερδίσει αποζημίωση από τον οργανισμό μέσω αστικής αποζημίωσης. Εντούτοις, τα μέτρα για την παρεμπόδιση του εκφοβισμού στα σχολεία είναι λιγότερο ανεπτυγμένα στη Γαλλία. Η προηγούμενη κυβέρνηση ήταν η πρώτη που άρχισε να εξετάζει το ζήτημα, αλλά στις περισσότερες περιπτώσεις οι γονείς πρέπει πρώτα να έρθουν σε επαφή με τις γαλλικές ενώσεις των δασκάλων για να εκφράσουν τις απόψεις τους. Ο τρόπος με τον οποίο διαχειρίζονται την κατάσταση εξαρτάται στη συνέχεια από τις περιστάσεις και την ατομική σχολική πολιτική.

Η Σουηδία ήταν η πρώτη και παραμένει ένα από τα λίγα κράτη με νόμους που απαγορεύουν συγκεκριμένα τον εκφοβισμό στο χώρο εργασίας. Αυτή η νομοθεσία παραβιάζει «επαναλαμβανόμενες, κατακριτέες ή σαφώς αρνητικές ενέργειες που στρέφονται εναντίον μεμονωμένων υπαλλήλων κατά τρόπο προσβλητικό και μπορεί να οδηγήσει στην τοποθέτηση αυτών των εργαζομένων εκτός της κοινότητας του χώρου εργασίας». Ο νόμος απαιτεί από τους εργοδότες να διερευνούν και να αντιμετωπίζουν οποιεσδήποτε περιπτώσεις εκφοβισμού κατά την

εμφάνισή τους αλλά επίσης να υιοθετούν μια «μη τιμωρητική» προσέγγιση σε περιπτώσεις εκφοβισμού και να επιλύουν προβλήματα μέσω διαλόγου και συναίνεσης και όχι με την επιβολή κυρώσεων. Η Σουηδία έχει επίσης προχωρήσει προοδευτικά στην ανάληψη δράσης σχετικά με τον εκφοβισμό στα σχολεία, τοποθετώντας το βάρος της πρόληψης στο θεσμικό όργανο.

Γ. ΜΕΣΑ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ - SOCIAL MEDIA

1. Τα Μέσα Κοινωνικής Δικτύωσης - Social Media

Instagram, Facebook, Twitter, είναι μερικοί από τους όρους της καθομιλουμένης που, πλέον χωρίς καμία υπερβολή θα ακούσει κανείς να βγαίνουν από τα στόματα ανθρώπων κάθε ηλικίας. Ο λόγος για τα Social Media, τα οποία δεν αποτελούν κάτι πρόσκαιρο και εφήμερο στην εποχή μας, αλλά ένα πολυπολιτισμικό φαινόμενο που μέρα με τη μέρα, χρόνο με το χρόνο εξελίσσεται ραγδαία. Γεγονός άλλωστε που αποδεικνύεται και από των αριθμό των χρηστών αυτών.

1.1 Η ιστορική εξέλιξη των Μέσων Κοινωνικής Δικτύωσης - Social Media

Σύμφωνα με τον οικονομολόγο Bernd Wirtz, ως μέσα μαζικής επικοινωνίας «*ορίζονται όλα τα τεχνικά μέσα για την επικοινωνία και την προμήθεια πληροφοριών σε ένα ευρύ κοινό σε έντυπη, ακουστική ή οπτική μορφή*». Ο ορισμός αυτός θα λέγαμε ότι παραπέμπει στα παραδοσιακά μέσα ενημέρωσης όπως η τηλεόραση, η εφημερίδα, το ραδιόφωνο.

Τα παραδοσιακά μέσα μαζικής επικοινωνίας αποτελούν πομπούς πληροφόρησης, οι οποίοι όμως δημιουργούν κανάλια επικοινωνίας μίας κατεύθυνσης, μη παρέχοντας την δυνατότητα στους χρήστες να μοιραστούν τις απόψεις τους. Με την έλευση του Web 2.0 όμως υπεισήρθε το στοιχείο της **διαδραστικότητας** και της **αλληλεπίδρασης** στα μέσα επικοινωνίας επιτρέποντας έτσι την ενεργή συμμετοχή των χρηστών. Το κοινωνικό στοιχείο λοιπόν ως δεύτερο συστατικό των μέσων κοινωνικής δικτύωσης είναι αυτό που τα διαφοροποιεί από τις συμβατικές τεχνολογίες των μέσων ενημέρωσης.

1.2 Ο ορισμός των Μέσων Κοινωνικής Δικτύωσης- Social Media

Η ελληνική απόδοση του όρου ακούει στο όνομα **μέσα κοινωνικής δικτύωσης**, ή στον όρο **κοινωνικά δίκτυα**. Λόγω του τεράστιου ενδιαφέροντος του παγκόσμιου αυτού φαινομένου, προέκυψε μεγάλο ενδιαφέρον της Ακαδημαϊκής Κοινότητας και συνάμα πληθώρα ορισμών της έννοιας των μέσων κοινωνικής δικτύωσης. Ενδεικτικά θα αναφέρουμε κάποιους από τους ορισμούς που διατυπώθηκαν.

Οι καθηγητές Andreas M. Kaplan και Michael Haenlein, στο άρθρο τους «Users of the world, unite! The challenges and opportunities of Social Media», ορίζουν τα μέσα κοινωνικής

δικτύωσης «σαν ένα σύνολο από διαδικτυακές εφαρμογές που βασίζονται στα ιδεολογικά και τεχνολογικά θεμέλια του Web 2.0 και επιτρέπουν την δημιουργία και την ανταλλαγή περιεχομένου User Generated Content».

Επιπλέον, τα Social Media κατά τον Dave Evans αποτελούν τον εκδημοκρατισμό της πληροφορίας, αφού μέσα από την χρήση τους οι άνθρωποι γίνονται εκδότες ενός περιεχομένου και δεν παραμένουν απλοί αναγνώστες. Ενώ παράλληλα αποτελούν ένα πολύπλευρο μέσω επικοινωνίας μεταξύ των χρηστών.

Παράλληλα, τα κοινωνικά δίκτυα μπορούν να περιγραφούν ως εφαρμογές ιστού που επιτρέπουν στους χρήστες να δημιουργήσουν ένα ημι-δημόσιο προφίλ τους. Τα περισσότερα άτομα συμμετέχουν σε κοινωνικά δίκτυα για να διανέμουν τα δεδομένα τους και να διατηρούν επαφή με άτομα τα οποία γνωρίζουν. Το κύριο χαρακτηριστικό των μέσων κοινωνικής δικτύωσης είναι η εύρεση «φίλων» που επιτρέπει στους χρήστες των μέσων κοινωνικής δικτύωσης να αναζητούν άτομα που γνωρίζουν και στη συνέχεια να δημιουργήσουν τη δική τους διαδικτυακή κοινότητα. Οι περισσότεροι χρήστες των μέσων κοινωνικής δικτύωσης μοιράζονται μεγάλο μέρος των προσωπικών τους πληροφοριών στον χώρο των κοινωνικών τους δικτύων. Ένας μεγάλος αριθμός χρηστών μοιράζονται τις πληροφορίες τους δημόσια χωρίς προσεκτική εξέταση. Κατά συνέπεια, τα μέσα κοινωνικής δικτύωσης έχουν γίνει ένας «χώρος» όπου αποθηκεύεται μεγάλο μέρος ευαίσθητων δεδομένων μας. Ακόμη, οι χρήστες των μέσων κοινωνικής δικτύωσης τείνουν να έχουν υψηλό επίπεδο εμπιστοσύνης έναντι των άλλων χρηστών (των μέσων κοινωνικής δικτύωσης). Τείνουν με άλλα λόγια, να δέχονται εύκολα αιτήματα φίλων και εμπιστεύονται αντικείμενα που τους στέλνουν οι εικονικοί τους «φίλοι». Τα ζητήματα απορρήτου και ασφάλειας στα μέσα κοινωνικής δικτύωσης – για τα οποία θα γίνει λόγος και κατωτέρω - είναι τα πιο δημοφιλή προβλήματα στον χώρο των social media. Τα θέματα ασφάλειας και απορρήτου είναι εντελώς διαφορετικά προβλήματα. Από τη μία πλευρά, ζητήματα ασφαλείας προκύπτουν όταν οι χάκερ αποκτούν μη εξουσιοδοτημένη πρόσβαση σε προστατευμένη κωδικοποίηση ή γραπτή γλώσσα ενός ιστότοπου. Από την άλλη πλευρά, ζητήματα ιδιωτικής φύσεως, εκείνα που περιλαμβάνουν την αδικαιολόγητη πρόσβαση σε ιδιωτικές πληροφορίες, δεν πρέπει απαραίτητα να περιλαμβάνουν παραβιάσεις ασφάλειας. Εμπιστευτικές πληροφορίες, όπως πληκτρολόγηση κωδικού πρόσβασης, μπορούν να αποκαλυφθούν σε όλους. Όμως και οι δύο τύποι παραβιάσεων συνδέονται συχνά στα κοινωνικά δίκτυα, ειδικά «*αφού οποιοσδήποτε παραβιάζει το δίκτυο ασφαλείας ενός ιστότοπου ανοίγει την πόρτα για εύκολη πρόσβαση σε ιδιωτικές πληροφορίες που ανήκουν σε οποιονδήποτε χρήστη*». (C. Stergiou, K. E. Psannis, A. P. Plageras, T. Xifilidis, B. B. Gupta, "Security and Privacy of Big Data for Social Networking Services in Cloud", in Proceedings of IEEE conference on Computer Communications (IEEE INFOCOM 2018), 15-20 April 2018, Honolulu, HI, USA.,

https://www.researchgate.net/publication/323036016_Security_and_Privacy_of_Big_Data_for_Social_Networking_Services_in_Cloud σελ:439).

1.3 Κατηγοριοποίηση των social media

Εκατοντάδες μέσα κοινωνικής δικτύωσης συναντώνται σήμερα στο διαδίκτυο, ενώ η εμφάνιση καινούριων μέσων αυξάνεται με ταχύτητα φωτός. Τα μέσα κοινωνικά δικτύωσης μπορούν να πάρουν διάφορες μορφές όπως σελίδες κοινωνικής δικτύωσης, blogging, ανταλλαγή πολυμέσων.

Δεν ήταν λίγοι οι ερευνητές που προσπάθησαν να τα κατηγοριοποιήσουν χρησιμοποιώντας μάλιστα διαφορετικές βάσεις. Οι Kaplan & Heinlein βασισμένοι στον συνδυασμό 2 κύριων στοιχείων των Social Media, της κοινωνικής διεργασίας και της θεωρίας των μέσων μαζικής ενημέρωσης, οι Boyd & Ellison βασισμένοι στην αλληλεπίδραση και την κοινωνικοποίηση που προσφέρει κάθε μέσο, ο Owyang βασισμένος στις δυνατότητες του κάθε μέσου.

Οι Kaplan & Heinlein διακρίνουν 5 βασικές κατηγορίες Social Media βασισμένοι σε 2 κύρια στοιχεία των Social Media, την κοινωνική διεργασία και την θεωρία των μέσων μαζικής ενημέρωσης, οι οποίες και είναι:

1. **Συνεργατικά έργα (Collaborative projects)**
2. **Ιστολόγια (Blogs)**
3. **Κοινότητες περιεχομένου (Content communities)**
4. **Εικονικοί κόσμοι (virtual worlds)**
5. **Ιστοσελίδες Κοινωνικής δικτύωσης (social networking sites).**

Από τις ως άνω κατηγορίες σκόπιμο είναι να γίνει μία αναφορά στην τελευταία, ήτοι αυτής των ιστοσελίδων κοινωνικής δικτύωσης, καθότι αποτελεί και έννοια που πραγματευόμαστε στην παρούσα διπλωματική.

Οι σελίδες κοινωνικής δικτύωσης αποτελούν σύμφωνα με τον Won Kim & al, ιστοσελίδες που επιτρέπουν στον χρήστη να σχηματίσει on line κοινότητες και να μοιραστεί περιεχόμενο μέσα σε αυτές. Αποτελούν εικονικές κοινότητες όπου μέσα σε αυτές ο χρήστης έχει την δυνατότητα να αλληλεπιδρά με φίλους ή να συμμετέχει σε ομάδες κοινών ενδιαφερόντων, δημιουργώντας αρχικά ένα προφίλ με προσωπικές πληροφορίες. Τα πιο δημοφιλή κοινωνικά δίκτυα είναι το Facebook και το Instagram. Αποτελούν την πιο διαδεδομένη μορφή των Social Media και ιστορικά προϋπήρχαν από τις υπόλοιπες μορφές μέσων κοινωνικής δικτύωσης. Ιστορικά, αξίζει να αναφέρουμε ότι οι σελίδες Classmates.Com και SixDegrees.com αποτελούν τις πρώτες επίσημες ιστοσελίδες κοινωνικής δικτύωσης, οι οποίες εμφανίστηκαν το 1995 και το 1997 αντίστοιχα.

Επιπλέον, μια επίσης περιεκτική κατηγοριοποίηση των μέσων κοινωνικής δικτύωσης καταγράφεται στο άρθρο «Social Media and Distance Education» του Zhang σύμφωνα με τον οποίο τα Social Media διακρίνονται στις παρακάτω βασικές κατηγορίες :

- Κοινωνικά δίκτυα ή σελίδες κοινωνικής δικτύωσης(social networks): Facebook
- Μέσα κοινωνικής σελιδοσήμανσης (social bookmarking) : Digg, delicious
- Ιστοσελίδες συνεργατικής συγγραφής (collaborative authoring) :Wikipedia, Google Docs.
- Ιστοσελίδες ανταλλαγής πολυμέσων (multimedia sharing): YouTube, Flickr
- Ιστολόγια (blogs- micro blogging): Blogger, Word Press, Twitter
- Διαδικτυακές τηλεδιασκέψεις (Web conferencing):WebEx, GoToMeeting, DimDim.

Στην εικόνα που παρατίθεται αμέσως μετά παρουσιάζεται η κατηγοριοποίηση κατά Bard, σύμφωνα με την οποία τα Social Media διακρίνονται σε 15 κατηγορίες.

Σχήμα 1 – **Κατηγοριοποίηση των Social Media κατά Bard (2010),**

Link φωτογραφίας: https://images.app.goo.gl/SsZuyTCuuTGX9YEk9

Χρονολογικά η τελευταία κατηγοριοποίηση που συναντήσαμε είναι αυτή του Frédéric Cavazza το 2011, ο οποίος παρομοιάζει τα Social Media *σαν ένα πλούσιο οικοσύστημα με αέναη εξέλιξη.* Δεδομένης της τεράστιας αναγνωρισιμότητας και χρήσης του Facebook ο Cavazza, το

τοποθετεί στο επίκεντρο μαζί με την Google και διακρίνει τα υπόλοιπα Social Media σε 7 κατηγορίες:

- Δημοσιεύσεις (Publish) : ιστολόγια, wikis για παράδειγμα Twitter, Wikipedia.
- Διαμοιρασμός (Share): YouTube, Flickr, Digg.
- Συζήτηση (Discuss): forums, εργαλεία κοινωνικής αναζήτησης όπως τα 4Chan, Mahalo
- Εμπόριο (Commerce): περιλαμβάνονται λύσεις για reviews πελατών (BazaarVoice), κοινότητες συστάσεων (Polyvore), εντοπισμένα κουπόνια (Groupon).
- Τοποθεσία (Location):τοπικά κοινωνικά δίκτυα (Loopt), events sharing (Eventful, Patrasevents).
- Δίκτυο (Network): Hi5, My Life, Ning.
- Παιχνίδια (Games).

1.4 Τα βασικά χαρακτηριστικά των Μέσων Κοινωνικής Δικτύωσης - Social Media

Τα μέσα κοινωνικής δικτύωσης μπορούν να γίνουν αντιληπτά ως μια ομάδα νέων μορφών διαδικτυακών μέσων που διαμορφώνονται σύμφωνα με τα παρακάτω χαρακτηριστικά (Mayfield, 2008):

- **Συμμετοχή:** Τα μέσα κοινωνικής δικτύωσης ενθαρρύνουν τη συμβολή και αντίδραση οποιουδήποτε ενδιαφερόμενου. Στην πράξη, θολώνουν τα όρια ανάμεσα στο μέσο επικοινωνίας και στο κοινό.
- **Ανοιχτός χαρακτήρας:** Τα περισσότερα μέσα κοινωνικής δικτύωσης είναι ανοιχτά στην ανάδραση και στη συμμετοχή. Ενθαρρύνουν τα σχόλια και τη συμμετοχή στις πληροφορίες. Παρουσιάζουν ελάχιστα εμπόδια στην πρόσβαση και την παραγωγή περιεχομένου και δεν ενθαρρύνουν την προστασία περιεχομένου με κωδικούς πρόσβασης.
- **Συνομιλία:** Σε αντίθεση με τα παραδοσιακά μέσα, τα μέσα κοινωνικής δικτύωσης θεωρείται ότι ενθαρρύνουν σημαντικά την ανάδραση και το διάλογο.
- **Κοινότητα:** Τα μέσα κοινωνικής δικτύωσης επιτρέπουν στις κοινότητες των ατόμων να σχηματιστούν γρήγορα και να επικοινωνήσουν αποτελεσματικά. Οι κοινότητες μοιράζονται κοινά ενδιαφέροντα, όπως την αγάπη για τη φωτογραφία, ένα πολιτικό θέμα ή μια αγαπημένη τηλεοπτική εκπομπή.
- **Συνδεσιμότητα:** Οι περισσότερες κατηγορίες των μέσων κοινωνικής δικτύωσης προάγουν τη συνδεσιμότητα, χρησιμοποιούν συνδέσμους με άλλους ιστότοπους, πηγές και ανθρώπου.

Δ. ΕΛΛΗΝΙΚΗ ΝΟΜΟΛΟΓΙΑ ΓΙΑ ΤΗΝ ΠΟΙΝΙΚΗ ΑΝΤΙΜΕΤΩΠΙΣΗ ΕΚΔΗΛΩΣΕΩΝ ΡΑΤΣΙΣΜΟΥ ΞΕΝΟΦΟΒΙΑΣ, ΕΞΥΒΡΙΣΗΣ, ΚΑΙ ΕΚΒΙΑΣΜΟΥ ΣΤΟ ΔΙΑΔΙΚΤΥΟ.

Την θεωρητική ανάλυση που προηγήθηκε συμπληρώνει η παράθεση δικαστικών αποφάσεων που αφορούν υποθέσεις στις οποίες τα ελληνικά δικαστήρια και καθ' επέκταση η ελληνική Δικαιοσύνη, κλήθηκαν αντιμέτωποι με περιπτώσεις εκδηλώσεων ρατσισμού, ξενοφοβίας, εξύβρισης, και εκβιασμού στο διαδίκτυο.

1.Νομολογία για την Ποινική Αντιμετώπιση Εκδηλώσεων Ρατσισμού και Ξενοφοβίας στο διαδίκτυο

Η αλήθεια είναι πως παρά την ολοένα και αυξανόμενη χρήση του διαδικτύου και των εφαρμογών αυτού, όπως είναι τα μέσα κοινωνικής δικτύωσης, όσον αφορά τις εκδηλώσεις ρατσισμού και ξενοφοβίας στα τελευταία, η ερεύνα για αποφάσεις δικαστηρίων της ουσίας κατέστη δυσχερής. Αυτό ίσως έχει να κάνει με το γεγονός πως και ο ίδιος ο νόμος ο 927/1979, παρά και τις μετέπειτα τροποποιήσεις του με τους νόμους 4285/2014 και 4491/2017, δεν ήταν και ιδιαίτερα δημοφιλής στην χώρα μας. Παρ' όλα αυτά κρίνεται σκόπιμο – αν και δεν γίνεται ευθεία αναφορά στις παρακάτω αποφάσεις στα μέσα κοινωνικής δικτύωσης – να αναφερθούμε σε ορισμένες αποφάσεις των ελληνικών δικαστηρίων με αποκορύφωμα αυτή του Αρείου Πάγου, την με αριθ. 3/2010, οι οποίες και αφορούν περιπτώσεις ρατσισμού και ξενοφοβίας.

Η μοναδική αμετάκλητη καταδίκη στην Ελλάδα για τον Ν. 927/1979 σημειώνεται στις με αριθμούς αποφάσεις 5800/2008 και 5919/2008 αποφάσεις του Τριμελούς Εφετείου Αθηνών, οι οποίες και επικύρωσαν την με αριθ. 16819/2008 πρωτόδικη απόφαση Τριμελούς Πλημμελειοδικείου Αθηνών. Πρόκειται για δίκη για άρνηση εγκλημάτων (άρθρο 2 ν. 927/1979 πριν την τροποποίησή του) με κατηγορουμένους δύο στελέχη της εφημερίδας «Ελεύθερος Κόσμος», ο εκδότης και διευθυντής της, ο αρχισυντάκτης και ένας αρθρογράφος, τα οποία σύμφωνα με το κατηγορητήριο *«(...) εξέφρασαν ιδέες προσβλητικές κατά ομάδος προσώπων λόγω της εθνικής καταγωγής και του θρησκεύματος των προσώπων αυτών (...) με κατάχρηση του τύπου ως μέσου, καταχώρησαν και δημοσίευσαν στο υπ' αριθμ. 142 Φύλλο της εν λόγω εφημερίδας της 12-3-2006, δημοσίευμα – άρθρο, συνταχθέν υπό του 3ου εξ αυτών, υπό τον τίτλο ''Οι Εβραίοι ζωντανεύουν την Θεσσαλονίκη'', και με το ακόλουθο περιεχόμενο ''Δόξα τω Θεώ, ούτε 1500 Εβραίοι δεν έχουν μείνει στη Θεσσαλονίκη, που ο ιδρυτής του Σιωνισμού Θεόδωρος Χέρτζλ αποκαλούσε στις αρχές του 20ου αιώνας 'Δεύτερη Ιερουσαλήμ'. Κι όμως: Όλοι οι υποψήφιοι*

άρχοντες της πόλεως γλείφουν αηδιαστικά τους απογόνους του Αβραάμ, για να εξασφαλίσουν αντιρατσιστικές περγαμηνές. (....) Ίδιες ακριβώς απόψεις για την παρακμή της Θεσσαλονίκης μετά την υποτιθέμενη 'σαπωνοποίηση' των Εβραίων εξέφρασε προ καιρού (...)».

Οι συμπεριφορές αυτές οδήγησαν στην πρωτόδικη ερήμην καταδίκη των τριών κατηγορουμένων (με τον αρθρογράφο να είναι πιθανότατα ανύπαρκτο πρόσωπο κατά τις εκτιμήσεις του ΕΠΣΕ) με την απόφαση Τριμελούς Πλημμελειοδικείου Αθηνών 16819/2008. Η καταδίκη επιβεβαιώθηκε από το Τριμελές Εφετείο Αθηνών με τις αποφάσεις του 5800 και 5919/2008, οι οποίες αργότερα κατέστησαν αμετάκλητες, με την επιβολή ποινής πέντε μηνών φυλάκισης με αναστολή στον κάθε καταδικασθέντα. Σημειωτέον ότι η εφετειακή απόφαση απέβαλε την πολιτική αγωγή εκ μέρους του ΕΠΣΕ και του Κεντρικού Ισραηλιτικού Συμβουλίου Ελλάδας.

1.1 Η με αριθ. 3/2010 απόφαση της Ολομέλειας του Αρείου Πάγου

Στο σημείο αυτό σκόπιμο είναι ν' αναφερθούμε στην έκδοση της υπ' αρ. 3/2010 Απόφασης της Ολομέλειας του Αρείου Πάγου. Αφορμή στάθηκε το βιβλίο του Κ. Πλεύρη με τίτλο «Οι Εβραίοι. Όλη η αλήθεια». Κάποιες από τις εκφράσεις είναι οι ακόλουθες: «*Έτσι θέλουν οι Εβραίοι γιατί έτσι μόνο καταλαβαίνουν: εντός 24 ωρών και εκτελεστικό απόσπασμα*». «Εβραίος και *άνθρωπος είναι έννοιες αντιφατικές, δηλαδή η μία αποκλείει την άλλη*». «*Η όλη των εγκληματική συμπεριφορά δικαιολογεί τις πράξεις των Ναζί εναντίον των και κάτι περισσότερο. Τας δικαιώνει*». «*Τους καταφρονούμε δια την ηθική των, δια την θρησκεία των, δια τας πράξεις των, που όλα μαζί αποδεικνύουν ότι είναι υπάνθρωποι*».

Συγκεκριμένα, κατά του Κωνσταντίνου Πλεύρη ασκήθηκε ποινική δίωξη για παράβαση των διατάξεων του Ν. 927/1979. Η εν λόγω ποινική δίωξη ασκήθηκε με αφορμή το βιβλίο του με τίτλο «*Οι Εβραίοι. Όλη η αλήθεια»* και τις εκφράσεις που αυτό περιέχει κάποιες από τις οποίες προεκτέθησαν. Για τη στοιχειοθέτηση της αντικειμενικής υπόστασης της διάταξης του άρθρου 1 του Ν.927/1979, απαιτείται δημόσια προτροπή από τον δράστη προς άλλον ή άλλους σε πράξεις οι οποίες μπορούν να προκαλέσουν διακρίσεις, μίσος ή βία εναντίον προσώπων ή ομάδας προσώπων, εξαιτίας της φυλετικής ή εθνικής καταγωγής τους και μόνο ή εξαιτίας του θρησκεύματός τους., ενώ για την αντικειμενική υπόσταση του άρθρου 2 του ως άνω νόμου απαιτείται η δημόσια έκφραση ιδεών για κάποιο πρόσωπο ή ομάδα προσώπων, οι οποίες είναι προσβλητικές λόγω της φυλετικής ή εθνικής καταγωγής τους ή λόγω του θρησκεύματός τους. Μέσα τέλεσης των εγκλημάτων των παρ. 1 και 2 μπορεί να είναι ο προφορικός λόγος, ο τύπος γραπτός και ηλεκτρονικός, καθώς και κάθε άλλο πρόσφορο μέσο.

Το Τριμελές Εφετείο Πλημμελημάτων πρωτοδίκως είχε καταδικάσει των Κωνσταντίνο Πλεύρη σε ποινή φυλάκισης 14 μηνών (με τριετή αναστολή). Το Πενταμελές Εφετείο Αθηνών όμως με την με αριθ. 913/2009 απόφασή του, απήλλαξε τον συγγραφέα κατά πλειοψηφία από την κατηγορία της δημόσιας προτροπής σε πράξεις, οι οποίες μπορούν να προκαλέσουν διακρίσεις, μίσος ή βία εναντίον προσώπων λόγω της φυλετικής ή εθνικής καταγωγής τους. Και αυτό με τη σκέψη ότι «….*από όλο το περιεχόμενο του βιβλίου δεν προκύπτει ότι ο κατηγορούμενος είχε πρόθεση να προτρέψει τον αναγνώστη σε πράξεις ή ενέργειες που μπορούν να προκαλέσουν διακρίσεις, μίσος ή βία κατά των Εβραίων, ούτε να εκφράσει προσβλητικές ιδέες κατ' αυτών, εκ μόνου του λόγου της φυλετικής ή εθνικής καταγωγής τους. Τούτο δε, γιατί δεν αναφέρεται συλλήβδην κατά των Εβραίων, αλλά κατά των Εβραιοσιωνιστών, οι οποίοι προέβησαν στις συγκεκριμένες πράξεις που αναφέρονται στο βιβλίο και οι οποίες στηλιτεύονται από τον συγγραφέα με οξύτατες εκφράσεις και αιχμηρά σχόλια και χαρακτηρισμούς. Η παραδοχή της αντίθετης εκδοχής θα οδηγούσε σε περιορισμό της ελευθερίας της έκφρασης και της διάδοσης των ιδεών*.»

Παρ' όλα αυτά, κατά της ως άνω εφετειακής απόφασης, ο αντεισαγγελέας του Αρείου Πάγου άσκησε αίτηση αναίρεσης υπέρ του νόμου. Και αυτό με τη σκέψη, ότι «….*η εμπάθεια και ο φανατισμός που αποτυπώνονται σε ορισμένα κομμάτια του βιβλίου καθιστούν άνευ ετέρου αυταπόδεικτο το γεγονός ότι ο συγγραφέας από πρόθεση εξέφρασε δημόσια απόψεις ικανές να προκαλέσουν διακρίσεις, μίσος και βία κατά των Εβραίων, και προσέβαλε πρόσωπα και ομάδα προσώπων λόγω της εθνοτικής τους καταγωγής*».

Συγκεκριμένα, όσον αφορά την ελευθερία της έκφρασης καθώς και τον τρόπο με τον οποίο πρέπει να ερμηνεύεται και να εφαρμόζεται ο Ν. 927/1979, ο Άρειος Πάγος έκανε ορισμένες επισημάνσεις. Αρχικά, σύμφωνα με τον Άρειο Πάγο, «…. *κατά την έννοια του νόμου, δεν συνιστά προτροπή η απλή έκφραση γνώμης, επιστημονικής κριτικής, έστω και δυσάρεστης ή επικριτικής για τα μέλη μίας φυλής ή εθνικότητας. Η προτροπή ενέχει παρότρυνση, παρόρμηση, διέγερση, ενθάρρυνση και παρακίνηση για την τέλεση πράξεων ή ενέργειας, προυπόθεση η οποία δεν συντρέχει όταν βλέπει το υποκείμενο της προτροπής στην αποδοχή και μόνο των απόψεών του*.» Επιπλέον, ο Άρειος Πάγος τόνισε ότι «….*στο πλαίσιο προστασίας των συνταγματικών δικαιωμάτων περιλαμβάνεται τόσο η ελευθερία του επιστήμονα (ιστορικού) να συγγράψει και να κυκλοφορήσει έργο στο οποίο θα καταγράφει, ερμηνεύει και αξιολογεί ιστορικά γεγονότα, όσο και το δικαίωμα κάθε πολίτη στην απρόσκοπτη και ελεύθερη πληροφόρηση, μέσω και γραπτών κειμένων για τα ιστορικά γεγονότα και τις πράξεις προσώπων που συμμετείχαν στη διαμόρφωση των γεγονότων αυτών κατά τρόπο υποκειμενικό και σύμφωνα με την κοσμοθεωρία του και τις εν γένει πολιτικές και κοινωνικές του αντιλήψεις, καταφεύγοντας και σε οξεία κριτική και δυσμενείς χαρακτηρισμούς των ιστορικών*

προσώπων και των πράξεών τους, υπό τους περιορισμούς όμως που θέτουν τα άρθρα 10 παρ. 2 της ΕΣΔΑ, 2 παρ. 1, 5 παρ. 1 και 25 παρ. 3 του Συντάγματος και τα συναφή άρθρα των ποινικών εν γένει νόμων».

Απ' όλα τα παραπάνω συνάγεται το συμπέρασμα πως πολλές από τις εκφράσεις του συγγραφέα είναι τόσο ακραίες και μισαλλόδοξες, ώστε θα ήταν αδιανόητο να θεωρηθεί ότι συμβάλλουν στον διάλογο και ότι συντελούν στην αναζήτηση της ιστορικής αλήθειας. Ο Άρειος Πάγος με τις ειδικότερες σκέψεις του στην με αριθ. 3/2010 απόφασή του, περί της προνομιακής μεταχείρισης της ελευθερίας της έκφρασης και περί της συσταλτικής και αυστηρής ερμηνείας του Ν. 927/1979, εναρμονίζεται με τη νομολογία των δικαιοδοτικών οργάνων του Στρασβούργου, σύμφωνα με την οποία η εν λόγω ελευθερία δεν είναι απλώς ένα δικαίωμα που αναγνωρίζεται στο άτομο, για την προβολή των ιδεών και την υπεράσπιση των συμφερόντων του: είναι επί πλέον μια διαδικαστική εγγύηση για την εκφορά, την υπεράσπιση, τη σύγκρουση και εν τέλει τη σύνθεση αντιτιθέμενων γνωμών και απόψεων.

1.2.Νομολογία για την Ποινική Αντιμετώπιση Εκδηλώσεων Εξύβρισης στο διαδίκτυο

Ενδεικτικά γίνεται παράθεση ορισμένων αποφάσεων των ελληνικών δικαστηρίων που σχετίζονται με το ζήτημα της εξύβρισης στα μέσα κοινωνικής δικτύωσης.

- 1765/2015 απόφαση του Πολυμελούς Πρωτοδικείο Αθηνών

Επρόκειτο για υπόθεση προσβολής προσωπικότητας μέσω αναρτήσεων, μεταξύ άλλων και στο Twitter ως διαδικτυακό μέσο κοινωνικής δικτύωσης. Συγκεκριμένα, σύμφωνα με την απόφαση «*……ο ενάγων, με την υπό κρίση αγωγή του, ιστορεί ότι ο εναγόμενος, ως συνεντευξιαζόμενος σε τηλεοπτική εκπομπή, που προεβλήθη από τον τηλεοπτικό σταθμό «....», με συντονιστή-παρουσιαστή, το δημοσιογράφο ....., κατά την ημερομηνία της 29ης-04-2012, ισχυρίσθηκε τα ειδικότερα εκτιθέμενα στο αγωγικό δικόγραφο ψευδή γεγονότα, εν γνώσει της αναλήθειάς τους, και, πιο συγκεκριμένα τον αποκάλεσε απατεώνα και πλαστογράφο, ενώ τον συνέδεσε με διατελέσαντα υπουργό της χούντας, με τον οποίο ευρισκόταν τότε σε αντιδικία, με αποτέλεσμα να προσβάλει τοιουτο τρόπως παρανόμως και υπαιτίως το δικαίωμα στην προσωπικότητά του, πλήττοντας την τιμή και την υπόληψή του. Ότι, περαιτέρω, τη 15η-12-2012, ο εναγόμενος σε ανάρτησή του στον ιστότοπο κοινωνικής δικτυώσεως «Twitter», τέλεσε σε βάρος του την αξιόποινη πράξη της εξυβρίσεως, καθώς αναφερόμενος στο πρόσωπό του, τον αποκάλεσε «προστατευόμενο» και «εθνικό μας μαλάκα»*

Το δικαστήριο δέχτηκε την τέλεση από τον εναγόμενο του αδικήματος της συκοφαντικής δυσφήμισης σε βάρος του ενάγοντος κατ' εφαρμογή των διατάξεων 363-362 του Ποινικού Κώδικα καθώς και την υπαγωγή στην έννοια του Τύπου για τις δημοσιεύσεις *«μέσω ηλεκτρονικού εγγράφου*

στο διαδίκτυο», αναφέροντας ότι «*…οποιαδήποτε προσβολή της προσωπικότητας πραγματοποιείται μέσω διαδικτύου («Internet»)…*συνιστά διά του Τύπου προσβολή και εφάρμοσε το άρθρο 681Δ του ΚΠολΔ.

1.3 Νομολογία για την Ποινική Αντιμετώπιση Εκδηλώσεων Εκφοβισμού – Εκβιασμού στο διαδίκτυο

Δημοσιευμένες αποφάσεις τόσο στις ηλεκτρονικές ιστοσελίδες όσο και σε περιοδικά που να σχετίζονται με το ζήτημα του εκφοβισμού, του εκβιασμού στο διαδίκτυο ή άλλως του cyber bulling, δεν κατέστη εφικτό να εξευρεθούν. Αυτό ίσως έχει να κάνει και με το γεγονός πως τα περισσότερα θύματα των παράνομων αυτών ενεργειών, πιθανόν να αποκρύπτουν τις εγκληματικές αυτές ενέργειες στις αρχές με αποτέλεσμα οι δράστες των εγκλημάτων αυτών να παραμένουν ατιμώρητοι. Παρακάτω γίνεται παράθεση κάποιων υποθέσεων με τις οποίες ασχολήθηκε και δημοσιοποίησε η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος καθώς και με περιπτώσεις που έγιναν γνωστές στο ευρύ κοινό λόγω της δημοσιότητας που είχαν.

Αρχικά, κάποιες από τις υποθέσεις με τις οποίες και ασχολήθηκε η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, είναι τα κατωτέρω τρία πολύ σοβαρά περιστατικά cyber bullying:

1) Μία 13χρονη μαθήτρια έκανε διαδικτυακό σεξ με έναν 14χρονο αγόρι που γνώριζε από το σχολείο της. Το κορίτσι ήταν ερωτευμένο και έκανε ότι του έλεγε ο ανήλικος. Εκείνος, ωστόσο, κατέγραψε τις σκηνές που απεικόνιζαν τη μαθήτρια γυμνή να κάνει το επονομαζόμενο «cyber sex» και στη συνέχεια ανέβασε το βιντεάκι στο διαδίκτυο για να το δουν οι συμμαθητές τους. Το αποτέλεσμα ήταν η 13χρονη να υποστεί ψυχολογικό σοκ. Ζήτησε μάλιστα από τους γονείς της να αλλάξουν τόπο διαμονής και σχολείο. Πληροφορίες αναφέρουν ότι το κορίτσι ζει σήμερα σε πόλη της επαρχίας και δεν έχει ξεπεράσει ακόμα αυτό που του συνέβη.

2) Σε σχολείο μεγάλης πόλης της περιφέρειας μία 16χρονη κατήγγειλε ότι συμμαθητής της πήρε φωτογραφία που είχε στο προφίλ της σε σελίδα στα socialmedia και μετά από μοντάζ την εμφάνιζε να συμμετέχει σε ταινία πορνό. Το βίντεο το είδαν οι φίλοι και οι φίλες του θύματος με αποτέλεσμα να του ασκηθεί τεράστια ψυχολογική πίεση. Η ΕΛ.ΑΣ. ανέλαβε τη διαλεύκανση της υπόθεσης βρίσκοντας τα ηλεκτρονικά ίχνη του 16χρονου δράστη και κατεβάζοντας από το διαδίκτυο το επίμαχο υλικό.

3) Σε πόλη της Πελοποννήσου 14χρονος χάκαρε την κάμερα που είχε ανήλικη φίλη του στον φορητό υπολογιστή της. Έτσι, κατάφερε να παρακολουθεί κρυφά όλες της τις κινήσεις και να

τις καταγράφει σε βίντεο. Είχε κρατήσει τις σκηνές που η μαθήτρια ήταν γυμνή στο δωμάτιό της και τις είχε κάνει βίντεο, το οποίο απειλούσε ότι θα ανεβάσει στο διαδίκτυο. Το κορίτσι μίλησε στους γονείς της για τις απειλές και αυτοί με τη σειρά τους ειδοποίησαν την Αστυνομία.

Φυσικά δεν θα μπορούσε να γίνει αναφορά και σε μία σοβαρή υπόθεση από το πρόσφατο παρελθόν, την υπόθεση αυτοκτονία της φοιτήτριας από την Θεσσαλονίκη, Σταυρούλας Κοεμτζή. Συγκεκριμένα, τον Νοέμβριο του 2017 και η 22χρονη φοιτήτρια Σταυρούλα Κοεμτζή κάνει βουτιά θανάτου από την ταράτσα της φοιτητικής εστίας του Αριστοτελείου Πανεπιστημίου. Οι εξελίξεις είναι συγκλονιστικές καθώς αποκαλύπτεται διαδικτυακό bulling και εκβιασμός με ροζ βίντεο, με την κοπέλα να μην αντέχει την ντροπή που ένιωθε και να βάζει τέρμα στη ζωή της. Σύμφωνα με τα στοιχεία που κατέθεσε η οικογένεια αρχικά η κοπέλα εκβιαζόταν από ένα άτομο που φέρεται ως φωτογράφος και ήθελε να την προωθεί ως μοντέλο. Όμως και πάλι σύμφωνα με πληροφορίες της οικογένειας της άτυχης φοιτήτριας αυτός δεν ήταν φωτογράφος, αλλά φοιτητής στα Χανιά και είχε πείσει την 22χρονη ότι μπορεί να την κάνει μοντέλο. Έτσι την τραβούσε φωτογραφίες που κάποιες από αυτές ήταν γυμνές και κάποιες ημίγυμνες. Ωστόσο όπως έγινε γνωστό τις φωτογραφίες αυτές το άτομο αυτό, τις ανάρτησε χωρίς την άδειά της στο προσωπικό ιστολόγιο της 22χρονης με αποτέλεσμα να τις οικειοποιηθούν επιτήδειοι και στη συνέχεια να την εκβιάζουν.

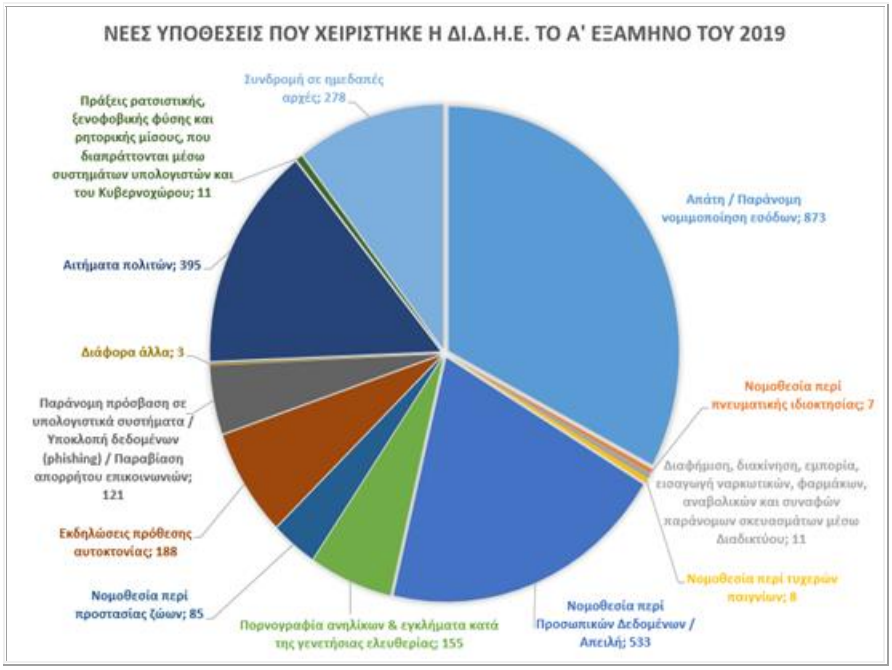
Ε. ΣΤΑΤΙΣΤΙΚΑ ΣΤΟΙΧΕΙΑ ΤΗΣ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ ΑΝΑΦΟΡΙΚΑ ΜΕ ΤΗΝ ΔΙΩΞΗ ΤΩΝ ΕΓΚΛΗΜΑΤΩΝ ΠΟΥ ΔΙΑΠΡΑΤΤΟΝΤΑΙ ΜΕΣΩ ΔΙΑΔΙΚΤΥΟΥ Η' ΜΕ ΤΗ ΧΡΗΣΗ ΑΥΤΟΥ.

Σύμφωνα με τα επίσημα στοιχεία της ελληνικής αστυνομίας, η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, κατά το Α΄ Εξάμηνο του έτους 2019, ανέπτυξε πλήθος δράσεων αφενός στον τομέα της πρόληψης και ενημέρωσης των πολιτών για ζητήματα ασφαλούς πλοήγησης στο Διαδίκτυο κι αφετέρου στον τομέα της την δίωξη των εγκλημάτων που διαπράττονται μέσω διαδικτύου η με τη χρήση αυτού.

Ειδικότερα, στον τομέα της δίωξης των εγκλημάτων που διαπράττονται μέσω Διαδικτύου ή με τη χρήση αυτού, το Α' εξάμηνο του 2019, η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος εκτέλεσε **(1.815)** Εισαγγελικές Παραγγελίες για Προκαταρκτική Εξέταση ή Προανάκριση, από όλες τις Εισαγγελίες Πρωτοδικών της Χώρας. Από αυτές **(1.449)** χειρίσθηκε η Διεύθυνση και **(366)** η Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος Βορείου Ελλάδος.

Ο συνολικός αριθμός νέων υποθέσεων το Α΄ εξάμηνο έτους 2019 ανήλθε σε **2.668**. (Ο αριθμός αυτός αναφέρεται στα νέα πρωτόκολλα που εκδόθηκαν, είτε επρόκειτο για νέα εισαγγελική παραγγελία, είτε για προανακριτικό υλικό, εγκλήσεις πολιτών κ.λπ.).

Συγκεκριμένα, η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος χειρίστηκε, κατά περίπτωση, τις εξής υποθέσεις:



Σχήμα 2 – **Υποθέσεις που χειρίστηκε η ΔΙ.Δ.Η.Ε. το Α' εξάμηνο του 2019**

Link φωτογραφίας: http://www.astynomia.gr/images/stories//2019/photos2019b/16092019-a_examino17.png

Όπως προκύπτει και από το ως άνω σχήμα που δημοσιοποίησε η ελληνική αστυνομία στην επίσημη ιστοσελίδα της, η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, εκτός των άλλων υποθέσεων ασχολήθηκε και με υποθέσεις που αφορούν πράξεις ρατσιστικής, ξενοφοβικής φύσης και ρητορικής μίσους που διαπράχθηκαν μέσω των συστημάτων υπολογιστών και του Κυβερνοχώρου, έντεκα στο σύνολο τους.

Παρά το γεγονός, πως αν και από το σχήμα αυτό αλλά και τα επίσημα στοιχεία της ελληνικής αστυνομίας δεν μπορούμε να γνωρίζουμε ακριβώς το είδος των πράξεων αυτών, πώς ασκήθηκαν, κατά ποίου στρέφονταν, πώς ενήργησαν τα θύματα, και εάν πήραν εν τέλει τον δρόμο της δικαιοσύνης, καταλήγουμε στο εξής συμπέρασμα: Δυστυχώς ακόμη και στις μέρες μας, ο ρατσισμός, η ξενοφοβία, ο εκβιασμός, με πομπούς (και) τα μέσα κοινωνικής δικτύωσης και αποδέκτες κατά κύριο λόγο αδύναμα πρόσωπα, τα οποία για προσωπικούς, ψυχολογικούς, οικονομικούς λόγους δυστυχώς αδυνατούν να υπερασπιστούν τον εαυτό τους, και ίσως σε αυτό να

οφείλεται το γεγονός πως για το πρώτο εξάμηνο του 2019 η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος να ασχολήθηκε μόνο με έντεκα τέτοιες υποθέσεις, είναι καλά «ριζωμένοι».

Αποτελεί υποχρέωση για τον καθένα από εμάς ξεχωριστά και φυσικά τόσο για την ελληνική αστυνομία όσο και για την Δικαιοσύνη που έχει και τον κύριο λόγο, να σταθούμε απέναντι σε κάθε μορφή ρατσιστικών, ξενοφοβικών, εκβιαστικών πράξεων, απ' οπουδήποτε και εάν εκδηλώνονται αυτές, έτσι ώστε αυτές να περιοριστούν και γιατί όχι με την συνδρομή των αρχών να εξαφανιστούν και να μην εκδηλωθούν ξανά.

ΣΤ. ΣΥΜΠΕΡΑΣΜΑΤΑ

Το Σύνταγμά μας, οι διεθνείς και ευρωπαϊκοί θεσμοί, αποτελούν το μανδύα προστασίας της ελευθερίας της έκφρασης. Τόσο η νομολογία των Ελληνικών δικαστηρίων, όσο και του Ευρωπαϊκού Δικαστηρίου Ανθρωπίνων Δικαιωμάτων αποτελούν χρήσιμο εργαλείο για την επίτευξη του επιθυμητού αυτού στόχου, ήτοι της προστασίας του δικαιώματος της ελευθερίας της έκφρασης. Αξίζει δε στο σημείο αυτό να αναφέρουμε πως οι περιορισμοί που τίθενται, έχοντας ως βάση πάντα την αρχή της αναλογικότητας, δεν «υποτιμούν» την ίδια την αξία του δικαιώματος της ελευθερίας της έκφρασης, αλλά κρίνονται αναγκαίοι για την άσκηση άλλων δικαιωμάτων που ad hoc κρίνονται σημαντικότερα για το ίδιο το συμφέρον της κοινωνίας, ή για την κάλυψη κάποιων επιτακτικών αναγκών.

Φυσικά, πάρα την αξία του δικαιώματος της ελευθερίας της έκφρασης, την οποία και τονίσαμε ήδη από τα πρώτα κεφάλαια της παρούσας διπλωματικής, δεν γίνεται να μην αναφερθούμε και στις προσπάθειες εξάλειψης φαινομένων ρατσισμού, ξενοφοβίας, εκβιασμού και εξύβρισης, φαινόμενα που «εκφράζονται» και βρίσκουν έρεισμα και μέσω των μέσων κοινωνικής δικτύωσης, τα οποία και διαδραματίζουν σημαντικό ρόλο στην καθημερινότητα του σύγχρονου ανθρώπου. Τα μέσα κοινωνικής δικτύωσης δυστυχώς αποτελούν φερέφωνα όλων εκείνων, οι οποίοι εκμεταλλευόμενοι την ανωνυμία που αυτά μπορούν να προσφέρουν, εκφράζονται ρατσιστικά, εξυβρίζουν και εκβιάζουν ανθρώπους με κίνητρα άλλοτε οικονομικά, άλλοτε αποκλειστικά και μόνο να βλάψουν την τιμή και την υπόληψη των υποψήφιων θυμάτων τους.

Αβίαστα επομένως προκύπτει το συμπέρασμα, πως η κοινωνία με την αρωγή φυσικά και πρωτίστως της Δικαιοσύνης, η οποία και λειτουργεί «τυφλά», χωρίς να κάνει διακρίσεις ανάμεσα σε φύλο, εθνικότητα, χρώμα, οικονομική κατάσταση, μπορεί να σταθεί απέναντι σε όλους αυτούς τους εκβιασμούς και τις εξυβρίσεις που λαμβάνουν χώρα μέσω των μέσων κοινωνικής δικτύωσης. Η αλήθεια είναι, πως μπορεί τουλάχιστον στο κομμάτι της Ελληνικής Δικαιοσύνης, οι αποφάσεις που σχετίζονται με τα social media και τις προσβολές και τους εκβιασμούς που συμβαίνουν μέσω

αυτών να είναι ελάχιστες και αυτό ίσως να έχει να κάνει με το γεγονός ότι τα θύματα πιθανόν να φοβούνται να στραφούν κατά του θύτη τους και να ζητήσουν την βοήθεια είτε των αστυνομικών αρχών είτε της Δικαιοσύνης, παρ' όλα αυτά γίνονται θα λέγαμε σοβαρές και σημαντικές προσπάθειες και από τους δύο αυτούς σημαντικούς πυλώνες της ασφάλειας και της δικαιοσύνης για την πάταξη των εγκλημάτων που λαμβάνουν χώρα μέσω των μέσων κοινωνικής δικτύωσης. Τόσο η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος όσο και η ύπαρξη Εισαγγελέα που άπτεται αποκλειστικά των θεμάτων που σχετίζονται με το ηλεκτρονικό έγκλημα, αποδεικνύουν πως η πολιτεία δεν δέχεται να συμβαίνουν στους κόλπους της εγκλήματα που θίγουν προσωπικότητες και οδηγούν ακόμη και στον θάνατο ανθρώπους, και τα οποία συμβαίνουν μέσω των μέσων κοινωνικής δικτύωσης.

Βέβαια, αξίζει τέλος να αναφέρουμε πως και οι πάροχοι των μέσων κοινωνικής δικτύωσης, θέτουν στις σελίδες τους όρους και προϋποθέσεις αναφορικά με τον τρόπο προστασίας των χρηστών από περιπτώσεις εκβιασμού και εκφοβισμού. Ειδικότερα, στην σελίδα www.facebook.com, για παράδειγμα, σε ειδική φόρμα ο χρήστης μπορεί, αφού απαντήσει αρχικά σε κάποιες ερωτήσεις και αφού περιγράψει το περιστατικό, να αποστέλλει τα στοιχεία αυτά στο facebook για περαιτέρω διερεύνηση της υπόθεσης. Στην ίδια σελίδα δε υπάρχει και το μήνυμα πως ο χρήστης, εφόσον αντιληφθεί ότι έχει πέσει θύμα εκβιασμού ή εκφοβισμού, εκτός από το ίδιο το facebook, θα πρέπει να το αναφέρει απευθείας στις τοπικές διωκτικές αρχές.

Β.ΜΕΡΟΣ

1.ΟΡΙΣΜΟΣ CLOUD COMPUTING

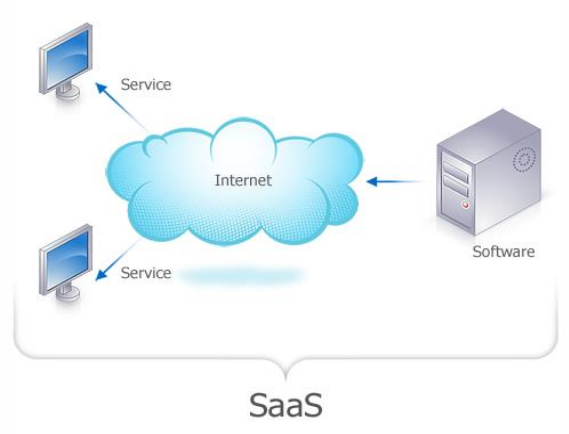
Με μία απλή αναζήτηση τόσο στο Internet όσο και σε πληθώρα επιστημονικών άρθρων και μελετών, μπορεί κανείς να βρει διάφορους ορισμούς του Cloud computing. Σύμφωνα με μία γνώμη η οποία θα λέγαμε πως αποτυπώνει απλά και κατανοητά την έννοια που εξετάζουμε, αναφέρει πως το **Cloud computing** *είναι μία δομή, με την οποία μας δίνεται η δυνατότητα να έχουμε πρόσβαση και να χρησιμοποιούμε web εφαρμογές χωρίς να τις διαθέτουμε στον υπολογιστή μας ή σε κάποια άλλη συσκευή που είναι διασυνδεδεμένη με το ίντερνετ. Σε αυτή τη δομή η εφαρμογή βρίσκεται σε ένα server και εμείς τη χρησιμοποιούμε χωρίς να χρειάζεται να την εγκαταστήσουμε στον υπολογιστή μας,* ενώ, το **Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας** (National Institute of Standards and Technology - NIST) χαρακτηρίζει το cloud computing ως «…..*ένα μοντέλο αμοιβής ανά χρήση για τη διευκόλυνση της πρόσβασης σε δίκτυο σε κοινόχρηστο σύνολο διαμορφωμένων πόρων πληροφορικής (π.χ. δίκτυα, διακομιστές, αποθήκευση, εφαρμογές, υπηρεσίες) που μπορούν να παρασχεθούν γρήγορα και να απελευθερωθούν με ελάχιστη προσπάθεια διαχείρισης ή*

αλληλεπίδρασης παρόχου υπηρεσιών (a pay-per-use model for enabling available, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.)

1.2. Βασικά είδη υπηρεσιών που προσφέρει το Cloud Computing – Cloud models.

i. Software as Service (SasS)

Σε αυτό τον τύπο υπάρχει ένα application το οποίο βρίσκεται σε ένα **cloud server** και ο χρήστης μπορεί να έχει πρόσβαση σε αυτό μέσω μίας απλή σύνδεσης στο ίντερνετ. Το software αυτό ανήκει σε κάποιον κατασκευή και ο χρήστης το πληρώνει ανάλογα με την χρήση που του κάνει και τους πόρους που χρειάζεται. Το βασικό πλεονέκτημα του μοντέλου «**software as service**» είναι ότι ο κατασκευαστής αναλαμβάνει τα έξοδα συντήρησης του software καθώς και τη φιλοξενία του σε κάποιον cloud server. Ο χρήστης πληρώνει μόνο την χρήση που κάνε(αν και υπάρχουν και **cloud applications** που είναι δωρεάν).Επίσης το μοντέλο SasS είναι δημιουργημένο με βασικό γνώμονα τη σωστή λειτουργία του software με χρήση **browser**. Όσον αφορά την ασφάλεια των διαφόρων εφαρμογών, συνήθως χρησιμοποιείται SSL (Secure Sockets Layer) το οποίο είναι παγκοσμίως αναγνωρισμένο. Έτσι, οι χρήστες μπορούν με ασφάλεια να χρησιμοποιήσουν το cloud application.

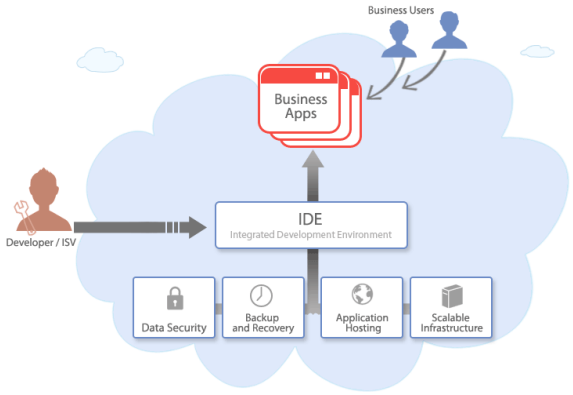


Σχήμα 3 - **Software as Service (SasS)**

Link φωτογραφίας: http://c.teamwox.com/articles/2010/4/SaaS_pic.png

ii. Platform as Service (PasS)

Αυτό το μοντέλο μοιάζει πολύ με το προηγούμενο. Το βασικό του στοιχείο είναι ότι παρέχει την πλατφόρμα την οποία χρησιμοποιεί ένας χρήστης για να δημιουργήσει κάτι, για παράδειγμα ένα web application, χωρίς να εγκαταστήσει τίποτα. Το «platform as service» μοντέλο χρησιμοποιείται πιο πολύ για δημιουργία web interfaces, web εφαρμογών κλπ. Ένα σημαντικό πρόβλημα που υπάρχει με αυτό το μοντέλο είναι ότι αυτή η εφαρμογή που δημιουργούμε βασίζεται σε ένα συγκεκριμένο framework και υπάρχει πιθανότητα αν θελήσουμε να την μεταφέρουμε σε άλλο παροχέα cloud υπηρεσιών αυτή να μη λειτουργεί σωστά.



Σχήμα 4 - **Platform as Service (PasS)**

Link φωτογραφίας:http://www.zoho.com/creator/images/subpages/paas.gif

iii. Storage as a service (StaaS)

Στο μοντέλο αυτό υπάρχει κάποιος πάροχος αποθηκευτικού χώρου online ο οποίος στην ουσία τον νοικιάζει έναντι κάποιας αμοιβής. Ένα παράδειγμα απλό θα μπορούσε να θεωρηθεί το Dropbox, το Icloud καθώς και το Google Drive

Σχήμα 5 - **Storage as a service (StaaS)**

Link φωτογραφίας: http://freewarefeed.com/how-to-get-100-gb-free-online-storage/

iv. Hardware as Service (HaaS)

Εδώ τα πράγματα έχουν ως εξής: Ο προμηθευτής αυτής της cloud υπηρεσίας παρέχει στον χρήστη έναντι «ενοικίου»-αμοιβής το hardware που χρειάζεται όπως web servers, μνήμη CPU ,αποθηκευτικό χώρο και ότι άλλο χρειάζεται ο χρήστης σε επίπεδο hardware. Τα χρήματα που πληρώνει κάποιος στο HaaS είναι αντίστοιχα της χρήσεως των πόρων του συστήματος που κάνει.

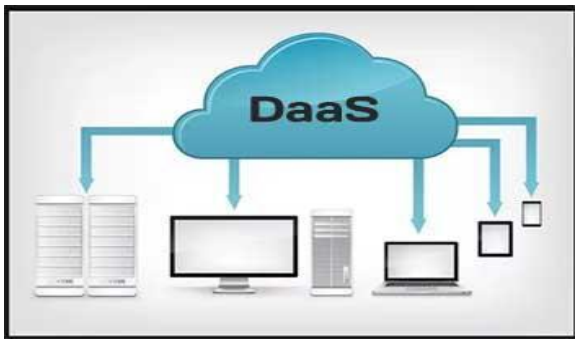
Σχήμα 6 - **Hardware as Service (HaaS**

Link φωτογραφίας: http://www.mis.com.bd/hardware-as-a-service/

v. Database as Service (DaaS)

Σε αυτό το μοντέλο υπάρχει μία υπηρεσία online παρέχει την βάση δεδομένων την οποία μπορούμε να χρησιμοποιήσουμε με κάποιο web application. Σε αυτό το μοντέλο το βασικό πλεονέκτημα είναι ότι πληρώνουμε ανάλογα με την χρήση. Ουσιαστικά όσο πιο πολύ κόσμος

χρησιμοποιεί την εφαρμογή μας τόσο περισσότερα χρήματα πληρώνουμε. Μία τέτοια υπηρεσία είναι η mongoDB.

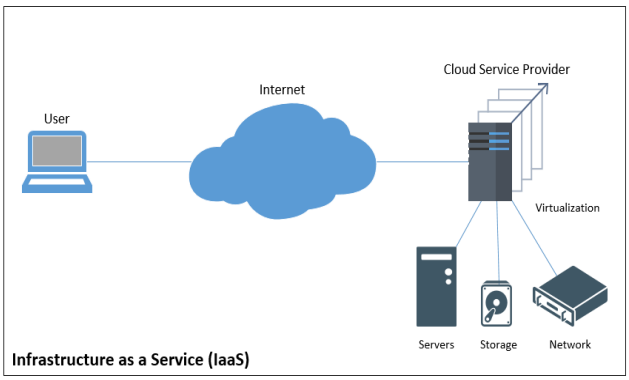


Σχήμα 7 - **Database as Service (DaaS)**

Link φωτογραφίας: https://oracle-patches.com/en/databases/3327-what-is-daas-data-as-a-service

vi. Infrastructure as a Service (IaaS)

Οι υποδομές ως υπηρεσία, χρησιμοποιούνται για την παρακολούθηση και τη διαχείριση απομακρυσμένων υποδομών κέντρου δεδομένων, όπως υπολογιστικά (virtualized ή «γυμνά μέταλλα»), αποθήκευση. Οι χρήστες μπορούν να αγοράζουν IaaS με βάση την κατανάλωση, παρόμοια με άλλες χρεώσεις χρηστών. Οι χρήστες του IaaS έχουν την ευθύνη να είναι υπεύθυνοι για τις εφαρμογές, τα δεδομένα, το χρόνο εκτέλεσης. Οι πάροχοι μπορούν ακόμα να διαχειριστούν την εικονικοποίηση (virtualization), τους servers, την αποθήκευση και την δικτύωση. Οι πάροχοι IaaS προσφέρουν βάσεις δεδομένων, και άλλες υπηρεσίες πάνω από το επίπεδο εικονικοποίησης.



Σχήμα 8 - **Infrastructure as a Service (IaaS)**

Link φωτογραφίας: https://www.oreilly.com/library/view/information-security-handbook/9781788478830/f564b882-1317-4292-baa8-b8980823be6c.xhtml

1.3.Ουσιώδη χαρακτηριστικά του Cloud Computing

Πέντε είναι τα ουσιώδη χαρακτηριστικά του Cloud Computing, τα οποία εξηγούν τόσο τη σχέση όσο και τη διαφορά που υφίσταται συγκριτικά με τις παραδοσιακές υπολογιστικές μεθόδους.

- Αυτό - εξυπηρέτηση κατ' απαίτηση (on demand self- service)

Οι καταναλωτές μπορούν να εφοδιάζονται ή να απορρίπτουν την παροχή υπηρεσιών, χωρίς ανθρώπινη διαμεσολάβηση με τον πάροχο υπηρεσιών.

- Διάθεση πόρων (resourse pooling)

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

- Ευρεία πρόσβαση στο δίκτυο.

Παρέχεται ικανότητα καλύψης δικτύου και πρόσβαση μέσω τυποποιημένων μηχανισμών.

- Ταχεία ελαστικότητα.

Υπηρεσίες μπορούν να παρέχονται γρήγορα και ελαστικά

- Μετρούμενη υπηρεσία

Τα συστήματα Cloud Computing οργανώνουν και βελτιστοποιούν αυτόματα την διάθεση των πόρων παρέχοντας δυνατότητα μέτρησης των χρησιμοποιούμενων υπηρεσιών ανάλογα το είδος (για παράδειγμα: αποθήκευσης, επεξεργασίας, εύρους σύνδεσης ή διαθέσιμων λογαριασμών χρηστών).

Στην παρούσα μελέτη θα ασχοληθούμε με το δεύτερο από τα ως άνω περιγραφόμενα είδη - μοντέλα του Cloud Computing, ήτοι το **Storage as a service (StaaS),** και συγκεκριμένα θα αναλυθεί η έννοια του ως άνω όρου, θα καταγραφούν τα ιδιαίτερα χαρακτηριστικά του, η ασφάλεια που παρέχει στον χρήστη που κάνει χρήση αυτού. Βέβαια, δεν θα μπορούσε να μην γίνει αναφορά - αποτελεί εξάλλου και αντικείμενο της παρούσας μελέτης - στον τρόπο χρήσης του από τον απλό χρήστη «εν δυνάμει» όμως κατηγορούμενο καθώς και τον τρόπο προστασίας των «εν δυνάμει» θυμάτων του τελευταίου, με παραπομπές στην Νομολογία των Δικαστηρίων.

2. STORAGE AS A SERVICE (STAAS)

2.1. Έννοια – ερμηνεία του StaaS

Αν μπορούσαμε να δώσουμε μία ερμηνεία στον όρο που μας απασχολεί στο παρόν κεφάλαιο της μελέτης, θα λέγαμε πως η αποθήκευση (storage) ως υπηρεσία (**STaaS**) είναι ένα μοντέλο υπολογιστικού νέφους στο οποίο οι συνδρομητές μπορούν να «ενοικιάσουν» αποθηκευτικούς χώρους από παρόχους υπηρεσιών του cloud. Η υπηρεσία χρησιμοποιείται κυρίως για την επίλυση προβλημάτων αποθήκευσης καθώς και εξωτερικών backup προκλήσεων (π.χ. καταστροφή σκληρού δίσκου υπολογιστή).

Η αποθήκευση (storage) εκμισθώνεται με συνδρομή μηνιαία, ή ετήσια. Επιτρέπει στους πελάτες - χρήστες να αποθηκεύουν εύκολα τα δεδομένα τους (αρχεία, εικόνες κ.λπ.) στο λογαριασμό του παρόχου. Για όλα τα αποθηκευμένα δεδομένα τους, οι πελάτες – χρήστες, μπορούν να αποκτήσουν πρόσβαση από οπουδήποτε, αρκεί φυσικά να υπάρχει πρόσβαση στο διαδίκτυο. Επιπλέον, η υπηρεσία αυτή βοηθά τον πελάτη – χρήστη να εξοικονομήσει κόστος, καθώς η παροχή του δικού του χώρου αποθήκευσης είναι δαπανηρότερη από την ενοικίαση χώρου αποθήκευσης από τον πάροχο της υπηρεσίας cloud.

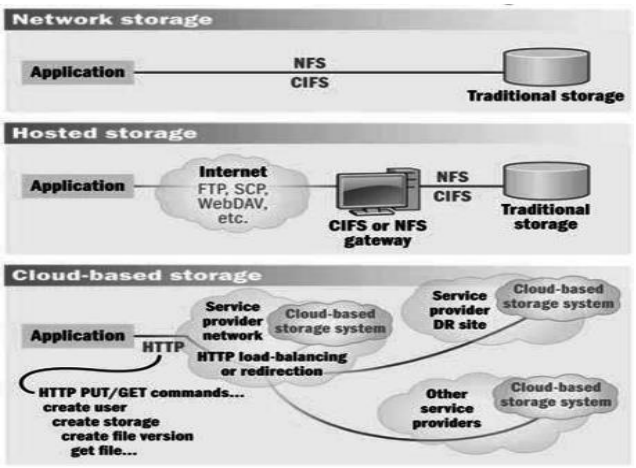
Παράλληλα, αξίζει να αναφέρουμε ότι η αποθήκευση στο cloud στις μέρες μας είναι άμορφη, χωρίς ούτε σαφώς καθορισμένο σύνολο δυνατοτήτων ούτε κάποια αρχιτεκτονική. Οι επιλογές αφθονούν, με πολλούς παραδοσιακούς φιλοξενούμενους ή διαχειριζόμενους παρόχους υπηρεσιών (ManagedServiceProviders), οι οποίοι προσφέρουν αποκλεισμό ή αποθήκευση αρχείων, συνήθως παράλληλα με τα παραδοσιακά πρωτόκολλα απομακρυσμένης πρόσβασης, ή εικονικό ή φυσικό διακομιστή φιλοξενίας. Άλλες λύσεις έχουν αναδυθεί, που έχουν χαρακτηριστεί από την υπηρεσία Amazon S3, που μοιάζει με επίπεδες βάσεις δεδομένων σχεδιασμένες για την αποθήκευση μεγάλων αντικειμένων. Ο όμιλος Taneja (ομάδα αναλυτών και συμβούλων που εδρεύει στο Hopkinton της Μασαχουσέτης. Ιδρύθηκε το 2003 και παρέχει ανάλυση και συμβουλές για τον κλάδο της

τεχνολογίας. Ειδικεύεται στην αποθήκευση και την εικονικοποίηση) ορίζει την αποθήκευση στο cloud ως μια συγκεκριμένη κατηγορία εντός του μεγαλύτερου *«storage in the clou»* λύσεων.

Επίσης, η αποθήκευση στο cloud περιλαμβάνει παραδοσιακά φιλοξενούμενα αποθήκευση, συμπεριλαμβανομένων των προσφορών που έχουν πρόσβαση από το FTP, WebDAV, NFS / CIFS ή πρωτόκολλα αποκλεισμού είτε από απόσταση είτε από ένα φιλοξενούμενο περιβάλλον. Η αποθήκευση στο cloud, είναι μια εξέλιξη αυτής της φιλοξενούμενης τεχνολογίας αποθήκευσης (hosted storage technology) περιβάλλει πιο εξελιγμένα APIs (**A**pplication**P**rogramming**I**nterface**)**, χώρους ονομάτων, αρχεία ή την εικονικοποίηση τοποθεσίας δεδομένων και τα εργαλεία διαχείρισης, γύρω από την αποθήκευση.

Υπάρχουν εκατοντάδες διαφορετικά συστήματα αποθήκευσης στο cloud. Μερικά έχουν ένα πολύ συγκεκριμένο προσανατολισμό, όπως η αποθήκευση μηνυμάτων ηλεκτρονικού ταχυδρομείου ή ψηφιακών εικόνων. Άλλα είναι διαθέσιμα για να αποθηκεύουν όλες τις μορφές των ψηφιακών δεδομένων. Ορισμένα συστήματα αποθήκευσης στο cloud, είναι μικρές λειτουργίες, ενώ άλλες είναι τόσο μεγάλες ώστε ο «φυσικός» εξοπλισμός να μπορεί να γεμίσει μία ολόκληρη αποθήκη. Οι εγκαταστάσεις που φιλοξενούν συστήματα αποθήκευσης στο σύννεφο καλούνται κέντρα δεδομένων (Data Centers). Στο πιο βασικό επίπεδο, ένας χώρος αποθήκευσης στο σύννεφο (cloud storage), χρειάζεται μόνο έναν διακομιστή δεδομένων συνδεδεμένο με το Διαδίκτυο. Ένας πελάτης (για παράδειγμα, ένας χρήστης του υπολογιστή που είναι συνδρομητής σε μια υπηρεσία αποθήκευσης νέφους) στέλνει αντίγραφα των αρχείων μέσω του Διαδικτύου στον διακομιστή δεδομένων (Data Server), ο οποίος στη συνέχεια καταγράφει το πληροφορίες. Όταν ο πελάτης επιθυμεί να ανακτήσει τις πληροφορίες, αυτός ή αυτή έχει πρόσβαση στον διακομιστή δεδομένων μέσω ενός διαδικτυακού περιβάλλοντος. Ο διακομιστής τότε είτε στέλνει τα αρχεία πίσω στον πελάτη ή επιτρέπει στον πελάτη να έχει πρόσβαση και να διαχειρίζεται τα αρχεία του στον ίδιο τον διακομιστή.

Το σχήμα 7 δείχνει την εξέλιξη της αποθήκευσης στο σύννεφο (Cloud Storage), βασιζόμενο στην παραδοσιακή αποθήκευση στο δίκτυο (Network Storage) και στην φιλοξενούμενη αποθήκευση (Hosted Storage).



Σχήμα 9 - **Evolution of Cloud Storage**

Link φωτογραφίας:

https://www.researchgate.net/publication/234166321_Cloud_Computing-Storage_as_Service/figures?lo=1&utm_source=google&utm_medium=organic

2.2. Τα τρία κύρια μοντέλα αποθήκευσης (storage) στο νέφος

- Οι δημόσιες υπηρεσίες αποθήκευσης (storage) στο cloud, όπως η υπηρεσία απλής αποθήκευσης (S3) της Amazon, οι οποίες παρέχουν ένα περιβάλλον αποθήκευσης που είναι το πλέον κατάλληλο για αδόμητα δεδομένα.
- Οι ιδιωτικές υπηρεσίες αποθήκευσης (storage) στο cloud, οι οποίες παρέχουν ένα αποκλειστικό περιβάλλον που προστατεύεται πίσω από το τείχος προστασίας ενός οργανισμού. Τα ιδιωτικά σύννεφα είναι κατάλληλα για χρήστες που χρειάζονται προσαρμογή και μεγαλύτερο έλεγχο των δεδομένων τους.
- Η υβριδική αποθήκευση (storage) στο cloud. Πρόκειται για έναν συνδυασμό των άλλων δύο μοντέλων που περιλαμβάνει τουλάχιστον ένα ιδιωτικό cloud και μία δημόσια cloud υποδομή. Μια οργάνωση μπορεί, για παράδειγμα, να αποθηκεύει δεδομένα που χρησιμοποιούνται ενεργά και δομημένα σε ένα ιδιωτικό σύννεφο, καθώς και μη δομημένα και αρχειακά δεδομένα σε ένα δημόσιο σύννεφο.

2.3 Υπηρεσίες Cloud

Ως κατέστη σαφές και ανωτέρω, η έννοια του υπολογιστικού νέφους αν και είναι δύσκολο να γίνει κατανοητή, παρ' όλα αυτά, έχουν υλοποιηθεί πολλές εφαρμογές οι οποίες χρησιμοποιούνται, εδώ και αρκετά χρόνια, σε καθημερινή βάση. Τόσο η εξέλιξη της τεχνολογίας,

όσο και η συνεχής αύξηση της ζήτησης της αγοράς, έχουν ως αποτέλεσμα να αυξάνεται συνεχώς και η ανάγκη για περισσότερους υπολογιστικούς πόρους. Η ανάγκη αυτή, οδήγησε στη δημιουργία μιας πληθώρας εφαρμογών, όπως, το ICloud, το Google Drive, το OneDrive, το Dropbox οι οποίες προορίζονται τόσο για προσωπική χρήση όσο και για τη διευκόλυνση των εταιριών στην αποθήκευση, στο διαμοιρασμό και τη διαχείριση των αρχείων. Ειδικότερα:

2.3.1 Onedrive

Το OneDrive είναι η cloud υπηρεσία της Microsoft, η οποία παρέχει δωρεάν χώρο στο Διαδίκτυο, δίνοντας μας την δυνατότητα, να αποθηκεύσουμε, να επεξεργαστούμε φωτογραφίες, βίντεο και έγγραφα είτε μόνη μας, είτε με την «βοήθεια» και άλλον ατόμων, έχοντας απλά πρόσβαση από οποιονδήποτε υπολογιστή. Κάθε έγγραφο που δημιουργείται, μπορεί να αποθηκευτεί αυτόματα στο OneDrive, με διαφορετικά δικαιώματα πρόσβασης, ανάλογα με το τι έχει εκχωρηθεί από τους δημιουργούς των αρχείων. Για να περιορίσει τη πρόσβαση στα ιδιωτικά αρχεία ενός χρήστη ή στον διαμοιρασμό τους με επαφές, χρησιμοποιεί την υπηρεσία Windows Live ID. Ο βοηθός εισόδου Windows Live ID, επιτρέπει σε μια εφαρμογή Windows, που εκτελείται σε έναν υπολογιστή, να αναγνωρίζει και να επικοινωνεί με άλλους υπολογιστές που έχουν συσχετιστεί με το ίδιο Windows Live ID. Επιπλέον, υπάρχει η δυνατότητα απευθείας ανάρτησης αρχείων, δημιουργίας φακέλων για ταξινόμηση και εκχώρηση δικαιωμάτων και είναι συνδεδεμένο με έναν λογαριασμό ηλεκτρονικού ταχυδρομείου (Outlook.com). Τέλος, τα αποθηκευμένα αρχεία, είναι διαθέσιμα ακόμα και αν βρίσκεται κανείς εκτός σύνδεσης. Όταν συνδεθεί ξανά στο Διαδίκτυο, τότε το OneDrive ενημερώνει τις εκδόσεις online, με όποια αλλαγή έγινε εκτός σύνδεσης.

2.3.2 Google Drive

Το Google Drive, είναι η υπηρεσία αποθήκευσης φωτογραφιών, βίντεο, ειδήσεων και συνημμένων αρχείων του ηλεκτρονικού ταχυδρομείου της Google. Ο αποθηκευτικός χώρος, λειτουργεί μέσω του Drive, του Gmail (ηλεκτρονικό ταχυδρομείο της Google) και το Google Photos. Τα αρχεία, είναι προσβάσιμα οποιαδήποτε χρονική στιγμή τα χρειαστούμε και από κάθε συσκευή (υπολογιστή, κινητό, tablet), ακόμα και αν η συσκευή βρίσκεται εκτός σύνδεσης, επιλέγοντας μια λειτουργία της εφαρμογής. Επιπλέον, παρέχει τη δυνατότητα κοινής χρήσης των αρχείων σε άλλους χρήστες, με σκοπό την επεξεργασία ή την άμεση προβολή τους, τη δημιουργία υπολογιστικών φύλλων, κ.ά. Ακόμα, μπορεί να αναγνωρίσει αντικείμενα πάνω στις φωτογραφίες και σε σαρωμένα κείμενα, με αποτέλεσμα να εμφανίζεται κάθε σχετικό αρχείο ή φάκελος σχετικά με τη λέξη/φράση που έγινε η αναζήτηση ή ακόμα και να επεξεργαστεί τις αποθηκευμένες φωτογραφίες αυτόματα.

2.3.3 Dropbox

Το Dropbox αποτελεί και αυτό μια υπηρεσία αποθήκευσης και συγχρονισμού αρχείων και εικόνων στο Διαδίκτυο. Λειτουργεί με την εγκατάσταση της εφαρμογής στον υπολογιστή, δημιουργώντας έναν φάκελο μέσα στον οποίο γίνονται όλες οι λειτουργίες. Παρόλο που είναι μια εφαρμογή εγκατεστημένη στον υπολογιστή, ο χρήστης έχει τη δυνατότητα πρόσβασης στα αρχεία από οποιοδήποτε μέσο (υπολογιστή, tablet, κινητό) που είναι συνδεδεμένο με τον συγκεκριμένο λογαριασμό. Επιπλέον, όπως και στο OneDrive, έτσι και εδώ, υπάρχει η δυνατότητα κοινόχρηστων αρχείων ή φακέλων, όπου μια ομάδα ατόμων έχει τη δυνατότητα πρόσβασης και επεξεργασίας αυτών.

2.3.4 ICloud

Το iCloud είναι ένα πρόγραμμα αποθήκευσης που ξεκίνησε από την Apple το 2011. Από το 2018, η υπηρεσία είχε κατ 'εκτίμηση 850 εκατομμύρια χρήστες, από 782 εκατομμύρια χρήστες το 2016. Το iCloud επιτρέπει στους χρήστες να αποθηκεύουν δεδομένα όπως έγγραφα, φωτογραφίες και μουσική σε απομακρυσμένους διακομιστές για λήψη σε συσκευές iOS, macOS ή Windows, να μοιράζονται και να στέλνουν δεδομένα σε άλλους χρήστες και να διαχειρίζονται τις συσκευές Apple τους σε περίπτωση απώλειας ή κλοπής.

Το iCloud παρέχει επίσης τα μέσα ασύρματης δημιουργίας αντιγράφων ασφαλείας των συσκευών iOS απευθείας στο iCloud, αντί να εξαρτώνται από τη χρήση μη αυτόματων αντιγράφων ασφαλείας σε έναν υπολογιστή Mac ή Windows που χρησιμοποιεί το iTunes. Οι χρήστες των υπηρεσιών μπορούν επίσης να μοιράζονται άμεσα φωτογραφίες, μουσική και παιχνίδια με τη σύνδεση λογαριασμών μέσω ασύρματης σύνδεσης AirDrop.

Στο σημείο αυτό κρίνεται σκόπιμο να γίνει αναφορά στον ρόλο των παρόχων υπηρεσιών cloud computing και συγκεκριμένα στον χαρακτηρισμό τους είτε ως υπεύθυνους επεξεργασίας είτε ως εκτελούντες την επεξεργασίας, έτσι ώστε -όπως θα αναλυθεί και εν συνεχεία – να προσδιοριστεί ο ρόλος τους καθώς και το μέγεθος της ευθύνης σε περιπτώσεις παραβίασης των προσωπικών δεδομένων.

2.3.5 Ρόλος παρόχων υπηρεσιών στο Cloud

Αρχικά, η αλήθεια είναι πως η διάκριση μεταξύ υπεύθυνου επεξεργασίας και εκτελούντος την επεξεργασία δεδομένων προσωπικού χαρακτήρα σε περιβάλλον cloud computing, καθίσταται δύσκολη λόγω της ίδιας της φύσης των υπηρεσιών αυτών. Εκτός από δύσκολη όμως κρίνεται καθοριστική και απαραίτητη, καθώς όπως αναφέρθηκε και ανωτέρω, ο προσδιορισμός της «ταυτότητας» του παρόχου υπηρεσιών cloud computing, προσδιορίζει και την ευθύνη του. Η Ομάδα εργασίας του Άρθρου 29 τόσο στην με αριθ. 01/2010 όσο και στην με αριθ. 05/2012 γνώμες

της, αναφέρει μεταξύ άλλως πως «……*στις υπηρεσίες υπολογιστικού νέφους, και μάλιστα στην τεχνική εκδοχή της Υποδομής ή Πλατφόρμας ως Υπηρεσίας, ο πάροχος υπηρεσιών υπολογιστικού νέφους δεν γνωρίζει το περιεχόμενο των δεδομένων των οποίων γίνεται επεξεργασία στο πλαίσιο των προγραμμάτων και εφαρμογών, αλλά τις πληροφορίες αυτές τις διαθέτει μόνο ο πελάτης των υπηρεσιών νεφοϋπολογιστικής. Συνεπώς, ακόμη κι αν ο πάροχος γνωρίζει ποιος είναι υπεύθυνος επεξεργασίας δεδομένων, δεν γνωρίζει ποια δεδομένα επεξεργάζεται για λογαριασμό του (και ακόμη εάν αποτελούν δεδομένα προσωπικού χαρακτήρα είτε όχι), ούτε και τους σκοπούς για τους οποίους αυτά υφίστανται επεξεργασία. Ούτε φυσικά ο πάροχος των υπηρεσιών είναι αυτός που κατανέμει αρμοδιότητες για την επεξεργασία των δεδομένων εντός αυτού. Σ' αυτές τις περιπτώσεις, λοιπόν, ο πάροχος υπηρεσιών υπολογιστικού νέφους δεν μπορεί να είναι ο υπεύθυνος επεξεργασίας αφού δεν είναι αυτός που καθορίζει τους στόχους και τον τρόπο επεξεργασίας των δεδομένων προσωπικού χαρακτήρα.*»

Ο ρόλος, ωστόσο, του παρόχου των υπηρεσιών σ' αυτές τις περιπτώσεις είναι αυτός του εκτελούντος την επεξεργασία, καθώς αποτελεί χωριστή νομική οντότητα από τον υπεύθυνο επεξεργασίας και επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπεύθυνου επεξεργασίας. Σε πολλές περιπτώσεις επεξεργασίας, όμως, υπηρεσιών, για παράδειγμα Υπηρεσιών Λογισμικού, ο πελάτης του παρόχου νεφοϋπολογιστικής -ο οποίος, σύμφωνα με τα παραπάνω, είναι ο υπεύθυνος επεξεργασίας δεδομένων- αναθέτει στον πάροχο των υπηρεσιών υπολογιστικού νέφους να επιλέγει τις μεθόδους, τα τεχνικά και οργανωτικά μέσα που θα χρησιμοποιήσει για να επιτύχει τους στόχους του (ο πελάτης-υπεύθυνος επεξεργασίας) και ως αποτέλεσμα, παρόλο που ο πάροχος προσφέρει τα μέσα και την πλατφόρμα στον πελάτη για την υλοποίηση των τεχνολογικών εφαρμογών για λογαριασμό του υπεύθυνου επεξεργασίας, τότε ο πάροχος είναι φορέας που ναι μεν εκτελεί επεξεργασία, αλλά δεν δρα ως υπεύθυνος επεξεργασίας.

Αν, όμως, ο πάροχος υπηρεσιών νεφοϋπολογιστικής διαδραματίζει και το ρόλο του υπεύθυνου επεξεργασίας, καθώς προβαίνει σε επεξεργασία δεδομένων για δικούς του σκοπούς ή καθώς καθορίζει από κοινού με τον υπεύθυνο επεξεργασία τους σκοπούς και τον τρόπο επεξεργασίας, τότε για τις διαδικασίες επεξεργασίας αυτές βαρύνεται με όλες τις υποχρεώσεις κάθε υπεύθυνου επεξεργασίας, όπως ορίζονται στο Νέο Γενικό Κανονισμό για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα.

3. ΖΗΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΣΤΑ «ΣΥΝΝΕΦΑ»

Τα μοντέλα υπηρεσιών του Cloud παρέχουν, όχι μόνο διαφορετικούς τύπους υπηρεσιών στους χρήστες, αλλά αποκαλύπτουν επίσης πληροφορίες που επαυξάνουν τα ζητήματα ασφάλειας και τους κινδύνους των συστημάτων Cloud Computing. Οι υποδομές ως υπηρεσία (**IaaS)**

βρίσκονται στο κάτω στρώμα, το οποίο παρέχει άμεσα την πιο ισχυρή λειτουργικότητα ολόκληρου του Cloud. Το IaaS επιτρέπει επίσης στους χάκερ να εκτελέσουν επιθέσεις, όπως για παράδειγμα *brute-forcing, cracking*, που χρειάζονται υψηλή υπολογιστική ισχύ. Πολλαπλές εικονικές μηχανές υποστηρίζονται από το IaaS, παρέχουν μια ιδανική πλατφόρμα για τους χάκερ για να ξεκινήσουν επιθέσεις που απαιτούν μεγάλο αριθμό επιθέσεων. Η απώλεια δεδομένων είναι ένας άλλος κίνδυνος ασφάλειας των cloud models.

Τα δεδομένα στα cloud models, μπορούν εύκολα να προσπελαθούν από μη εξουσιοδοτημένους εσωτερικούς υπαλλήλους σε μία επιχείρηση για παράδειγμα, καθώς και από εξωτερικούς χάκερς. Οι εσωτερικοί υπάλληλοι μπορούν εύκολα να έχουν πρόσβαση σε δεδομένα εκ προθέσεως ή τυχαία. Οι εξωτερικοί χάκερ μπορούν να αποκτήσουν πρόσβαση σε βάσεις δεδομένων χρησιμοποιώντας τεχνικές πειρατείας, όπως *session hijacking and network channel eavesdropping.* Ιοί, ο Trojan μπορούν να «ανέβουν» σε συστήματα cloud και να προκαλέσουν βλάβες.

Είναι σημαντικό να προσδιοριστούν οι πιθανές απειλές στο cloud, για να εφαρμοστεί ένα σύστημα το οποίο διαθέτει μηχανισμούς καλύτερης ασφάλειας για την προστασία του cloud computing περιβάλλοντος. Παρακάτω, θα παρατεθούν ορισμένα παραδείγματα απειλών στο cloud.(βλ. C. Stergiou, K. E. Psannis, "Recent advances delivered in Mobile Cloud Computing's Security and Management challenges", IGI Global, Modern Principles, Practices, and Algorithms for Cloud Security, 2019, σελ. 6-7)

3.1. Απειλές στο cloud

- **«Πειρατεία» λογαριασμού (Account hijacking)**

Το «ψάρεμα» (phishing), η απάτη και η εκμετάλλευση λογισμικού είναι πολύ επικρατέστερες σήμερα και οι υπηρεσίες cloud προσθέτουν μια νέα διάσταση στην απειλή, επειδή οι επιτιθέμενοι μπορούν να καταργήσουν τις δραστηριότητες, να χειραγωγήσουν τις συναλλαγές και να τροποποιήσουν τα δεδομένα. Οι επιτιθέμενοι ενδέχεται να είναι σε θέση να χρησιμοποιήσουν την εφαρμογή του cloud για να ξεκινήσουν άλλες επιθέσεις. Οι οργανισμοί πρέπει να απαγορεύουν την κοινή χρήση των διαπιστευτηρίων του λογαριασμού μεταξύ χρηστών και υπηρεσιών και πρέπει να καθιστούν πολλαπλές παραμέτρων ταυτοποίησης, εφόσον υπάρχουν. Οι λογαριασμοί, πρέπει να παρακολουθούνται έτσι ώστε κάθε συναλλαγή να εντοπίζεται σε έναν άνθρωπο ιδιοκτήτη. Το κλειδί είναι να προστατεύετε τα διαπιστευτήρια του λογαριασμού από την κλοπή.

- **Παραβιάσεις δεδομένων (Data breaches)**

Τα περιβάλλοντα στα σύννεφα, αντιμετωπίζουν πολλές από τις ίδιες απειλές με τα παραδοσιακά εταιρικά δίκτυα, αλλά δεδομένου ότι η μεγάλη ποσότητα των δεδομένων αποθηκεύονται σε διακομιστές του cloud, οι πάροχοι αυτών, έχουν γίνει ένας ελκυστικός στόχος. Η σοβαρότητα της βλάβης τείνει να εξαρτάται από την ευαισθησία των δεδομένων που εκτίθενται. Οι προσωπικές οικονομικές πληροφορίες αποτελούν το αποκορύφωμα θα λέγαμε των πιο «καταστροφικών» παραβιάσεων, αλλά οι παραβιάσεις που αφορούν κυβερνητικές πληροφορίες, εμπορικά – επαγγελματικά μυστικά, είναι πιο καταστροφικές. Όταν συντελείται μία παραβίαση, η εταιρεία υπόκειται σε νομικές ενέργειες. Οι έρευνες για παραβίαση καθώς και οι εξατομικευμένες έρευνες παραβίασης μπορούν να προκαλέσουν σημαντικές δαπάνες. Οι έμμεσες επιπτώσεις μπορεί να περιλαμβάνουν ζημιές στο «σήμα», στο όνομα μίας επιχείρησης και οι απώλειες των επιχειρήσεων μπορεί να επηρεάσουν το μέλλον των οργανώσεων για χρόνια.

- **Ανεπαρκής επιμέλεια (Inadequate diligence)**

Οι οργανισμοί, οι απλοί χρήστες, δέχονται εφαρμογές υπολογιστικού νέφους (cloud computing) χωρίς να έχουν πλήρη κατανόηση του περιβάλλοντος και των κινδύνων που συνδέονται με αυτό, οι οποίοι ενδέχεται να παρουσιάζουν μεγάλο αριθμό εμπορικών, οικονομικών, τεχνικών, και νομικών ρίσκων. Η επιμέλεια δε, είναι απαραίτητη είτε ο οργανισμός ή ο χρήστης επιχειρεί να «μεταναστεύσει» στο σύννεφο, είτε να συγχωνευθεί με άλλη εταιρεία στο cloud. Για παράδειγμα, οι οργανισμοί που αποτυγχάνουν να εξετάσουν μια σύμβαση ενδέχεται να μην έχουν επίγνωση του ευθύνη του παρόχου σε περίπτωση απώλειας ή παραβίασης δεδομένων της ως άνω σύμβασης. Επιχειρησιακά και τεχνικά ζητήματα θα μπορούσαν να προκύψουν εάν μία ομάδα ανάπτυξης ενός οργανισμού δεν είναι εξοικειωμένη με τις τεχνολογίες του cloud, όπως με τις εφαρμογές που αναπτύσσονται σε ένα συγκεκριμένο νέφος. Ένας οργανισμός θα πρέπει να κάνει επαρκή έρευνα πριν «μετακινηθεί» στο cloud, λόγω του κινδύνου που συνδέεται με αυτό.

- **Επιθέσεις DoS (Denial of Service Attacks)**

Οι επιθέσεις DoS υπήρχαν εδώ και πολύ καιρό και έχουν κερδίσει την πρωτοκαθεδρία και πάλι χάρη στο cloud computing, καθώς συχνά επηρεάζουν τη διαθεσιμότητα. Τα συστήματα ενδέχεται να εκτελούνται αργά ή με χρονοκαθυστέρηση. Αυτές οι επιθέσεις DoS καταναλώνουν μεγάλα ποσά επεξεργαστικής ισχύος (processing power), έναν λογαριασμό που ο πελάτης πρέπει

τελικά να πληρώσει. Οι επιθέσεις DDoS σε μεγάλη ένταση είναι πολύ συχνές, αλλά οι οργανώσεις/οι χρήστες θα πρέπει επίσης να είναι σε αφύπνιση για τις ασύμμετρες και application-level επιθέσεις DoS, οι οποίες στοχεύουν στον Web server και στα τρωτά σημεία των βάσεων δεδομένων. Οι πάροχοι cloud είναι προτιμότερο να αντιμετωπίζουν τις επιθέσεις DoS παρά τους πελάτες τους. Το κλειδί είναι να έχουμε ένα σχέδιο για να αμβλύνουμε την επίθεση πριν ξεσπάσει από αυτό, έτσι ώστε οι διαχειριστές να έχουν πρόσβαση σε αυτές τις πηγές όταν τις χρειάζονται.

4. ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ ΣΤΟ CLOUD

Τα πληροφοριακά δεδομένα που βρίσκονται στο υπολογιστικό νέφος, στα οποία περιλαμβάνονται τα δεδομένα προσωπικού χαρακτήρα καθώς και τα ευαίσθητα προσωπικά δεδομένα αποθηκεύονται σε κάποιον εξυπηρετητή ή data center. Η φυσική τοποθεσία του συστήματος αποθήκευσης των δεδομένων προσωπικού χαρακτήρα ή ευαίσθητων προσωπικών δεδομένων είναι καθοριστική για την δικαιοδοσία και εφαρμογή του νομικού πλαισίου προστασίας του υποκειμένου αυτών των δεδομένων. Σύμφωνα με το άρθρο 3 του Γενικού Κανονισμού για την Προστασία των Προσωπικών Δεδομένων, «…. *Ο κανονισμός εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο των δραστηριοτήτων μιας εγκατάστασης ενός υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία στην Ένωση, ανεξάρτητα από το κατά πόσο η επεξεργασία πραγματοποιείται εντός της Ένωσης*. –άρθρο 3§1» Επιπλέον, « *ο παρών κανονισμός εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα υποκειμένων των δεδομένων που βρίσκονται στην Ένωση από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία μη εγκατεστημένο στην Ένωση, εάν οι δραστηριότητες επεξεργασίας σχετίζονται με: α) την προσφορά αγαθών ή υπηρεσιών στα εν λόγω υποκείμενα των δεδομένων στην Ένωση, ανεξαρτήτως εάν απαιτείται πληρωμή από τα υποκείμενα των δεδομένων, ή β) την παρακολούθηση της συμπεριφοράς τους, στον βαθμό που η συμπεριφορά αυτή λαμβάνει χώρα εντός της Ένωσης.* – άρθρο 3§2». Και επίσης, «*Ο παρών κανονισμός εφαρμόζεται για την επεξεργασία δεδομένων προσωπικού χαρακτήρα από υπεύθυνο επεξεργασίας μη εγκατεστημένο στην Ένωση, αλλά σε τόπο όπου εφαρμόζεται το δίκαιο κράτους μέλους δυνάμει του δημόσιου διεθνούς δικαίου.* – άρθρο 3§3».

Επομένως, είναι σημαντικό σε κάθε περίπτωση χρήσης υπηρεσιών υπολογιστικού νέφους οι χρήστες να γνωρίζουν από τον πάροχο αυτού, που βρίσκεται το υπολογιστικό σύστημα στο οποίο αποθηκεύονται τα δεδομένα τους. Η γνώση αυτή θα πρέπει να προκύπτει από τις συμβάσεις παροχής υπηρεσιών υπολογιστικού νέφους των χρηστών με τον πάροχο αυτού ή/και των χρηστών που συμβάλλονται με εταιρείες παροχής υπηρεσιών υπολογιστικού νέφους, που με τη σειρά τους, συμβάλλονται αυτές με τον πάροχο νεφουπολογιστικής.

4.1. Κίνδυνοι για τα προσωπικά δεδομένα στο cloud

Αναμφίβολα, λόγω της πολυπλοκότητας των λειτουργιών στο υπολογιστικό νέφος, η νεφοϋπολογιστική ως μια νέα τεχνολογική καινοτομία, επιτείνει τους υφιστάμενους κινδύνους περί τη μη σύννομη χρήση δεδομένων προσωπικού χαρακτήρα. Οι κίνδυνοι αυτοί διακρίνονται στην πλειονότητα τους σε δύο μεγάλες κατηγορίες: α) στην έλλειψη ελέγχου επί των δεδομένων και β) στην ανεπάρκεια πληροφοριών σχετικά με την ίδια την επεξεργασία (έλλειψη διαφάνειας).

Σύμφωνα με την με αριθ. **05/2012** Γνώμη της Ομάδας Εργασίας του Άρθρου 29 για την προστασία των δεδομένων σχετικά με τη νεφοϋπολογιστική, ελλοχεύουν οι εξής κίνδυνοι:

- **Κίνδυνοι σχετιζόμενοι με την έλλειψη ελέγχου**:

I. Έλλειψη διαθεσιμότητας λόγω έλλειψης διαλειτουργικότητας (εξάρτηση από τον εκάστοτε προμηθευτή): Εάν ο πάροχος υπηρεσιών νεφοϋπολογιστικής χρησιμοποιεί ιδιόκτητη τεχνολογία, ο πελάτης υπηρεσιών νεφοϋπολογιστικής ενδέχεται να δυσκολευτεί να μεταφέρει τα δεδομένα και τα έγγραφά του από ένα σύστημα που έχει ως βάση τη νεφοϋπολογιστική σε άλλο (φορητότητα δεδομένων) ή να ανταλλάξει πληροφορίες με οντότητες που χρησιμοποιούν υπηρεσίες νεφοϋπολογιστικής οι οποίες τελούν υπό τη διαχείριση διαφορετικών παρόχων (διαλειτουργικότητα).

II. Έλλειψη ακεραιότητας λόγω επιμερισμού των πόρων: Κάθε νέφος αποτελείται από επιμερισμένα συστήματα και υποδομές. Οι πάροχοι υπηρεσιών νεφοϋπολογιστικής 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.

III. Μη τήρηση του απορρήτου σε περίπτωση υποβολής αιτημάτων για σκοπούς επιβολής του νόμου απευθείας σε παρόχους υπηρεσιών νεφοϋπολογιστικής: 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.

IV. Αδυναμία παρέμβασης λόγω της πολυπλοκότητας και της δυναμικής της αλυσίδας εξωτερικής ανάθεσης: Κάθε υπηρεσία νεφοϋπολογιστικής που παρέχεται από έναν πάροχο μπορεί να είναι αποτέλεσμα συνδυασμού υπηρεσιών οι οποίες παρέχονται από διάφορους άλλους παρόχους, ο αριθμός των οποίων μπορεί να αυξομειώνεται δυναμικά κατά τη διάρκεια ισχύος της σύμβασης του πελάτη.

V. Αδυναμία παρέμβασης (δικαιώματα των προσώπων στα οποία αναφέρονται τα δεδομένα): Οι πάροχοι υπηρεσιών νεφοϋπολογιστικής είναι πιθανό να μην παρέχουν στον υπεύθυνο της επεξεργασίας τα μέτρα και τα εργαλεία που χρειάζεται για να διαχειρίζεται ευκολότερα τα δεδομένα (π.χ. πρόσβαση σε αυτά και διόρθωση ή διαγραφή τους).

VI. Έλλειψη απομόνωσης των δεδομένων: Οι πάροχοι υπηρεσιών νεφοϋπολογιστικής είναι πιθανό να εκμεταλλεύονται τον φυσικό έλεγχο που ασκούν επί δεδομένων που προέρχονται από διαφορετικούς πελάτες με σκοπό τη σύνδεση των δεδομένων προσωπικού χαρακτήρα μεταξύ τους. Εάν παρέχονται στους διαχειριστές επαρκώς προνομιακά δικαιώματα πρόσβασης που διευκολύνουν το έργο τους (ρόλοι υψηλού κινδύνου), τότε μπορούν κάλλιστα να συνδέουν τις πληροφορίες που προέρχονται από διαφορετικούς πελάτες.

- **Κίνδυνοι σχετιζόμενοι με την έλλειψη πληροφοριών όσον αφορά την επεξεργασία (διαφάνεια)**

Η μη παροχή επαρκών πληροφοριών σχετικά με τις διαδικασίες επεξεργασίας που εκπονούνται στο πλαίσιο της παροχής υπηρεσιών νεφοϋπολογιστικής εγκυμονεί κινδύνους για τους υπεύθυνους της επεξεργασίας καθώς και για τα πρόσωπα στα οποία αναφέρονται τα δεδομένα, καθώς δεν τους επιτρέπει να γνωρίζουν τις πιθανές απειλές και τους κινδύνους, με αποτέλεσμα να μην λαμβάνουν τα μέτρα που θεωρούν αναγκαία.

Για κάποιες δυνητικές απειλές δύναται μάλιστα να ευθύνεται ο υπεύθυνος της επεξεργασίας ο οποίος δεν γνωρίζει ότι:

I. τα δεδομένα υφίστανται αλυσιδωτή επεξεργασία στην οποία συμμετέχουν πολυάριθμοι εκτελούντες την επεξεργασία και υπεργολάβοι.

II. τα δεδομένα προσωπικού χαρακτήρα υφίστανται επεξεργασία σε διαφορετικές γεωγραφικές τοποθεσίες εντός του ΕΟΧ, γεγονός που έχει άμεσο αντίκτυπο στη νομοθεσία η οποία διέπει τις διαφορές που ενδέχεται να προκύψουν μεταξύ χρήστη και παρόχου όσον αφορά την προστασία των δεδομένων.

III. τα δεδομένα προσωπικού χαρακτήρα διαβιβάζονται σε τρίτες χώρες εκτός του ΕΟΧ. Είναι πιθανόν οι τρίτες χώρες να μην εξασφαλίζουν επαρκές επίπεδο προστασίας των δεδομένων και η διαβίβαση των τελευταίων να μην προστατεύεται από κατάλληλα μέτρα (π.χ. τυποποιημένες συμβατικές ρήτρες ή δεσμευτικούς εταιρικούς κανόνες), και, ως εκ τούτου, ενδέχεται να είναι παράνομη.

4.2 Γενικός Κανονισμός Προσωπικών Δεδομένων και Υπηρεσίες Cloud Computing

Αρχικά, ο Γενικός Κανόνας Προστασίας Δεδομένων, παρά το γεγονός ότι αποτελεί μια βέλτιστη νομοθετική ρύθμιση για την ασφάλεια των προσωπικών δεδομένων, στοχεύει παράλληλα

με τις διατάξεις του να ρυθμίσει επαρκώς αλλά και να προστατέψει τα δεδομένα προσωπικού χαρακτήρα στο νέο τεχνολογικό περιβάλλον. Αναμφίβολα, η διατήρηση τόσο των επιπέδων προστασίας δεδομένων όσο και της ιδιωτικότητας αυτών στα υπολογιστικά νέφη αποτελεί μια νέα πρόκληση. Καθώς οι υπηρεσίες cloud επεξεργάζονται τα δεδομένα των χρηστών σε μηχανές που οι τελευταίοι είτε δεν κατέχουν είτε δεν λειτουργούν τόσο οι χρήστες όσο και οι υπεύθυνοι επεξεργασίας, αυτόματα δημιουργούνται ζητήματα προστασίας της ιδιωτικής ζωής. Η τεχνολογία συνεχώς εξελίσσεται, επακόλουθο δε αυτής της εξέλιξης της είναι (η τεχνολογία) να διεισδύει σε κάθε πτυχή της επαγγελματικής και προσωπικής ζωής κάθε ατόμου, με αποτέλεσμα άνθρωποι αλλά και επιχειρήσεις να γίνονται ολοένα και περισσότερο ευάλωτοι σε παραβιάσεις των προσωπικών τους δεδομένων. Ως κατέστη σαφές και ανωτέρω (βλ. κεφάλαιο - 2.3 Υπηρεσίες Cloud), οι υπηρεσίες υπολογιστικού νέφους, εξ 'ορισμού συγκεντρώνουν μεγάλες ποσότητες δεδομένων είτε ως εγκαταστάσεις για αποθήκευση δεδομένων των εταιριών, είτε ως μέρος αιτημάτων επεξεργασίας, συλλέγοντας δύο τύπους δεδομένων: **α)** δεδομένα που η υπηρεσία συλλέγει αυτόματα ως μέρος της δραστηριότητας ή της διαφημιστικής της πολιτικής και **β)** πληροφορίες όπου ο χρήστης παρέχει οικειοθελώς στην υπηρεσία ως μέρος χρήσης τους.

Πρόκληση αποτελεί για τους μηχανικούς λογισμικού η σχεδίαση υπηρεσιών cloud με τέτοιο τρόπο ώστε να μειώνεται ο κίνδυνος της ιδιωτικότητας και να εξασφαλίζεται η συμμόρφωση με το νόμο. Οι απειλές που συνδέονται με τις υπηρεσίες υπολογιστικού νέφους έχουν να κάνουν με την απομακρυσμένη αποθήκευση και επεξεργασία αυτών, λόγω της αυξημένης χρήσης εικονικοποίησης (virtualization) και κοινής χρήσης πλατφορμών μεταξύ χρηστών. Ένα ακόμα χαρακτηριστικό των υπηρεσιών cloud είναι το δυναμικό τους περιβάλλον. Τόσο η ταχύτητα, όσο και η ευελιξία που χαρακτηρίζουν τα συστήματα υπολογιστικού νέφους, αναγκάζουν τις επιχειρήσεις να προσαρμοστούν άμεσα με τα νέα αυτά δεδομένα, έχοντας ως αποτέλεσμα τα προσωπικά και ευαίσθητα δεδομένα πιθανώς να μετακινούνται πέρα από τα όρια συγκατάθεσης του υποκειμένου. Ωστόσο, όπως ορίζεται και στο άρθρο **6 § 4** του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων, που μιλά για την επεξεργασία των Προσωπικών Δεδομένων *«... Όταν η επεξεργασία για σκοπό άλλο **από αυτόν για τον οποίο έχουν συλλεγεί τα δεδομένα προσωπικού χαρακτήρα** δεν βασίζεται στη συγκατάθεση του υποκειμένου των δεδομένων ή στο δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους το οποίο αποτελεί αναγκαίο και αναλογικό μέτρο σε μια δημοκρατική κοινωνία για τη διασφάλιση των σκοπών που αναφέρονται στο άρθρο 23 παράγραφος 1, ο υπεύθυνος επεξεργασίας, προκειμένου να εξακριβωθεί κατά πόσο η επεξεργασία για άλλο σκοπό είναι συμβατή με τον σκοπό για τον οποίο συλλέγονται αρχικώς τα δεδομένα προσωπικού χαρακτήρα, λαμβάνει υπόψη, μεταξύ άλλων:*

*α) **<u>τυχόν σχέση μεταξύ των σκοπών για τους οποίους έχουν συλλεχθεί τα δεδομένα προσωπικού χαρακτήρα και των σκοπών της επιδιωκόμενης περαιτέρω επεξεργασίας</u>**,*

β) το πλαίσιο εντός του οποίου συλλέχθηκαν τα δεδομένα προσωπικού χαρακτήρα, ιδίως όσον αφορά τη σχέση μεταξύ των υποκειμένων των δεδομένων και του υπευθύνου επεξεργασίας,

γ) τη φύση των δεδομένων προσωπικού χαρακτήρα, ιδίως για τις ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία, σύμφωνα με το άρθρο 9, ή κατά πόσο δεδομένα προσωπικού χαρακτήρα που σχετίζονται με ποινικές καταδίκες και αδικήματα υποβάλλονται σε επεξεργασία, σύμφωνα με το άρθρο 10,

δ) τις πιθανές συνέπειες της επιδιωκόμενης περαιτέρω επεξεργασίας για τα υποκείμενα των δεδομένων,

ε) την ύπαρξη κατάλληλων εγγυήσεων, που μπορεί να περιλαμβάνουν κρυπτογράφηση ή ψευδωνυμοποίηση.

*(*υπογράμμιση και μαύρισμα δικό μου)

Τέλος, ερωτήματα τίθενται αναφορικά με το κατά πόσο μπορούν να καταστραφούν και να διαγραφούν τα δεδομένα που έχουν αποθηκευτεί στο νέφος, καθώς αφενός έχουν δημιουργηθεί πολλαπλά αντίγραφα, αφετέρου η καταστροφή των δεδομένων δεν είναι εφικτή λόγω του κινδύνου που δημιουργείται στους υπόλοιπους «συν-ενοίκους» (Multi-tenant - *Multitenancy: αναφέρεται σε μια αρχιτεκτονική λογισμικού στην οποία μια ενιαία παρουσία λογισμικού τρέχει σε έναν διακομιστή και εξυπηρετεί πολλούς ενοικιαστές. Ένας μισθωτής (tenant) είναι μια ομάδα χρηστών που μοιράζονται μια κοινή πρόσβαση με συγκεκριμένα προνόμια στην περίπτωση του λογισμικού*), ζήτημα για το οποίο θα γίνει αναφορά στην συνέχεια με αναφορά και στα δεδομένα της ελληνικής πραγματικότητας και Νομολογίας.

<u>4.2.1.Νομικό Πλαίσιο για την Προστασία των Προσωπικών Δεδομένων στο Cloud</u>

<u>Α. Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων</u>

Σύμφωνα με τον Γενικό Κανονισμό για την Προστασία των Προσωπικών Δεδομένων (εφεξής: ΓΚΠΔ) και συγκεκριμένα σύμφωνα με το άρθρο **6§3** αυτού: « .... ***Η βάση*** *για την επεξεργασία που αναφέρεται στην παράγραφο 1 στοιχεία γ) και ε) ορίζεται σύμφωνα με: α) το δίκαιο της Ένωσης, ή β) το δίκαιο του κράτους μέλος στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας*.». Ο υπεύθυνος επεξεργασίας μάλιστα, όπως προβλέπεται και στο άρθρο **7 § 1** του **ΓΚΠΔ** «*..είναι σε θέση να* ***αποδείξει ότι το υποκείμενο των δεδομένων συγκατατέθηκε για την επεξεργασία των δεδομένων του προσωπικού χαρακτήρα***. Ενώ σε περίπτωση ανηλίκου τέκνου κάτω των 16 ετών, όπως προβλέπεται στον ΓΚΠΔ, «*…Ο υπεύθυνος επεξεργασίας καταβάλλει εύλογες προσπάθειες για να επαληθεύσει στις περιπτώσεις αυτές ότι η συγκατάθεση παρέχεται ή εγκρίνεται από το πρόσωπο*

*που έχει τη γονική μέριμνα του παιδιού, λαμβάνοντας υπόψη τη διαθέσιμη τεχνολογία» (*άρθρο **8§2 ΓΚΠΔ).**

Επιπλέον, ο υπεύθυνος επεξεργασίας, «…….***λαμβάνει τα κατάλληλα μέτρα για να παρέχει στο υποκείμενο των δεδομένων κάθε πληροφορία*** *που αναφέρεται στα άρθρα 13 και 14 και κάθε ανακοίνωση στο πλαίσιο των άρθρων 15 έως 22 και του άρθρου 34 σχετικά με την επεξεργασία σε συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση, ιδίως όταν πρόκειται για πληροφορία απευθυνόμενη ειδικά σε παιδιά……»* **(**άρθρο **12 §1 ΓΚΠΔ)** και επιπλέον, *«……. **διευκολύνει την άσκηση των δικαιωμάτων** των υποκειμένων των δεδομένων που προβλέπονται στα άρθρα 15 έως 22. ….»* (άρθρο **12§2 ΓΚΠΔ).**

Παράλληλα, <u>ο υπεύθυνος επεξεργασίας</u>, σύμφωνα με τον Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων, « *Λαμβάνοντας υπόψη τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, (*άρθρο **24§1 ΓΚΠΔ**) και «*…τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων από την επεξεργασία (*άρθρο **25§1 ΓΚΠΔ**), *«…εφαρμόζει **κατάλληλα τεχνικά και οργανωτικά μέτρα** προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον παρόντα κανονισμό.» (*άρθρο **24§1 ΓΚΠΔ**) και «….*εφαρμόζει αποτελεσματικά, τόσο κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας, κατάλληλα τεχνικά και οργανωτικά μέτρα, όπως η ψευδωνυμοποίηση, σχεδιασμένα για την εφαρμογή αρχών προστασίας των δεδομένων, όπως η ελαχιστοποίηση των δεδομένων, και την ενσωμάτωση των απαραίτητων εγγυήσεων στην επεξεργασία κατά τρόπο ώστε να πληρούνται οι απαιτήσεις του παρόντος κανονισμού και να προστατεύονται τα δικαιώματα των υποκειμένων των δεδομένων» (*άρθρο **25§ ΓΚΠΔ**) .

Επίσης, σε περιπτώσεις που οι υπεύθυνοι επεξεργασίας είναι περισσότεροι του ενός, οι υποχρεώσεις του Κανονισμού βαρύνουν αυτούς από κοινού «*σε περίπτωση που δύο ή περισσότεροι υπεύθυνοι επεξεργασίας καθορίζουν από κοινού τους σκοπούς και τα μέσα της επεξεργασίας, αποτελούν από κοινού υπευθύνους επεξεργασίας» (*άρθρο **26§1 ΓΚΠΔ**) .

Επιπρόσθετα, στην περίπτωση που ο πάροχος υπηρεσιών υπολογιστικού νέφους ενεργεί ως <u>εκτελών την επεξεργασία (</u>όπως εδώ, βλ. ανωτέρω κεφάλαιο «2.3.5 Ρόλος παρόχων υπηρεσιών στο Cloud») τότε αυτός υποχρεούται να παρέχει στον υπεύθυνο επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, σύμφωνα και με το άρθρο **28§1 ΓΚΠΔ**, «*…**επαρκείς διαβεβαιώσεις για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών** μέτρων, κατά τρόπο ώστε η επεξεργασία να πληροί τις απαιτήσεις του παρόντος κανονισμού και να διασφαλίζεται η προστασία των δικαιωμάτων*

του υποκειμένου των δεδομένων. Ακόμη, όπως προβλέπεται στην παράγραφο **2** του άρθρου **28** του **ΓΚΠΔ,** ο εκτελών την επεξεργασία, «….***δεν προσλαμβάνει άλλον εκτελούντα την επεξεργασία χωρίς προηγούμενη ειδική ή γενική γραπτή άδεια του υπευθύνου επεξεργασίας***. *Σε περίπτωση γενικής γραπτής άδειας, ο εκτελών την επεξεργασία ενημερώνει τον υπεύθυνο επεξεργασίας για τυχόν σκοπούμενες αλλαγές που αφορούν την προσθήκη ή την αντικατάσταση των άλλων εκτελούντων την επεξεργασία, παρέχοντας με τον τρόπο αυτό τη δυνατότητα στον υπεύθυνο επεξεργασίας να αντιταχθεί σε αυτές τις αλλαγές.».* Αξίζει δε στο σημείο αυτό να αναφέρουμε, πως *«…… η επεξεργασία από τον εκτελούντα την επεξεργασία* ***διέπεται από σύμβαση*** *ή άλλη νομική πράξη υπαγόμενη στο δίκαιο της Ένωσης ή του κράτους μέλους,* ***που δεσμεύει*** *τον εκτελούντα την επεξεργασία σε σχέση με τον υπεύθυνο επεξεργασίας και καθορίζει το αντικείμενο και τη διάρκεια της επεξεργασίας, τη φύση και τον σκοπό της επεξεργασίας, το είδος των δεδομένων προσωπικού χαρακτήρα και τις κατηγορίες των υποκειμένων των δεδομένων και τις υποχρεώσεις και τα δικαιώματα του υπευθύνου επεξεργασίας,…»*, σύμφωνα με το άρθρο **28§3** του **ΓΚΠΔ.**

Ακόμη, σύμφωνα με το άρθρο **29** του **ΓΚΠΔ,** «*Ο εκτελών την επεξεργασία και κάθε πρόσωπο που ενεργεί υπό την εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, το οποίο έχει πρόσβαση σε δεδομένα προσωπικού χαρακτήρα, επεξεργάζεται τα εν λόγω δεδομένα μόνον* ***κατ' εντολή*** *του υπευθύνου επεξεργασίας, εκτός εάν υποχρεούται προς τούτο από το δίκαιο της Ένωσης ή του κράτους μέλους.».* Μάλιστα, όπως καθιστά σαφές η ομάδα εργασίας του άρθρου 29 για την προστασία των προσωπικών δεδομένων στην με αριθ. 05/2012 Γνώμη της σχετικά με την νεφοϋπολογιστική, «*Στην παροχή υπηρεσιών νεφοϋπολογιστικής δύναται να εμπλέκονται διάφοροι συμβαλλόμενοι που ενεργούν ως εκτελούντες την επεξεργασία. Συνηθίζεται επίσης οι εκτελούντες την επεξεργασία να προσλαμβάνουν με υπεργολαβία πρόσθετους (υπό-)εκτελούντες την επεξεργασία, οι οποίοι αποκτούν με τη σειρά τους πρόσβαση στα δεδομένα προσωπικού χαρακτήρα. Εάν οι εκτελούντες την επεξεργασία αναθέτουν με 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 νεφοϋπολογιστικής***». Σ'αυτές τις περιπτώσεις περισσότερων που ενεργούν ως εκτελούντες την επεξεργασία, ο συμβατικός καθορισμός με σαφήνεια των υποχρεώσουν και αρμοδιοτήτων τους είναι σημαντικός για την ευχερή εφαρμογή του νόμου. Σ' αυτόν το συμβατικό καθαρισμό των υποχρεώσεων των εκτελούντων την επεξεργασία θα πρέπει να προβλέπεται, όπως ορθά επισημαίνει η ομάδα εργασίας του άρθρου 29 στην ίδια ως άνω γνώμη «…. *σε περίπτωση που ο υπό-εκτελών την επεξεργασία αδυνατεί να ανταποκριθεί στις συναφείς με την προστασία των δεδομένων υποχρεώσεις του που*

απορρέουν από τη γραπτή συμφωνία, ***ο εκτελών την επεξεργασία διατηρεί την πλήρη και απεριόριστη ευθύνη έναντι του υπευθύνου της επεξεργασίας*** *για την εκπλήρωση των υποχρεώσεων του υπό- εκτελούντος την επεξεργασία που απορρέουν από τη συμφωνία. Μια τέτοια διάταξη θα μπορούσε να χρησιμοποιείται σε όλες τις συμβατικές ρήτρες μεταξύ του υπεύθυνου της επεξεργασίας και του παρόχου υπηρεσιών νεφοϋπολογιστικής, όταν ο τελευταίος σκοπεύει να παρέχει υπηρεσίες μέσω συμβάσεων υπεργολαβίας, έτσι ώστε να διασφαλίζονται οι απαιτούμενες εγγυήσεις για την υπό-εκτέλεση της επεξεργασίας.».*

Αναμφίβολα, με τον ΓΚΠΔ δίνεται μεγάλη έμφαση στην ενίσχυση όχι μόνο της διαφάνειας, αλλά και του ελέγχου στην διαχείριση των δεδομένων προσωπικού χαρακτήρα σε περιβάλλον υπολογιστικού νέφους. Δηλαδή ο ΓΚΠΔ, αποβλέπει στην ρύθμιση της προστασίας των προσωπικών δεδομένων στο περιβάλλον της νεφοϋπολογιστικής, έτσι ώστε να επιτυγχάνονται και οι περιγραφόμενοι και ρυθμιζόμενοι σε αυτόν βασικοί στόχοι της ασφάλειας των δεδομένων προσωπικού χαρακτήρα, ήτοι η ακεραιότητα, η διαθεσιμότητα, το απόρρητο των δεδομένων, η διαφάνεια, η απομόνωνση, η δυνατότητα παρέμβασης και η φορητότητας των δεδομένων. Φυσικά, σκόπιμο είναι να τηρείται η αρχή του προσδιορισμού και του περιορισμού του σκοπού της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, να διασφαλίζεται η δυνατότητα διαγραφής τους μόλις πάψει να είναι απαραίτητη η διατήρηση τους, και να εφαρμόζονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας τους καθόλη τη διάρκεια της επεξεργασίας και διατήρηση τους.

Β. Κώδικας Δεοντολογίας για τους παρόχους των υπηρεσιών cloud computing

Αξίζει στο σημείο αυτό να αναφέρουμε, πως για την προστασία των προσωπικών δεδομένων δημιουργήθηκε τον Απρίλιο του 2013, η ομάδα **Cloud Select Industry Group (C-SIG)** με τον δικό της κώδικα δεοντολογίας για την προστασία των προσωπικών δεδομένων. Ο κώδικας αυτός δεοντολογίας εστιάζεται έντονα στη βελτίωση της διαφάνειας και στη διευκόλυνση της κατανόησης από τους νέους αλλά και παλαιούς πελάτες, ζητημάτων που άπτονται της προστασίας δεδομένων και του τρόπου αντιμετώπισής τους από τους παρόχους υπηρεσιών cloud. Μάλιστα, ο κώδικας δεοντολογίας αναγνωρίζεται ρητά και ενθαρρύνεται στον Γενικό Κανονισμό για την Προστασία των Προσωπικών Δεδομένων, καθώς συμπληρώνει την εφαρμογή του νόμου παρέχοντας καθοδήγηση και σαφήνεια τόσο στους παρόχους όσο και στους χρήστες. Συγκεκριμένα, σύμφωνα με το άρθρο **40§1** του **ΓΚΠΔ,** «*Τα κράτη μέλη, οι εποπτικές αρχές, το Συμβούλιο Προστασίας Δεδομένων και η Επιτροπή ενθαρρύνουν την* ***εκπόνηση κωδίκων δεοντολογίας*** *που έχουν ως στόχο να συμβάλουν στην ορθή εφαρμογή του παρόντος κανονισμού, λαμβάνοντας υπόψη τα ειδικά χαρακτηριστικά των διάφορων τομέων επεξεργασίας και τις ειδικές*

ανάγκες των πολύ μικρών, των μικρών και των μεσαίων επιχειρήσεων.». Η ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων, διατύπωσε την με αριθ. **02/2015** Γνώμη σχετικά με τον κώδικα δεοντολογίας της ομάδας C-SIG για το υπολογιστικό νέφος, αναφέροντας μάλιστα πως, «…..***Ο κώδικας πρέπει να αναφέρει σαφώς ότι η προσχώρηση δεν καθιστά έναν πάροχο υπηρεσιών υπολογιστικού νέφους απρόσβλητο έναντι αλλαγών στο ενωσιακό δίκαιο***. *Ειδικότερα, κάθε πάροχος υπηρεσιών υπολογιστικού νέφους που προσχωρεί στον κώδικα πριν ενσωματωθεί μια τροποποίηση της ενωσιακής νομοθεσίας στον κώδικα, πρέπει να εξασφαλίζει ότι συμμορφώνεται προς τη νέα νομοθεσία, ακόμη και αν αυτό συνεπάγεται νέες ή αντικρουόμενες υποχρεώσεις όσον αφορά τον κώδικα».* Επιπλέον, η ομάδα εργασίας του 29, σε άλλο σημείο της, κάνει σαφές πως η προσχώρηση στον κώδικα **δεν εξασφαλίζει οποιαδήποτε αυτόματη προστασία από ενδεχόμενες παρεμβάσεις ή ενέργειες από τις αρμόδιες ΑΠΔ (ή άλλες αρχές) στο πλαίσιο των δραστηριοτήτων τους εποπτείας και επιβολής.** Ενώ καθιστά το σημείο αυτό σαφές, η ομάδα WP29 ενθαρρύνει τους παρόχους υπηρεσιών υπολογιστικού νέφους να προσχωρούν στους εν λόγω κώδικες συμπεριφοράς. Η συμμόρφωση με τις απαιτήσεις των κωδίκων αυτών θα βοηθήσει τους εν λόγω παρόχους υπηρεσιών υπολογιστικού νέφους να αποδείξουν ότι λογοδοτούν όσον αφορά τους κανόνες για την προστασία των δεδομένων, γεγονός που θα έχει οπωσδήποτε θετικό αντίκτυπο στο πλαίσιο των δραστηριοτήτων εποπτείας και επιβολής.

Γ. Μηχανισμοί Πιστοποιήσεων

Ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (European Union Agency for Network and Information Security (ENISA), σε συνεργασία τόσο με την Ευρωπαϊκή Ένωση, όσο και με την ομάδα Cloud Select Industry Group (C-SIG), δημιούργησαν και δημοσίευσαν ένα οδηγό που σχετίζεται με τις **πιστοποιήσεις** γύρω από τις υπηρεσίες υπολογιστικού νέφους. Μάλιστα, και στον ΓΚΠΔ στο άρθρο **42§1** αυτού, προβλέπεται ότι: «*1.Τα κράτη μέλη, οι εποπτικές αρχές, το Συμβούλιο Προστασίας Δεδομένων και η Επιτροπή παροτρύνουν, ιδίως σε ενωσιακό επίπεδο,* ***τη θέσπιση μηχανισμών πιστοποίησης προστασίας δεδομένων*** *και σφραγίδων και σημάτων προστασίας δεδομένων, με σκοπό την απόδειξη της συμμόρφωσης προς τον παρόντα κανονισμό των πράξεων επεξεργασίας από τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία. Λαμβάνονται υπόψη οι ειδικές ανάγκες των πολύ μικρών, των μικρών και των μεσαίων επιχειρήσεων.»,* ενώ στο άρθρο 43§1 του ΓΚΠΔ μεταξύ προβλέπεται ότι: «*Με την επιφύλαξη των καθηκόντων και των αρμοδιοτήτων της αρμόδιας εποπτικής αρχής σύμφωνα με τα άρθρα 57 και 58, οι φορείς πιστοποίησης που διαθέτουν το ενδεδειγμένο επίπεδο εμπειρογνωμοσύνης σε σχέση με την προστασία των δεδομένων, αφού ενημερώσουν την εποπτική αρχή προκειμένου να μπορέσει να ασκήσει τις αρμοδιότητές της δυνάμει του άρθρου 58 παράγραφος 2 στοιχείο η) όπου*

απαιτείται, χορηγούν και ανανεώνουν πιστοποιήσεις. Το κράτος μέλος διασφαλίζει ότι η διαπίστευση των εν λόγω φορέων πιστοποίησης πραγματοποιείται από ένα ή αμφότερα τα ακόλουθα:….».

Τα σχέδια πιστοποίησης είναι δύο: το Cloud Certification Schemes List (CCSL), και το Cloud Certification Schemes Metaframework (CCSM). Όσον αφορά το πρώτο σχέδιο (CCSL) αποτελεί μία λίστα με υπάρχοντες –ήδη μηχανισμούς πιστοποίησης, σχετικούς με τις υπηρεσίες υπολογιστικού νέφους και παρέχει στους υποψήφιους πελάτες των υπηρεσιών αυτών μία σφαιρική εικόνα των αντικειμενικών χαρακτηριστικών ανά σχεδιάγραμμα, βοηθώντας τους πελάτες να κατανοήσουν πως λειτουργεί η κάθε υπηρεσία του παρόχου και εάν ταιριάζει με τις δικές τους ανάγκες. Όσον αφορά το Cloud Certification Schemes Metaframework (CCSM), πρόκειται για ένα υπέρ-πλαίσιο των υπαρχόντων μηχανισμών πιστοποίησης, το οποίο καθορίζει λεπτομερώς τις απαιτήσεις ασφαλείας του δημόσιου τομέα και τις προδιαγραφές ασφαλείας των παρόχων, όπως προκύπτουν από τους υπαρκτούς μηχανισμού πιστοποίησης. Στόχος του υπέρ-πλαισίου αυτού αποτελεί να προσφέρει περισσότερη διαφάνεια και βοήθεια στους υποψήφιους πελάτες του δημόσιου τομέα για τη διαδικασία επιλογής υπηρεσιών υπολογιστικού νέφους.

4.2.2 Θέματα ασφαλείας που σχετίζονται με την αποθήκευση των προσωπικών δεδομένων στο cloud.

Τα θέματα ασφάλειας που σχετίζονται με την αποθήκευση των δεδομένων στο υπολογιστικό νέφος, συγκεντρώνονται γύρω από τρεις έννοιες για τις οποίες έχουν γραφτεί άρθρα, μελέτες, έχουν διατυπωθεί γνώμες, και δεν είναι άλλες από **τις έννοιες της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας. (**βλ. Konstantinos E. Psannis, Stavroula Rizou, Eugenia Alexandropoulou-Egyptiadou. "GDPR Interference With Next Generation 5G and IoT Networks" date of publication June 8, 2020", σελ.2, https://ieeexplore.ieee.org/Xplore/home.jsp)

- **Εμπιστευτικότητα**

Αρχικά, η έννοια της εμπιστευτικότητας, αποτελεί γενική αρχή του Γενικού Κανονισμού για την Προστασία των Προσωπικών Δεδομένων. Σύμφωνα με το άρθρο **5§1 περ. στ' του ΓΚΠΔ**, «*1.Τα δεδομένα προσωπικού χαρακτήρα:….. στ) υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων («ακεραιότητα και εμπιστευτικότητα»).* Η εμπιστευτικότητα, έχει να κάνει κυρίως με την προφύλαξη, αν μπορούμε να χρησιμοποιήσουμε την λέξη αυτήν, με την έννοια ότι τα δεδομένα μας, προφυλάσσονται από τον πάροχο των υπηρεσιών νέφους, με δυνατότητα πρόσβασης σε αυτά μόνο σε **εξουσιοδοτημένα**

πρόσωπα. Άλλωστε, και το άρθρο **32§1 περ. β' του ΓΚΠΔ,** καθιστά σαφές πως «*1.Λαμβάνοντας υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων,* ***ο υπεύθυνος επεξεργασίας*** *και ο εκτελών την επεξεργασία εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων, περιλαμβανομένων, μεταξύ άλλων, κατά περίπτωση:….* ***β) της δυνατότητας διασφάλισης του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση***». Στο ρόλο του Υπευθύνου της Επεξεργασίας, προστίθεται και η υποχρέωση της διασφάλισης του απόρρητου των προσωπικών δεδομένων. Παράλληλα, και ο εκτελών την επεξεργασία, οφείλει να σέβεται την αρχή της εμπιστευτικότητας και του απορρήτου, καθώς, όπως ορίζεται και στο άρθρο **28§3 περ. β' του ΓΚΠΔ**, «*…Η επεξεργασία από τον εκτελούντα την επεξεργασία διέπεται από σύμβαση ή άλλη νομική πράξη υπαγόμενη στο δίκαιο της Ένωσης ή του κράτους μέλους, που δεσμεύει τον εκτελούντα την επεξεργασία σε σχέση με τον υπεύθυνο επεξεργασίας και καθορίζει το αντικείμενο και τη διάρκεια της επεξεργασίας, τη φύση και τον σκοπό της επεξεργασίας, το είδος των δεδομένων προσωπικού χαρακτήρα και τις κατηγορίες των υποκειμένων των δεδομένων και τις υποχρεώσεις και τα δικαιώματα του υπευθύνου επεξεργασίας. Η εν λόγω σύμβαση ή άλλη νομική πράξη προβλέπει ειδικότερα ότι ο εκτελών την επεξεργασία:….β)* ***διασφαλίζει*** *ότι τα πρόσωπα* ***που είναι εξουσιοδοτημένα*** *να επεξεργάζονται τα δεδομένα προσωπικού* ***χαρακτήρα έχουν αναλάβει δέσμευση τήρησης εμπιστευτικότητας*** *ή τελούν υπό τη δέουσα κανονιστική υποχρέωση τήρησης εμπιστευτικότητας»* . Η εμπιστευτικότητα μπορεί να εξασφαλιστεί, με καθορισμό της έννοιας των δικαιωμάτων και των ρόλων σύμφωνα με την αρχή της αναγκαιότητας με την ενεργό συμμετοχή του Υπευθύνου Επεξεργασίας, που θα καθορίζει τα άτομα που θα έχουν πρόσβαση στα δεδομένα και στις επεξεργασίες αυτών, καθορισμένα περιβάλλοντα εργασίας (κτίρια, αίθουσες) που θα είναι εξοπλισμένα για τη διασφάλιση της εμπιστευτικότητας, συμβατικές υποχρεώσεις όπως η υποχρέωση τήρησης απορρήτου δεδομένων, συμφωνίες εμπιστευτικότητας μεταξύ εργαζομένων και εξωτερικών συνεργατών των υπευθύνων επεξεργασίας και φυσικά πρόβλεψη κυρώσεων για τυχόν παραβίαση, προστασία από εξωτερικές επιδράσεις (κατασκοπεία), κρυπτογράφηση των αποθηκευμένων ή μεταφερθέντων δεδομένων, καθώς και καθορισμός διαδικασιών για τη διαχείριση και προστασία των κρυπτογραφικών πληροφοριών (κρυπτογραφική έννοια).

Η κρυπτογράφηση (βλ. C. Stergiou, K. E. Psannis, B.-G. Kim, B. Gupta, "Secure integration of IoT and Cloud Computing", Elsevier, Future Generation Computer Systems, vol. 78, part 3, σελ.8), φυσικά αποτελεί το καταλληλότερο μέτρο που μπορεί να «εγγυηθεί» υψηλά επίπεδα

ασφαλείας αναφορικά με την επεξεργασία των προσωπικών δεδομένων. «*Η κρυπτογράφηση είναι μία μαθηματική λειτουργία κατά την οποία χρησιμοποιείται ένα μυστικό στοιχείο – το κλειδί – με τη βοήθεια του οποίου κωδικοποιούνται τα δεδομένα, έτσι ώστε μόνο χρήστες με πρόσβαση στο κλειδί να μπορούν να διαβάσουν τις πληροφορίες αυτές. Το κλειδί που χρησιμοποιείται για να πραγματοποιηθεί η κρυπτογράφηση είναι ιδιαιτέρως σημαντικό, καθώς τυχόν απώλειά του, συνεπάγεται ότι τα δεδομένα που κρυπτογραφήθηκαν με αυτό είναι πλήρως άχρηστα, καθώς κανένας δεν μπορεί να έχει πρόσβαση σε αυτά.»(* Information Commissioner's Office – ICO). Όπως εξειδικεύει και η ομάδα εργασίας του άρθρου 29 στην με αριθ. 05/2012 Γνώμη της, η κρυπτογράφηση δύναται να συμβάλει καθοριστικά στην προστασία του απορρήτου των δεδομένων προσωπικού χαρακτήρα εφόσον εφαρμόζεται σωστά, παρότι δεν καθιστά τα δεδομένα προσωπικού χαρακτήρα αμετακλήτως ανώνυμα. Η κρυπτογράφηση δεδομένων προσωπικού χαρακτήρα προτείνεται να χρησιμοποιείται σε όλες τις περιπτώσεις κατά τις οποίες τα δεδομένα βρίσκονται «σε κίνηση» και, εφόσον είναι διαθέσιμη, όταν τα δεδομένα βρίσκονται «σε αδράνεια». Σε ορισμένες περιπτώσεις (π.χ. υπηρεσία αποθήκευσης IaaS), ο πελάτης υπηρεσιών νεφοϋπολογιστικής δύναται να μην επιλέξει τη λύση της κρυπτογράφησης που προσφέρει ο πάροχος υπηρεσιών νεφοϋπολογιστικής, αλλά να προτιμήσει να προβεί σε κρυπτογράφηση των δεδομένων προσωπικού χαρακτήρα προτού τα στείλει στο υπολογιστικό νέφος. Η κρυπτογράφηση δεδομένων σε αδράνεια απαιτεί ιδιαίτερη προσοχή όσον αφορά τη διαχείριση των κρυπτογραφικών κλειδιών, δεδομένου ότι η ασφάλεια των δεδομένων εξαρτάται ουσιαστικά από την προστασία του απορρήτου των κλειδιών κρυπτογράφησης.

- **Ακεραιότητα**

Ως ακεραιότητα νοείται η ιδιότητα των δεδομένων να διατηρούν τη γνησιότητά τους και να μην υφίστανται κακόβουλη ή τυχαία τροποποίηση κατά τη διάρκεια της επεξεργασίας, της αποθήκευσης ή της διαβίβασης. Η έννοια της ακεραιότητας μπορεί να επεκταθεί σε συστήματα τεχνολογιών της πληροφορίας, με την προϋπόθεση να παραμένει αμετάβλητη η επεξεργασία δεδομένων προσωπικού χαρακτήρα στα συστήματα αυτά. Τυχόν μεταβολές σε δεδομένα προσωπικού χαρακτήρα μπορούν να εντοπιστούν με τη βοήθεια κρυπτογραφικών μηχανισμών ελέγχου της γνησιότητας, όπως οι κωδικοί ή οι υπογραφές ελέγχου γνησιότητας μηνύματος. Απόπειρες παραβίασης της ακεραιότητας των συστημάτων τεχνολογιών της πληροφορίας εντός του υπολογιστικού νέφους μπορούν να προληφθούν ή να εντοπιστούν με τη βοήθεια συστημάτων εντοπισμού/πρόληψης εισβολών ((IPS/IDS). Αυτό είναι ιδιαίτερα σημαντικό για τα περιβάλλοντα ανοιχτού δικτύου στα οποία λειτουργούν συνήθως τα νέφη.

Αν μπορούσαμε να δώσουμε μερικά παραδείγματα εξασφάλισης της ακεραιότητας των δεδομένων, αποτελούν η τήρηση κανόνων σχετικά με το χρονικό διάστημα διατήρησης των δεδομένων, συχνοί έλεγχοι για την αξιοπιστία και την τεκμηρίωση της λειτουργικότητας, των κινδύνων, η χρήση κρυπτογραφικών μηχανισμών ελέγχου της γνησιότητας, όπως οι ηλεκτρονικοί κωδικοί ή οι ηλεκτρονικές υπογραφές ελέγχου γνησιότητας μηνύματος.

- **Διαθεσιμότητα**

Ως εξασφάλιση διαθεσιμότητας νοείται η διασφάλιση έγκαιρης και αξιόπιστης πρόσβασης σε δεδομένα προσωπικού χαρακτήρα. Σοβαρή απειλή για τη διαθεσιμότητα εντός του υπολογιστικού νέφους συνιστά η τυχαία απώλεια της σύνδεσης δικτύου μεταξύ του πελάτη και του παρόχου ή η διακοπή της εύρυθμης λειτουργίας του διακομιστή λόγω κακόβουλων ενεργειών όπως οι επιθέσεις (κατανεμημένης) άρνησης υπηρεσίας (DoS). Άλλοι κίνδυνοι που απειλούν τη διαθεσιμότητα είναι οι τυχαίες αστοχίες του υλισμικού τόσο στο δίκτυο και στο νεφοϋπολογιστικό σύστημα επεξεργασίας όσο και στο σύστημα αποθήκευσης δεδομένων, οι διακοπές ρεύματος και λοιπά προβλήματα υποδομής.

Οι υπεύθυνοι της επεξεργασίας δεδομένων προτείνεται να ελέγχουν εάν ο πάροχος υπηρεσιών νεφοϋπολογιστικής λαμβάνει ή όχι εύλογα μέτρα για την αντιμετώπιση των διαφόρων συναφών κινδύνων, όπως εφεδρικούς διαδικτυακούς συνδέσμους δικτύου, μηχανισμούς πολλαπλής αποθήκευσης και αποτελεσματικής εφεδρικής αποθήκευσης δεδομένων.

Όπως ορίζεται και στο άρθρο **12§1 του ΓΚΠΔ** «*Ο υπεύθυνος επεξεργασίας λαμβάνει τα κατάλληλα μέτρα για να παρέχει στο υποκείμενο των δεδομένων κάθε πληροφορία που αναφέρεται στα άρθρα 13 και 14 και κάθε ανακοίνωση στο πλαίσιο των άρθρων 15 έως 22 και του άρθρου 34 σχετικά με την επεξεργασία σε συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση, ιδίως όταν πρόκειται για πληροφορία απευθυνόμενη ειδικά σε παιδιά. Οι πληροφορίες παρέχονται γραπτώς ή με άλλα μέσα, μεταξύ άλλων, εφόσον ενδείκνυται, ηλεκτρονικώς. Όταν ζητείται από το υποκείμενο των δεδομένων, οι πληροφορίες μπορούν να δίνονται προφορικά, υπό την προϋπόθεση ότι η ταυτότητα του υποκειμένου των δεδομένων είναι αποδεδειγμένη με άλλα μέσα».*

Μερικά παραδείγματα εξασφάλισης της διαθεσιμότητας αποτελεί η προετοιμασία αποτελεσματικής εφεδρικής αποθήκευσης των δεδομένων, εφεδρικών διαδικτυακών συνδέσμων δικτύου, μηχανισμών πολλαπλής αποθήκευσης, ιστορικού συναλλαγών, προστασία απέναντι σε εξωτερικούς κινδύνους, τεκμηρίωση μέσω πολιτικών για την προστασία των προσωπικών δεδομένων με σκοπό τη διασφάλιση της διαθεσιμότητας.

4.2.3 Παραβίαση Προσωπικών Δεδομένων στο cloud – Υποχρεώσεις Υπεύθυνου Επεξεργασίας και Εκτελούντος της Επεξεργασία

Αρχικά, όταν μιλάμε για παραβίαση δεδομένων μιλάμε για καταστροφή, απώλεια, αλλοίωση αυτών, πρόσβαση σε αυτά από άτομα μη εξουσιοδοτημένα. Ο Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων, στο άρθρο **33** και επόμενα, περιγράφει εναργώς τα «βήματα» που πρέπει να ακολουθεί τόσο ο υπεύθυνος επεξεργασίας, όσο και ο εκτελών την επεξεργασία σε περίπτωση παραβίασης των προσωπικών δεδομένων.

Ειδικότερα, σύμφωνα με το άρθρο **33§1** του **ΓΚΠΔ**: «*Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα,* ***ο υπεύθυνος επεξεργασίας γνωστοποιεί αμελλητί*** *και, αν είναι δυνατό, εντός* ***72 ωρών*** *από τη στιγμή που αποκτά γνώση του γεγονότος την παραβίαση των δεδομένων προσωπικού χαρακτήρα στην* ***εποπτική αρχή*** *που είναι αρμόδια σύμφωνα με το άρθρο 55, εκτός εάν η παραβίαση δεδομένων προσωπικού χαρακτήρα δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Όταν η γνωστοποίηση στην εποπτική αρχή δεν πραγματοποιείται εντός 72 ωρών, συνοδεύεται από αιτιολόγηση για την καθυστέρηση.».* Αντίστοιχα και ο εκτελών την επεξεργασία, ο πάροχος δηλαδή των υπηρεσιών cloud computing, οφείλει χωρίς υπαίτια καθυστέρηση – *αμελλητι,* όπως αναφέρεται στην παράγραφο **2** του άρθρου **33 του ΓΚΠΔ**, να ειδοποιήσει τον υπεύθυνο επεξεργασίας, μόλις αντιληφθεί παραβίαση δεδομένων προσωπικού χαρακτήρα. **(**βλ. και Konstantinos E. Psannis, Stavroula Rizou, Eugenia Alexandropoulou-Egyptiadou. "GDPR Interference With Next Generation 5G and IoT Networks" date of publication June 8, 2020", σελ.4, https://ieeexplore.ieee.org/Xplore/home.jsp).

Εκτός όμως από την ενημέρωση της εποπτικής αρχής, ως αναφέρθηκε ανωτέρω, ο υπεύθυνος επεξεργασίας στην περίπτωση που υπάρχει κίνδυνος για τα προσωπικά δεδομένα, λόγω της παραβίασης αυτών, οφείλει σύμφωνα με το άρθρο **34 του ΓΚΠΔ** να ενημερώσει και το Υποκείμενο των δεδομένων. Συγκεκριμένα, όπως αναφέρεται στο άρθρο **34 §1 του ΓΚΠΔ**: «*Όταν η παραβίαση δεδομένων προσωπικού χαρακτήρα ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας ανακοινώνει αμελλητί την παραβίαση των δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων.* Μάλιστα κατά την ανακοίνωση αυτή, ο υπεύθυνος επεξεργασίας, σύμφωνα με την παράγραφο **2** του άρθρου **34 του ΓΚΠΔ:** περιγράφει «*.....με σαφήνεια η φύση της παραβίασης των δεδομένων προσωπικού χαρακτήρα και περιέχονται τουλάχιστον οι πληροφορίες και τα μέτρα που αναφέρονται στο άρθρο 33 παράγραφος 3 στοιχεία β), γ) και δ).»*

Μόνο εφόσον συντρέξουν οι περιπτώσεις του άρθρου **34§3 του ΓΚΠΔ**, ο υπεύθυνος επεξεργασίας δεν υποχρεούται να προβεί σε καμία ενημέρωση και γνωστοποίηση προς το

υποκείμενο των δικαιωμάτων Συγκεκριμένα, ο υπεύθυνος επεξεργασίας δεν απαιτείται να ανακοινώσει την παραβίαση στο υποκείμενο σε περίπτωση που εφάρμοσε κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας, και τα μέτρα αυτά εφαρμόστηκαν στα επηρεαζόμενα από την παραβίαση δεδομένα προσωπικού χαρακτήρα, κυρίως μέτρα που καθιστούν μη κατανοητά τα δεδομένα προσωπικού χαρακτήρα σε όσους δεν διαθέτουν άδεια πρόσβασης σε αυτά, όπως η κρυπτογράφηση, σε περίπτωση που έλαβε στη συνέχεια μέτρα που διασφαλίζουν ότι δεν είναι πλέον πιθανό να προκύψει ο αναφερόμενος στην παράγραφο **1** του άρθρο **34 του ΓΚΠΔ** υψηλός κίνδυνος για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, και τέλος στην περίπτωση που η ανακοίνωση προϋποθέτει δυσανάλογες προσπάθειες. Στην περίπτωση αυτή, γίνεται αντ' αυτής δημόσια ανακοίνωση ή υπάρχει παρόμοιο μέτρο με το οποίο τα υποκείμενα των δεδομένων ενημερώνονται με εξίσου αποτελεσματικό τρόπο.

Αβίαστα επομένως απ’ όλα τα παραπάνω, προκύπτει το συμπέρασμα πως οι πάροχοι υπηρεσιών cloud computing ως εκτελούντες την επεξεργασία (βλ. ανωτέρω κεφάλαιο «2.3.5 Ρόλος παρόχων υπηρεσιών στο Cloud») οφείλουν *αμελλητί,* ως ο Κανονισμός ορίζει, να ενημερώνουν – ειδοποιούν τον υπεύθυνο επεξεργασίας για τυχόν παραβίαση των προσωπικών δεδομένων των υποκειμένων.

5. ΕΛΛΗΝΙΚΗ ΔΙΚΑΙΟΣΥΝΗ ΚΑΙ CLOUD COMPUTING

Η αλήθεια είναι πως παρά την ευρέως διαδιδόμενη χρήση των εφαρμογών του cloud από άτομα κάθε ηλικίας, σε διάφορους τομείς και για διαφορετικούς λόγους χρήσης αυτών από τον κάθε χρήστη, η «παρουσία» του (του cloud computing) δεν έχει απασχολήσει τα Δικαστήρια της χώρας μας σε μεγάλο βαθμό. Αυτό, ίσως έχει να κάνει με το γεγονός πως η ελληνική κοινωνία και κατ’ επέκταση και η ελληνική δικαιοσύνη δεν είναι και τόσο εξοικειωμένη με τα τεχνολογικά επιτεύγματα, χωρίς αυτό να σημαίνει πως η χώρα μας και τα δικαστήρια μας είναι τεχνολογικά «ανάπηροι».

Κομμάτι της παρούσας διπλωματικής αποτελεί και το ζήτημα της αποθήκευσης των ρατσιστικών, εκβιαστικών, απειλητικών μηνυμάτων στο cloud του δράστη – εν δυνάμει κατηγορουμένου και οι τρόποι προστασίας του θύματος από την αποθήκευση αυτών σε ένα χώρο, στο σύννεφο δηλαδή, στο οποίο με μία πρώτη σκέψη η πρόσβαση είναι δύσκολη έως ανέφικτη. Αν θέλουμε με πολύ απλά λόγια να περιγράψουμε τι είναι αυτό που συμβαίνει, τι είναι αυτό που υπάρχει κάπου στα «σύννεφα», και το οποίο μας αφορά και φυσικά μας προσβάλλει, μας βλάπτει, μας φοβίζει, αλλά παρ’ όλα αυτά δεν μπορούμε να έχουμε άμεση πρόσβαση σε αυτό, θα λέγαμε τα εξής:

Αρχικά, όλα ξεκινάνε από την στιγμή που ο δράστης – εν δυνάμει κατηγορούμενος, θα στείλει ένα εκβιαστικό για παράδειγμα μήνυμα, οποιαδήποτε μορφής, ήτοι λεκτικό, ηχητικό, εικονικό στο υποψήφιο θύμα του. Το μήνυμα αυτό, αφού εισέλθει στην σφαίρα δράσης και κατοχής του θύματος, εκτός από την ύπαρξη και στο κινητό, στον ηλεκτρονικό υπολογιστή, στο tablet του δράστη, αυτομάτως αποθηκεύεται και στο «σύννεφό» του, ήτοι στο πάροχο των υπηρεσιών cloud στον οποίο διατηρεί ο τελευταίος λογαριασμό. Η συνέχεια μετά από μια φαινομενικά απλή αποστολή ενός μηνύματος εξαρτάται από τον τρόπο αντίδρασής του λήπτη – θύματος του εκβιαστικού αυτού μηνύματος. Ο λήπτης είτε δεν θα αντιδράσει και θα αγνοήσει το μήνυμα, γιατί μπορεί να μην ενδιαφέρεται, να μην θέλει να δώσει συνέχεια σε όλο αυτό που συμβαίνει ή να φοβάται να μιλήσει και να απευθυνθεί στις αρμόδιες αρχές, είτε θα αντιδράσει ζητώντας την αρωγή της Δικαιοσύνης.

Πώς όμως θα ενεργήσει η Δικαιοσύνη απέναντι στην διαμορφωθείσα αυτή κατάσταση; Είναι δυνατή η πρόσβαση στο cloud του δράστη και εάν ναι κάτω υπό ποιες προϋποθέσεις;

5.1.Απόφαση 613/2016 Πλημμελειοδικείου Αθηνών

Ως αναφέρθη και ανωτέρω, η νομολογία των ελληνικών δικαστηρίων είναι πενιχρή όσον αφορά υποθέσεις που αφορούν το cloud computing. Η υπ' αριθ. 613/2016 απόφαση του Πλημμελειοδικείου Αθηνών, αφορά περίπτωση παιδικής πορνογραφίας, όπου στο **cloud** του δράστη υπήρχε αποθηκευμένο τέτοιο υλικό και στο σκεπτικό της απόφασης τίθεται ζήτημα σχετικά με την εφαρμογή ή μη της διαδικασίας άρσης απορρήτου των επικοινωνιών για την ανεύρεση δεδομένων, αποθηκευμένων σε υπολογιστικό νέφος, η κατοχή και διακίνηση των οποίων συνιστά ποινικό αδίκημα.

Ειδικότερα, σύμφωνα με την απόφαση και την γνώμη της πλειοψηφίας, και σε αυτές τις περιπτώσεις, ήτοι στις περιπτώσεις αποθηκευμένων δεδομένων στο υπολογιστικό νέφος, πρέπει καταρχήν να τηρηθεί η διαδικασία των άρθρων 4 παρ. 4 και 5 του Ν 2225/1994. Και τούτο διότι πρωτίστως όλες οι πολιτικές απορρήτου των παρόχων των υπηρεσιών αποθήκευσης, δηλαδή των ιδιοκτητών ή μισθωτών των διακομιστών (servers), δεν εξασφαλίζουν την άμεση πρόσβαση προς χρήση όλων αυτών των αρχείων - δεδομένων, αλλά παρατηρείται ακριβώς το αντίθετο. Ειδικότερα σε όλες τις περιπτώσεις οι πάροχοι [ιδιοκτήτες ή μισθωτές των διακομιστών (servers)] ενημερώνουν το χρήστη ότι ναι μεν δεν μπορεί να ανεβάζει να διατηρεί και να διακινεί παράνομο περιεχόμενο, ωστόσο η κύρωση από τη μη τήρηση αυτών των όρων είναι το κλείσιμο του λογαριασμού του χρήστη από τον πάροχο. Οι πάροχοι ενημερώνουν ότι μπορούν να δώσουν

στοιχεία σε περίπτωση υποβολής νομότυπου αιτήματος και ότι η ικανοποίηση άλλων αιτημάτων επαφίεται στη διακριτική τους ευχέρεια.

Επομένως, σε κάθε περίπτωση για το νομότυπο σχετικού αιτήματος θα πρέπει να έχει τηρηθεί η διαδικασία της προηγούμενης δικαστικής άρσης απορρήτου κατά τις διατάξεις του Ν. 2225/1994, η οποία διαδικασία σε κάθε περίπτωση αναπληρώνει και τη συναίνεση του χρήστη ως προς τη χρήση των κωδικών του πρόσβασης στις υπηρεσίες αποθήκευσης (δεδομένου ότι η κάθε λειτουργία λογαριασμού - αποθηκευτικού χώρου προϋποθέτει κωδικούς χρήσης για την ταυτοποίηση του χρήστη - υποκειμένου). Όταν επομένως έχει μεσολαβήσει η δημιουργία λογαριασμού και η χρήση κωδικών πρόσβασης για τη χρήση της υπηρεσίας αποθήκευσης στο διακομιστή (server) του παρόχου, είναι αμφίβολο το αν μπορεί το υπολογιστικό αυτό νέφος (cloud storage) που ενδεχομένως βρίσκεται και σε άλλη ήπειρο να θεωρηθεί τμήμα υπολογιστή και ακολούθως να θεωρηθεί νόμιμη η χωρίς τις εγγυήσεις του άρθρου 253 του ΚΠΔ χρήση των δεδομένων αυτών σε δίκη. Μετά την τήρηση της διαδικασίας άρσης απορρήτου θα θεωρείται ότι τα αποκτηθέντα δεδομένα θα εξασφαλίζουν τις εγγυήσεις περί δίκαιης δίκης.

Αξίζει όμως στο σημείο αυτό, να αναφέρουμε και την γνώμη της μειοψηφίας, σύμφωνα με την οποία το αίτημα άρσης του απορρήτου των επικοινωνιών για την ανεύρεση αρχείων πορνογραφίας ανηλίκων αποθηκευμένων σε cloud storage, με τα οποία είναι συνδεδεμένοι οι υπολογιστές και οι συσκευές κινητής τηλεφωνίας, όπως dropbox, skydrive, google drive, πρέπει να απορριφθεί διότι αυτά δεν εμπίπτουν στην προστατευτική σφαίρα του απορρήτου της επικοινωνίας, με αποτέλεσμα, για την εργαστηριακή επεξεργασία τους να μην απαιτείται, καταρχήν, η διαδικασία άρσης του απορρήτου των επικοινωνιών. Ειδικότερα, με τον όρο cloud storage ή τον παρόμοιο (όταν πρόκειται για υπηρεσίες αποθήκευσης, όπως το icloud, google drive, dropbox, onedrive κ.λπ., όπως εν προκειμένω) όρο cloud computing, που αποδίδεται στα ελληνικά ως «υπολογιστικό νέφος», υποδηλώνεται η χρήση υπολογιστικής ισχύος που βρίσκεται σε απομακρυσμένα —σε σχέση με το χρήστη— δίκτυα, για την αποθήκευση και διαχείριση δεδομένων, δηλαδή «μέσα από το σύννεφο». Ο χρήστης, ο οποίος διατηρεί πορνογραφικά δεδομένα αποθηκευμένα σε υπολογιστικό νέφος (cloud computing), έχει τις ίδιες εξουσίες που θα είχε και εάν τα αποθήκευε σε ένα τοπικό αποθηκευτικό μέσο, καθώς μπορεί να τα διαχειριστεί κατά τη βούλησή του (π.χ. να τα αναπαράγει, να τα τροποποιεί, να τα διαγράφει ή να τα αποστέλλει σε τρίτους), εφόσον έχει πλήρη δικαιώματα πρόσβασης στην εν λόγω «τοποθεσία» του υπολογιστικού νέφους, η οποία και να του παρέχει τις παραπάνω εξουσίες. Πρόκειται, δηλαδή, στην πραγματικότητα, στην περίπτωση αυτή, για έναν εικονικό, απομακρυσμένο, εξωτερικό σκληρό δίσκο ή άλλης μορφής αποθηκευτικό μέσο (cd, usb flash drive κ.λπ.) και, ως τέτοιο πρέπει να αντιμετωπισθεί ως προς το ζήτημα της άρσης του απορρήτου των επικοινωνιών. Δηλαδή, οι διωκτικές Αρχές όταν διαπιστώσουν την ύπαρξη

μίας τέτοιας εφαρμογής υπηρεσιών αποθήκευσης στον υπολογιστή του δράστη, νομιμοποιούνται να πράξουν ό,τι θα έπρατταν εάν διαπίστωναν την ύπαρξη ενός εξωτερικού σκληρού δίσκου ή άλλης μορφής αποθηκευτικό μέσο. Δηλαδή, όπως στην περίπτωση ενός εξωτερικού σκληρού δίσκου ή άλλου υλικού φορέα, ο οποίος ανήκει στον ύποπτο τέλεσης ορισμένου εγκλήματος, οι διωκτικές Αρχές έχουν π.χ. το δικαίωμα κατάσχεσης και ελέγχου αυτού, έτσι και στην περίπτωση του λογαριασμού του δράστη σε υπολογιστικό νέφος, οι διωκτικές Αρχές νομιμοποιούνται να έχουν άμεση πρόσβαση σε αυτόν, χωρίς να απαιτείται άρση του απορρήτου των επικοινωνιών, αφού, οι υπηρεσίες αποθήκευσης, από μόνες τους δεν συνιστούν μορφή επικοινωνίας, με αποτέλεσμα, για την εργαστηριακή επεξεργασία των στοιχείων αυτών να μην απαιτείται η διαδικασία άρσης του απορρήτου των επικοινωνιών.

Βεβαίως, το συνταγματικά κατοχυρωμένο απόρρητο των επικοινωνιών, που κατοχυρώνεται στο άρθρο 19 του Συντάγματος, ισχύει και στην περίπτωση των υπηρεσιών νέφους. Προϋπόθεση, όμως, για να ενεργοποιείται η προστασία του απορρήτου των επικοινωνιών στην περίπτωση του υπολογιστικού νέφους, είναι η ύπαρξη επικοινωνίας. Εφόσον δηλαδή διαπιστωθεί ύπαρξη οιασδήποτε μορφή επικοινωνίας στον λογαριασμό του χρήστη, εάν δηλαδή διαπιστωθεί ότι εκεί ο χρήστης έχει αποθηκεύσει μηνύματα ηλεκτρονικού ταχυδρομείου (email) ή οποιαδήποτε άλλης μορφής επικοινωνία, όπως ανταλλαγή μηνυμάτων, φωτογραφιών κ.λπ. μέσω διαφόρων κοινωνικών δικτύων (π.χ. facebook, twitter, instagram), τότε βεβαίως πρέπει να ζητείται, για τα ευρήματα αυτά άρση του απορρήτου των επικοινωνιών κατά τις κείμενες διατάξεις.

6.ΣΥΜΠΕΡΑΣΜΑΤΑ – ΠΡΟΤΑΣΕΙΣ

Τελικά το θύμα, πώς θα προστατευτεί από τον κίνδυνο δημοσιοποίησης των εκβιαστικών, απειλητικών μηνυμάτων που δέχτηκε από τον θύτη και που βρίσκονται αποθηκευμένα στο cloud του τελευταίου, ο οποίος οποιαδήποτε στιγμή μπορεί να τα εκθέσει σε δημόσια «θέα», ακόμη και μετά από επιβολή ποινής που αφορά όμως την διάπραξη άλλων εγκλημάτων (π.χ. προσβολή τιμής – υπόληψης θύματος) και όχι την διατήρηση αυτών καθ' αυτών των μηνυμάτων στο cloud του;

Τα κενά στην ελληνική νομολογία είναι μεγάλα και αυτό γιατί μέχρι και σήμερα το ζήτημα αυτό δεν έχει απασχολήσει τα ελληνικά Δικαστήρια. Από την μια μεριά, η υπ' αριθ. 613/2016 απόφαση του Πλημμελειοδικείου Αθηνών, αναφέρεται μονάχα στο εάν θα πρέπει να διαταχθεί η άρση του απορρήτου και στις περιπτώσεις εκείνες που είναι αποθηκευμένα σε υπολογιστικό νέφος δεδομένα, η κατοχή και διακίνηση των οποίων συνιστά ποινικό αδίκημα. Από τη άλλη, ως αναφέρθη και ανωτέρω, οι πάροχοι [ιδιοκτήτες ή μισθωτές των διακομιστών (servers)] ενημερώνουν το χρήστη ότι ναι μεν δεν μπορεί να ανεβάζει να διατηρεί και να διακινεί παράνομο

περιεχόμενο, ωστόσο η κύρωση από τη μη τήρηση αυτών των όρων είναι το κλείσιμο του λογαριασμού του χρήστη από τον πάροχο.

Ακόμη δηλαδή και αν διαταχθεί από τις διωκτικές αρχές η άρση του απορρήτου προκειμένου τα αρμόδια όργανα να λάβουν γνώση των δεδομένων που έχει αποθηκευμένα στο cloud ο δράστης και η κατοχή αυτών συνιστά ποινικό αδίκημα, ακόμη και εάν επιβληθεί ποινή στον δράστη λόγω της κατοχής των δεδομένων αυτών, τι γίνεται με τα δεδομένα αυτά; Εξακολουθούν να υπάρχουν στο cloud και μπορούν να ανασυρθούν από τον δράστη όποτε ο ίδιος επιθυμεί; Η απάντηση μάλλον είναι θετική. Εξακολουθούν να υπάρχουν στο σύννεφο του δράστη. Και αυτό γιατί δεν υπάρχει πρόβλεψη είτε νομοθετική είτε από πλευράς των παρόχων για το ποια θα είναι η τύχη των παράνομων αυτών δεδομένων, σε περίπτωση καταδίκης του κατόχου. Πρόβλεψη που καθίσταται επιβεβλημένη αν αναλογιστεί κανείς το τεράστιο ζήτημα που δημιουργείται από την πλευρά του θύματος, το οποίο θα ζει με τον φόβο και το άγχος πως όσα μηνύματα του έχει στείλει ο δράστης, θα μπορούν να «κατέβουν» από το σύννεφο του τελευταίου και να προσγειωθούν και πάλι μπροστά του ή μπροστά στα μάτια οποιουδήποτε επιθυμεί ο δράστης, αν αναλογιστεί κανείς πως το κοινό του διαδικτύου είναι αναρίθμητο.

Αυτό που θα μπορούσε να γίνει προκειμένου να διαφυλαχτούν τα δικαιώματα και κατ' επέκταση η προσωπικότητα του θύματος, είναι με την έκδοση απόφασης που θα καταδικάζει τον κατηγορούμενο για κατοχή παράνομου υλικού στο «σύννεφο», να διατάζεται ταυτόχρονα το «κατέβασμα» των παράνομων αυτών δεδομένων με την οριστική διαγραφή και του λογαριασμού του χρήστη – κατηγορουμένου από το cloud, έτσι ώστε να επιτυγχάνεται και η αδυναμία πρόσβασής του σε αυτόν. Όλα αυτά βέβαια θα μπορέσουν να λάβουν χώρα εφόσον υπάρχει τροποποίηση και των όρων και προϋποθέσεων του εκάστοτε πάροχου με τον οποίο «συμβάλλεται» ο χρήστης - κατηγορούμενος, καθώς όπως αναφέρθηκε και ανωτέρω αυτό που μέχρι και σήμερα προβλέπεται είναι η ενημέρωση απλά του χρήστη ότι ναι μεν δεν μπορεί να ανεβάζει να διατηρεί και να διακινεί παράνομο περιεχόμενο, ωστόσο η κύρωση από τη μη τήρηση αυτών των όρων είναι το κλείσιμο του λογαριασμού του χρήστη από τον πάροχο.

Κρίνεται επομένως επιβεβλημένη μία συνεργασία μεταξύ των αρμόδιων αρχών (δικαστικών – κυβερνητικών – διεθνών οργανισμών) και των παρόχων υπηρεσιών cloud computing προκειμένου να δημιουργηθεί ένας νέος προστατευτικός μανδύας για όλα εκείνα τα πρόσωπα, των οποίων προσωπικά δεδομένα που προσβάλουν την υπόστασή τους και θίγουν την υπόληψη τους, βρίσκονται αποθηκευμένα στο cloud του δράστη και στο οποία φυσικά δεν έχουν πρόσβαση. Δεν αρκεί δηλαδή η καταδίκη του κατηγορουμένου για την αποστολή εκβιαστικών, ρατσιστικών, απειλητικών μηνυμάτων στον θύμα. Χρειάζεται να γίνει ένα βήμα επιπλέον με την βοήθεια όλων των αρμοδίων φορέων, προκειμένου να διαφυλαχτεί στο ακέραιο η προσωπικότητα του θύματος

με την ολοσχερή διαγραφή όλων εκείνων των δεδομένων, σε οποιαδήποτε μορφή και αν βρίσκονται αυτά, ήτοι λεκτικά, ηχητικά, εικονικά, έτσι ώστε να μην υπάρχει ο κίνδυνος στο μέλλον τα προσβλητικά για το θύμα δεδομένα έρθουν ξανά στην επιφάνεια, με επιβλαβής για το τελευταίο συνέπειες.

ΒΙΒΛΙΟΓΡΑΦΙΑ

➢ Ελληνικές πηγές και βιβλιογραφία

Δημητρόπουλος Α. (2008), Συνταγματικά Δικαιώματα, Γενικό Μέρος-Ειδικό Μέρος: Μητρικά Δικαιώματα- Φυσική Υπόσταση- Πνευματική Υπόσταση, Σύστημα Συνταγματικού Δικαίου Τόμος Γ΄- Τεύχος Ι-ΙΙΙ Β΄Έκδοση, Εκδόσεις Σάκκουλα, Αθήνα-Θεσσαλονίκη.

Δαγτόγλου Π. (2005), Συνταγματικό Δίκαιο, Ατομικά δικαιώματα Α΄, Β΄ αναθεωρημένη έκδοση, Αντ. Ν. Σάκκουλας, Αθήνα-Κομοτηνή.

Δαλακούρας Θ. (2019), Ηλεκτρονικό Έγκλημα, **κεφ. 6:** Ποινική ευθύνη ενδιάμεσων παρόχων, ιδίως φορέων μέσων κοινωνικής δικτύωσης, για fake news και προσβολές της τιμής στο διαδίκτυο, σελ. 95 Ιωάννης Μοροζίνης, **κεφ. 7:** Ιδιαιτερότητες στην ποινική αντιμετώπιση του ρατσισμού που εκδηλώνεται μέσω του διαδικτύου, σελ. 113 Χρήστος Νάιντος, **κεφ. 13:** Η επιβολή περιορισμών στα μέσα κοινωνικής δικτύωσης μετά τον νέο γερμανικό Νόμο περί Βελτίωσης της Επιβολής της Νομοθεσίας στα Κοινωνικά Δίκτυα (Netzwerkdurchsetzungsgesetz), Επίθεση στην ελευθερία έκφρασης ή αναγκαίο μέσο καταπολέμησης της διαδικτυακής εγκληματικότητας; σελ. 223, Δημήτριος Καραγκούνης, εκδόσεις Νομική Βιβλιοθήκη

Κτιστάκις Γ. (2004), Θρησκευτική ελευθερία και Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου, Ίδρυμα Μαραγκοπούλου για τα δικαιώματα του ανθρώπου, Αντ. Ν. Σάκκουλας, Αθήνα - Κομοτηνή.

Κουσουνή-Πανταζοπούλου Α. (2012), Νομικές διαστάσεις του cloud computing, ΔiΜΕΕ 2012, 177.

Μάνεσης Α. (1977), Η συνταγματική προστασία της ελεύθερης κυκλοφορίας των εντύπων και η εφαρμογή της στην πράξη, Το Σύνταγμα (Ιανουάριος - Μάρτιος, σ. 1-36.

Μαρίνος Παπαδόπουλος και Παντελής Ευγενίδης (2016), Νεφοϋπολογιστική (cloud computing) και προστασία προσωπικών δεδομένων Cloud Computing and protection of Personal Data –, δημοσίευση στο:

https://www.academia.edu/26398604/%CE%9D%CE%B5%CF%86%CE%BF%CF%8B%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%B9%CE%BA%CE%AE_cloud_computing_%CE%BA%CE%B1%CE%B9_%CF%80%CF%81%CE%BF%CF%83%CF%84%CE%B1%CF%83%CE%AF%CE%B1_%CF%80%CF%81%CE%BF%CF%83%CF%89%CF%80%CE%B9%CE%BA%CF%8E%CE%BD_%CE%B4%CE%B5%CE%B4%CE%BF%CE%BC%CE%AD%CE%BD%CF%89%CE%BD_Cloud_Computing_and_protection_of_Personal_Data

Μοροζίνης Ι. (2010), Απαγόρευση διακρίσεων και ελευθερία της έκφρασης, ΠΧ. 450

Μποτόπουλος Β. (1989), Εισήγηση επί της ΣτΕ 5148/1987, ΤοΣ , σελ 120

Πελεγρίνης Θ. (2013), Λεξικό της Φιλοσοφίας, Οι έννοιες, οι θεωρίες, οι σχολές, τα Ρεύματα και τα Πρόσωπα - Εξάγλωσση Ορολογία, Εκδόσεις Πεδίο.

Σισιλιάνος Λ-Α. (2013), Ευρωπαική Σύμβαση Δικαιωμάτων του Ανθρώπου, Ερμηνεία κατ' άρθρο, Νομική Βιβλιοθήκη, Αθήνα.

Σκουρής Β. - Ιωάννου Κ. (1996), Η ελευθερία της διαφήμισης, Εκδόσεις Σάκκουλα, Θεσσαλονίκη.

Χρυσογόνος Κ. (2002), Ατομικά και κοινωνικά δικαιώματα, Β΄ έκδοση αναθεωρημένη και συμπληρωμένη , Αντ. Ν. Σάκκουλας, Αθήνα - Κομοτηνή.

➢ **Ξένες πηγές και βιβλιογραφία**

C. Stergiou, K. E. Psannis, "Recent advances delivered in Mobile Cloud Computing's Security and Management challenges", IGI Global, Modern Principles, Practices, and Algorithms for Cloud Security, 2019.

C. Stergiou, K. E. Psannis, B.-G. Kim, B. Gupta, "Secure integration of IoT and Cloud Computing", Elsevier, Future Generation Computer Systems, vol. 78, part 3, pp. 964-975, January 2018.http://doi.org/10.1016/j.future.2016.11.031, https://www.researchgate.net/publication/311338093_Secure_integration_of_IoT_and_Cloud_Computing

C. Stergiou, K. E. Psannis, A. P. Plageras, T. Xifilidis, B. B. Gupta, "Security and Privacy of Big Data for Social Networking Services in Cloud", in Proceedings of IEEE conference on Computer Communications (IEEE INFOCOM 2018), 15-20 April 2018, Honolulu, HI, USA.

https://www.researchgate.net/publication/323036016_Security_and_Privacy_of_Big_Data_for_Social_Networking_Services_in_Cloud

Data Protection Code of Conduct for Cloud Service Providers. https://ec.europa.eu/digital-singlemarket/en/news/data-protection-code-conduct-cloud-service-providers

Evans D, (2008), "Social Media Marketing: an hour a day", Wiley Publishing, Inc. Indianapolis

Jiyi WU1,2, Lingdi PING1, Xiaoping GE3,Ya Wang4, Jianqing FU1, (2010) International Conference on Intelligent Computing and Cognitive Informatics, ―Cloud Storage as the Infrastructure of Cloud Computing

Kaplan, A. M. & Haenlein, M., (2010), «Users of the world, unite! The challenges and opportunities of Social Media. Business Horizons», Vol. 53, pp. 59-68, https://www.slideshare.net/Twittercrisis/kaplan-and-haenlein-2010-social-media

Konstantinos E. Psannis, Stavroula Rizou, Eugenia Alexandropoulou-Egyptiadou. "GDPR Interference With Next Generation 5G and IoT Networks" date of publication June 8, 2020" https://ieeexplore.ieee.org/document/9110555

Mayfield (2008) icrossing, «What is social media», http://www.icrossing.co.uk/fileadmin/uploads/eBooks/What_is_Social_Media_iCrossing_ebook.pdf

Rohan Jathanna, Dhanamma Jagli (2017), Cloud Computing and Security Issues, https://www.academia.edu/33632399/Cloud_Computing_and_Security_Issues

Rajkumar Buyya «The University of Melbourne and Manjrasoft Pty Ltd., Australia», James Broberg «The University of Melbourne, Australia», Andrzej Goscinski Deakin University, Australia (March 2011), CLOUD COMPUTING Principles and Paradigms» Edited by - Published by John Wiley & Sons (κεφάλαιο 8.1 σελ.221, κεφάλαιο 24.7 σελ.611)

Wirtz Bernd (2011), «Media and Internet Management» http://berndwirtz.com/downloads/mim_lm_extract.pdf.

J. Blocher, (2009), στο Reputation as Property in Virtual Economies, The Yale Law Journal Pocket Part, sel.123

- **<u>Νομοθετήματα – Δικαστικές Αποφάσεις</u>**

Γενικός Κανονισμός για την Προστασία Δεδομένων

Γνώμη 02/2015 σχετικά με τον κώδικα δεοντολογίας της ομάδας C-SIG για το υπολογιστικό νέφος της ομάδας εργασίας του άρθρου 29 για την προστασία των δεδομένων.

Γνώμη 05/2012 σχετικά με τη νεφοϋπολογιστική της ομάδας εργασίας του άρθρου 29 για την προστασία των δεδομένων.

Ποινικός Κώδικας

Σύνταγμα της Ελλάδος

Τριμελές Εφετείο Αθηνών 5800/2008 και 5919/2008

ΟΔΗΓΙΑ 2002/58/ΕΚ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 12ης Ιουλίου 2002 σχετικάμε την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες).

Ολ. ΑΠ 3/2010

Πενταμελές Εφετείο Αθηνών 913/2009

Πολυμελές Πρωτοδικείο Αθηνών 1765/2015

Στε Ολ. 2098/1988

Τριμελές Πλημμελειοδικείο Αθηνών 16819/2008

- **<u>Ιστοσελίδες</u>**

https://el.wikipedia.org/wiki/ICloud

http://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/11975/KOUROGIORGA_MTD1708.pdf?sequence=1&isAllowed=y

https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V1.0.pdf

http://users.uom.gr/~kpsannis/Lect-NetSySecPartA.pdf

http://moritzlaw.osu.edu/students/groups/is/files/2014/03/Black.pdf

http://webapptester.com/ti-einai-cloud-computing/

https://policies.google.com/privacy

https://www.apple.com/legal/internet-services/icloud/gr/terms.html

https://en.wikipedia.org/wiki/Taneja_Group

https://www.academia.edu/6172724/Cloud_Storage_as_Service

https://searchstorage.techtarget.com/feature/Understanding-cloud-storage-services-A-guide-for-beginners

ikee.lib.auth.gr › files › 05 Κεφάλαιο 3 Η εποχή του Cloud Computing

http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=81&Itemid=73&lang=

https://ec.europa.eu/digital-single-market/en/news/data-protection-code-conduct-cloud-service-providers

https://el-gr.facebook.com/help/contact/567360146613371

https://www.huffingtonpost.gr/entry/koinonia_gr_7466008

http://www.nomothesia.net/archives/2876

https://lawdb.intrasoftnet.com/nomos/3_nomologia_rs_sub.php