ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ
ΤΜΗΜΑ ΝΟΜΙΚΗΣ

ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

Η ΠΡΟΚΛΗΣΗ ΒΛΑΒΗΣ ΜΕ ΣΥΝΕΧΗ ΣΚΛΗΡΗ ΣΥΜΠΕΡΙΦΟΡΑ ΜΕΣΩ ΔΙΑΔΙΚΤΥΟΥ (CYBERBULLYING)-ΝΟΜΙΚΕΣ, ΗΘΙΚΕΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΚΕΣ ΠΡΟΕΚΤΑΣΕΙΣ

Διπλωματική Εργασία

της

Άννας Ντέμου

Θεσσαλονίκη, Μάρτιος 2024

Η ΠΡΟΚΛΗΣΗ ΒΛΑΒΗΣ ΜΕ ΣΥΝΕΧΗ ΣΚΛΗΡΗ ΣΥΜΠΕΡΙΦΟΡΑ ΜΕΣΩ ΔΙΑΔΙΚΤΥΟΥ (CYBERBULLYING)-ΝΟΜΙΚΕΣ, ΗΘΙΚΕΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΚΕΣ ΠΡΟΕΚΤΑΣΕΙΣ

Άννα Ντέμου
Πτυχίο Νομικής Α.Π.Θ 2007

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΟ ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέποντες καθηγητές
Θεοχάρης Δαλακούρας
Ιωάννης Μαυρίδης

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 01/03/2024

Θεοχάρης Δαλακούρας Ιωάννης Μαυρίδης Νικόλαος Σαββίδης

Άννα Ντέμου

Περίληψη

Στις μέρες μας, το Διαδίκτυο και τα μέσα κοινωνικής δικτύωσης χρησιμοποιούνται για διασκέδαση, πληροφόρηση, μάθηση, ανταλλαγή απόψεων και ανταλλαγή ιδεών, ακόμα και για εργασία, όπως συνέβη με την πρόσφατη πανδημία του Covid-19. Εκατομμύρια άνθρωποι συνδέονται ψηφιακά, ανεξαρτήτως χρόνου, τοποθεσίας και απόστασης, μέσω της χρήσης των μέσων κοινωνικής δικτύωσης. Η ανωνυμία του Διαδικτύου όμως, έχει πολλές φορές ως αποτέλεσμα έναν τεράστιο αριθμό διαδικτυακών εγκλημάτων, καθιστώντας πιο δύσκολη την παρακολούθηση αυτών, όπως είναι ο διαδικτυακός εκφοβισμός. Ο διαδικτυακός εκφοβισμός είναι ένα από τα πιο σοβαρά ηθικά ζητήματα στο Διαδίκτυο και ο αριθμός των ανθρώπων που έχουν πέσει θύματα διαδικτυακού εκφοβισμού αυξάνεται συνεχώς. Η παρούσα διπλωματική έχει σκοπό να αναλύσει τι ακριβώς σημαίνει Cyberbullying (διαδικτυακός εκφοβισμός), ποιες είναι οι μορφές του, πως η συμπεριφορά μας στο διαδίκτυο μας κάνει επιρρεπείς στον διαδικτυακό εκφοβισμό, εάν η πανδημία Covid-19 είχε αντίκτυπο στη ζωή μας στο διαδίκτυο. Η παρούσα διπλωματική εργασία πραγματεύεται επίσης την ποινική δίωξη αποστολής υβριστικών, δυσφημιστικών και εκβιαστικών μηνυμάτων στο διαδίκτυο, σύμφωνα με τον Ελληνικό Ποινικό Κώδικα και άλλα ξένα νομικά συστήματα, το πως συνδέεται η ελευθερία του λόγου και η προστασία των προσωπικών δεδομένων με τον διαδικτυακό εκφοβισμό, καθώς και τεχνολογικά και νομικά ζητήματα που έχουν να κάνουν με την ανίχνευση του εγκλήματος στον κυβερνοχώρο και τέλος πως μπορούμε να προστατεύσουμε τον εαυτό μας και τους άλλους από διαδικτυακούς εκφοβιστές.

Περιέχει επίσης μια συζήτηση πάνω στα αποτελέσματα μιας μικρής έρευνας, σχετικά με τον διαδικτυακό εκφοβισμό, καθώς και σχετικά στατιστικά στοιχεία που διατέθηκαν από τη Δίωξη Ηλεκτρονικού Εγκλήματος.

Λέξεις Κλειδιά: διαδικτυακός εκφοβισμός, δυσφήμιση, προστασία προσωπικών δεδομένων, ελευθερία του λόγου, ανίχνευση εγκλήματος στον κυβερνοχώρο

Abstract

Nowadays, Internet and social media are used for fun, information, learning, sharing opinions, and exchanging ideas, even for working, as happened during the Covid-19 pandemic. Millions of people are digitally connected, regardless of time, location, and distance, using the social media. The anonymity of the Internet has many times resulted in a huge number of online crimes, such as cyberbullying, making their activities more difficult to monitor. Cyberbullying is one of the most serious ethical issues on the Internet, and the number of people who have been victims of cyberbullying, is constantly increasing. The purpose of this thesis is to analyze what exactly the term cyberbullying means, which are its forms, how our behavior online makes us prone to cyberbullying, whether the Covid-19 pandemic had an effect on our on-line lives. This thesis also deals with the criminal prosecution of sending abusive, defamatory and extortionate messages on the internet, according to the Greek Penal Code and other foreign legal systems, how the freedom of speech and the personal data protection are connected with cyberbullying, the technical and legal issues that have to do with cyber-crime detection and finally how we can protect ourselves and others from online bullies.

It also contains a discussion on the results of an opinion survey on cyberbullying, as well as related statistical data provided by the Cyber Crime Unit of Hellenic Police.

Keywords: cyberbullying, defamation, personal data protection, freedom of speech, cybercrime detection

Πρόλογος – Ευχαριστίες

Θα ήθελα να ευχαριστήσω τους επιβλέποντες καθηγητές μου, κκ Θεοχάρη Δαλακούρα και Ιωάννη Μαυρίδη, για την υποστήριξή τους κατά τη συγγραφή της εργασίας. Επιπλέον, θα ήθελα να ευχαριστήσω όλους τους καθηγητές που συμμετείχαν στο Διατμηματικό Μεταπτυχιακό Πρόγραμμα Σπουδών «Δίκαιο και Πληροφορική» για τις πολύτιμες γνώσεις που μας μετέδωσαν, ειδικότερα στα πεδία που μας ήταν τελείως άγνωστα πριν ξεκινήσουμε τη φοίτηση σε αυτό, καθώς και τους συμφοιτητές μου, για τις όμορφες στιγμές που ζήσαμε κατά τη διάρκεια των μαθημάτων.

Περιεχόμενα

1 Εισαγωγή

1.1 Πρόβλημα – Σημαντικότητα του θέματος

Στις μέρες μας, το διαδίκτυο έχει γίνει μέρος της ζωής μας. Ηλεκτρονικές συσκευές, ιδίως τα κινητά τηλέφωνα, αποτελούν προέκταση του χεριού μας. Ιδιαιτέρως οι μικρότερες ηλικίες, αλλά και μεγάλοι ασυνείδητα και σχεδόν μαζικά, ανεβάζουν μανιωδώς στιγμές από την προσωπική τους ζωή. Αξίζει να σημειωθεί ότι η χρήση του διαδικτύου έχει διευρυνθεί και σε πολύ μικρότερες ηλικίες. Ακόμα και τα παιδιά μπορούν να έχουν πρόσβαση πλέον ανέλεγκτα οποιαδήποτε ώρα ακόμη και όταν βρίσκονται στην άνεση του σπιτιού τους. Αγνοούν όμως το ότι όσα ανεβάζουν μπορούν να αποτελέσουν το περιεχόμενο υβριστικών, συκοφαντικών ή εκβιαστικών μηνυμάτων που θα απευθύνονται στο υποκείμενο που ανεβάζει αυτές τις πληροφορίες. Κατά τη διάρκεια της πανδημίας του κορωνοϊού, η χρήση των κοινωνικών δικτύων λόγω του εγκλεισμού, διευρύνθηκε ακόμα πιο πολύ. Το φαινόμενο λοιπόν του διαδικτυακού εκφοβισμού, χρήζει αντιμετώπισης γιατί ουσιαστικά, προσβάλλει το δικαίωμα του ατόμου να χρησιμοποιεί ελεύθερα και χωρίς φόβο το διαδίκτυο.

1.2 Σκοπός – Στόχοι

Σκοπός της συγκεκριμένης διπλωματικής εργασίας είναι να γίνει μια μελέτη πάνω στις νομικές, ηθικές/κοινωνικές και τεχνολογικές προεκτάσεις του φαινομένου του cyberbullying. Συγκεκριμένα, αναλύεται το νομοθετικό πλαίσιο που υπάρχει στην Ελλάδα και στον κόσμο για την προστασία του χρήση του διαδικτύου από το bullying. Αναλύεται το πόσο σχετίζεται η προστασία των προσωπικών δεδομένων με το φαινόμενο του κυβερνοεκφοβισμού. Επίσης προσεγγίζονται οι αιτίες που μπορούν να οδηγήσουν στο φαινόμενο αυτό, οι ιδιαίτερες περιπτώσεις cyberbullying, οι τεχνικές που εφαρμόζονται για τον εντοπισμό των δραστών.

1.3 Συνεισφορά

Σχετικά με την βιβλιογραφική μελέτη, ένα μεγάλο μέρος της εργασίας προέρχεται από ξενόγλωσση βιβλιογραφία, καθώς υπήρχαν πολλά βιβλία και άρθρα τα οποία ανέλυαν το φαινόμενο του cyberbullying. Υπάρχει βέβαια και ελληνική βιβλιογραφία, αλλά και αρθρογραφία, καθώς και πλούσια νομολογία με πολλές δικαστικές αποφάσεις. Υπάρχει επίσης μια προσωπική έρευνα η οποία έγινε μέσω google form, καθώς και στατιστικά στοιχεία τα οποία ζητήθηκαν και δόθηκαν από τη Δίωξη Ηλεκτρονικού εγκλήματος.

1.4 Διάρθρωση της μελέτης

Οι όροι που χρησιμοποιούνται σε διεθνές επίπεδο ως προς την έννοια του ηλεκτρονικού εγκλήματος συμπυκνώνονται στο πρώτο μέρος της βιβλιογραφικής επισκόπησης, γίνεται μια προσπάθεια διάκρισης του ηλεκτρονικού εγκλήματος και ο ορισμός του cyberbullying ως μέρος αυτού, στο δεύτερο μέρος γίνεται μια κοινωνιολογική προσέγγιση του φαινομένου του cyberbullying. Περιλαμβάνεται η έρευνα που έγινε μέσω google forms και τα στοιχεία που δόθηκαν από τη Δίωξη Ηλεκτρονικού Εγκλήματος κατόπιν επικοινωνίας με αυτήν. Το τρίτο μέρος ασχολείται με το νομικό πλαίσιο προστασίας από το cyberbullying και τα λοιπά εγκλήματα κατά της τιμής, παρέχεται πλούσια νομολογία για τα θέματα προσβολών τιμής, η συσχέτιση

τους με τα προσωπικά δεδομένα ενώ στο τέταρτο μέρος αναφέρονται οι δυσκολίες στην ανίχνευση του ηλεκτρονικού εγκλήματος γενικά και κατά συνέπεια στα εγκλήματα κατά της τιμής.

2 Βασικές έννοιες και ορισμοί

2.1 Έννοια και διακρίσεις του ηλεκτρονικού εγκλήματος

Οι όροι που χρησιμοποιούνται σε διεθνές επίπεδο ως προς την έννοια του ηλεκτρονικού εγκλήματος συμπυκνώνονται αφενός στους γενικότερους όρους e-crime computer crime και αφετέρου στα ειδικότερα cybercrime και internet related crime με τους οποίους συνδέεται άρρηκτα το στοιχείο του διαδικτύου. Ως αντίστοιχοι όροι χρησιμοποιούνται στα Ελληνικά ο όρος ηλεκτρονικό έγκλημα ως γενικότερος και οι ειδικότεροι δικτυακό έγκλημα και κυβερνοέγκλημα ή έγκλημα του κυβερνοχώρου, οι οποίοι περιλαμβάνουν το στοιχείο της δικτύωσης. Εφαρμόζοντας τους όρους αυτούς, μπορούν να καταχωρισθούν ως μορφές του ηλεκτρονικού εγκλήματος αφενός τα εγκλήματα που διαπράττονται με τη χρήση ηλεκτρονικών υπολογιστών (computer crimes) και αφετέρου τα εγκλήματα που διαπράττονται ειδικά μέσω διαδικτύου και αναφέρονται ως κυβερνοεγκλήματα (cyber crimes) συνιστώντας μια ειδικότερη μορφή του ηλεκτρονικού εγκλήματος. Περαιτέρω, όπως εύστοχα έχει επισημανθεί, το ηλεκτρονικό έγκλημα οφείλει να κατανοηθεί υπό το φως μια τριπλής προσέγγισης ήγουν: α) ως μια νέα μορφή εγκλήματος που διαπράττεται με τη χρήση ηλεκτρονικών υπολογιστών, β) ως μια παραλλαγή των ήδη υπαρχόντων εγκλημάτων, τα οποία διαπράττονται με υπολογιστές και γ) ως μια εγκληματική πράξη που εκδηλώνεται με τη συμμετοχή καθ' οποιονδήποτε τρόπο ενός ηλεκτρονικού υπολογιστή. Η τριπλή αυτή προσέγγιση θεωρείται αναγκαία, καθώς το ηλεκτρονικό έγκλημα δε διακρίνεται από το «κοινό» ή «συμβατικό έγκλημα» μόνον σε σχέση με το διαφέρον (ηλεκτρονικό ή διαδικτυακό) περιβάλλον διάπραξης. Εύλογα άλλωστε, αφού κάποια από τα εν λόγω εγκλήματα διαπράττονται τόσο σε κοινό όσο και σε ηλεκτρονικό περιβάλλον, κάποια άλλα διαπράττονται μόνον σε περιβάλλον ηλεκτρονικών υπολογιστών μη συνδεδεμένων με το διαδίκτυο ή υπολογιστών εκτός διαδικτύου και κάποια άλλα τελούνται αποκλειστικά σε περιβάλλον του κυβερνοχώρου.

Υπό το φως του κριτηρίου τέλεσής τους τα υπό συζήτηση ηλεκτρονικά εγκλήματα μπορούν να διακριθούν, κατά την άποψη της πλειοψηφίας :

α) Σε εγκλήματα που διαπράττονται τόσο σε «κοινό» περιβάλλον, όσο και στο διαδίκτυο, όπως λ.χ. η συκοφαντική δυσφήμηση ή η αντιγραφή ενός μουσικού έργου ή μιας κινηματογραφικής ταινίας ή ενός προγράμματος ηλεκτρονικού υπολογιστή. Σε περίπτωση διάπραξης κάποιου από τα εγκλήματα αυτά σε «περιβάλλον διαδικτύου» καταφάσκεται η τέλεση του εγκλήματος σχετιζόμενου με τον κυβερνοχώρο ή διαπραττόμενου στον κυβερνοχώρο ή τελούμενου με τη βοήθεια του κυβερνοχώρου (internet related crime).

β) Σε εγκλήματα που διαπράττονται αποκλειστικά σε περιβάλλον ηλεκτρονικών υπολογιστών, χωρίς τη χρήση του διαδικτύου. Στην εν λόγω κατηγορία εντάσσονται τα εγκλήματα που προβλέπονται από το άρθρο 370Γ παρ. 1ΠΚ.

γ)Σε εγκλήματα που διαπράττονται στον κυβερνοχώρο και χαρακτηρίζονται ως κυβερνοεγκλήματα (cybercrime) όπως λ.χ. η μεταβίβαση κρυπτογραφικών κειμένων χωρίς σχετική άδεια ή η διάδοση παιδικού πορνογραφικού υλικού δια του κυβερνοχώρου (αρθρ. 348 Α ΠΚ).

Εξειδικεύοντας περαιτέρω, στην έννοια του «κυβερνοεγκλήματος», αξονικό στοιχείο της οποίας αποτελεί στο σύνολο των περιπτώσεων ο «διασυνδεδεμένος σε σύστημα πληροφοριών ηλεκτρονικός υπολογιστής» αλλά και τα smartphones είτε ως στόχος της επίθεσης, είτε ως το βασικό μέσο της επίθεσης, είτε τέλος ως ένα βοηθητικό εργαλείο για τη διάπραξη της επίθεσης, μπορούν να συγκαταλεχθούν τρεις κατηγορίες ποινικών αδικημάτων:

α) Τα γνήσια πληροφορικά εγκλήματα, όπως αυτά που τελούνται μέσω ηλεκτρονικού υπολογιστή και μέσω συστημάτων πληροφοριών (λ.χ. απάτη, πλαστογραφία).

β) Τα εγκλήματα με ψηφιακό περιεχόμενο, όπως αυτά που σχετίζονται με τη διακίνηση παράνομου περιεχομένου μέσω συστημάτων πληροφοριών (λ.χ. παιδική πορνογραφία)

γ) Τα εγκλήματα κατά πληροφοριακών συστημάτων, όπως αυτά που διαπράττονται κατά της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριακών συστημάτων και των ψηφιακών δεδομένων, συνιστώντας υποκατηγορία των κυβερνοεγκλημάτων (Δαλακούρας,2018).

2.2 Το φαινόμενο του cyberbullying- τι ειναι

Ο Διαδικτυακός εκφοβισμός ή Κυβερνοεκφοβισμός (Cyberbullying) αποτελεί εξέλιξη του παραδοσιακού εκφοβισμού σε τεχνολογικό επίπεδο και αφορά «οποιαδήποτε πράξη εκφοβισμού, ψυχολογικής κακοποίησης, επιθετικότητας, απειλής, ταπείνωσης, παρενόχλησης, τρομοκρατικής ή αυταρχικής συμπεριφοράς παιδιών, προ εφήβων και εφήβων που πραγματοποιείται μέσω του Διαδικτύου, κινητών τηλεφώνων είτε άλλων ψηφιακών τεχνολογιών από ομηλίκους τους και η οποία επαναλαμβάνεται σε βάθος χρόνου σε τακτικά ή άτακτα χρονικά διαστήματα» (stopcyberbullying.org, 2010). Ο πρώτος που χρησιμοποίησε τον όρο ήταν ο Καναδός παιδαγωγός Bill Belsey το 2004 και εντάσσεται, σύμφωνα με τους στις συμπεριφορές προληπτικής επιθετικότητας (Αντωνιάδου-Κόκκινος,2013), οι οποίες διεξάγονται από άτομο ή ομάδα ατόμων με απώτερο στόχο την πρόκληση συναισθηματικής ή/και σωματικής βλάβης στο εκάστοτε θύμα. Ο ορισμός αυτός έχει αρχίσει να θεωρείται παρωχημένος, καθώς συχνά παρουσιάζονται ως θύματα και ενήλικα άτομα.

Ο Κυβερνοεκφοβισμός, όπως προαναφέρθηκε, αποτελεί τη συνέχεια του παραδοσιακού εκφοβισμού, με συγκεκριμένες διαφοροποιήσεις οι οποίες και εστιάζονται στα ακόλουθα σημεία (διαδικτυακό σεμινάριο CSI institute) :

- Δυνατότητα άμεσης και ταυτόχρονης θυματοποίησης των χρηστών του διαδικτύου μέσα στο προσωπικό τους χώρο, σε παγκόσμιο επίπεδο, με μηδαμινό κόστος και συνεχή παρακολούθηση από πλευράς θυτών. Επιπλέον υπάρχει η απουσία φυσικών αποδείξεων-ενδείξεων.

- Παροχή «ανωνυμίας» από πλευράς διαδικτύου, η οποία και δημιουργεί μια αίσθηση ελευθερίας και ασφάλειας. Ο εκάστοτε θύτης κρυμμένος πίσω από μια ψεύτικη ταυτότητα, μπορεί να διαπράξει την εν λόγω εγκληματική συμπεριφορά, παραμένοντας αόρατος και αφήνοντας ελάχιστα ή και καθόλου ψηφιακά ίχνη με αποτέλεσμα όχι μόνο να γίνεται πιο δύσκολος ο εντοπισμός τους από πλευράς διωκτικών αρχών, αλλά και να αίρονται οι όποιες αρχικές αναστολές τέλεσης του εγκλήματος. Οι θύτες μάλιστα θεωρούν ψυχολογικά ότι έχουν μικρότερο μερίδιο ευθύνης, καθώς η επίθεση δε γίνεται κατά πρόσωπο. Αντιθέτως τα θύματα δε νιώθουν ότι έχουν ασφάλεια ούτε μέσα στο ίδιο τους το σπίτι. (διαδικτυακό σεμινάριο CSI institute)

- Η ύπαρξη μεγάλου αριθμού μαρτύρων, ακούσιων ή εκούσιων (bystanders), οι οποίοι και χωρίζονται σε δυο κύριες κατηγορίες: α. οι επιβλαβείς για το θύμα, οι οποίοι και μέσω της συμπεριφοράς τους είτε επικροτούν την εγκληματική συμπεριφορά, είτε παραμένουν αδιάφοροι και οι β. οι βοηθοί παρατηρητές οι οποίοι μέσω της άμεσης αντίδρασής τους κινητοποιούν περισσότερα άτομα για την καταπολέμηση του φαινομένου.

- Η ίδια η φύση του διαδικτύου η οποία και καταρρίπτει την ανάγκη της επανάληψης, καθώς όποια βίντεο ή αναρτήσεις (σε ένα blog, στο YouTube, στο Facebook και σε άλλα μέσα κοινωνικής δικτύωσης) είναι συνέχεια διαθέσιμα δημόσια, ήτοι ορατά από απροσδιόριστο αριθμό ατόμων οπουδήποτε και οποτεδήποτε, αυξάνοντας έτσι με ευκολία τον αντίκτυπο στο θύμα.

- Η μη ανάγκη ύπαρξης δυσανάλογης δύναμης μεταξύ θύτη και θύματος, μιας και μέσω των ηλεκτρονικών μέσων ακόμη και ένα άτομο χωρίς ιδιαίτερες σωματικές ικανότητες μπορεί να γίνει θύτης σε απεριόριστο αριθμό ατόμων. (Kowalski et al., 2014).

- Είναι θέμα που πλήττει κυρίως τον εφηβικό πληθυσμό, αλλά αυτό δεν είναι πάντα αναγκαίο καθώς το Διαδίκτυο χρησιμοποιείται από όλες τις ηλικίες.

- Το άτομο που επιτίθεται είναι συνήθως γνωστό του θύματος (Li et al., 2022). Δεν αποκλείεται όμως να επιτεθεί, ιδίως σε ανοιχτές συζητήσεις σε social media να επιτεθεί λεκτικά κάποιο παντελώς άγνωστο άτομο (αυτό είναι πολύ συχνό φαινόμενο στο Twitter).

-Το προσβλητικό περιεχόμενο μπορεί να προβληθεί και μοιραστεί από άλλους και έχει τη δυνατότητα να προσεγγίσει ένα μεγάλο κοινό. Αυτός ο τύπος διαδικτυακού εκφοβισμού, όπου ο κυβερνοεκφοβιστής δεν κατευθύνει την αρνητική ηλεκτρονική επικοινωνία στον στόχο του, αναφέρεται επίσης μερικές φορές ως «έμμεσος διαδικτυακός εκφοβισμός» (Langos, 2012).

Ο διαδικτυακός εκφοβισμός μπορεί δυστυχώς να έχει αντίκτυπο για μεγαλύτερο χρονικό διάστημα, επειδή στο παραδοσιακό bullying η επιθετικότητα τελειώνει όταν απομακρύνεται το θύμα σωματικά από τους θύτες (π.χ. όταν ένα παιδί γυρίζει σπίτι από το σχολείο), ενώ ο διαδικτυακός εκφοβισμός βιώνεται ακόμη και όταν

ο επιτιθέμενος δεν είναι παρών στο διαδίκτυο (πχ είναι κάποιος offline και του στέλνουν υβριστικά μηνύματα). Ο αντίκτυπός του στα θύματα είναι πολύ μεγαλύτερος από αυτόν της παραδοσιακής επιθετικότητας (Ferrara et al., 2018)

Ο ηλεκτρονικός εκφοβισμός μπορεί να λάβει χώρα μέσω του διαδικτύου, του ηλεκτρονικού ταχυδρομείου, δωματίων συνομιλίας (Chat Rooms), σελίδων κοινωνικής δικτύωσης (social networking sites), των ιστολογιών (blogs), μέσω άλλων ιστοσελίδων σχετικών με ηλεκτρονικά παιχνίδια ή υπηρεσιών άμεσης ανταλλαγής μηνυμάτων καθώς και μέσω κινητών τηλεφώνων. Πιο συγκεκριμένα, οι μορφές που μπορεί να πάρει μπορούν, βάσει των kids-safety (2015) και Willard (2007) να κατηγοριοποιηθούν σε 13 σημεία, τα οποία και εμπίπτουν σε μια από τις 3 μεγάλές κατηγορίες τις δυσφήμισης, της παρενόχλησης και της εξαπάτησης:

1. Flaming (Στην πυρά) – Ηλεκτρονικές αντιπαλότητες μέσω e-mails με σκληρή και στην πλειοψηφία χυδαία γλώσσα
2. Online harassment (Διαδικτυακή παρενόχληση) – Επανειλημμένη αποστολή προσβλητικών μηνυμάτων
3. Cyberstalking (Καταδίωξη) – Διαδικτυακή παρενόχληση μέσω απειλών πρόκλησης βλάβης ή με υπερβολικό εκφοβισμό
4. Cyberthreats (Απειλές) – Γενικές δηλώσεις μίσους, οι οποίες συνήθως καθιστούν το συντάκτη της δήλωσης συναισθηματικά αναστατωμένο με ενδεχόμενο είτε να βλάψει τον εαυτό του, είτε να αυτοκτονήσει.
5. Denigration (Δυσφήμιση) – Αποστολή προς άλλα άτομα επιβλαβών, αναληθών ή σκληρών δηλώσεων σχετικά με ένα πρόσωπο ή δημοσίευση τέτοιου υλικού στο διαδίκτυο με σκοπό τη βλάβη.
6. Impersonation (Μίμηση) – Υιοθέτηση άλλης ταυτότητας και αποστολή επιβλαβούς υλικού με σκοπό τη βλάβη
7. Outing (Δημοσιοποίηση προσωπικών στοιχείων) – Αποστολή ή δημοσίευση προσωπικών στοιχείων σχετικά με ένα πρόσωπο που περιέχει ευαίσθητες προσωπικές ή ενοχλητικές πληροφορίες, συμπεριλαμβανομένης της προώθησης προσωπικών μηνυμάτων ή εικόνων.
8. Trickery (Εξαπάτηση/Εμπαιγμός) – Ξεγέλασμα του θύματος με απότοκο την αποκάλυψη μυστικών και ενοχλητικών πληροφοριών για να τα μοιραστεί και ο ίδιος διαδικτυακά

9. Exclusion (Εξοστρακισμός) – Ωμή και σκληρή εξαίρεση ή/και αποβολή κάποιου από ηλεκτρονική ομάδα στο διαδίκτυο (πχ ομάδα στο Facebook, ομάδα συνομιλίας στο Viber)

10. Bash boards (τελειωτικό χτύπημα) – Διαδικτυακοί πίνακες ανακοινώσεων με πρόστυχες και κακόβουλες δημοσιοποιήσεις μίσους.

11. Happy slapping (Χαρωπό χαστούκισμα)– Προσωπική επίθεση σε ανυποψίαστο θύμα, η οποία και βιντεοσκοπείται ή φωτογραφίζεται και μετά το εν λόγω διανέμεται ηλεκτρονικά (ως φάρσα)

12. Text Wars/Attacks (Πόλεμοι κειμένου) – Δημιουργία «συμμορίας» με στοχευμένη αποστολή εκατοντάδων επιβλαβών μηνυμάτων με απότοκο τη συναισθηματική καταπόνηση

13. Online polls (Διαδικτυακές δημοσκοπήσεις) – Ψήφισμα επί επιβλαβών και υποτιμητικών θεμάτων από τους αναγνώστες της εκάστοτε σελίδας.

Σε μελέτη των Γρηγοράκη, Περάκη και Πολίτη το 2014, γίνεται αναφορά στα χαρακτηριστικά τόσο των θυτών όσο και των θυμάτων της εν λόγω εγκληματικής συμπεριφοράς. Πιο συγκεκριμένα οι θύτες συνήθως παραπέμπουν σε άτομα που υφίστανται και τα ίδια σωματική ή λεκτική βία στο ενδοοικογενειακό περιβάλλον, ή ζουν σε υπερβολικά πειθαρχημένα περιβάλλοντα, οπότε με τη συμπεριφορά του τραμπουκισμού, προσπαθούν να επιβληθούν στους άλλους. Μπορεί να είναι κυρίαρχες και ιδιαίτερα δημοφιλείς προσωπικότητες με μεγάλη αυτοπεποίθηση και ιδιαίτερα θετική άποψη για τον εαυτό τους, που συνήθως δυσκολεύονται να ακολουθήσουν κανόνες, ενώ συνήθως παρουσιάζουν και άλλες αντικοινωνικές συμπεριφορές όπως ροπή σε μικροκλοπές, κατανάλωση αλκοόλ, κάπνισμα, προβλήματα αυτοελέγχου, πρόκληση υλικών ζημιών και αδιαφορία για το σχολείο. Τα θύματα από την άλλη πλευρά είναι άτομα ευαίσθητα και εσωστρεφή, ιδιαιτέρως ευάλωτα και ανασφαλή, με χαμηλή αυτοπεποίθηση και δημοφιλία, ενώ δεν εμφανίζουν επιθετική ή προκλητική συμπεριφορά. Συνήθως η σωματική τους αδυναμία και κάποια ιδιαίτερα χαρακτηριστικά τους (παχυσαρκία, τραυλισμός, σεξουαλικές προτιμήσεις, κάποιου είδους αναπηρία) αποτελούν στοιχεία προσέλκυσης εκφοβιστικών επιθέσεων. (http://www.indeepanalysis.gr/koinwnia/kybernoekfobismos-mia-nea-morfi-bias). Τα παραπάνω βέβαια αφορούν ανήλικα άτομα, αλλά όπως προειπώθηκε το φαινόμενο το διαδικτυακού εκφοβισμού έχει αρχίσει να πλήττει και ενήλικες.

Δυστυχώς, το φαινόμενο του Διαδικτυακού εκφοβισμού εγκυμονεί σοβαρές επιπτώσεις για την ψυχική υγεία του θύματος. Αποτελεί τις περισσότερες φορές μύθο, το ότι «τα θύματα γίνονται πιο δυνατά σε χαρακτήρα», καθώς αυτό αφορά τη μειοψηφία και συμβαίνει περισσότερο, αφότου έχουν σταματήσει οι εκφοβισμοί. (McQuade,2009). Η «πικρή αλήθεια» είναι ότι το bullying, δημιουργεί μεγάλο πόνο στα θύματα. Έρευνες εντοπίζουν επιπτώσεις όπως αυξημένο άγχος, το οποίο μπορεί να εκδηλωθεί με σωματικά προβλήματα όπως πονοκεφάλους, πόνους στο στομάχι, συναισθηματική δυσφορία, απόσυρση από κοινωνικές δραστηριότητες, απώλεια ενδιαφέροντος για καθημερινές δραστηριότητες, κατάθλιψη, ακόμα και τάσεις για αυτοτραυματισμό και αυτοκτονία. Διαιωνίζονται έτσι τα αρνητικά συναισθήματα και οι σκέψεις που μπορεί να επηρεάσουν την ψυχική υγεία και ευημερία (διαδικτυακό σεμινάριο CSI institute).

Πέραν των προαναφερθέντων ερευνών, μια σειρά από επιστημονικές μελέτες παρουσιάζουν στατιστικά ευρήματα τα οποία και υπογραμμίζουν τη σημαντική κατά τα τελευταία χρόνια αύξηση του φαινομένου, ειδικότερα μετά την άνοδο των μέσων κοινωνικής δικτύωσης (Facebook, Twitter, YouTube, blog, κτλ.). Σύμφωνα με τους Αντωνιάδου και Κόκκινο (2013), ο εκφοβισμός και η παρενόχληση στον κυβερνοχώρο αποτελούν τμήμα της καθημερινότητας παιδιών και εφήβων, με τα δύο φύλα να συμμετέχουν εξίσου αλλά με διαφορετικούς τρόπους εκδήλωσης της επιθετικότητας. Τα αγόρια έχουν μεγαλύτερη ροπή προς φαινόμενα στα οποία εμπεριέχεται σωματική βία, ενώ τα κορίτσια τείνουν να χρησιμοποιούν το διαδίκτυο για τη σπίλωση της υπόληψης των θυμάτων τους με στόχο την περιθωριοποίηση τους από την υπόλοιπη ομάδα.

3 ΚΟΙΝΩΝΙΟΛΟΓΙΚΗ ΠΡΟΣΕΓΓΙΣΗ ΤΟΥ ΦΑΙΝΟΜΕΝΟΥ

3.1 Η μεγαλύτερή ενασχόληση με το Διαδίκτυο ως μια από τις πηγές του κακού

Το Διαδίκτυο (ή Internet) αποτελεί μέρος της ζωής μας εδώ και τρεις περίπου δεκαετίες, με μεγαλύτερη άνοδο στη χρησιμοποίησή του την τελευταία δεκαπενταετία. Αποτελεί ένα εργαλείο πληροφόρησης, παρέχει ευκαιρίες για κοινωνική δικτύωση και

ευκαιρία για διεύρυνση γνώσεων. Αυτό που έχει αλλάξει, ιδίως την τελευταία δεκαετία, είναι το γεγονός ότι υπάρχει μεγάλη αύξηση του αριθμού των συσκευών μέσα των οποίων ο άνθρωπος έχει πρόσβαση στο Διαδίκτυο.

Αρχικά ενώ η πρόσβαση γινόταν κυρίως μέσω κάποιου ηλεκτρονικού υπολογιστή (σταθερού ή φορητού) στις μέρες μας υπάρχουν τα έξυπνα κινητά, οι υπολογιστές ταμπλέτες (tablets), η smart τηλεόραση, καθώς και άλλες συσκευές διασκέδασης, όπως οι διάφορες ψηφιακές παιχνιδομηχανές ή κονσόλες (game consoles). Επίσης με την τεχνητή νοημοσύνη (AI) όσο και με τη χρήση συσκευών IoT που έχουν παρουσιάσει αύξηση τα τελευταία χρόνια, εκθέτουμε ακόμα περισσότερο προσωπικές μας πληροφορίες στο Διαδίκτυο. Επιπλέον, η πρόσβαση στο Διαδίκτυο είναι πλέον πολύ φθηνότερη (πολλές φορές ακόμα και δωρεάν) και διαθέσιμη σχεδόν παντού μέσω των ασύρματων δικτύων (Wi-Fi) ή και τα megabyte των δικτύων κινητής τηλεφωνίας . Όλα αυτά τα στοιχεία ενώ από την μια πλευρά έχουν συμβάλει στο να πραγματοποιείται απρόσκοπτα η πρόσβαση του ανθρώπου στην πληροφορία και να είναι άμεση η επικοινωνία μεταξύ των χρηστών του Διαδικτύου, από την άλλη πλευρά, το Διαδίκτυο έχει τη δυνατότητα να προκαλέσει ψυχολογική ζημιά, όταν δε γίνεται ορθά ή τουλάχιστον με έναν βαθμό σύνεσης η χρήση του.

Έχουν γίνει πολλές έρευνες ότι τα γνωστά slots ή αλλιώς όπως ονομάζονται από πολλούς στην Ελλάδα φρουτάκια ή κουλοχέρηδες, βασίζονται, όπως και οι εφαρμογές των κινητών (apps), στην ίδια χημική διαδικασία του εγκεφάλου που προκαλεί εθισμό. (https://psychoedu.gr/o-kouloxeris-pou-exeis-panta-mazi-sou)

Πίσω από τη λειτουργία των slots υπάρχει ένας αλγόριθμος. Αυτός ο αλγόριθμος είναι προγραμματισμένος να δίνει ένα συγκεκριμένο χρηματικό ποσοστό πίσω στους παίχτες και να κρατάει ένα ποσοστό για το καζίνο, έτσι ώστε να μην απογοητεύεται ο παίχτης από την αποτυχία του και προσπαθεί να μένει όσο το δυνατόν περισσότερο στο παιχνίδι. Το επιτυγχάνει αυτό δηλαδή δίνοντας στον παίχτη μικρές νίκες ανά τακτά χρονικά διαστήματα.

Κάθε φορά που βγαίνει ο συγκεκριμένος συνδυασμός εικόνων και ο παίχτης κερδίζει, ο εγκέφαλος τον επιβραβεύει εκκρίνοντας ντοπαμίνη. Η ντοπαμίνη είναι η ουσία της επιβράβευσης και επηρεάζει τον άνθρωπο στη διάθεση, το κίνητρο και το κέντρο λήψης αποφάσεων. Η έκκριση ντοπαμίνης έχει θετικά οφέλη για τον οργανισμό, ελλοχεύει όμως και ο κίνδυνος του εθισμού. Αυτήν την παράμετρο εκμεταλλεύονται συνήθειες όπως ο τζόγος, τα ναρκωτικά και τα μέσα κοινωνικής δικτύωσης. (https://psychoedu.gr/o-kouloxeris-pou-exeis-panta-mazi-sou)

Τα social media, όπως και οι «κουλοχέρηδες», διατρέχονται από αλγόριθμους των οποίων στόχος είναι, ο χρήστης να παραμείνει όσο το δυνατόν περισσότερο μέσα στην εφαρμογή. Αυτό που εκμεταλλεύονται είναι η έμφυτη τάση του ανθρώπου για αποδοχή. Για παράδειγμα, σχεδόν κάθε φορά ανεβάζουμε μια άποψη, μια φωτογραφία, ένα τραγούδι, ή οτιδήποτε άλλο στα μέσα κοινωνικής δικτύωσης, περιμένουμε να λάβουμε το λεγόμενο "Like". Ασυναίσθητα επιζητάμε τα "Like" γιατί ο εγκέφαλος μας εκκρίνει ντοπαμίνη κάθε φορά που το δεχόμαστε. Ο αλγόριθμος λοιπόν είναι σχεδιασμένος να προσφέρει στο χρήστη ειδοποιήσεις, ανά τακτά χρονικά διαστήματα, για να τον κρατήσει ενεργό για όσο το δυνατόν μεγαλύτερο διάστημα. Πολλοί έχουν προσέξει ότι πχ στην εφαρμογή Instagram, πως αν δεν τη χρησιμοποιούμε για πολλή ώρα, στέλνει μια ειδοποίηση για αναρτήσεις, stories, reels τα οποία δεν έχουμε διαβάσει. Το Instagram άλλωστε έχει κατηγορηθεί από πολλούς ψυχολόγους ότι είναι αυτό που δημιουργεί ένα είδους συμπλέγματος κατωτερότητας στους χρήστες του, γιατί μπροστά τους παρουσιάζεται το τέλειο τοπίο, η τέλεια εξωτερική εμφάνιση, η τέλεια ανθρώπινη ερωτική ή φιλική σχέση, δημιουργώντας την ψευδαίσθηση σε αυτόν που παρακολουθεί ότι αυτός ποτέ δε θα γίνει αυτό το αψεγάδιαστο.

Κάθε φορά λοιπόν που ανοίγουμε την οθόνη του κινητού μας ή ακόμα και τον υπολογιστή, μπαίνουμε στην λογική της slot machine. Είναι σαν να πατάμε το κουμπί, στα «φρουτακια» περιμένοντας να πετύχει jackpot (να δούμε ειδοποίηση). «Σκρολάρουμε» σε μια σελίδα, μέχρι ο αλγόριθμος να «πετάξει» κάτι ενδιαφέρον ή αστείο. Ο εγκέφαλος εκκρίνει ντοπαμίνη και συνεχίζουμε μέχρι να ξαναεμφανιστεί το ίδιο αποτέλεσμα. Η ροδέλα στο ποντίκι έχει σαν στόχο να διατηρεί το χέρι ξεκούραστο κατά τη διάρκεια που σκρολάρουμε σε μια σελίδα. Ίδια λογική βρίσκεται και πίσω από την οθόνη αφής, όπως και πανομοιότυπη λογική και πίσω από την αλλαγή του μοχλού στον «κουλοχέρη» με ένα απλό κουμπί (Macït, H. B., Macït, G., & Güngör, O. 2018).

Επίσης, η υπερβολική ενασχόληση με το Διαδίκτυο έχει θεωρηθεί ότι δημιουργεί το φαινόμενο pop-corn brain: δηλαδή η τάση της προσοχής και της συγκέντρωσής μας να μετατοπίζεται γρήγορα από το ένα πράγμα στο άλλο, όπως σκάει το καλαμπόκι όταν γίνεται ποπ-κορν. μπορεί να επηρεάσει αρνητικά τις κοινωνικές αλληλεπιδράσεις, την υπομονή, τη συναισθηματική ευημερία και την παραγωγικότητά μας, ενώ αυξάνει το άγχος και τις πιθανότητες να πάθουμε burnout. (https://ischool.uw.edu/news/2016/12/too-much-screen-time-could-lead-popcorn-brain).

Εκθέτοντας λοιπόν συνεχώς τον εαυτό μας στο Διαδίκτυο, τον θέτουμε συνεχώς σε κίνδυνο παρενόχλησης από τους επίδοξους νταήδες.

3.2 Η επίδραση της πανδημίας του Covid19 στην έξαρση του φαινομένου cyberbullying

Λόγω των μέτρων κοινωνικής αποστασιοποίησης και περιορισμού μετακινήσεων στην πανδημία του COVID-19, μειώθηκε η φυσική αλληλεπίδραση, και κατά συνέπεια, η χρήση των μέσων κοινωνικής δικτύωσης αυξήθηκε και υπήρξε μεγαλύτερη δραστηριότητα στο περιβάλλον του κυβερνοχώρου. Αυτό ήταν πιο έντονο για έφηβους και νεαρούς ενήλικες με την αλλαγή στην εκπαίδευση εξ αποστάσεως από δια ζώσης, η οποία με τη σειρά της έκανε μεγαλύτερη εξάρτηση από διαδικτυακές πλατφόρμες. Ωστόσο, λίγα είναι ακόμη γνωστά για τα φαινόμενα διαδικτυακού εκφοβισμού στον παιδικό και νεανικό πληθυσμό κατά τη διάρκεια της πανδημίας και ποιες επιπτώσεις έχει αυτή η μείωση στις φυσικές επαφές και στον αντίποδα η αύξηση της κοινωνικοποίησης μέσω του διαδικτύου.

Σε έρευνα που πραγματοποιήθηκε στην Ισπανία που εξετάζει τον διαδικτυακό εκφοβισμό σε σχέση στην πανδημία COVID-19, αντιμετωπίζοντας επίσης τη συχνότητα και τους παράγοντες κινδύνου για την κυβερνοθυματοποίηση όχι μόνο σε νεανικό πληθυσμό, αλλά και σε υποομάδες πληθυσμού που θα μπορούσαν να είναι πιο ευάλωτες στον εκφοβισμό. Η αναφορά των Lobe et al. συμπεριλαμβανομένων 11 ευρωπαϊκών χωρών τονίζουν ότι μεταξύ των παιδιών που έχουν ήδη πέσει θύματα διαδικτυακού εκφοβισμού, σχεδόν τα μισά (44 τοις εκατό) ανέφερε αύξηση του φαινομένου κατά τη διάρκεια της πρώτης καραντίνας για τον COVID 19. Στη μελέτη αυτή, περισσότερο από το 50 τοις εκατό του δείγματος ήταν θύματα διαδικτυακού εκφοβισμού και συνολικά το 22,8 τοις εκατό των μαθητών ανέφεραν ότι ήταν θύματα και το 26,5 τοις εκατό δράστες διαδικτυακού εκφοβισμού για πρώτη φορά κατά τη διάρκεια της πανδημίας COVID-19, όπως έχει ήδη ανιχνευθεί σε άλλες περιοχές. Αυτή η μελέτη εστιάζει στην παρατήρηση πιθανών αλλαγών που θα μπορούσαν να έχουν συμβεί στο πλαίσιο της πανδημίας του COVID-19 και παρόλο που παρατηρήθηκε μια αύξηση στο χακάρισμα των προσωπικών λογαριασμών ως μορφή εκφοβισμού, τα αποτελέσματα δεν αντικατοπτρίζουν άλλες σημαντικές διαφορές στους τρόπους και μορφές διαδικτυακού εκφοβισμού κατά τη διάρκεια της πανδημίας. Το φαινόμενο

μπορεί να αποδοθεί στην ψυχολογική πίεση λόγω του εγκλεισμού (Morales-Arjona et al,2022)

3.3 Στατιστικά στοιχεία της Ελληνικής Αστυνομίας αναφορικά με τη δίωξη των εγκλημάτων που διαπράττονται μέσω διαδικτύου ή με τη χρήση αυτού

Κατόπιν ηλεκτρονικής επικοινωνίας με τη Δίωξη Ηλεκτρονικού Εγκλήματος για στατιστικά στοιχεία για καταγγελίες θυμάτων ενώπιον της Αρχής για περιστατικά δόθηκε η εξής απάντηση:

Γίνεται μνεία, από πλευράς ποινικής αξιολόγησης, το «cyberbullying» δεν πληροί την αντικειμενική υπόσταση θεσμοθετημένου αυτοτελούς εγκλήματος, αλλά εκδηλώνεται συχνά ως ένα σύνθετο και εμφανώς περίπλοκο φαινόμενο ποικίλων αξιόποινων συμπεριφορών οι οποίες μπορούν να ενταχθούν στην αντικειμενική υπόσταση πολλών εγκλημάτων (εξύβριση, απειλή, σωματική βλάβη, δυσφήμιση, συκοφαντική δυσφήμιση κ.ά.).

Κατόπιν των ανωτέρω στον παρακάτω πίνακα θα βρείτε τα στατιστικά στοιχεία υποθέσεων που χειρίστηκε η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος (όχι όλες οι Υπηρεσίες της Ελληνικής Αστυνομίας) για το έτος 2023:

ΑΔΙΚΗΜΑ	ΠΛΗΘΟΣ ΥΠΟΘΕΣΕΩΝ
312/Σωματική Βλάβη Αδύναμων Ατόμων	18
333/Απειλή	314
ΣΥΝΟΛΟ	**332**

Η έρευνα δε μας έχει δώσει περισσότερα στοιχεία, καθώς δε γνωρίζουμε ακριβώς το περιεχόμενο των απειλών, δείχνει όμως ότι υπάρχει ένας σχετικά μεγάλος βαθμός υποθέσεων που καταγγέλλονται.

3.4 Έρευνα για τον για τον Διαδικτυακό Εκφοβισμό

3.4.1 Ταυτότητα έρευνας

-Η έρευνα είχε τον εξής τίτλο:

«Διαδικτυακός εκφοβισμός (Cyberbullying)» και πραγματοποιήθηκε μέσω της εφαρμογής Google Form.

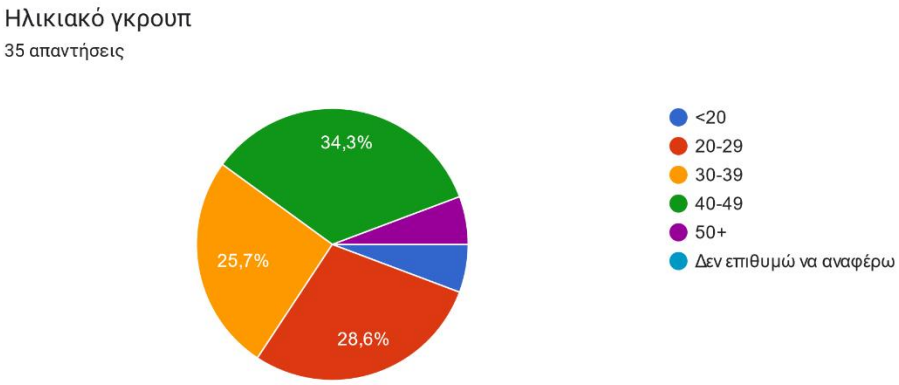
(https://docs.google.com/forms/d/1a1XDbavOsqSOeJ2ysSfcKIbfF76uFalerfQ2YltsbjM/edit?pli=1). Απευθύνθηκε σε ενήλικα άτομα που διαμένουν στην Ελλάδα. Το μεγαλύτερο πρόβλημα κατά τη διεξαγωγή αυτή της έρευνας ήταν η έλλειψη μεγάλης συμμετοχής, μόλις 35 άτομα, καθώς πολλές φορές το Facebook , όπου μοιράστηκε το ερωτηματολόγιο, κατέβαζε την ανάρτηση θεωρώντας την ως spam ανάρτηση, οπότε δεν μπορούσαν άτομα να τη δουν και να λάβουν μέρος. Αυτός ήταν ο κύριος λόγος για τον οποίο δεν κατέστη δυνατό να λάβουν μέρος περισσότερα άτομα. Οι ερωτήσεις ήταν:

3.4.2 Ερωτήσεις

1. Σε ποιο ηλικιακό γκρουπ ανήκετε;
2. Ποιο είναι το μορφωτικό σας επίπεδο;
3. Έχετε λογαριασμό σε οποιοδήποτε μέσο κοινωνικής δικτύωσης;
4. Στην περίπτωση που απαντήσατε ναι στην προηγούμενη ερώτηση, έχετε λογαριασμό σε: (επιτρέπονται πολλαπλές απαντήσεις)
5. Έχετε υπάρξει ποτέ θύμα παρενόχλησης στο Διαδίκτυο, είτε υπό τη μορφή εξύβρισης, είτε υπό τη μορφή απειλής (σωματικής ή μη ή με την απειλή διάδοσης προσωπικών στιγμών), είτε με διάδοση δυσφημίσεων;
6. Σε περίπτωση που απαντήσατε όχι, γνωρίζετε κάποιο άλλο πρόσωπο του κοντινού σας περιβάλλοντος (πχ μέλος οικογένειας, φίλος, συνάδερφος) που να έχει υπάρξει θύμα παρενόχλησης;
7. Αν απαντήσατε θετικά σε οποιαδήποτε από τις δύο προηγούμενες ερωτήσεις , τι αφορούσε η παρενόχληση αυτή;
8. Από ποιον προήλθε η παρενόχληση αυτή;
9. Με ποιον τρόπο έγινε παρενόχληση αυτή;
10. Στην περίπτωση της παρενόχλησης ποια ήταν η αντίδραση μου;
11. Γνωρίζετε αν υπάρχει στην Ελλάδα νομοθετικό πλαίσιο για την προστασία των χρηστών του Διαδικτύου από παρενοχλήσεις;
12. Κατά πόσο νομίζετε ότι έχει συμβάλει στην έκρηξη του φαινομένου η έκθεση των χρηστών στα social media?

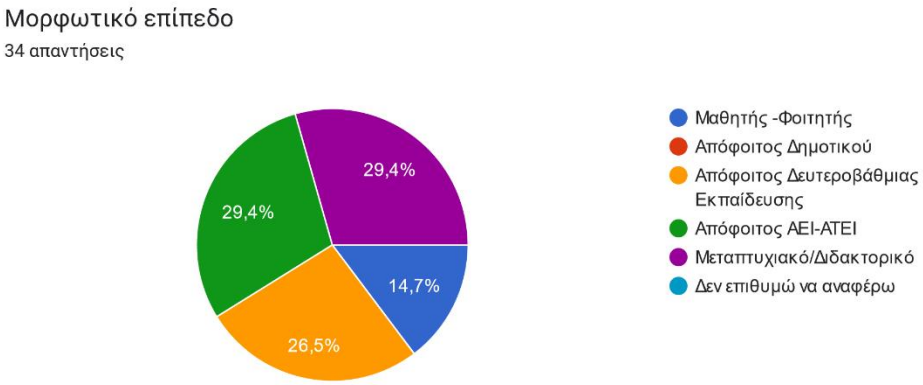
3.4.3 Απαντήσεις

Ερώτηση 1. Σε ποιο ηλικιακό γκρουπ ανήκετε;



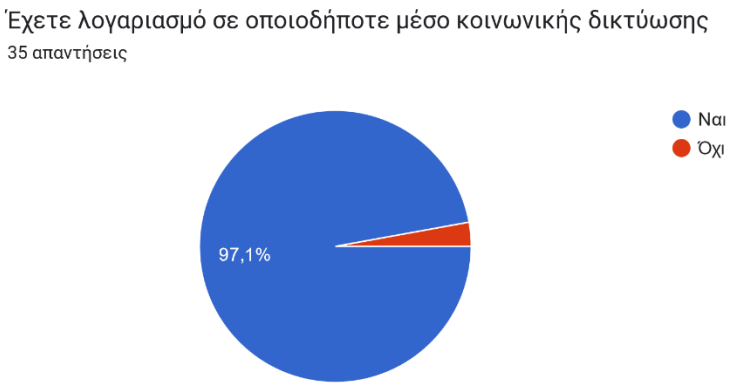
Σε αυτή την ερώτηση βλέπουμε ότι το μεγαλύτερο ποσοστό 34,3 %, είναι οι ηλικίες 40-49, ακολουθεί το ηλικιακό γκρουπ 20-29 με 28,6%, μετά οι ηλικίες 30-39 με 25,7% , ενώ από 5,7% το κάθε γκρουπ κάτω των 20 ετών και άνω των 50.

Ερώτηση 2. Ποιο είναι το μορφωτικό σας επίπεδο;



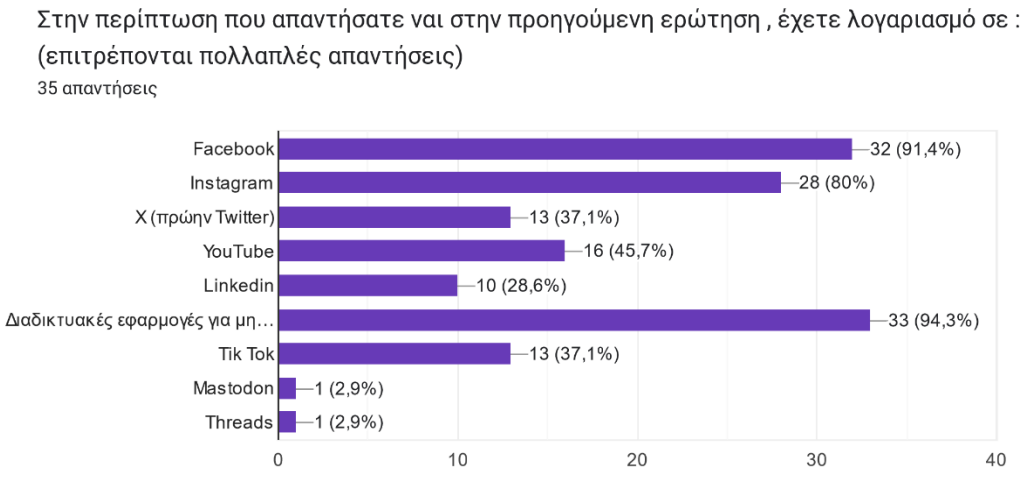
Σε ό,τι αφορά το μορφωτικό επίπεδο και οι απόφοιτοι ΑΕΙ-ΑΤΕΙ και οι κάτοχοι μεταπτυχιακού-διδακτορικού συγκεντρώνουν από 29,4% του ποσοστού των ερωτηθέντων, οι απόφοιτοι δευτεροβάθμιας εκπαίδευσης καταλαμβάνουν το 26,5% και οι μαθητές-φοιτητές το 14,7%

Ερώτηση 3. Έχετε λογαριασμό σε οποιοδήποτε μέσο κοινωνικής δικτύωσης;



Σε ό,τι αφορά τα μέσα κοινωνικής δικτύωσης, μόνο ένα άτομο απάντησε ότι δεν έχει λογαριασμό στα μέσα κοινωνικής δικτύωσης (καταλαμβάνει 2,9% ποσοστό)

Ερώτηση 4. Στην περίπτωση που απαντήσατε ναι στην προηγούμενη ερώτηση, σε ποιο από τα κοινωνικά δίκτυα έχετε λογαριασμό; (επιτρέπονται πολλαπλές απαντήσεις)



Σε αυτήν την ερώτηση, βλέπουμε ότι η συντριπτική πλειοψηφία (33 από τα 35 άτομα που ερωτήθηκαν και με ποσοστό 94,3% έχουν κάποια διαδικτυακή εφαρμογή για μηνύματα, όπως το Viber. Επίσης το 91,4% έχει λογαριασμό στο Facebook, το 80% στο Instagram, το 37,1% στο X/ Twitter, το 45,7% στο Youtube, 28,6% στο Linkedin, 37,1% στο TikTok και 2,9% το καθένα τα «καινούρια» Mastedon και Threads.

Ερώτηση 5. Έχετε υπάρξει ποτέ θύμα παρενόχλησης στο Διαδίκτυο, είτε υπό τη μορφή εξύβρισης, είτε υπό τη μορφή απειλής (σωματικής ή μη ή με την απειλή διάδοσης προσωπικών στιγμών), είτε με διάδοση δυσφημίσεων;

Εδώ η «πίτα» μοιράζεται σχεδόν στη μέση, καθώς το 51,4% απαντά ναι και το 48,6% όχι.

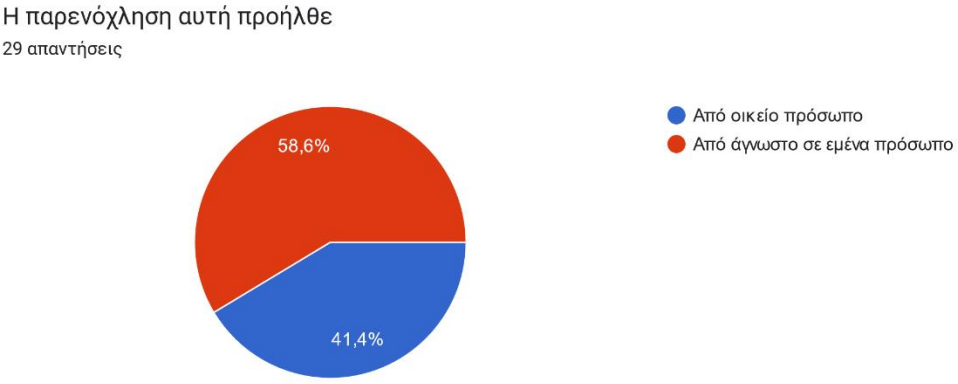
Ερώτηση 6. Σε περίπτωση που απαντήσατε όχι στην προηγούμενη, γνωρίζετε κάποιο άλλο πρόσωπο του κοντινού σας περιβάλλοντος (πχ μέλος οικογένειας, φίλος, συνάδερφος) που να έχει υπάρξει θύμα παρενόχλησης;

Στην ερώτηση αυτή, φαίνεται να απαντούν ότι ακόμα και αν δεν έχουν πέσει οι ίδιοι θύματα παρενόχλησης γνωρίζουν σε ποσοστό 51,4% κάποιο οικείο πρόσωπο που έχει παρενοχληθεί , το 22,9% δε γνωρίζει άτομα που να παρενοχλήθηκαν, ενώ το 22,9% απαντά ότι ενδεχομένως να γνωρίζει κάποιο άτομο.

Ερώτηση 7. Αν απαντήσατε θετικά σε οποιαδήποτε από τις δύο προηγούμενες ερωτήσεις , τι αφορούσε η παρενόχληση αυτή;

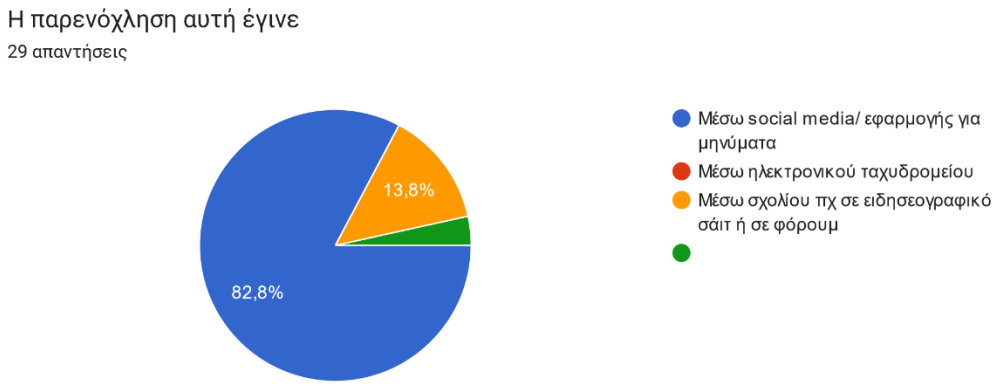
Σε αυτό το ερώτημα υπάρχει μεγάλη ποικιλία απαντήσεων, αν και το μεγαλύτερο ποσοστό δεικνύει ότι η παρενόχληση αφορούσε το επάγγελμα του θύματος (31%), το 13,8% αφορά την καταγωγή του θύματος, επίσης 13,8% δεν αναφέρει τι ακριβώς αφορούσε η παρενόχληση, ενώ μικρότερα ποσοστά από 1 απάντηση αφορούσε επίθεση από πρώην σύντροφο καθώς και από νυν σύντροφο πρώην σχέσης, επίσης από 1 απάντηση την οικονομική κατάσταση του θύματος, καθώς και 1 την εξωτερική εμφάνιση αυτού, επίσης 1 απάντηση αφορούσε επίθεση για αθλητική ομάδα που υποστηρίζει το θύμα.

Ερώτηση 8. Από ποιον προήλθε η παρενόχληση αυτή;



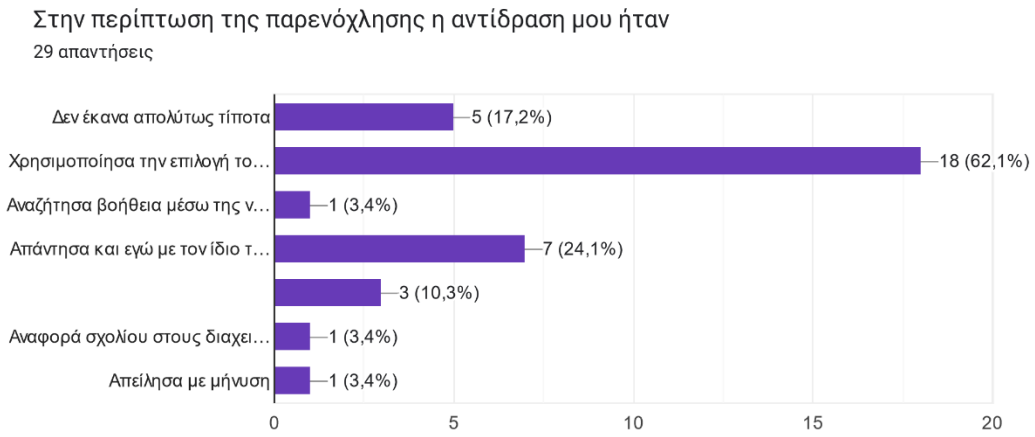
Ιδιαίτερο ενδιαφέρον και παρά τα όσα είδαμε παραπάνω στη βιβλιογραφική επισκόπηση(ότι συνήθως το πρόσωπο που επιτίθεται είναι γνωστό του θύματος), εδώ η πλειοψηφία 58,4% απαντά ότι η παρενόχληση προήλθε από άγνωστο προς το θύμα πρόσωπο.

Ερώτηση 9. Με ποιον τρόπο έγινε παρενόχληση αυτή;



Εδώ κανένας δε δήλωσε να έχει παρενοχληθεί μέσω ηλεκτρονικού ταχυδρομείου, αντιθέτως το 82,3% δήλωσε ότι παρενοχλήθηκε μέσω social media ή πλατφόρμας για μηνύματα και ένα ποσοστό 13,8% μέσω σχολίου σε ειδησεογραφικό σάιτ ή σε forum.

Ερώτηση 10. Στην περίπτωση της παρενόχλησης ποια ήταν η αντίδραση μου;



Στην περίπτωση της παρενόχλησης οι περισσότεροι (18 άτομα, 62,1%) δήλωσαν ότι χρησιμοποίησαν την επιλογή του μπλοκαρίσματος, το 24,1% (7 άτομα) δήλωσαν ότι απάντησαν με τον ίδιο τρόπο που παρενοχλήθηκαν, 5 άτομα δεν έπραξαν απολύτως τίποτα (17,2%), 3 άτομα (10,3%) δε δίνουν καμία διευκρίνιση για τον τρόπο αντίδρασης τους, 1 άτομο προέβη σε αναφορά του σχολίου στους διαχειριστές, 1 άτομο απείλησε με μήνυση, ενώ επίσης 1 άτομο αναζήτησε βοήθεια μέσω της νομικής οδού (3,4% ποσοστό το καθένα)

11. Γνωρίζετε αν υπάρχει στην Ελλάδα νομοθετικό πλαίσιο για την προστασία των χρηστών του Διαδικτύου από παρενοχλήσεις;

Και εδώ το ποσοστό είναι λίγο μοιρασμένο, καθώς το 51.4% δηλώνει ότι έχει γνώση για το αν υπάρχει στην Ελλάδα νομοθετικό πλαίσιο για την προστασία των χρηστών του Διαδικτύου από παρενοχλήσεις, ενώ το 48,6% όχι.

12. Κατά πόσο νομίζετε ότι έχει συμβάλει στην έκρηξη του φαινομένου του διαδικτυακού εκφοβισμού η έκθεση των χρηστών στα social media?

Εδώ η πλειοψηφία φαίνεται να παραδέχεται ότι έχει συμβάλει στην έκρηξη του φαινομένου η έκθεση των χρηστών στα social media (51,4% ποσοστό, 18 απαντήσεις, σε βαθμό 5, ότι δηλαδή έχει συμβάλει πάρα πολύ), 12 άτομα ότι μετράει η έκθεση στα social media σε βαθμό 4, 4 άτομα ότι μετράει σε βαθμό 3, ενώ ένα μόνο άτομο ότι συμβάλει σε πολύ μικρό βαθμό 2.

3.4.4 Συμπεράσματα έρευνας

Εσκεμμένα έχει χρησιμοποιηθεί η λέξη παρενόχληση στα ερωτήματα, ώστε να γίνει κατανοητή και από μη νομικούς και να μπορεί να καλύψει πολλές περιπτώσεις, όπως την εξύβριση, την απειλή και τη δυσφήμιση. Εντυπωσιακό είναι το γεγονός, ότι μια μόνο απάντηση στην ερώτηση «αν έχετε λογαριασμό σε οποιοδήποτε μέσο κοινωνικής δικτύωσης» ήταν αρνητική. Το πιο αγαπημένο μέσο κοινωνικής δικτύωσης φαίνεται να είναι το Facebook, καθώς το μεγαλύτερο ποσοστό των ερωτηθέντων απάντησε ότι έχει λογαριασμό σε αυτό.

Από όλη την έρευνα συνάγεται το συμπέρασμα ότι δυστυχώς πολλοί άνθρωποι, ακόμα και αν έχουν παρενοχληθεί στο διαδίκτυο, αγνοούν ότι μπορούν να προστατευθούν μέσω του νομοθετικού πλαισίου. Είναι μεν ελπιδοφόρο το ότι προκειμένου να σταματήσει η παρενόχληση που δέχτηκαν κατέφυγαν σε μεθόδους που προσφέρουν οι ίδιες οι διαδικτυακές πλατφόρμες, όπως το μπλοκάρισμα και η αναφορά σχολίου σε διαχειριστή. Επίσης, φαίνεται ότι αρχίζει να καταρρίπτεται ο μύθος ότι ο θύτης cyberbullying είναι γνωστός του θύματος, καθώς πολλοί ανέφεραν ότι έχουν παρενοχληθεί και από άγνωστα άτομα.

4 Νομικό πλαίσιο προστασίας από το cyberbullying και τα λοιπά εγκλήματα κατά της τιμής

4.1 Δικαίωμα ελευθερίας έκφρασης

Θα πρέπει πρώτα να μη λησμονούμε, ότι πρωτίστως προστατεύεται το δικαίωμα στην ελευθερία έκφρασης, πριν ο Νόμος να τιμωρήσει κάποιον για όσα λέει ή γράφει.

Η πρόοδος της τεχνολογίας, ιδίως μετά την εμφάνιση του διαδικτύου, έχει αλλάξει άρδην τα δεδομένα. Η έκφραση απόψεων και η διάδοση των πληροφοριών δεν περιορίζονται πλέον σε ένα εφήμερο κομμάτι χαρτί. Αποτυπώνονται στο διαδίκτυο και προορίζονται να μείνουν εκεί για πάντα. Το διαδίκτυο δεν ξεχνά. Επιπλέον, από τη στιγμή που κάτι αποτυπωθεί στο διαδίκτυο, μπορεί οποιοσδήποτε τρίτος να το διαδώσει περαιτέρω, ακόμα και για τελείως διαφορετικούς σκοπούς (Βλαχόπουλος,2018).

Ειδικά στην περίπτωση που η ελευθερία έκφρασης αφορά δημόσια πρόσωπα και σε ό,τι έχει να κάνει με τα προσωπικά τους δεδομένα, παίζει σημαντικό ρόλο η ιδιότητα αυτή. Εισέρχεται με αυξημένο βάρος στη διαδικασία της στάθμισης έναντι της προστασίας των προσωπικών δεδομένων (Βλαχόπουλος,2018).

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»*. Η παράγραφος αυτή κατοχυρώνει το σπουδαιότατο ατομικό δικαίωμα της ελευθερίας τα πνευματικής κινήσεως. Είναι η θετική ελευθερία του καθενός να μπορεί να εκδηλώνει τις σκέψεις του να μπορεί να εκφράζεται ελεύθερα(ή και να έχει τη δυνατότητα αν το θέλει να μην εκφράζεται), με τις διάφορες μορφές υπό τις οποίες η έκφραση αυτή μπορεί να εξωτερικευθεί σήμερα. Για το δικαίωμα αυτό χρησιμοποιούνται επίσης οι όροι ελευθερία γνώμης, ελευθερία λόγου, ελευθερία εκφράσεως λόγου, ελευθερία διάδοσης ιδεών. Ο λόγος εκφράζεται προφορικά, ή γραπτά με κάποιο έγγραφο ή με μέσα που καλύπτονται από τη γενικότερη έννοια του Τύπου (Παραράς, 2001)

Η ελευθερία έκφρασης συνιστά ένα από τα ουσιαστικά θεμέλια μιας δημοκρατικής κοινωνίας και μια από τις βασικές προϋποθέσεις για την πρόοδο της και για την αυτοπραγμάτωση κάθε ατόμου. Οι διατάξεις του άρθρου 10 της ΕΣΔΑ είναι εφαρμοστέα όχι μόνο σε πληροφορίες ή ιδέες, οι οποίες εκφράζουν επιδοκιμασία ή θεωρούνται μη προσβλητικές ή αδιάφορες , αλλά επίσης και σε εκείνες που προσβάλλουν σκανδαλίζουν ή ενοχλούν. Αυτό επιβάλλει ο πλουραλισμός, η ανοχή και η ευρύνοια, χωρίς τις οποίες δεν υφίσταται δημοκρατική κοινωνία(Δαγτόγλου,2005). Μπορεί βέβαια να υπόκειται σε εξαιρέσεις η ελευθερία της έκφρασης, όμως αυτό πρέπει να ερμηνεύεται στενά και η ανάγκη αυτών των περιορισμών να είναι πλήρως και πειστικά αιτιολογημένη (ΠολΠρΑθ 3667/2020)

Επίσης, το Άρθρο 19 της Οικουμενικής Διακήρυξης του 1948 για τα Ανθρώπινα Δικαιώματα δηλώνει: Ο καθένας έχει το δικαίωμα της ελευθερίας της γνώμης και έκφρασης. Αυτό το δικαίωμα περιλαμβάνει την ελευθερία να έχει απόψεις χωρίς παρεμβολές και να αναζητά, να λαμβάνει και να μεταδίδει πληροφορίες και ιδέες μέσω οποιουδήποτε μέσου ενημέρωσης και ανεξαρτήτως συνόρων. Ακολούθως, αυτό το δικαίωμα κατοχυρώθηκε από δεσμευτική νομική συνθήκη στο Άρθρο 19 του Διεθνούς Συμφώνου για τα Ατομικά και Πολιτικά Δικαιώματα. Αυτό απηχεί τη διατύπωση της Οικουμενικής Διακήρυξης Ανθρώπινων Δικαιωμάτων, αλλά προσθέτει μερικούς σαφείς λόγους, για τους οποίους το δικαίωμα αυτό μπορεί να περιορίζεται. Για τους

Ευρωπαίους, παρόλ' αυτά, η δεσμευτική προστασία του δικαιώματος της ελευθερίας έκφρασης ήρθε πολύ νωρίτερα. Η Σύμβαση για την Προστασία των Δικαιωμάτων του Ανθρώπου και Θεμελιωδών Ελευθεριών (γνωστή ως Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου ή ΕΣΔΑ) υιοθετήθηκε το 1950 και τέθηκε σε εφαρμογή το 1953. Η ΕΣΔΑ αναπτύχθηκε υπό την αιγίδα του Ευρωπαϊκού Συμβουλίου. Όλα τα αναγνωρισμένα κράτη στην Ευρωπαϊκή Ζώνη είναι μέρη της Σύμβασης σήμερα, πλην τριών: η Πόλη του Βατικανού, η Λευκορωσία και το Καζακστάν. Το Άρθρο 10 της ΕΣΔΑ προστατεύει την ελευθερία της έκφρασης με τους παρακάτω όρους: Ο καθένας έχει το δικαίωμα της ελευθερίας της έκφρασης. Αυτό το δικαίωμα πρέπει να περιλαμβάνει την ελευθερία να έχει απόψεις και να λαμβάνει και να μεταδίδει πληροφορίες και ιδέες χωρίς παρεμβολές από τη δημόσια αρχή και ανεξαρτήτως συνόρων. Το άρθρο δε θα αποτρέπει τα Κράτη από το να απαιτούν την αδειοδότηση των ραδιοτηλεοπτικών εκπομπών, τηλεοπτικών ή κινηματογραφικών επιχειρήσεων. Όσο για το Άρθρο 19 του Διεθνούς Συμφώνου για τα Αστικά και Πολιτικά Δικαιώματα (ΔΣΑΠΔ), το Άρθρο 10 περιγράφει επίσης μια σειρά από λόγους, για τους οποίους μπορεί να περιορίζεται το δικαίωμα της ελευθερίας της έκφρασης.

Είναι βέβαια κοινώς παραδεκτό ότι η χρήση του δικαιώματος της ελευθερίας της έκφρασης δεν είναι απεριόριστη, αλλά κατά τη διάσημη ρήση «τελεί υπό τη γενική επιφύλαξη του νόμου τηρώντας τους νόμους του Κράτους».

Επομένως, η ελευθερία της έκφρασης κάποιου δεν πρέπει να φτάσει ποτέ στο σημείο να προσβάλει την ελευθερία την τιμή και την υπόληψη κάποιου αλλού προσώπου. Πυξίδα είναι πάντα η αρχή της αναλογικότητας (αρθ.25 παρ.1 Συντάγματος). Ποτέ δε θα πρέπει να θίξει τον σκληρό πυρήνα της τιμής του ατόμου.

4.2 «Τιμωρητικές» διατάξεις για το cyberbullying

Το 2015, μετά τη θλιβερή υπόθεση Γιακουμάκη, υπήρξε η αλλαγή στο άρθρο το οποίο αφορούσε την προστασία της σωματικής και ψυχικής ακεραιότητας, η οποία μέχρι τότε αφορούσε μόνο ανηλίκους. Με το άρθρο 8 του Ν.4322/2015 αντικαταστάθηκε το άρθρο 312ΠΚ που τιμωρεί την πρόσκληση σωματικής κάκωσης ή άλλης βλάβης της σωματικής ή ψυχικής υγείας τρίτου, με συνεχή σκληρή συμπεριφορά. Με τη διάταξη αυτή τιμωρείται η λεκτική και σωματική βία που χαρακτηρίζεται και ως τραμπουκισμός (bullying) ή εκφοβισμός και το οποίο είναι φαινόμενο που δυστυχώς έχει πάρει σημαντικές διαστάσεις στη σύγχρονη εποχή καθώς με τη ραγδαία ανάπτυξη της τεχνολογίας και την εμφάνιση των υπηρεσιών

κοινωνικής δικτύωσης γίνεται δυνατή η ανώνυμη χρήση του διαδικτύου και των υπηρεσιών αυτών για τη στοχοποίηση ευάλωτων προσώπων (cyberbullying) (Ιγγλεζάκης,2018)

Με την τροποποίηση όμως του Ποινικού Κώδικα το 2019, η διάταξη αυτή καταργήθηκε. Επομένως, για να αντιμετωπιστεί το φαινόμενο του cyberbullying θα πρέπει να στραφούμε στις κλασικές διατάξεις νόμων που αφορούν την προσωπικότητα, την τιμή και την υπόληψη του ατόμου και καθώς και για την προστασία της σωματικής του ακεραιότητας και της γενετήσιας αξιοπρέπειας του.

4.3 Τα υβριστικά μηνύματα υπό το φως των ποινικών διατάξεων των άρθρων 361 επ

Αξίζει πρωτίστως να σημειωθεί ότι η συγγραφή της παρούσας διπλωματικής γίνεται κατά την περίοδο που ο νέος Ποινικός Κώδικας δεν έχει τεθεί σε ισχύ, καθώς θα αρχίσει να εφαρμόζεται από την 01/05/2024, σε κάποιες περιπτώσεις από την 01/07/2024. Επομένως, θα πρέπει να ερευνηθούν και οι διατάξεις που ίσχυαν μέχρι τώρα, αλλά και εκείνες που θα τεθούν λίαν συντόμως σε εφαρμογή.

Σύμφωνα με το άρθρο 361 παρ.1 του Ποινικού Κώδικα ν.4619/2019, *«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»*.

α. Αντικειμενική υπόσταση

Από το γράμμα του νόμου προκύπτει πως η αντικειμενική υπόστασή του είναι «Όποιος, εκτός από τις περιπτώσεις της δυσφήμησης, προσβάλλει την τιμή άλλου με λόγο ή με έργο ή με οποιονδήποτε άλλο τρόπο» και για στοιχειοθέτηση της χρειάζεται :

α) Προσβολή της τιμής: Πρέπει να διατυπωθούν από το δράστη γραπτά ή προφορικά, για κάποιον άλλο, λέξεις ή φράσεις που κατά την κοινή αντίληψη περιέχουν αμφισβήτηση της ηθικής και κοινωνικής αξίας του προσώπου του παθόντος,

είτε περιφρόνηση γι' αυτόν από το δράστη. Η τιμή λαμβάνεται υπό ευρεία έννοια και σημαίνει αξίωση το άτομο να μη τυγχάνει από κάποιον άλλο αρνητικής αξιολόγησης ή μεταχείρισης τέτοιας που να δηλώνει, έλλειψη εκτίμησης του δράστη προς τον παθόντα σχετικά με τη συνολική του αξία, ηθική και κοινωνική. Η «ποικιλία» των εκφράσεων για προσβολή της τιμής, εκτιμάται κατά την κοινή αντίληψη και πρέπει να λαμβάνονται υπόψη και οι περιστάσεις γενικά, δηλ. η ηλικία, ο βαθμός μόρφωσης και η κοινωνική θέση δράστη και θιγόμενου (Μαργαρίτης, 2020) β) Εξωτερίκευση της πρόθεσης αυτής, γραπτά ή προφορικά με λέξεις ή φράσεις ή όποιον άλλο τρόπο. Η εξύβριση με λόγια σημαίνει γραπτή ή προφορική εκφορά κατά του προσώπου φράσεων ή λέξεων προσβλητικών της τιμής και της υπόληψης. Τελείται με θετική πράξη και μόνο σε εξαιρετικές περιπτώσεις αρκεί και παράλειψη, εφόσον συντρέχουν οι προϋποθέσεις του 15 ΠΚ. Δεν έχει καμία σημασία, αν αυτά που εξωτερικεύθηκαν είναι ή όχι αληθινά, όπως απαιτείται στα 362 και 363 ΠΚ. Επίσης, για να υπάρξει εξύβριση, ο δράστης πρέπει να ισχυρίζεται γεγονός μειωτικό της τιμής, μόνο ενώπιον του ίδιου του θύματος, αλλιώς δεν έχουμε εξύβριση, αλλά δυσφήμιση (Καστανίδου, 1999). Πρέπει να υπάρχει μια περιφρόνηση εκ μέρους του δράστη, ο οποίος γνωρίζει ότι με μία τέτοια ενέργεια προσβάλλει την τιμή του άλλου. γ) Η προσβολή πρέπει να αφορά ζώντα φυσικά πρόσωπα (η μνήμη νεκρών προστατεύεται από το 365 ΠΚ), ασχέτως με την κατάσταση ή την ηλικία τους π.χ ανήλικα άτομα ή άτομα σε ψυχική νόσο. Αποτελεί υπαλλακτικώς μεικτό έγκλημα και η με περισσότερους τρόπους εκδήλωση της συνιστά ένα έγκλημα (Ζήσης, 2022).

Η εξύβριση όταν γίνεται δημόσια ή μέσω διαδικτύου, σύμφωνα με το εδαφ. β της παραγράφου 1, το οποίο προστίθεται ως επιβαρυντική περίσταση, τιμωρείται αυστηρότερα με φυλάκιση έως ένα έτος ή χρηματική ποινή λόγω επίτασης της προσβολής του προστατευόμενου αγαθού. Η ρύθμιση ακολουθεί την προϊσχύσασα νομοθεσία, αλλά η χρηματική ποινή δεν μπορεί να σωρευτεί στην ποινή φυλάκισης. (Ζήσης, 2022).

β. Υποκειμενική υπόσταση

Αναφορικά με την πλήρωση της υποκειμενικής υπόστασης του εγκλήματος της απαιτείται δόλος (καθώς πρόκειται για πλημμέλημα και πρέπει υποκειμενικά να καλύπτεται από το δόλο του δράστη, σύμφωνα με το 26 ΠΚ), αρκεί και ενδεχόμενος, που σημαίνει πρόθεση να προσβάλλει την τιμή και την υπόληψη του παθόντος με το χρησιμοποιηθέν μέσο. Χρειάζεται λοιπόν γνώση ότι η αξιόποινη συμπεριφορά είναι βέβαιο ή ενδεχόμενο να βλάψει αντικειμενικά την τιμή και την υπόληψη του θύματος

μειώνοντας την κοινωνική του παράσταση και τη θέληση μείωσης της τιμής. Αν ο δράστης αγνοεί ότι με κάποια φράση μειώνει την τιμή του προσώπου που αγνοεί τη σημασία της φράσης αυτής, υπάρχει πλάνη ως προς τα στοιχεία της αντικειμενικής υπόστασης της εξύβρισης, η οποία ως πραγματική, αποκλείει τον καταλογισμό της πράξης σε ενοχή του δράστη. Αν πάλι ο δράστης αγνοεί κάποια από τις προϋποθέσεις των 366,367 ΠΚ, η πλάνη του είναι νομική και αίρει τον καταλογισμό μόνο όταν είναι συγγνωστή (Φράγκος, 2020).

γ. Λόγοι άρσης του αδίκου/Ποινική δίωξη/Παραγραφή

Σύμφωνα με το 367 παρ.1 ΠΚ *(το 367 ΠΚ, αναμένεται να καταργηθεί στις 01/05/2024)*, ο άδικος χαρακτήρας της εξύβρισης αίρεται, όταν οι μειωτικές της τιμής εκφράσεις αποτελούν: α) δυσμενείς κρίσεις για επιστημονικές, καλλιτεχνικές ή επαγγελματικές εργασίες, β) δυσμενείς εκφράσεις που περιέχονται σε δημόσιο έγγραφο, γ) εκδηλώσεις που γίνονται για την εκτέλεση νόμιμων καθηκόντων και δ) σε ανάλογες περιπτώσεις. Η απαρίθμηση αυτή είναι ενδεικτική, καθώς ο νομοθέτης θέλησε να αναγάγει σε λόγους άρσης του αδίκου γενικά τις περιπτώσεις όπου η προσβολή της τιμής οφείλεται στην εκπλήρωση καθήκοντος, την ενάσκηση δικαιώματος ή σε άλλο αιτιολογημένο ενδιαφέρον.

Επίσης, μπορεί να υπάρξει λόγος άρσης του αδίκου, λόγω δικαιολογημένης αγανάκτησης, εξαιτίας προηγούμενης πράξης που ο παθών τέλεσε εναντίον του ή ενώπιόν του. Σε αυτή την περίπτωση βέβαια η προηγούμενη πράξη θα πρέπει να είναι ιδιαίτερα σκληρή, όχι απλώς σκληρή, ώστε να δικαιολογεί το «ξέσπασμα» μέσω εξύβρισης.

Τέλος, δεν αίρεται ο άδικος χαρακτήρας της πράξης της εξύβρισης ή της δυσφήμησης, όταν παραβιάζεται το καθήκον αληθείας του Τύπου. Συγκεκριμένα, από το πλέγμα των διατάξεων συνάγεται ότι από τον ενυπάρχοντα στη δημοσιογραφική δραστηριότητα αυξημένο κίνδυνο προσβολής της προσωπικότητας λόγω της δημοσιότητας που αποτελεί το πεδίο δράσης του τύπου, απορρέουν οι λεγόμενες συναλλακτικές υποχρεώσεις του τύπου μεταξύ των οποίων η υποχρέωση σεβασμού της προσωπικότητας και το καθήκον αλήθειας, που επιβάλλει να προηγηθεί ο έλεγχος της αλήθειας των πληροφοριών και των ειδήσεων, ώστε το περιεχόμενο να συμπίπτει με την πραγματικότητα. Οφείλει, συνεπώς, ο δημοσιογράφος να εξακριβώνει, πριν από τη δημοσίευση, την αλήθεια των δυσφημιστικών γεγονότων, χωρίς να μπορεί να θεωρηθεί, σε αντίθετη περίπτωση, ότι η παράδοση σε δημόσια ανυποληψία του δυσφημούμενου προσώπου τελεί σε αναλογία με την κοινωνική αποστολή του Τύπου.

Για την άσκηση της ποινικής δίωξης του εγκλήματος της εξύβρισης απαιτείται έγκληση, σύμφωνα με το 368 παρ.1 ΠΚ (καθώς δε θεωρείται σημαντικό έγκλημα ώστε να κινηθεί ο μηχανισμός ποινικής καταστολής, αν δεν το επιθυμεί ο ίδιος ο θιγόμενος και επιπλέον θεωρείται ότι με την κίνηση της ποινικής δίωξης μπορεί το θύμα να έχει εντονότερη προσβολή της τιμής του, λόγω της διάδοσης του γεγονότος της εξύβρισης). Το 368 ΠΚ, δε θα έχει κάποια μεταβολή με τον καινούριο Ποινικό Κώδικα, με τη διαφορά ότι δε θα αναφέρεται και στην απλή δυσφήμιση δεδομένου ότι αυτή θα καταργηθεί.

Κατά συνέπεια, από το συνδυασμό των διατάξεων 368 παρ.1 ΠΚ και 117 παρ 1 ΠΚ, γίνεται αντιληπτό, ότι αν δεν υποβάλλει το θύμα έγκληση για εξύβριση μέσα σε τρεις μήνες, θα υπάρχει παραγραφή (Μαργαρίτης, 2020).

δ. Η περίπτωση της τέλεσης των 361επ ΠΚ μέσω διαδικτύου

Στην περίπτωση της τέλεσης μέσω διαδικτύου, θα μπορούμε να μιλάμε για ένα μη γνήσιο ηλεκτρονικό έγκλημα, αφού θα υπάρχει η παραδοσιακή μορφή των εγκλημάτων «φυσικού χώρου» εξύβρισης/ δυσφήμησης μέσω δικτύων ηλεκτρονικής επικοινωνίας και συστημάτων πληροφοριών. Η τέλεση του αδικήματος αυτού μπορεί να γίνει με πολλούς τρόπους, όπως πχ. Αποστολή υβριστικών e-mail, μηνυμάτων στο messenger , αλλά ακόμα και προφορικά με φωνητική κλήση/ φωνητικά μηνύματα σε εφαρμογές όπως το Viber και το Whatsapp, το Telegram. Χαρακτηριστικό του θα είναι η ευκολία -χωρίς την φυσική μετακίνηση του δράστη- ο οποίος ενεργεί από το γραφείο ή το σπίτι του, πατώντας μόνο ορισμένα πλήκτρα του υπολογιστή του και χωρίς καν να έχει τη φυσική παρουσία του θύματος μπροστά του. Επίσης, χαρακτηριστική θα είναι η ταχύτητα -διαπράττεται σε χρόνο δευτερολέπτων και πολλές φορές δεν το αντιλαμβάνεται ούτε το ίδιο το θύμα, η ανωνυμία, καθώς η διάπραξη κυβερνοεγκλημάτων εκμεταλλεύεται την σχετική ανωνυμία, που προσφέρουν ορισμένες τεχνολογικές υποδομές του διαδικτύου, αλλά και η δυσκολία εύρεσης αποδεικτικών στοιχείων, καθώς στη περίπτωση της εξύβρισης, είναι δύσκολο να ασχοληθεί η Δίωξη Ηλεκτρονικού Εγκλήματος με τα ψηφιακά ίχνη του δράστη για αδίκημα που δεν είναι τόσο σοβαρό συγκριτικά με περιπτώσεις παιδικής πορνογραφίας και άλλων σοβαρών αδικημάτων.

Κατά τα λοιπά και στην περίπτωση του εγκλήματος μέσω διαδικτύου, εφαρμόζονται τα παραπάνω για την ποινική δίωξη και την παραγραφή.

Σε ό,τι αφορά την επικείμενη αλλαγή του Ποινικού Κώδικα με τον ν.5090/2024: Το 362 ΠΚ για την απλή δυσφήμιση αναμένεται να καταργηθεί. Για το

361 ΠΚ, η διάταξη θα ισχύει ως εξής: «*Όποιος, εκτός από τις περιπτώσεις της συκοφαντικής δυσφήμησης (άρθρο 363) προσβάλλει την τιμή άλλου με λόγο ή με έργο ή με οποιονδήποτε άλλον τρόπο, έχοντας τέτοιον σκοπό, τιμωρείται με φυλάκιση έως έξι (6) μήνες ή χρηματική ποινή. Αν τελεί την ανωτέρω πράξη δημόσια με οποιονδήποτε τρόπο ή μέσω διαδικτύου, επιβάλλεται φυλάκιση έως ένα (1) έτος ή χρηματική ποινή και αν η προσβολή ανάγεται σε σχέσεις του ιδιωτικού ή του οικογενειακού βίου, επιβάλλεται φυλάκιση έως δύο (2) έτη ή χρηματική ποινή*». Η προσθήκη αυτή που αφορά τον οικογενειακό ή τον ιδιωτικό βίο, έχει προφανώς σκοπό να προστατεύσει το αγαθό της τιμής του οικογενειακού και του ιδιωτικού βίου σε μεγαλύτερο βαθμό. Ενδεχομένως όμως να υπάρξουν προβλήματα στην κρίση για το τι ακριβώς αποτελεί ιδιωτικό βίο. Το 363 ΠΚ αναμένεται να ισχύει ως εξής: «*Όποιος με οποιονδήποτε τρόπο ενώπιον τρίτου ισχυρίζεται ή διαδίδει για κάποιον άλλον εν γνώσει του ψευδές γεγονός που μπορεί να βλάψει την τιμή ή την υπόληψη του άλλου τιμωρείται με φυλάκιση τουλάχιστον τριών (3) μηνών και χρηματική ποινή και αν τελεί την πράξη δημόσια με οποιονδήποτε τρόπο ή μέσω του διαδικτύου, με φυλάκιση τουλάχιστον έξι (6) μηνών και χρηματική ποινή. Στην έννοια του τρίτου δεν περιλαμβάνονται δημόσιοι λειτουργοί ή υπάλληλοι που λαμβάνουν γνώση των ισχυρισμών για τα δυαδικά μέρη, κατά την ενάσκηση καθήκοντος στο πλαίσιο πολιτικής, ποινικής ή διοικητικής δίκης*». Για πρώτη φορά δηλαδή, θα διευκρινίζεται στο ίδιο το άρθρο το ποιος θεωρείται τρίτος. Αναμένεται να καταργηθεί και το 367 ΠΚ, οπότε δε θα υπάρχουν λόγοι άρσης του αδίκου.

ε. Τόπος τέλεσης του εγκλήματος

Το διαδικτυακό έγκλημα χαρακτηρίζεται στην πλειοψηφία των περιπτώσεών του, από την ύπαρξη φυσικής απόστασης, μεταξύ του δράστη και του αποτελέσματος της πράξης του. Δεν μπορούμε να μιλήσουμε αορίστως περί τόπου τέλεσης του διαδικτυακού εγκλήματος, καθώς θα πρέπει να εξειδικεύσουμε την ad hoc αξιόποινη πράξη και στη συνέχεια να την εντάξουμε στις κατηγορίες εγκλημάτων. Άλλος ενδεχομένως ο τόπος τέλεσης ενός διαδικτυακού εγκλήματος αποτελέσματος και άλλος ενός εγκλήματος αφηρημένης διακινδύνευσης. Πχ ο Χ στέλνει στον Ψ ηλεκτρονική επιστολή με εξυβριστικό περιεχόμενο. Εδώ στο βαθμό που οι πράξεις συνιστούν έγκλημα, υπάρχει ο τόπος που βρίσκεται ο Α και ο τόπος όπου βρίσκεται ο Β, όπου και εξωτερικεύεται η συμπεριφορά.

Τι ίσχυε πριν το 2019: Σύμφωνα με την παρ.3 του άρθρου 5 ΠΚ, που προστέθηκε με το άρθρο 2 του Ν.4267/14, «Όταν η πράξη τελείται μέσω διαδικτύου ή άλλου μέσου επικοινωνίας, τόπος τέλεσης θεωρείται και η ελληνική επικράτεια, εφόσον στο έδαφός της παρέχεται πρόσβαση στα συγκεκριμένα μέσα, ανεξάρτητα από τον τόπο εγκατάστασής τους». Η αφορμή της θέσπισης της εν λόγω διάταξης ήταν η εναρμόνιση της ελληνικής νομοθεσίας με την Οδηγία 2011/93/ΕΕ προκειμένου να αντιμετωπισθούν λυσιτελώς τα αδικήματα πορνογραφίας ανηλίκων και άλλα συναφή (άγρα ανηλίκων με σκοπό την ασέλγεια κλπ).

Ο Έλληνας νομοθέτης με μια επίδειξη παγκόσμιας πρωτοτυπίας, αποφάσισε να καταστήσει για όλα τα εγκλήματα που τελούνται μέσω διαδικτύου τόπο τέλεσης την ημεδαπή, απλώς και μόνο επειδή παρέχεται πρόσβαση στα συγκεκριμένα μέσα, δημιουργείται δηλαδή με τον τρόπο αυτό μια νέα έννοια «ψηφιακής εδαφικότητας», που δεν αντιστοιχεί όμως με την αρχή εδαφικότητας των παρ. 1 και 2 του ιδίου άρθρου. Δηλαδή, αρκεί το απλό γεγονός ότι από την Ελλάδα υπάρχει πρόσβαση πχ σε λογαριασμό κοινωνικής δικτύωσης. Αυτή η λογική δημιουργεί βέβαια προβλήματα σύγκρουσης δικαιοδοσιών, αφού αν επρόκειτο να υιοθετηθεί και από άλλους εθνικούς νομοθέτες, όλες οι εθνικές νομοθεσίες θα είχαν εφαρμογή σε όλα τα διαδικτυακά εγκλήματα, ενώ οι αστυνομικές αρχές θα έπρεπε να επιφορτιστούν με τον εντοπισμό όλων των διαδικτυακών δραστών σε όλον τον πλανήτη (Δαλακούρας, 2018).

Με την τροποποίηση του Ποινικού Κώδικα το 2019, η Τρίτη παράγραφος καταργήθηκε.

Δεν αναμένεται επίσης με τον ν.5090/2024 κάποια αλλαγή στο 5 ΠΚ, η οποία να αφορά το διαδικτυακό έγκλημα.

Από τον συνδυασμό των άρθρων 5 παρ.1 Π.Κ με τίτλο «Εγκλήματα που τελέστηκαν στην ημεδαπή» και 16 Π.Κ, κατ΄εφαρμογή των αρχών της εδαφικότητας και της ενότητας, προκύπτει ότι ως ψηφιακή εδαφικότητα ενός διαδικτυακού εγκλήματος που επιφέρει ορισμένο αποτέλεσμα ορίζεται και ο τόπος όπου επήλθε το αξιόποινο αποτέλεσμα πέρα από τον τόπο της ψηφιακής δράσης του υπαιτίου (με το αποτέλεσμα να περιλαμβάνει τόσο την έννοια της βλάβης όσο και της διακινδύνευσης, την έννοια του τελικού αλλά και του ενδιάμεσου αποτελέσματος). Έτσι λοιπόν, εάν ο δράστης ενός διαδικτυακού εγκλήματος είχε πρόσβαση σε τραπεζικά στοιχεία, σε προσωπική σελίδα μέσων κοινωνικής δικτύωσης (Facebook, Instagram κλπ) ή σε ιστοσελίδες της Ελλάδας, πέρα από τον φυσικό χώρο όπου βρίσκεται ο υπολογιστής

του, του τόπου όπου ενδεχομένως αποθήκευσε τα κλαπέντα στοιχεία ή δεδομένα, εφόσον η βλάβη προκαλείται σε κάτοικο Ελλάδος, τότε τόπος τέλεσης της ψηφιακής εγκληματικής πράξης είναι και η Ελλάδα.

4.4 Η προσβολή της τιμής υπό το πρίσμα της προστασίας δεδομένων προσωπικού χαρακτήρα

Η προσβολή της τιμής, έχει κριθεί νομολογιακά ότι μπορεί να είναι αντικείμενο προστασίας και με τον Ν.2472/1997, πολλώ δε μάλλον από την εφαρμογή του ΓΚΠΔ της Ευρωπαϊκής Ένωσης. Σύμφωνα με την ΑΠ 509/2014 *«για να γεννηθεί αξίωση προστασίας από προσβολή της προσωπικότητας, κατά τις διατάξεις των άρθρων 57, 59, 914, 932 του ΑΚ, θα πρέπει η προσβολή να είναι παράνομη, να αντίκειται δηλαδή σε διάταξη που απαγόρευε συγκεκριμένη πράξη, με την οποία προσβάλλεται έκφανση αυτής, είναι δε αδιάφορο σε ποιο τμήμα δικαίου βρίσκεται η διάταξη που απαγορεύει την προσβολή. Έτσι, η προσβολή μπορεί να προέλθει και από ποινικά κολάσιμη πράξη, όπως εξύβριση, απλή δυσφήμηση ή συκοφαντική δυσφήμηση, που προβλέπονται και τιμωρούνται από τις διατάξεις των άρθρων 361, 362 και 363 του Π.Κ. Αντικείμενο προσβολής είναι η τιμή και η υπόληψη του φυσικού προσώπου. Ο νόμος θεωρεί ως προστατευόμενο αγαθό την τιμή ή την υπόληψη του προσώπου, το οποίο είναι μέλος μιας οργανωμένης κοινωνίας και κινείται στα πλαίσια της συναλλακτικής ευθύτητας. Η τιμή του προσώπου θεμελιώνεται επί της ηθικής αξίας, η οποία πηγή έχει την ατομικότητα και εκδηλώνεται με πράξεις ή παραλείψεις. Το άδικο των προβλεπομένων στα άρθρα 361 επ. Π.Κ. πράξεων αίρεται σύμφωνα με το άρθρο 367 παρ.1 περ.α'-δ' Π.Κ., μεταξύ των άλλων περιπτώσεων που προβλέπονται στο άρθρο αυτό, και όταν πρόκειται για εκδηλώσεις που γίνονται για την εκτέλεση νόμιμων καθηκόντων ,την άσκηση νόμιμης εξουσίας ή για τη διαφύλαξη (προστασία) δικαιώματος ή από άλλο δικαιολογημένο ενδιαφέρον ή σε ανάλογες περιπτώσεις (περ. γ' και δ'). Η τελευταία αυτή διάταξη (ΠΚ 367) για την ενότητα της έννομης τάξης εφαρμόζεται αναλογικά και στο χώρο το ιδιωτικού δικαίου, όπως αυτός οριοθετείται από τις προαναφερόμενες διατάξεις των άρθρων 57-59 και 914 επ. ΑΚ. Επομένως, αιρομένου του άδικου χαρακτήρα των προαναφερθεισών αξιόποινων πράξεων (με την επιφύλαξη της ΠΚ 367 § 2) αποκλείεται και το στοιχείο του παρανόμου της επιζήμιας συμπεριφοράς, ως όρος της αντίστοιχης αδικοπραξίας του αστικού δικαίου. Έτσι, η προβολή περίπτωσης του άρθρου 367 § 1 του ΠΚ, αποτελεί αυτοτελή ισχυρισμό καταλυτικό της αγωγής του προσβληθέντος λόγω άρσης του παρανόμου της προσβολής.*

Όμως, ο άδικος χαρακτήρας της προσβολής, ως προς τις εξυβριστικές ή δυσφημιστικές εκφράσεις που περιέχει, δεν αίρεται λόγω δικαιολογημένου ενδιαφέροντος κλπ. και συνεπώς παραμένει η ποινική ευθύνη των κατά το νόμο υπευθύνων, άρα και η υποχρέωση τους προς αποζημίωση κατά το αστικό δίκαιο, όταν συντρέχει μία από τις περιπτώσεις της ΠΚ 367 § 2, δηλαδή, όταν οι επίμαχες κρίσεις περιέχουν τα συστατικά στοιχεία του αδικήματος της συκοφαντικής δυσφήμισης των άρθρων 363-362 ΠΚ, ή όταν από τον τρόπο εκδηλώσεως, ή από τις περιστάσεις υπό τις οποίες τελέσθηκε η πράξη, προκύπτει σκοπός εξυβρίσεως, δηλαδή πρόθεση που κατευθύνεται ειδικά στην προσβολή της τιμής του άλλου». Επίσης συνεχίζει η ίδια απόφαση *«από τον συνδυασμό των διατάξεων των άρθρων 2 περ.α' και β', 4, 5 παρ.παρ.1, 2 περ.β' και 7 Ν.2472/1997 (Προστασία του ατόμου από την επεξεργασία προσωπικών δεδομένων) συνάγεται, ότι α) η επεξεργασία δεδομένων προσωπικού χαρακτήρος επιτρέπεται μόνον όταν το υποκείμενο των δεδομένων έχει δώσει την συγκατάθεσή του, κατ' εξαίρεση δε και χωρίς την συγκατάθεσή του, μεταξύ των άλλων περιπτώσεων και όταν η επεξεργασία είναι αναγκαία για την εκπλήρωση υποχρεώσεως του υπεύθυνου επεξεργασίας, η οποία επιβάλλεται από τον νόμο, β) ότι η συλλογή και επεξεργασία ευαίσθητων δεδομένων, στα οποία περιλαμβάνονται και τα δεδομένα τα οποία αφορούν ποινικές διώξεις ή καταδίκες, απαγορεύεται κατά κανόνα και κατ'εξαίρεση επιτρέπεται στις αναφερόμενες από τον νόμο περιπτώσεις, εφόσον προηγηθεί πάντοτε άδεια της Αρχής. Από την διάταξη δε του άρθρου 23 παρ.1 Ν.2472/1997 η οποία ορίζει: "Φυσικό πρόσωπο ή νομικό πρόσωπο ιδιωτικού δικαίου, που κατά παράβαση του παρόντος νόμου προκαλεί περιουσιακή βλάβη, υποχρεούται σε πλήρη αποζημίωση. Αν προκάλεσε ηθική βλάβη, υποχρεούται σε χρηματική ικανοποίηση. Η ευθύνη υπάρχει και όταν ο υπόχρεος όφειλε να γνωρίζει την πιθανότητα να επέλθει βλάβη σε άλλον", σε συνδυασμό με τις διατάξεις των άρθρων 57, 59, 299 και 932 Α.Κ. συνάγεται, ότι σε περίπτωση κατά την οποία ο υπεύθυνος επεξεργασίας προκαλεί ηθική βλάβη στο υποκείμενο των προσωπικών δεδομένων, η ευθύνη του πρώτου για χρηματική ικανοποίηση του τελευταίου είναι νόθος αντικειμενική και προϋποθέτει α) συμπεριφορά (πράξη ή παράλειψη) που παραβιάζει τις διατάξεις του ν.2472/1977 ή (και) των κατ'εξουσιοδότηση αυτού εκδοθεισών κανονιστικών πράξεων της Αρχής, β) ηθική βλάβη, γ) αιτιώδη σύνδεσμο μεταξύ της συμπεριφοράς και της ηθικής βλάβης και δ) υπαιτιότητα, ήτοι γνώση ή υπαίτια άγνοια αφενός των περιστατικών που συνιστούν την παράβαση και αφετέρου της πιθανότητας να επέλθει ηθική βλάβη. Η ύπαρξη υπαιτιότητας τεκμαίρεται, και ως εκ τούτου ο υπεύθυνος επεξεργασίας,*

προκειμένου να απαλλαγεί από την ευθύνη του, έχει το βάρος να αποδείξει ότι ανυπαιτίως αγνοούσε τα θεμελιωτικά του πταίσματος του πραγματικά γεγονότα».

4.5 Χρήση αναρτήσεων από κλειστή ομάδα ως αποδεικτικό μέσο ενώπιον δικαστηρίου, προσβολή ιδιωτικότητας και προσωπικών δεδομένων

Μία ενδιαφέρουσα απόφαση αναφορικά με την ευθύνη διαχειριστών κλειστής ομάδας στο Facebook για ψευδή και προσβλητικά σχόλια και αναρτήσεις, καθώς και το επιτρεπτό χρήσης των αναρτήσεων ως αποδεικτικών μέσων, εξέδωσε το Τριμελές Εφετείο Θεσσαλονίκης (Τριμ.Εφ.Θεσ. 2116/2020).

Η υπόθεση αφορά σε αγωγή ιατρού κατά των διαχειριστών μίας κλειστής ομάδας στο Facebook και ενός ακόμα ατόμου, το οποίο ισχυρίστηκε στην υποενότητα "forum" της εν λόγω ομάδας, μία σειρά από αναληθή και συκοφαντικά γεγονότα και υβριστικά σχόλια για το πρόσωπό του, με σκοπό να βλάψει την τιμή και τη υπόληψή του ως ιατρού και ως ανθρώπου.

Όπως ισχυρίστηκε ο ενάγων, τα σχόλια αυτά παρέμειναν αναρτημένα από υπαιτιότητα και υστεροβουλία των δύο πρώτων εναγομένων, οι οποίοι τα περιέλαβαν και επέτρεψαν την ανάρτηση και διατήρηση αυτών εν γνώσει τους για το προσβλητικό, για την προσωπικότητά του, περιεχόμενο, αν και είχαν τη δυνατότητα να μη τα δημοσιοποιήσουν, αλλά και να τα καθαιρέσουν άμεσα.

Το πρωτόδικο δικαστήριο απέρριψε ως αόριστη την αγωγή στο μέρος αφορούσε τους δύο πρώτους εναγόμενους, και την έκανε εν μέρει δεκτή στο μέρος που αφορούσε τον τρίτο εναγόμενο, τον οποίο υποχρέωσε να καταβάλει στον ενάγοντα το ποσό των πέντε χιλιάδων ευρώ, καθώς και να δημοσιεύσει, με δικά του έξοδα, το διατακτικό της απόφασης εντός της ομάδας αυτής.

Στην απόφαση του Εφετείου περιλαμβάνονται, μεταξύ άλλων, οι εξής ενδιαφέρουσες σκέψεις:

1. Ως προς την ευθύνη των διαχειριστών ως ενδιαμέσων:

«Ακόμη η ως άνω αγωγή ήταν επαρκώς ορισμένη και ως προς τους δύο πρώτους εναγόμενους, που φέρονται, κατά τα ιστορούμενα πραγματικά περιστατικά, ως κάτοχοι - ιδιοκτήτες του αναρτημένου στην πλατφόρμα του Facebook ιστολογίου και περιέλαβαν, εν γνώσει του δυσφημιστικού τους χαρακτήρα, τις ειδικότερα αναφερόμενες αναρτήσεις, δεν ήταν αναγκαίο δε στην αγωγή να γίνεται μνεία των όρων ευθύνης του άρθρου 13 του πδ 131/2003, που εφαρμόζεται στην προκείμενη περίπτωση, αφού κατά τις προηγούμενες νομικές παραδοχές της εν λόγω απόφασης, οι διαχειριστές ιστολογίων είναι και αυτοί ενδιάμεσοι φιλοξενίας (μεσάζοντες), με την stricto sensu έννοια της Οδηγίας 2000/31/ΕΚ για το Ηλεκτρονικό Εμπόριο και υπάγονται στη διάταξη του άρθρου 13 πδ 131/2003 για τη φιλοξενία, όπως ορθά δέχθηκε η προσβαλλόμενη απόφαση και επομένως θεμελιώνουν, με βάση την ως άνω διάταξη, νόμιμο λόγο απαλλαγής από την ευθύνη ενδιάμεσου φιλοξενίας (μεσάζοντος) και όχι νόμιμο λόγο ευθύνης [...]

[...] όσον αφορά τους δύο πρώτους εναγόμενους, μετά την εξαφάνιση της προσβαλλόμενης απόφασης για τους εναγόμενους αυτούς, η ένδικη αγωγή πρέπει απορριφθεί ως ουσία αβάσιμη. Και τούτο διότι αποδείχθηκε βάσιμος ο εκ του άρθρου 13 του πδ 131/2003 ισχυρισμός τους, που προέβαλαν παραδεκτά στο πρωτοβάθμιο Δικαστήριο και επαναφέρουν νομότυπα με τις προτάσεις τους και στο Δικαστήριο αυτό και δη, αποδείχθηκε ότι οι εναγόμενοι αυτοί, έχοντας χαλαρή εποπτεία στο ως άνω ιστολόγιο, δεν γνώριζαν τα γεγονότα και τις περιστάσεις από τα οποία προέκυπτε ότι οι ένδικες αναρτήσεις αφορούσαν ψευδή γεγονότα και είχαν δυσφημιστικό περιεχόμενο».

2. Ως προς την προσβολή ιδιωτικότητας ή απορρήτου, εξαιτίας της προσκόμισης και αξιοποίησης των αναρτήσεων:

«το ιστολόγιο αυτό μπορεί να ήταν κλειστό πλην όμως ήταν παντελώς ελεύθερο ως προς την εισαγωγή νέων μελών, ο αριθμός των οποίων δεν μπορούσε εκ των προτέρων να προσδιοριστεί (απροσδιόριστος) και πάντως δεν ήταν πεπερασμένος και επομένως ουδόλως μπορούσε να χαρακτηριστεί ως στενός. Σε συνδυασμό δε με το γεγονός ότι ο περιορισμός των προσώπων που είχαν πρόσβαση στην προσωπική ιστοσελίδα ήταν έννοια σχετική, λαμβανομένου υπόψη ότι κάθε καταχωρημένος «φίλος» τού χρήστη μπορούσε να αντιγράψει στον υπολογιστή του, να αναδημοσιεύσει στη δική του ιστοσελίδα ή να διαβιβάσει σε άλλες ιστοσελίδες κάθε πληροφορία που συνέλεγε, ή εγγεγραμμένος χρήστης με νόμιμη πρόσβαση μπορούσε να διαδώσει περαιτέρω τις

σχετικές πληροφορίες, ουδόλως μπορούσε να δημιουργηθεί στον οποιοδήποτε, ούτε και στον εναγόμενο αυτό, για το εν λόγω μέσο επικοινωνίας, δικαιολογημένη προσδοκία επικοινωνίας σε καθεστώς οικειότητας και ιδιωτικότητας.

Μη συντρεχόντων επομένως των όρων ύπαρξης επικοινωνίας μεταξύ πεπερασμένου και περιορισμένου (στενού) κύκλου προσώπων (ήδη επρόκειτο για ομάδα 337 ατόμων με δυνατότητα αυτή να αυξηθεί σε απροσδιόριστο εκ των προτέρων αριθμό προσώπων) και άρα επικοινωνίας σε καθεστώς οικειότητας και εμπιστευτικότητας, δεν τίθεται, με τη χρήση και αξιοποίηση των εν λόγω αναρτήσεων, θέμα προσβολής της ιδιωτικής ζωής και του δικαιώματος απορρήτου του τρίτου εναγομένου. Διότι, αφ' ής στιγμής ο τελευταίος καθιστούσε πτυχές της ιδιωτικής του ζωής δημοσίως γνωστές, τόσο σε ένα ευρύτατο αριθμό «φίλων» όσο και σε έναν απροσδιόριστο αλλά και μη πεπερασμένο αριθμό δυνάμενων να επισκεφθούν, τη σελίδα, επισκεπτών, τότε ο ίδιος ο χρήστης αποδέχθηκε και την ένταξη στοιχείων της ιδιωτικής του ζωής στο δημόσιο βίο και στη δημόσια επικοινωνία.

Ακόμη πρέπει να σημειωθεί ότι δεν τίθεται θέμα προσβολής του απορρήτου και για τον πρόσθετο λόγο, πως αποδείχθηκε ότι οι ως άνω αναρτήσεις αποκτήθηκαν από τον ενάγοντα εκ του ιστότοπου, όχι όταν αυτές βρίσκονταν στη διαδικασία μετάδοσης, αλλά αργότερα από τους φίλους και γνωστούς του, όταν δηλαδή αυτές βρίσκονταν σε ηλεκτρονική αποθήκευση και σύμφωνα με τις παραδοχές της μείζονας σκέψης δεν υφίσταται προσβολή του δικαιώματος απορρήτου και της ιδιωτικότητας». Επομένως, γίνεται αντιληπτό από τα παραπάνω, ότι η παράνομη επεξεργασία προσωπικών δεδομένων, μπορεί να στοιχειοθετήσει και το αδίκημα της προσβολής της τιμής.

4.6 Ιδιαίτερες περιπτώσεις cyberbullying

4.6.1Το cyberstalking ως μορφή cyberbullying

Θεωρείται ως μια προέκταση του κυβερνοεκφοβισμού. Ως cyberstalking περιγράφεται η εγκληματική συμπεριφορά όπου ο επιτιθέμενος με τη χρήση ηλεκτρονικών μέσων επικοινωνίας όπως το Διαδίκτυο και τα κινητά τηλέφωνα, εκβιάζει, απειλεί, εκφοβίζει και γενικά παρενοχλεί το θύμα του για διάφορους λόγους, όπως επίλυση προσωπικών διαφορών και εκδίκηση. Μπορεί να είναι είτε άμεση ,όταν τα μηνύματα στέλνονται απευθείας στο θύμα, είτε έμμεση, όταν στέλνεται σε τυχαία πρόσωπα, περιλαμβάνοντας όμως απειλητικό περιεχόμενο προς το θύμα

(Βλαχόπουλος,2007). Γενικά η παρενοχλητική παρακολούθηση (“stalking”), ποινικοποιήθηκε στο πλαίσιο του Ποινικού Κώδικα.

Συγκεκριμένα, με τον ν. 4531/2018, στο άρθρο 333 του Ποινικού Κώδικα, που αναφέρεται στο ποινικό αδίκημα της απειλής, προστέθηκε δεύτερο εδάφιο σύμφωνα με το οποίο *«Με την ποινή του προηγούμενου εδαφίου (φυλάκιση μέχρι ενός έτους ή με χρηματική ποινή) τιμωρείται και όποιος, χωρίς απειλή βίας ή άλλης παράνομης πράξης ή παράλειψης, προκαλεί σε άλλον τρόμο ή ανησυχία, με την επίμονη καταδίωξη ή παρακολούθησή του, όπως ιδίως με την επιδίωξη διαρκούς επαφής μέσω τηλεπικοινωνιακού ή ηλεκτρονικού μέσου ή με επανειλημμένες επισκέψεις στο οικογενειακό, κοινωνικό ή εργασιακό περιβάλλον αυτού, παρά την εκπεφρασμένη αντίθετη βούλησή του».*

Η ανωτέρω νομοθετική πρωτοβουλία ήρθε σε συνέχεια του άρθρου 34 (Παρενοχλητική Παρακολούθηση) της Σύμβασης του Συμβουλίου της Ευρώπης για την πρόληψη και την καταπολέμηση της βίας κατά των γυναικών και της ενδοοικογενειακής βίας (Σειρά Συνθηκών Συμβουλίου της Ευρώπης, CETS Αριθ.210, Κωνσταντινούπολη, 11.5.2011) την οποία έχει υπογράψει η χώρα μας, το οποίο ορίζει ότι «Τα Μέρη θα λάβουν τα απαραίτητα νομοθετικά ή άλλα μέτρα για να διασφαλίσουν ότι η σκόπιμη επαναλαμβανόμενη ενασχόληση με απειλητική ενέργεια που απευθύνεται προς κάποιο άλλο άτομο, προκαλώντας του φόβο για την ασφάλειά του, ποινικοποιείται».

Πρόκειται για μία αναγκαία νομοθετική πρόβλεψη, ιδίως με δεδομένη την ευρύτατη χρήση του διαδικτύου και των μέσων κοινωνικής δικτύωσης στις μέρες μας, μέσα από τα οποία μπορεί να λαμβάνουν χώρα, συχνά και κατά τρόπο επαναλαμβανόμενο, ανεπιθύμητες επικοινωνίες για τον δέκτη, ακόμα και από άγνωστα πρόσωπα.

Το έννομο αγαθό που προστατεύεται με τη διάταξη του 333 ΠΚ, είναι εκείνο της προσωπικής ελευθερίας του ατόμου. Η αξιόποινη συμπεριφορά συνίσταται στην με βία ή άλλη παράνομη πράξη ή παράλειψη απειλή άλλου ένεκα της οποίας αυτός περιέρχεται σε τρόμο ή ανησυχία. Ως απειλή νοείται η προαναγγελία ενός κακού που πρόκειται να επέλθει στον παθόντα. Αυτή μπορεί να γίνει κατά οποιονδήποτε τρόπο, γραπτώς ή προφορικώς, ρητώς ή σιωπηρώς. Το περιεχόμενο της απειλής πρέπει να

αφορά βία ή άλλη παράνομη πράξη ή παράλειψη. Η βία μπορεί να είναι είτε σωματική είτε ψυχολογική. Η απειλή άλλης παράνομης πράξεως ή παραλείψεως περιλαμβάνει κάθε συμπεριφορά αντίθετη σε οποιοδήποτε κανόνα δικαίου, γραπτό ή εθιμικό. Το έγκλημα είναι τετελεσμένο, όταν ο απειληθείς περιέλθει διά της απειλής σε τρόμο και ανησυχία. Ανησυχία είναι το συναίσθημα κλονισμού της πεποιθήσεως των πολιτών για την συνέχιση της ειρηνικής ζωής σε συγκεκριμένο κοινωνικό χώρο και χρόνο. Εξάλλου, τρόμος είναι εντονότερη συναισθηματική κατάσταση σε σχέση με την ανησυχία, που οδηγεί σε ανέλεγκτες (ενστικτώδεις) κινήσεις (υπερβολικός ή αιφνίδιος φόβος). Από άποψη υποκειμενικής υποστάσεως απαιτείται δόλος, ο οποίος προϋποθέτει γνώση του υπαιτίου ότι η απειλούμενη ενέργειά του συνιστά βία ή άλλη παράνομη πράξη και την θέλησή του να προκαλέσει στον άλλο τρόμο ή ανησυχία.

Η διάταξη του 333 παρ.1 ΠΚ που αφορά το stalking, δεν αναμένεται να έχει κάποια μεταβολή με τον νέο Ποινικό Κώδικα.

4.6.2 Μπορεί το Revenge Porn να θεωρηθεί Cyberbullying?

. «Άρθρο 346 Προσβολές της γενετήσιας ζωής

1. Όποιος χωρίς δικαίωμα κοινολογεί σε τρίτο πρόσωπο ή αναρτά σε κοινή θέα, πραγματική, αλλοιωμένη ή σχεδιασμένη εικόνα ή κάθε είδους οπτικό ή οπτικοακουστικό υλικό, στο οποίο αποτυπώνεται μη δημόσια πράξη άλλου που αφορά στη γενετήσια ζωή του, τιμωρείται με φυλάκιση τουλάχιστον τριών (3) ετών και χρηματική ποινή.

2. Όποιος απειλεί άλλον ότι θα τελέσει τις πράξεις της παρ. 1 τιμωρείται με ποινή φυλάκισης τουλάχιστον ενός (1) έτους. Αν ο υπαίτιος της πράξης του προηγούμενου εδαφίου εξαναγκάζει άλλον σε πράξη ή παράλειψη ή ανοχή για την οποία αυτός δεν έχει υποχρέωση, τιμωρείται με ποινή φυλάκισης τουλάχιστον δύο (2) ετών.

3. Με κάθειρξη έως οκτώ (8) έτη και χρηματική ποινή τιμωρείται η πράξη της παρ. 1 αν τελείται: α) με ανάρτηση στο διαδίκτυο ή σε μέσο κοινωνικής δικτύωσης με αόριστο αριθμό αποδεκτών, β) από ενήλικο και αφορά σε ανήλικο, γ) σε βάρος νυν ή πρώην συζύγου ή συντρόφου του υπαιτίου ή σε βάρος προσώπου που συνοικεί με αυτόν ή έχει μαζί του σχέση εργασίας ή υπηρεσίας ή βρίσκεται υπό την επιμέλεια ή την προστασία του ή δεν μπορεί να υπερασπίσει τον εαυτό του, δ) με σκοπό να προσπορίσει ο υπαίτιος στον εαυτό του ή σε άλλον περιουσιακό όφελος.

4. Αν κάποια από τις πράξεις των προηγούμενων παραγράφων οδήγησε το θύμα σε απόπειρα αυτοκτονίας επιβάλλεται κάθειρξη και χρηματική ποινή. Αν η πράξη του προηγούμενου εδαφίου οδήγησε στο θάνατο επιβάλλεται κάθειρξη τουλάχιστον δέκα (10) ετών και χρηματική ποινή.»

Σύμφωνα με την αιτιολογική έκθεση, με την προτεινόμενη ρύθμιση τυποποιείται ως αξιόποινη πράξη που προσβάλλει τα έννομα αγαθά της γενετήσιας ζωής και ελευθερίας και υπό προϋποθέσεις και της ανηλικότητας, η μη συναινετική κοινολόγηση ή η ανάρτηση στο διαδίκτυο ή σε μέσα κοινωνικής δικτύωσης, προσωπικών εικόνων ή οπτικοακουστικού υλικού που ανάγονται στη γενετήσια ζωή του παθόντος, ακόμα και αν αυτές δημιουργήθηκαν με τη συναίνεσή του.

Η εν λόγω συμπεριφορά συνιστά μορφή σύγχρονης κυβερνοβίας (σύμφωνα με τον ορισμό του Συμβουλίου της Ευρώπης, διαθέσιμος σε: https://www.coe.int/en/web/cyberviolence), η οποία αποσκοπεί στο να εκθέσει, στιγματίσει και προσβάλλει τους αποδέκτες της.

Η θέσπιση της εν λόγω διάταξης αποσκοπεί, σε εναρμόνιση με ευρωπαϊκές πρακτικές που αντιμετωπίζουν ως έγκλημα τέτοιες συμπεριφορές, στην αντιμετώπιση των φαινομένων αυτής της σύγχρονης μορφής βίας, η οποία:

α) έχει συχνότατα ως μέσο τέλεσης την ψηφιακή τεχνολογία και τα μέσα κοινωνικής δικτύωσης (internet, smartphone, computer, social networks),

β) δίνει τη δυνατότητα στους δράστες, για τη μη συναινετική , πραγματική, προσομοιωμένη ή και εικονική προβολή κάθε υλικού που αποτυπώνει εκδηλώσεις της γενετήσιας δραστηριότητας των παθόντων,

γ) έχει ως συχνότερους αποδέκτες, ευάλωτες κοινωνικά ομάδες, όπως ενδεικτικά είναι οι ανήλικοι ή κάθε άλλο πρόσωπο που αδυνατεί να υπερασπιστεί τον εαυτό του και

δ) λόγω της βαρύτητας και της κοινωνικής έκτασης της προσβολής, προκαλεί ως επίπτωση στα θύματά της σοβαρές βλάβες της ψυχικής ή σωματικής υγείας, συχνά ανεπανόρθωτες, που τα έχουν οδηγήσει, ακόμα και σε απόπειρα ή τελεσμένη αυτοχειρία.

Το εν λόγω έγκλημα διαμορφώνεται ως ουσιαστικό (αποτελέσματος) καθώς η ίδια η κοινολόγηση συνίσταται στη βλάβη της γενετήσιας ζωής του θύματος.

Για να επέλθει η βλάβη αυτή πρέπει ωστόσο, η πράξη του δράστη να παραπέμπει σε ταυτοποιήσιμο πρόσωπο, δηλαδή να διακρίνεται είτε το πρόσωπο είτε τα ιδιαίτερα χαρακτηριστικά του θύματος που το καθιστούν αναγνωρίσιμο.

Επιπρόσθετα, στην παρ. 2 κρίθηκε σκόπιμο και δικαιοπολιτικά αναγκαίο, να τυποποιηθεί ως αξιόποινη και η απειλή τέλεσης των ανωτέρω πράξεων, καθώς έχει αποδειχθεί ότι προκαλεί στον απειλούμενο αφόρητη ψυχολογική πίεση που δύναται να οδηγήσει, όπως ακριβώς και η τέλεσή τους, σε πράξη, παράλειψη ή ανοχή για την οποία αυτό δεν έχει υποχρέωση.

Στην παρ. 3 προβλέπονται διακεκριμένες κακουργηματικές μορφές του εγκλήματος που επισύρουν ποινή κάθειρξης μέχρι οκτώ (8) ετών και χρηματική ποινή, όταν αυτό τελείται

α) με ανάρτηση στο διαδίκτυο ή σε μέσο κοινωνικής δικτύωσης με αόριστο αριθμό αποδεκτών,

β) από ενήλικο που αφορά ανήλικο λόγω της ιδιαίτερης απαξίας της εν λόγω συμπεριφοράς που επιπλέον προσβάλλει και την ανηλικότητα,

γ) σε βάρος νυν ή πρώην συζύγου ή συντρόφου του υπαιτίου ή σε βάρος προσώπου που συνοικεί με αυτόν ή έχει μαζί του σχέση εργασίας ή υπηρεσίας ή βρίσκεται υπό την επιμέλεια ή την προστασία του ή δεν μπορεί να υπερασπίσει τον εαυτό του, δηλαδή σε βάρος προσώπων στα οποία η εγγύτητα και η ιδιαίτερη σχέση εμπιστοσύνης ή εξάρτησης που έχει δημιουργηθεί με τον δράστη, τους καθιστά αδύναμους να αντιδράσουν ή να υπερασπιστούν τον εαυτό τους,

δ) με σκοπό να προσπορίσει ο υπαίτιος στον εαυτό του ή σε άλλον περιουσιακό όφελος, δηλαδή από πρόσωπο που προσδοκά τον προσπορισμό περιουσιακού οφέλους από την εγκληματική πράξη.

Τέλος, στην παρ. 4 καθιερώνονται οι εκ του αποτελέσματος ιδιαίτερα διακεκριμένες μορφές του εν λόγω αδικήματος, όταν οι πράξεις των προηγούμενων παραγράφων είχαν ως αποτέλεσμα να οδηγήσουν το θύμα σε αυτοκτονία ή σε απόπειρά της.

Ευνόητο είναι ότι η ως άνω διάταξη δεν αποκλείει την ποινική τιμωρία του δράστη και για άλλες αξιόποινες πράξεις, εφόσον αυτές διαπράττονται από τον τελευταίο. Δε θα υπάρξει αλλαγή στο άρθρο αυτό με τον νέο Ποινικό Κώδικα.

Επομένως δεδομένου ότι πρόκειται για έγκλημα που θίγει περισσότερο τη γενετήσια αξιοπρέπεια του θύματος, εκφεύγει της κλασικής μορφής του cyberbullying, μπορεί όμως να θεωρηθεί μια εκτεταμένη μορφή αυτού.

4.6.3 Τα emoticons ως τρόπος προσβολής της τιμής

Τα emojis (το e σημαίνει εικόνα και το moji χαρακτήρας), μπορεί να πρωτογεννήθηκαν το 1982 από έναν ερευνητή και να άρχισαν να χρησιμοποιούνται ευρέως το 1999 όταν ιαπωνική εταιρεία τηλεπικοινωνιών τα εισήγαγε ως τρόπο επικοινωνίας, αποτελούν όμως μια νέα γλώσσα της εποχής μας, όπως σημειώνουν οι ειδικοί, με ορισμένους πανεπιστημιακούς να διαφωνούν αν πρέπει να αναγνωριστεί ως μια νέα παγκόσμια γλώσσα, καθώς χρησιμοποιείται ως δεύτερος ηλεκτρονικός τρόπος επικοινωνίας από τους αποκαλούμενους ως Millennials και τη Gen Z. Το ότι είναι ευρέως αποδεκτά αποδεικνύεται και από το γεγονός ότι σύμφωνα με μελέτη του αμερικανικού Πανεπιστημίου Σάντα Κλάρα (η οποία καθόλου τυχαία δημοσιεύθηκε στη Νομική Επιθεώρηση Washington Law Review) κάθε χρόνο αποστέλλονται τουλάχιστον 2,3 τρισεκατομμύρια μηνύματα με emojis μέσω κινητών παγκοσμίως. (https://www.protothema.gr/world/article/1453523/i-lista-me-ti-simasia-ton-emojis-poia-boroun-na-se-steiloun-akoma-kai-fulaki/)

Η ΜΠλημΒολ 1456/2018, ήταν η πρώτη απόφαση η οποία αναφέρθηκε σε emoji ως τρόπο έκφρασης και έγινε αφορμή το emoticon για καταδικαστική απόφαση. Βάσει αυτής κηρύσσεται ένοχος ο κατηγορούμενος για την πράξη της παραβίασης δικαστικής απόφασης κατ' εξακολούθηση. Εν προκειμένω, στο μμέτρο που στόχος του ευρύτατου διατακτικού της σχετικής απόφασης ήταν η διασφάλιση της παράλειψης ενασχόλησης του κατηγορουμένου με την πολιτικώς ενάγουσα υπό όλες τις ιδιότητές της με κάθε μέσο και τρόπο, η εκμετάλλευση των δυνατοτήτων της τεχνολογίας να εκφράζεται - σχολιάζει κάποιος χλευαστικά - υποτιμητικά εμπίπτει οπωσδήποτε στο ανωτέρω διατακτικό, όπου ασφαλώς δεν μμπορούσαν να προβλεφθούν όλοι οι τρόποι προσβολής της προσωπικότητας της υπερ' ης η απόφαση και για τον λόγο αυτό απαγορεύθηκε η προσβολή της προσωπικότητάς της γενικά προς πληρέστερη δικαστική της προστασία με πρόβλεψη απαγόρευσης τέτοιας προσβολής και στην ιστοσελίδα κοινωνικής δικτύωσης Facebook. Άλλωστε, εδώ η κατηγορία δεν αφορά το ποινικό αδίκημα της συκοφαντικής δυσφήμισης, οπότε και μόνο θα μμπορούσε να ανακύψει ο προβληματισμός ότι δεν υπήρξε ισχυρισμός ενώπιον τρίτων διά της χρήσης του επίμαχου ιδεογράμματος (emoticon). Επομένως, ο σχολιασμός της πολιτικώς ενάγουσας διά της χρήσης ιδεογράμματος πρέπει να θεωρηθεί ως παράβαση του διατακτικού της παραπάνω απόφασης, ώστε να μην τεθεί εκποδών το περιεχόμενό της

εκ πλαγίου, ήτοι διά της χρήσης ενός τρόπου σχολιασμού που προέκυψε από την πρόοδο της τεχνολογίας και ήταν αδύνατον να εξειδικευθεί με μία δικαστική απόφαση τόσο αναλυτικά, όπως αδύνατο είναι ενδεχομένως να προβλεφθούν και άπαντες οι δυνατοί τρόποι προσβολής της προσωπικότητας κάποιου, αρκούσας έτσι της γενικής απαγόρευσης στο κείμενο της δικαστικής απόφασης τέτοιας προσβολής και με οποιονδήποτε τρόπο, η οποία καταλαμβάνει όλες τις μεθόδους προσβολής, γνωστούς και μη, όπως και την προαναφερόμενη, ενόψει μάλιστα και της απαγόρευσης σχολιασμού του προσώπου της πολιτικώς ενάγουσας μέσω της ιστοσελίδας Facebook. Είναι δε αβάσιμος ο ισχυρισμός του κατηγορουμένου ότι έκανε ασυναίσθητα κλικ στο προμνημονευόμενο ιδεόγραμμα, διότι θα μπορούσε ανά πάσα στιγμή να ακυρώσει το σχόλιό του, μόλις αντιλήφθηκε την ενέργειά του, ώστε να μην εμφανίζεται το τελευταίο στην ιστοσελίδα της Κ.Γ., πράγμα που ουδέποτε έπραξε, γεγονός που καταδεικνύει τη δόλια δράση του. Εξάλλου, το συγκεκριμένο ιδεόγραμμα, που αποτελεί στη γλώσσα της ιστοσελίδας κοινωνικής δικτύωσης «Facebook» σχόλιο και μάλιστα εκδήλωση χλεύης, είναι πρόδηλο ότι στην περίπτωση του κατηγορουμένου αποτελούσε προσβλητικό σχόλιο/ανάρτηση, εφόσον για να του προσδοθεί η ορθή διάσταση πρέπει να αξιολογηθεί όχι μεμονωμένα αλλά υπό το πρίσμα της μέχρι τότε συμπεριφοράς του απέναντι στην πολιτικώς ενάγουσα, με το πρόσωπο της οποίας είχε αποκτήσει εμμονή και τη σχολίαζε παντοιοτρόπως αρνητικά σε έντυπες και ηλεκτρονικές εφημερίδες και μέσω της ιστοσελίδας κοινωνικής δικτύωσης «Facebook» επωνύμως, αναρτώντας μάλιστα και φωτογραφίες της

Στη Μεγάλη Βρετανία ένας 10χρονος έχει προσφύγει στη Δικαιοσύνη και έχει ξεκινήσει καμπάνια για να αντικαταστήσει η Apple το emoji του «σπασίκλα», μια και το συγκεκριμένο εικονίδιο εμφανίζει ένα πρόσωπο με γυαλιά και δύο μεγάλα μπροστινά δόντια, ο 10χρονος είδε μια ομοιότητα με το πρόσωπό του, γεγονός που τον προσβάλει. Και αυτές δεν είναι οι μόνες υποθέσεις. Στη Μασαχουσέτη, το 2014, οι ένορκοι του Ανωτάτου Δικαστηρίου των ΗΠΑ καταδίκασαν τον Φράνκλιν Καστάνο για τη δολοφονία της φίλης του Σολάνλι Παουλίνο με κύριο στοιχείο ένα εικονίδιο. Το Ανώτατο Δικαστήριο επικύρωσε την καταδίκη ως υπόθεση ανθρωποκτονίας εκ προμελέτης, εν μέρει, επειδή ένας φίλος του καταδικασθέντος κατέθεσε ότι ο Καστάνο του έστειλε ένα emoji με το ανθρωπάκι με Χ στα μάτια τη νύχτα που πέθανε η Παουλίνο. Το εικονίδιο αυτό μεταφράζεται ως «νεκρός-ή». Σε άλλη υπόθεση, στην Καλιφόρνια, ένας άνδρας καταδικάστηκε σε υπόθεση πορνείας αφού έστειλε σε

συνομιλία emojis με στέμμα, ψηλά τακούνια και emoji με μια τσάντα με χρήματα (https://www.protothema.gr/world/article/1453523/i-lista-me-ti-simasia-ton-emojis-poia-boroun-na-se-steiloun-akoma-kai-fulaki/)

4.7 Απαγόρευση ρατσιστικών σχολίων

Ανάμεσα σε όλες τις απαγορεύσεις προσβολής της τιμής, ιδιαίτερη σημασία έχει και η απαγόρευση εκφοράς ρατσιστικού λόγου

Σύμφωνα με την ΑΠ 858/2020, υπάρχει ο ποινικός κολασμός του ρατσιστικού εκκλησιαστικού λόγου ως απτή προστασία της σεξουαλικής διαφορετικότητας. Η πρώτη μεγάλη συνεισφορά της σχολιαζόμενης απόφασης είναι οι σκέψεις σύμφωνα με τις οποίες η κρίσιμη (ως άνω) διάταξη του Ν.4285/2014 επιβάλλει ποινική καταδίκη για ένα κείμενο (γραπτό ή ηλεκτρονικό), εκλαμβανόμενο σαν «ενιαίο νοηματικό σύνολο», όταν συντρέχουν, ιδίως, οι ακόλουθες προϋποθέσεις:

α. «Εχει προφανή σκοπό να θυματοποιήσει (στοχοποιήσει) την ομάδα προσώπων που προσδιορίζονται από τον σεξουαλικό προσανατολισμό τους και δη τους ομοφυλόφιλους με τη διέγερση εχθρικών συναισθημάτων σε βάρος τους» ενώ «περιέχει και προτροπές και ενέχει απειλές εναντίον της παραπάνω ομάδας προσώπων… πρόσφορες να προκαλέσουν τρόμο και ανησυχία σ'αυτούς…»

β. «Συνεπεία αυτών των προτροπών κινδυνεύει η ομαλή συμβίωση αυτών και ακόμη υφίσταται κίνδυνος προσβολής των ατομικών δικαιωμάτων των μελών της ομάδας αυτής αφού η συγκεκριμένη συμπεριφορά μπορεί να υποκινήσει μίσος κατά των ομοφυλοφίλων και είναι πρόσφορη λόγω της έντασης των λόγων της, των χαρακτηρισμών που χρησιμοποιεί και των προτροπών του, που φθάνουν μέχρι πλήρους κοινωνικού αποκλεισμού τους, σε συνδυασμό με το κύρος της ως άνω ιδιότητάς του αναιρεσείοντος, να προκαλέσει στον μέσο άνθρωπο έντονα συναισθήματα απέχθειας, αποστροφής και ιδιαίτερης εχθρότητας κατά των μελών της ομάδας αυτής. Αυτά τα συναισθήματα, είναι αντικειμενικά δυνατόν να οδηγήσουν σε τέλεση πράξεων βίας κατά των συγκεκριμένων προσώπων, διασαλεύοντας την κοινωνική συμβίωση αυτών»

γ. «Οι πράξεις και οι ενέργειες στις οποίες προτρέπει το υποκείμενο του εγκλήματος, πρέπει να είναι ικανές και πρόσφορες να προκαλέσουν "διακρίσεις, μίσος

ή βία" χωρίς και να απαιτείται να προκληθούν βιαιοπραγίες. Η παραδοχή για δυνατότητα πρόκλησης μίσους κατά των ως άνω προσώπων, δημιουργεί την προσφορότητα που απαιτείται κατά την κρίσιμη διάταξη, να προκληθούν και βίαιες πράξεις εναντίον τους, δεδομένου ότι το μίσος αντικειμενικά αποτελεί το υπόβαθρο και την ιδιαίτερη εκείνη ψυχολογική κατάσταση για να εκτραπεί ο άνθρωπος σε βιαιότητες ή σε ενέργειες που απειλούν ή προσβάλλουν την ζωή, την ελευθερία και την σωματική ακεραιότητα άλλων, εν προκειμένω μέλους ή μελών της εν λόγω ομάδας προσώπων…»

δ. «Η αξιόποινη πράξη του άρθρου 1 παρ. 1 ν. 927/1979 [όπως τροποποιήθηκε από το άρθρο 1 του Ν.4285/2014] απαιτεί κοινό δόλο και η αντικειμενική της υπόσταση πληρούται με τη γνώση και θέληση των στοιχείων της αντικειμενικής υπόστασης αυτού χωρίς να απαιτείται ιδιαίτερη αιτιολογία για τη στοιχειοθέτηση του στοιχείου αυτού…»

Οι ως άνω προϋποθέσεις εντάσσονται χωρίς αποκλίσεις ή εξαιρέσεις στο γενικότερο ερμηνευτικό πλαίσιο που έχει διαμορφώσει η συνταγματική θεωρία, ελληνική και ευρωπαϊκή, ενώ εναρμονίζονται πλήρως και με την σχετική πλούσια νομολογία των ελληνικών δικαστηρίων και του ΕΔΔΑ.

Ωστόσο, εξ ίσου σημαντική είναι και η δεύτερη νομολογιακή συνεισφορά της σχολιαζόμενης απόφασης, η οποία αφορά τα ερμηνευτικά κριτήρια που πρέπει να χρησιμοποιούνται για την στάθμιση μεταξύ αφ'ενός της ελευθερίας της έκφρασης και αφ'ετέρου της απαγόρευσης των διακρίσεων σε βάρος των ομοφυλοφίλων.

Εν προκειμένω, βέβαια, οι σχετικές σκέψεις είναι πιο λιτές. Με δεδομένο ότι είχε ήδη απορρίψει, κατά τα ανωτέρω, τον ισχυρισμό ότι ο τ. μητροπολίτης Καλαβρύτων και Αιγιαλείας στρεφόταν κατά των πολιτικών που θέλουν να υπογράψουν το σύμφωνο συμβίωσης –που αποσκοπούσε προφανώς στο να καλυφθεί ο καταδικασθείς πίσω από το δικαίωμα κριτικής στην εξουσία, ως προνομιακά προστατευμένη έκφανση της ελευθερίας της έκφρασης– προέβη, στη συνέχεια, στις ακόλουθες κρίσεις:

«Ο αναιρεσείων αντιτείνει ότι το επίμαχο κείμενο περιέχει αξιολογικές κρίσεις για τις θέσεις της Εκκλησίας για την ομοφυλοφιλία, μάλιστα αναφέρεται σε "οξεία και καυστική κριτική για μια μεγάλη αμαρτία", επικαλείται ότι ως ιεράρχης έχει καθήκον να νουθετεί το χριστεπώνυμο πλήρωμα και ότι απέβλεπε στη δημόσια αποδοκιμασία ενός ηθικού κακού… Το Δικαστήριο δέχεται με επαρκή αιτιολογία ότι οι προτροπές του αναιρεσείοντα δεν αποτελούσαν έκφραση γνώμης και έτσι δεν πλήττεται το δικαίωμα έκφρασης αυτού, καθώς το κείμενο που δημοσίευσε αυτός ήταν πρόσφορο να προκαλέσει διακρίσεις και μίσος σε βάρος των ομοφυλόφιλων».

Με βάση το ανωτέρω σκεπτικό, η στάθμιση που προκρίνει ο Άρειος Πάγος είναι απλή και εναρμονίζεται πλήρως με την ευρωπαϊκή νομολογιακή αντιμετώπιση του ρατσιστικού λόγου, μέσω του ΕΔΔΑ, ενώ, αντίθετα, διαφοροποιείται σαφώς απέναντι σε αυτήν των ΗΠΑ, όπου –παρά τις όποιες κατά καιρούς διαφοροποιήσεις– η κυρίαρχη τάση είναι η ερμηνευτική μυθοποίηση της «αγοράς των ιδεών», που αντιμετωπίζεται προνομιακά, έναντι άλλων ελευθεριών, με το –μονομερές κατά την άποψή μου– επιχείρημα ότι αυτή αποτελεί το σημαντικότερο θεμέλιο μιας πλουραλιστικής κοινωνίας(https://www.constitutionalism.gr/2021-01-sotirelis-ap858-2020-misallodoxos-logos/).

4.8 Δυσφήμηση δημοσίων προσώπων με βάση υποτιθέμενες δηλώσεις τους (362,363 ΠΚ)

Τα εγκλήματα κατά της τιμής καλούνται σήμερα να φέρουν το κύριο βάρος των προσβολών της προσωπικότητας που συντελούνται κατά κόρον στα μέσα κοινωνικής δικτύωσης, όπου η λεγόμενη «δολοφονία χαρακτήρων» είναι σύνηθες φαινόμενο. Με δεδομένο ότι τα fake news έχουν την ψευδή αναφορά πληροφορία περί γεγονότος στον εννοιολογικό τους πυρήνα, την τιμητική της έχει εδώ η δυσφήμηση, και ιδίως η συκοφαντική, αφού υποστηρίζεται η άποψη ότι η θετική γνώση του ψεύδους συνιστά εννοιολογικό προαπαιτούμενο των fake news (Μοροζίνης, 2018).

Μια ιδιαίτερα επίκαιρη προβληματική στην θεματική των fake news είναι οι περιπτώσεις εκείνες που κάποιος «βάζει στο στόμα» δημοσίων προσώπων, και ιδίως πολιτικών, δηλώσεις, τις οποίες δεν έχουν κάνει. Το ζήτημα που τίθεται εδώ είναι, αν η ψευδής αναφορά περί του γεγονότος ότι έλαβε χώρα η συγκεκριμένη δήλωση από το συγκεκριμένο πρόσωπο θίγει την τιμή αυτού που φέρεται ότι την έκανε, ακόμη και

όταν η δήλωση είναι απλώς μη σύμφωνη με τις γενικότερες πολιτικές, ιδεολογικές ή κοσμοθεωρητικές αντιλήψεις του φερόμενου ως υποκειμένου της εξωτερίκευσης, ή ακόμη και αξιολογικά ουδέτερη. Π.χ. ένα tweet ή ένα post, με το οποίο γνωστοποιείται δήθεν ανάρτηση του γνωστού blogger Μητροπολίτη Αιγιαλείας, η οποία εξαίρει την ιδέα της αποδοχής της ομοφυλοφιλίας από την εκκλησία ή ένα post στο Facebook, με το οποίο ο ηγέτης ακροδεξιού κόμματος φέρεται να τάσσεται υπέρ της χορήγησης ασύλου σε όλους τους παράνομους μετανάστες(Μοροζίνης, 2018).

Μια τέτοια περίπτωση προκάλεσε μεγάλη συζήτηση στη Γερμανία, καθώς το Δεκέμβρη του 2016 εμφανίστηκε μια ανάρτηση στο Facebook, η οποία αναπαρήγαγε μία δήθεν δήλωση της βουλευτού των Οικολόγων Πράσινων και προέδρου της κοινοβουλευτικής επιτροπής δικαιοσύνης της γερμανικής Βουλής Renate Kunast στη Suddeutsche Zeitung με το γνωστό και στη χώρα και δήθεν ανήλικο Αφγανό, ο οποίος αφού τραυμάτισε σοβαρά μια κοπέλα στην Κέρκυρα για να τη ληστέψει, εξέτισε ως (κατά δήλωσή του) ανήλικος (ενώ όπως αποδείχθηκε από την ανθρωπολογική πραγματογνωμοσύνη που διεξήγαγε μετέπειτα η γερμανική δικαιοσύνη δεν είχε την ιδιότητα αυτή ούτε κατά τον χρόνο τέλεσης του αδικήματος του στην Ελλάδα) μια μικρή ποινή, απολύθηκε υφ' όρον και μετέβη ως ασυνόδευτος στη Γερμανία, όπου τέλεσε καθ' ομολογίαν του τα αδικήματα του βιασμού και της ανθρωποκτονίας εις βάρος μιας νεαρής Γερμανίδας εθελόντριας στο Freiburg. Η ψεύτικη δήλωση της Kunast ανέφερε: «Ο νεαρός πρόσφυγας που υποφέρει από ψυχολογικό τραύμα σκότωσε μεν, όμως πρέπει παρ' όλα αυτά να βοηθηθεί».

Υπενθυμίζεται εδώ ότι η περιγραφή της νομοτυπικής μορφής της δυσφήμισης στο άρθρο 362 (τουλάχιστον όπως ίσχυε μέχρι σήμερα, καθώς αναμένεται η κατάργησή του) έχει χαρακτηριστική διατύπωση εγκλήματος επικινδυνότητας ή, κατά την παραδοσιακή ορολογία, αφηρημένης συγκεκριμένης διακινδύνευσης («που μπορεί να βλάψει την τιμή») και έτσι είναι έγκλημα απλής συμπεριφοράς, αφού αν προϋποθέτει επέλευση αποτελέσματος υπό μορφή συγκεκριμένου κινδύνου ή βλάβης για την τιμή. Ερωτάται λοιπόν αν αυτή η προσφορότητα του ισχυρισμού ψεύδους γεγονότος να βλάψει την τιμή ή την υπόληψη, υπάρχει, ακόμη και όταν η συγκεκριμένη εξωτερίκευση, που φέρεται να προέρχεται από το δημόσιο πρόσωπο, ανταποκρίνεται ή πάντως, δεν αντιβαίνει στις θεμελιώδεις αξιολογήσεις τις έννομης τάξης, όπως αυτές αποτυπώνονται στην τάξη αξιών του Συντάγματος. Εν προκειμένω η ψεύτικη δήλωση της Kunast είναι σύμφωνη π.χ. με το τεκμήριο αθωότητας και με την αρχή της αξίας του ανθρώπου, την οποία ο δυτικός νομικός πολιτισμός δεν αρνείται ακόμη και σε

εκείνος που εκμεταλλεύτηκε τις αρχές και τις ευαισθησίες του για να εγκληματήσει ξανά (Μοροζίνης, 2018).

Η γερμανική νομολογία δέχεται παγίως ότι ακόμη και σε περιπτώσεις που η εξωτερίκευση μπορεί να δημιουργήσει αναστάτωση σε ευρύτερες πληθυσμιακές ομάδες εις βάρος του φερόμενου ως υποκειμένου της, δεν μπορεί να γίνει λόγος για προσβολή της τιμής του, εφόσον η εξωτερίκευση είναι σύμφωνη με τις αξιολογήσεις της έννομης τάξης. Έτσι δεν προστατεύεται η δημόσια φήμη ενός πολιτικού, μολονότι η δήλωση που «έβαλαν στο στόμα του» τα troll του διαδικτύου μπορεί να συνεπάγεται σημαντικές ζημιές για την πολιτική σταδιοδρομία του ή το εκλογικό αποτέλεσμα του κόμματος, στο οποίο ανήκει. Αυτή η κανονιστική θεώρηση δεν είναι ορθή λόγω της απολυτότητάς της, καθώς δεν εναρμονίζεται με την σύνδεση του έννομου αγαθού της τιμής με τον πυρήνα της ανθρώπινης προσωπικότητας και επομένως και με τον αυτοπροσδιορισμό της ατομικότητας. Πρέπει δηλαδή να συνεκτιμάται και το ηθικό σκέλος, αλλά και η παράσταση που επιθυμεί ο ίδιος ο φορές της τιμής να έχουν οι άλλοι γι'αυτόν, καθώς και οι πραγματικές συνέπειες της ψεύτικης δήλωσης για την εικόνα που έχουν οι λοιποί κοινωνικοί σχετικά με την εκπλήρωση των ηθικών καθηκόντων και των κοινωνικών ρόλων του. Έτσι η fake δήλωση ενός συντηρητικού πολιτικού, με την οποία εκθειάζονται οι επισκέψεις σε πόρνες, δεν μπορεί να κριθεί ως ποινικά αδιάφορη επειδή η πορνεία είναι νόμιμη (Μοροζίνης, 2018).

4.9 Ποινική ευθύνη των φορέων μέσων κοινωνικής δικτύωσης για fake news που παράγουν και διακινούν οι χρήστες

Η ρύθμιση της ποινικής ευθύνης των ενδιάμεσων παρόχων από το ΠΔ 131/2003

Ποια θα μπορούσε όμως να είναι η ευθύνη του Facebook ή του X/ Twitter για όλα αυτά:

Το διαδίκτυο δεν μπορεί να υπάρξει χωρίς κάποιες επιχειρήσεις, οι οποίες παρέχουν υπηρεσίες απολύτως αναγκαίες για τη λειτουργία του, τους λεγόμενους ενδιάμεσους παρόχους (ή internet – providers). Η ποινική ευθύνη των ενδιαμέσων παρόχων παρουσιάζει μια ιδιομορφία που δεν συναντούμε πουθενά αλλού στην ελληνική έννομη τάξη. Ο αποκλεισμός της ρυθμίζεται στο ΠΔ 131/2003 που ενσωμάτωσε την Οδηγία 2000/31/ΕΚ «για το ηλεκτρονικό εμπόριο», η οποία ακολούθησε το πρότυπο του προϋφιστάμενου γερμανικού Teledienstgestz (TDG).

Έτσι, τα άρθρα 11- 14 του ΠΔ 131/ 2003 περιλαμβάνουν ειδικές διατάξεις που ισχύουν συλλήβδην τόσο για το αστικό και το διοικητικό, όσο και για το ποινικό δίκαιο. Σκοπός του κοινοτικού νομοθέτη του Γερμανού νομοθέτη, τον οποίο ο πρώτος ακολούθησε σχεδόν κατά γράμμα, με αποτέλεσμα η γερμανική ρύθμιση (που είχε θεσπιστεί μετά την πολύκροτη (υπόθεση Somm)να διαχυθεί σε όλες τις ευρωπαϊκές έννομες τάξεις, ήταν να περιστείλει τις κάθε είδους έννομες συνέπειες εις βάρος των φορέων παροχής διαδικτυακών υπηρεσιών και να τις περιορίσει σε έλλογα πλαίσια, χωρίς να ενδιαφέρεται αν κατά τα εθνικά δίκαια οι παραπάνω έννομες συνέπειες έχουν τη μορφή, αστικών, διοικητικών ή και ποινικών κυρώσεων.

Το ΠΔ 131/2003 προβλέπει τριών ειδών ενδιαμέσους παρόχους (υπηρεσιών) με βάση τη διάκριση/ τριχοτόμηση των υπηρεσιών που παρέχονται για τη λειτουργία του διαδικτύου σε α) απλή μετάδοση δεδομένων, β) αποθήκευση σε κρυφή μνήμη και γ) φιλοξενία. Αυτοί αντιδιαστέλλονται προς τον πάροχο του περιεχομένου (content provider), για τον οποίο δεν ισχύει, φυσικά, ειδική ρύθμιση και η ποινική ευθύνη του εξετάζεται κατά τα γενικώς ισχύοντα. Πάροχος περιεχομένου είναι όποιος προσφέρει στο διαδίκτυο πρόσβαση σε δικές του πληροφορίες (ενν. υπό μορφή ψηφιακών δεδομένων) και ιδίως ο δημιουργός των ψηφιακών δεδομένων, που θέτει αυτά σε κυκλοφορία στο διαδίκτυο μέσω της ανάρτησης ιστοσελίδων στον παγκόσμιο ιστό, προσωπικών πληροφοριών σε ιστοτόπους κοινωνικής δικτύωσης, όπως το Facebook και Twitter κλπ., μηνυμάτων ηλεκτρονικού ταχυδρομείου κ.α.

Οι νόμιμες διαδικτυακές πλατφόρμες, ιδίως τα μέσα κοινωνικής δικτύωσης, παρέχουν τη δυνατότητα επικοινωνίας στους χρήστες τους. Όλες οι πληροφορίες που «αναρτούν» υπό μορφή ψηφιακών δεδομένων οι χρήστες αποθηκεύονται στα πληροφοριακά συστήματα, δηλαδή στους διακομιστές (server), του διαχειριστή της πλατφόρμας, προκειμένου να δημοσιοποιούνται σε αυτή. Πρόκειται λοιπόν αναμφισβήτητα για host service– providers, δηλαδή παρόχους υπηρεσιών φιλοξενίας, αφού οι υπηρεσίες «φιλοξενίας» συνίστανται στην αποθήκευση ψηφιακών δεδομένων με πληροφορίες, οι οποίες περιλαμβάνονται σε ιστοσελίδες κλπ. Έτσι ώστε να επιτυγχάνεται η πρόσβαση σε αυτές από τους χρήστες του διαδικτύου (Μοροζίνης, 2018).

4.10 Τι ισχύει σε άλλες χώρες για το cyberbullying

Τα τελευταία χρόνια, ο διαδικτυακός εκφοβισμός έχει γίνει τόσο συχνό φαινόμενο που πολλές χώρες λαμβάνουν μέτρα για την αντιμετώπισή του.

Στις ΗΠΑ ο Πάτρικ Χάλιγκαν απειλούνταν και ελάμβανε χλευαστικά σχόλια για τη σεξουαλικότητα του. Τελικά, ο Χάλιγκαν αυτοκτόνησε. Απαντώντας εν μέρει στην αυτοκτονία, το νομοθετικό σώμα της πολιτείας του Βερμόντ ψήφισε έναν νόμο «κατά του διαδικτυακού εκφοβισμού» το 2004. Πλέον 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

Στη Γερμανία, τα προβλήματα που αναφύονται αναφορικά με τον κυβερνοεκφοβισμό εμπίπτουν στον νόμο για τις τηλεπικοινωνίες και στη νομοθεσία σχετικά με την προστασία των ανηλίκων από αθέμιτο περιεχόμενο των μέσων μαζικής ενημέρωσης. Στην Πορτογαλία η απουσία ειδικού νόμου καλύπτεται από την αναλογική εφαρμογή του Ποινικού Κώδικα, από τη Σύμβαση της Βουδαπέστης για το κυβερνοέγκλημα, η οποία κυρώθηκε το 2009 και από τον νόμο για το κυβερνοέγκλημα, ο οποίος επίσης ψηφίστηκε το 2009. Στην Ιρλανδία και στην Ισπανία παρομοίως εφαρμόζονται οι ποινικοί νόμοι για την αντιμετώπιση παρόμοιων περιστατικών. Στην Ιταλία ισχύουν οι διατάξεις του Ιταλικού ΑΚ για προσβολή προσωπικότητας.

Στο Ηνωμένο Βασίλειο δε διατυπώνεται νομικός ορισμός της διαδικτυακής παρενόχλησης και του διαδικτυακού εκφοβισμού. Ωστόσο, υφίσταται μια νομική εργαλειοθήκη, η οποία μπορεί να αξιοποιηθεί, όπως διευκρινίζεται σε σχετικές κατευθυντήριες Οδηγίες της Εισαγγελικής Υπηρεσίας. Παραδείγματα αποτελούν οι εξής νομοθετικές πράξεις: ‘’Protection from Harassment Act 1997”, “Criminal Justice Act and Public Order Act 1994”, “Malicious Communication Act 1998”, “Communications Act 2003”, “Breach of the Peace (Scotland)” και η “Defamation Act 2013”, η οποία τέθηκε σε ισχύ τον Ιανουάριο του 2014. Παράλληλα, στις πράξεις Education and Inspection Act (2006) εμπεριέχονται κάποιες ρυθμίσεις σχετικά με τον κυβερνοεκφοβισμό και τα περιθώρια επέμβασης του διευθυντή του σχολείου στην συμπεριφορά των μαθητών, όταν είναι εκτός σχολείου, συμπεριλαμβανομένης και της κατάσχεσης του κινητού τηλεφώνου τους ή άλλων παρόμοιων αντικειμένων. Ωστόσο, ούτε στο Ηνωμένο Βασίλειο ο κυβερνοεκφοβισμός αποτελεί αυτοτελές ποινικό αδίκημα, αλλά εφαρμόζονται αναλογικά οι διατάξεις του ποινικού κώδικα που

αναφέρονται στην παρενόχληση και την απειλή. Χωριστό νομοθετικό πλαίσιο για το cybullying, διαθέτει η Μαλαισία.

4.11 Το Ευρωπαϊκό Συμβούλιο για τη ρητορική μίσους

Η ρητορική μίσους, είτε στο διαδίκτυο είτε εκτός σύνδεσης, αποτελεί απειλή για τη δημοκρατία και τα ανθρώπινα δικαιώματα. Η αντιμετώπισή του αποτελεί επείγουσα πρόκληση σε όλα τα κράτη μέλη του Συμβουλίου της Ευρώπης.

Τα πρότυπα και οι πρακτικές του Συμβουλίου της Ευρώπης που σχετίζονται με την αντιμετώπιση της ρητορικής μίσους έχουν καθοδηγήσει το έργο της Επιτροπής Εμπειρογνωμόνων για την Καταπολέμηση της Ρητορικής Μίσους (ADI/MSI-DIS). Κατάρτισε σύσταση για μια συνολική προσέγγιση για την αντιμετώπιση της ρητορικής μίσους στο πλαίσιο των ανθρωπίνων δικαιωμάτων, μεταξύ άλλων στο πλαίσιο ενός διαδικτυακού περιβάλλοντος.

Η τελική Σύσταση εγκρίθηκε από την Επιτροπή Υπουργών τον Μάιο του 2022. Παρέχει μη δεσμευτική καθοδήγηση για τα κράτη μέλη, βασιζόμενη στη σχετική νομολογία του Ευρωπαϊκού Δικαστηρίου Ανθρωπίνων Δικαιωμάτων και δίνοντας ιδιαίτερη προσοχή στο διαδικτυακό περιβάλλον στο οποίο η σημερινή ρητορική μίσους μπορεί να βρεθεί. Τα θεματικά ενημερωτικά δελτία για τη ρητορική μίσους εκδίδονται τακτικά.

Το έγκλημα μίσους καλύπτεται εν μέρει από το πρόσθετο πρωτόκολλο της Σύμβασης της Βουδαπέστης για την ξενοφοβία και τον ρατσισμό, και συνεπώς αντιμετωπίζει την κυβερνοβία που υποκινείται από ορισμένες προκαταλήψεις, αλλά όχι εάν υποκινείται από άλλα αντιληπτά χαρακτηριστικά όπως το φύλο, ο σεξουαλικός προσανατολισμός ή η αναπηρία. Το έργο του Συμβουλίου της Ευρώπης και άλλων οργανισμών για τις διακρίσεις και τη μισαλλοδοξία είναι επίσης σχετικό. Βασικά ζητήματα είναι ο ρόλος των παρόχων υπηρεσιών και το ζήτημα της ρητορικής μίσους έναντι της ελευθερίας του λόγου. Μια Επιτροπή Εμπειρογνωμόνων για την Καταπολέμηση του Εγκλήματος Μίσους (PC/ADI-CH) ξεκίνησε τις εργασίες της το 2022.

Ελεύθερος λόγος έναντι ρητορικής μίσους:

Οι χώρες έχουν διαφορετικές απόψεις σχετικά με τον βαθμό στον οποίο ο λόγος πρέπει να περιορίζεται από την κοινωνία – δηλαδή πού να τεθεί η ισορροπία μεταξύ

του θεμελιώδους δικαιώματος ενός ατόμου να εκφράζεται και του θεμελιώδους δικαιώματος ενός άλλου ατόμου στην ασφάλεια.

Μια εκπαιδευτική εκστρατεία για τη νεολαία, που ονομάζεται «Κίνημα χωρίς ρητορική μίσους», διοργανώθηκε από το Συμβούλιο της Ευρώπης μεταξύ 2012-2018. Αυτή η εκστρατεία στόχευε στην καταπολέμηση της διαδικτυακής ρητορικής μίσους κινητοποιώντας τους νέους και τις οργανώσεις νεολαίας να αναγνωρίσουν και να δράσουν ενάντια σε αυτές τις παραβιάσεις των ανθρωπίνων δικαιωμάτων. Το κίνημα No Hate Speech Movement ανέπτυξε, μεταξύ άλλων, μια επισκόπηση της δομής αναφοράς για ρητορική μίσους και διαδικτυακό εκφοβισμό σε εθνικές δομές και άνοιξε το δρόμο για πρωτοβουλίες παρακολούθησης τόσο στο Συμβούλιο της Ευρώπης όσο και σε εθνικό επίπεδο.

4.12 Ο νόμος για την επιβολή περιορισμών στα μέσα κοινωνικής δικτύωσης μετά τον νέο γερμανικό Νόμο περί Βελτίωσης της Επιβολής της Νομοθεσίας στα Κοινωνικά Δίκτυα

Ο νόμος για την επιβολή περιορισμών στα μέσα κοινωνικής δικτύωσης μετά τον νέο γερμανικό Νόμο περί Βελτίωσης της Επιβολής της Νομοθεσίας στα Κοινωνικά Δίκτυα (Netzwerkdurchsetzungsgesetz, NetzDG Γερμανικά: Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken), επίσης γνωστός στην καθομιλουμένη ως νόμος του Facebook (Facebook-Gesetz), είναι ένας γερμανικός νόμος που ψηφίστηκε στην Ομοσπονδιακή Δημοκρατία της Γερμανίας. για την καταπολέμηση των ψεύτικων ειδήσεων, της ρητορικής μίσους και της παραπληροφόρησης στο διαδίκτυο.

Ο νόμος υποχρεώνει τις πλατφόρμες μέσων κοινωνικής δικτύωσης με περισσότερους από 2 εκατομμύρια χρήστες να αφαιρούν το «σαφώς παράνομο» περιεχόμενο εντός 24 ωρών και όλο το παράνομο περιεχόμενο εντός 7 ημερών από τη δημοσίευσή του, διαφορετικά αντιμετωπίζουν μέγιστο πρόστιμο 50 εκατομμυρίων ευρώ. Το διαγραμμένο περιεχόμενο πρέπει να αποθηκευτεί για τουλάχιστον 10 εβδομάδες μετά και οι πλατφόρμες πρέπει να υποβάλλουν αναφορές διαφάνειας για την αντιμετώπιση παράνομου περιεχομένου κάθε έξι μήνες. Ψηφίστηκε από την Bundestag τον Ιούνιο του 2017 και τέθηκε σε πλήρη ισχύ τον Ιανουάριο του 2018. (https://en.wikipedia.org/wiki/Network_Enforcement_Act)

Ο νόμος έχει επικριθεί τόσο στη Γερμανία όσο και σε διεθνές επίπεδο από πολιτικούς, ομάδες ανθρωπίνων δικαιωμάτων, δημοσιογράφους και ακαδημαϊκούς για την παροχή κινήτρων στις πλατφόρμες των μέσων κοινωνικής δικτύωσης να λογοκρίνουν προληπτικά την έγκυρη και νόμιμη έκφραση και να τις καθιστούν ως κριτές του τι συνιστά ελεύθερη έκφραση και περιορίζει την ελευθερία του λόγου στη Γερμανία. Είναι γεγονός ότι από το πρώτο εξάμηνο του 2018, όπου και άρχισε να εφαρμόζεται, έγιναν διαγραφές σε μεγάλο ποσοστό, αποδεικνύοντας τους φόβους που υπήρχαν για overblocking. Η πρώτη υπόθεση διαγραφής ήταν η διαγραφή ενός tweet του περιοδικού Titanic, το οποίο ειρωνευόταν μια πολιτικό της AfD, χρησιμοποιώντας τη φρασεολογία αυτής για τους πρόσφυγες (Καραγκούνης, 2018)

5 Δυσκολίες στην ανίχνευση του ηλεκτρονικού εγκλήματος γενικά και κατά συνέπεια στα εγκλήματα κατά της τιμής

5.1 Γενικές δυσκολίες ως προς το ηλεκτρονικό έγκλημα

Οι δυσκολίες θα μπορούσαν να συνοψισθούν στα εξής:

-Ο μη οπτικός χαρακτήρας των αποδείξεων

Η έρευνα και η ποινική δίωξη του ηλεκτρονικού εγκλήματος απαιτεί τον έλεγχο στα δεδομένα που έχουν αποθηκευτεί σε ένα υπολογιστικό σύστημα. Πολλά από αυτά δεν μπορούν να αναγνωστούν από τον μέσο άνθρωπο, αλλά είναι συγκεντρωμένα σε ηλεκτρονικές συσκευές μνήμης, οι οποίες αναγνωρίζονται μόνο από τον υπολογιστή. Το πρόβλημα εμφανίζεται από τη στιγμή που οι αρμόδιες εισαγγελικές αρχές αντιμετωπίζουν την έλλειψη ορατών και κατανοήσιμων αποδείξεων, που προκαλούνται από την ανωνυμία, τη συμπίεση ή την κωδικοποίηση των ηλεκτρονικά αποθηκευμένων πληροφοριών. «Το πληροφορικό έγκλημα ονομάζεται disembodied crime», κατά τους Michalowski και Pfuhl, το οποίο μάλλον θα μπορούσαμε να το μεταφράσουμε έγκλημα χωρίς ενσωμάτωση. Δεδομένα μπορούν να κλαπούν εύκολα χωρίς καν να μετακινηθούν από τον παραβάτη. Η μη εξουσιοδοτημένη πρόσβαση γίνεται εφικτή κωδικοποιημένη ως μια επικοινωνία μεταξύ υπολογιστών που σε πολλές περιπτώσεις δεν αφήνει καν ίχνη στα αρχεία καταγραφής.

Σε άμεση συνάφεια βρίσκεται και το γεγονός ότι οι τροποποιήσεις στα προγράμματα ή τα δεδομένα δεν αφήνουν ίχνη, ανάλογα αυτών που αξιοποιούνται στα πλαίσια της κλασικής απόδειξης των παραδοσιακών εγκλημάτων. Για παράδειγμα, η

ανάλυση χειρογράφου δεν υφίσταται πλέον στις ηλεκτρονικές βάσεις δεδομένων, άρα και στις υποθέσεις των πληροφορικών εγκλημάτων (Λάζος, 2001).

-Η εξάλειψη των αποδείξεων

Οι παραβάτες, στην προσπάθειά τους να αποφύγουν την ποινική δίωξη, μπορούν να εξαφανίσουν τα αποδεικτικά στοιχεία. Αυτό επιτυγχάνεται κυρίως μέσα από ρυθμίσεις στο λειτουργικό σύστημα ενός υπολογιστή. Χαρακτηριστικό είναι το παράδειγμα ενός λαθρέμπορου όπλων: έχοντας αποθηκεύσει τα ονόματα των πελατών του σε έναν μικρό υπολογιστή, άλλαξε τις ενσωματωμένες εντολές του λειτουργικού συστήματος κατά τρόπο ώστε, αν κάποιος επιχειρούσε να τις καλέσει/εισαγάγει εξαφανίζονταν όλα τα αρχεία. Όπως και στην περίπτωση της «μεταμφίεσης του ηλεκτρονικού εγκλήματος» (δηλαδή όταν το ηλεκτρονικό έγκλημα δεν παρουσιάζεται σαν τέτοιο, πχ χρονοκλοπή(time theft), ηλεκτρονική κατασκοπεία.

Πέρα από τον μη οπτικό χαρακτήρα των αποδείξεων, κάποιος δράστης μπορεί να δυσκολέψει τις διαδικασίες ποινικής δίωξης προστατεύοντας τα δεδομένα μέσω κάποιων μηχανισμών ασφαλείας, όπως τα συνθηματικά και η κρυπτογράφηση. Χρησιμοποιώντας αυτές τις τεχνικές, ο hacker ή ο υπάλληλος κάποιας εταιρείας έχουν τη δυνατότητα να παρεμποδίσουν τον έλεγχο της διασυνοριακής μεταφοράς δεδομένων: με μία κρυπτογραφημένη τηλεφωνική κλήση διάρκειας μερικών δευτερολέπτων είναι σε θέση να ολοκληρώσει τη μη εξουσιοδοτημένη μεταβίβαση κεφαλαίων. Ακόμα και στο πεδίο των παραβιάσεων της ιδιωτικότητας, οι κρυπτογραφικές τεχνικές καθιστούν δύσκολο τον έλεγχο των αποθηκευμένων πληροφορικών (Λάζος, 2001).

- Ο μεγάλος αριθμός δεδομένων

Η μεθοδολογία αρκετών ηλεκτρονικών εγκλημάτων περιλαμβάνει πολύπλοκα μοντέλα ενεργειών. Για να διαπραχθούν, απαιτείται πολύ καλή γνώση του χειρισμού της πληροφορικής τεχνολογίας (κυρίως σε επίπεδο λειτουργικών συστημάτων). Κατά τον έλεγχο που πραγματοποιούν οι αρμόδιες δικαστικές και αστυνομικές αρχές στα δεδομένα που σχετίζονται με ένα αδίκημα, μπορεί να προκύψουν προβλήματα από τις πολλές επιμέρους ενέργειες, οι οποίες εκτελούνται αυτόματα από έναν υπολογιστή και ως αποτέλεσμα δυσχεραίνουν την ολοκλήρωση του ελέγχου. Οι δυσκολίες αποκάλυψης ενός αδικήματος λόγω του μεγάλου αριθμού δεδομένων, μπορούν να ελαχιστοποιηθούν με τη χρήση του. Οι ελεγκτές και οι εισαγγελείς πρέπει να

στηριχθούν σε εργαλεία λογισμικού με σκοπό την υποβοήθηση της ποινικής δίωξης (Λάζος, 2001).

5.2 Πως είναι δυνατόν να ανιχνευθεί από τις διωκτικές αρχές μια διεύθυνση IP

Στον κυβερνοχώρο, η διεύθυνση IP μπορεί να αποδοθεί με δύο πιθανούς τρόπους: στατικά ή δυναμικά. Στη στατική περίπτωση: η εκχώρηση διεύθυνσης IP γίνεται σε συγκεκριμένο οργανισμό ή πρόσωπο με σκοπό να μείνει αμετάβλητη. Μερικές φορές, ένας υπολογιστής με στατική διεύθυνση IP χρησιμοποιείται ως δρομολογητής(router) ή ως διακομιστής μεσολάβησης (proxy) για έλεγχο των ιδιωτικών δικτύων. Είναι απαραίτητο να αναγνωρίσουμε τη μοναδική ταυτότητα της σχέσης μιας δυναμικής διεύθυνσης IP και της χρονικής περιόδου που αυτή χρησιμοποιήθηκε από έναν οικιακό χρήστη ή λογαριασμό συστήματος πριν από την έρευνα. Ο ISP συχνά αντιστοιχίζει μια σειρά δυναμικών διευθύνσεων IP, στους οικιακούς χρήστες μιας γειτονιάς. Ένα ιδιαίτερο χαρακτηριστικό είναι το γεγονός ότι οι λογαριασμοί των οικιακών χρηστών χρησιμοποιούν μια δυναμική διεύθυνση IP μόνο μία φορά, γεγονός που συνήθως χρησιμοποιείται από ανακριτές εγκλήματος στον κυβερνοχώρο για την παρακολούθηση ενός υπόπτου (Kao, 2008).

Το διαδίκτυο είναι μία συγχώνευση υπολογιστών και συστημάτων επικοινωνίας, μία διασύνδεση υπολογιστών όλων των ειδών σε όλο τον κόσμο, που επιτρέπει στους χρήστες να επικοινωνούν μέσω e-mail, να μεταφέρουν δεδομένα μέσω FTP, να βρίσκουν πληροφορίες στον Παγκόσμιο Ιστό και να αποκτούν πρόσβαση σε βάσεις δεδομένων. Ωστόσο, αυτοί οι υπολογιστές, που βρίσκονται σε όλο τον κόσμο, βρίσκονται σε διαφορετικές ζώνες ώρας και σπάνια συγχρονίζονται. Αυτό τονίζει τη σημασία του προσδιορισμού της ακριβούς ώρας του εγκλήματος. Ο χρόνος μπορεί να ελεγχθεί και να αναλυθεί για να προσδιοριστεί εάν οι πληροφορίες που συλλέγονται είναι σωστές ή όχι. Εάν οι ρυθμίσεις διαμόρφωσης του υπολογιστή προορισμού δεν έχουν τροποποιηθεί, τότε τα στοιχεία είναι πιθανότατα έγκυρα. Επομένως, οι ψηφιακές ενδείξεις πρέπει να αναλυθούν όσο το δυνατόν συντομότερα. Το GMT αναφέρεται στην "Μέση ώρα Γκρίνουιτς" και αναπαρίσταται ως “+ 0000”. Το CST υποδεικνύει «Τυπική ώρα Κίνας», που ισούται με «+ 0800». Όλες οι ζώνες ώρας θα πρέπει να μεταφραστούν στην τοπική ζώνη ώρας, επειδή ο ακριβής χρονισμός είναι ζωτικής σημασίας στην περίπτωση εγκλήματος στον κυβερνοχώρο. Εξαιρουμένης της

περαιτέρω επιπλοκής της θερινής ώρας, η ίδια ακριβώς χρονική στιγμή μπορεί να δηλωθεί ως "07:33:43 Τετάρτη 13 Φεβρουαρίου 2008 + 0000" στην περίπτωση του GMT και «15:33:43 Τετάρτη 13 Φεβρουαρίου 2008 + 0800» στην περίπτωση του CST.

Μόλις ο υπολογιστής επανασυνδεθεί στο Διαδίκτυο, ο πάροχος θα εκχωρήσει αυτόματα μια νέα δυναμική διεύθυνση IP. Όταν στη συνέχεια, συνδεθεί με τον απομακρυσμένο υπολογιστή με σκοπό τη διάπραξη του εγκλήματος, προκύπτει ακόμα μια καταγραφή με την αντίστοιχη χρονική σήμανση (Kao et al., 2006). Ο ανακριτής θα πρέπει να θεωρεί όλους τους χρόνους που καταγράφονται σε αρχεία καταγραφής υπολογιστή μόνο ως εκτίμηση, εκτός και αν αυτοί οι χρόνοι συγκεντρώνονταν περιοδικά ή αντιστοιχίζονταν με άλλα αξιόπιστα αρχεία καταγραφής.

Μύθος: η αρχική «διεύθυνση IP» και το στιγμυότυπο χρόνου μπορούν να ταυτοποιήσουν τον ύποπτο.

Σε κάθε διαδικτυακό μήνυμα, υπάρχουν διάφορες ενδείξεις που αποκαλύπτουν κάτι για την πηγή. Πιστεύεται ότι το όνομα διακομιστή και η διεύθυνση IP οι οποίες αντιστοιχούν σε έναν διακομιστή είναι ο τρόπος αναγνώρισης υπολογιστών στο διαδίκτυο. Κάθε είδους ψηφιακή εγκληματολογική ανάλυση συνήθως ξεκινά με τη διεύθυνση IP και τη χρονική σήμανση στο διαδίκτυο. Αυτά τα δύο στοιχεία στα αρχεία καταγραφής του υπολογιστή έχουν γίνει τα διαδικτυακά ισοδύναμα ενός δακτυλικού αποτυπώματος σε μια λαβή πόρτας ή ενός κομματιού ελαστικών στη λάσπη. Ωστόσο, αυτό δεν είναι πάντα σωστό. Μια δυναμική διεύθυνση IP χρησιμοποιείται συχνά σε οικιακές συνδέσεις. Επομένως, όταν ο χρήστης του υπολογιστή συνδεθεί στο σύστημα του παρόχου, το σύστημα επαληθεύει το αναγνωριστικό χρήστη και το συνθηματικό, και παρέχει μια δυναμική διεύθυνση IP για σύνδεση με άλλους υπολογιστές μέσω του Διαδικτύου. Μόλις ο χρήστης αποσυνδεθεί, η διεύθυνση IP είναι και πάλι ελεύθερη και διαθέσιμη σε έναν νέο χρήστη. Οι δυναμικές διευθύνσεις IP εκχωρούνται συνήθως σε υπολογιστές εντός μιας καθορισμένης γειτονιάς. Οι οικιακοί χρήστες χρησιμοποιούν τις δυναμικές διευθυνσεις IP μόνο μια φορά. Έτσι, μια δυναμική διεύθυνση IP και μια χρονική σήμανση μπορεί να περιορίσει τον αριθμό των πιθανών υπόπτων.

Το ερώτημα είναι: Είναι αυτή η μέθοδος αξιόπιστη και ακριβής; Πώς μπορούμε να συμπεράνουμε αν ο χρήστης είναι αθώος ή ένοχος;

Κανένα πρόσωπο δεν μπορεί να στερηθεί τη ζωή, την ελευθερία ή την περιουσία χωρίς τη δέουσα νομική διαδικασία. Ενώ η αποκάλυψη υπόπτων είναι

σημαντική, η αποφυγή άδικων κατηγοριών αξίζει την ίδια προσοχή. Το να λέμε ότι «το μόνο που χρειάζεται ένας ανακριτής εγκλημάτων στον κυβερνοχώρο είναι οι πληροφορίες της διεύθυνσης IP και της χρονικής σφραγίδας» είναι μύθος. Ειδικά, όταν τα αποδεικτικά στοιχεία εναντίον του υπόπτου βασίζονται μόνο σε διεύθυνση IP και χρόνο, ο ένορκος ή ο δικαστής θα αντιμετωπίσει δυσκολίες στη λήψη της απόφασης. Πριν ληφθεί η τελική απόφαση, ασκείται κατηγορητήριο εναντίον κάποιου. Είναι σχεδόν αδύνατο να γνωρίζει κανείς τα γεγονότα, εκτός κι αν είναι το άτομο που διέπραξε το έγκλημα. Οι δικαστικές αποφάσεις πρέπει να βασίζονται μόνο σε τεκμηριωμένα στοιχεία. Δεν είναι δεδομένο ότι θα υπάρχουν πάντα τα «σωστά» στοιχεία για να αποδειχθούν τα πάντα. Οι ανακριτές θα πρέπει να το γνωρίζουν αυτό και να κάνουν ό,τι μπορούν για να αποφύγουν τα λάθη.

Γεγονός: Η αλήθεια μπορεί να εξαχθεί από σχετικές πληροφορίες.

Αυτό είναι απλώς το σημείο εκκίνησης της συλλογής των πληροφοριών διεύθυνσης IP και χρονικής στιγμής/περιόδου που απαιτούνται για την έρευνα. Πρόσθετες ενδείξεις πρέπει να εντοπιστούν και να αναλυθούν από τεχνικούς εμπειρογνώμονες και εγκληματολόγους. Διαφορετικά, θα ήταν πολύ εύκολο για τους ποινικούς ανακριτές να βγάλουν αβάσιμα συμπεράσματα, τα οποία θα μπορούσαν να έχουν ως αποτέλεσμα την εσφαλμένη καταδίκη ενός ατόμου. Επομένως, για να αποκαλυφθεί η αλήθεια, οι έρευνες για το έγκλημα στον κυβερνοχώρο θα πρέπει να βασίζονται στην πιο πρόσφατη τεχνολογία της πληροφορικής. Συχνά οι εγκληματικές δραστηριότητες έχουν αφήσει ένα ίχνος επικοινωνίας σε συνδεδεμένα περιβάλλοντα δικτύου. Είναι δυνατό να εξαχθούν ενδείξεις και από αυτές τις τοποθεσίες.

Οι Kao, Wang και Huang πρότειναν έναν τυπικό τρόπο παρακολούθησης των εγκληματιών του κυβερνοχώρου με βάση τα στοιχεία της διεύθυνσης IP και της χρονοσφραγίδας (timestamp) ή στιγμιότυπου χρόνου. Η προσέγγισή τους για τη βελτίωση της έρευνας του εγκλήματος στον κυβερνοχώρο προτείνεται σε τρία στάδια: ανεξάρτητη επαλήθευση ψηφιακών ενδείξεων, αντίστοιχες πληροφορίες από διαφορετικές πηγές και προετοιμασίας ενός ορθού νομικού επιχειρήματος (Kao et al., 2006).

5.3 Εντοπισμός των μηνυμάτων cyberbullying με χρήση κατάλληλου αλγορίθμου

Μία ομάδα από τη Σαουδική Αραβία, είχε την ιδέα δημιουργίας ενός αλγόριθμου, ο οποίος εντοπίζει αυτόματα μηνύματα cyberbullying. Όπως είναι γνωστό, η μηχανική μάθηση (machine learning,ML) είναι ένα υποπεδίο της τεχνητής νοημοσύνης (AI) που προσφέρει συστήματα με δυνατότητα μάθησης και βελτίωσης Η τεχνητή νοημοσύνη συμμετέχει στις διαδικασίες αυτοματισμού από προηγούμενη εμπειρία, ακόμα και αν δεν προγραμματιστεί συγκεκριμένα για αυτό. Είναι απαραίτητο για δραστηριότητες και εργασίες που είναι αρκετά περίπλοκες για έναν άνθρωπο, όπως στην περίπτωση εντοπισμού διαδικτυακού εκφοβισμού. Υπάρχουν δύο προσεγγίσεις μηχανικής μάθησης: εποπτευόμενη και μη εποπτευόμενη.

Σε αλγόριθμους εποπτευόμενης μάθησης, το σύνολο δεδομένων εκπαίδευσης περιέχει ετικέτες κλάσεων για τη δημιουργία ενός μοντέλου που μπορεί στη συνέχεια να χρησιμοποιηθεί για την πρόβλεψη μη επισημασμένων δεδομένων. Τα Decision Tree, Naïve Bayes (NB), K-Nearest Neighbors και το Support Vector Machine (SVM) είναι παραδείγματα αλγόριθμων που δείχνουν εύλογη ακρίβεια και απόδοση. Το SVM είναι ένας δυαδικός ταξινομητής που προϋποθέτει ότι τα δείγματα δεδομένων είναι σαφώς διαφοροποιημένα. Ωστόσο, οι αλγόριθμοι μάθησης χωρίς επίβλεψη χρησιμοποιούν σύνολα δεδομένων εκπαίδευσης χωρίς ετικέτα.

Η εποπτευόμενη μάθηση μπορεί να δώσει γρηγορότερα αποτελέσματα, αλλά προϋποθέτει πρότερη γνώση και ενδέχεται να προσκολληθεί στα δεδομένα της εκπαίδευσης (υπερεκπαίδευση ή overfitting). Αντιθέτως, η μη εποπτευόμενη μηχανική μάθηση μπορεί να χρησιμοποιηθεί γενικότερα, αλλά ενδέχεται να αργήσει περισσότερο να δώσει αποτελέσματα.

Η Επεξεργασία Φυσικής Γλώσσας (NLP) είναι ένας τομέας της επιστήμης των υπολογιστών που σκοπεύει να διευκολύνει την επικοινωνία μεταξύ μηχανών και ανθρώπων. Η κύρια ιδέα πίσω από αυτό αφορά τη δημιουργία ενός αυτοματοποιημένου περιβάλλοντος για την κατανόηση και επεξεργασία της ανθρώπινης γλώσσας.

Η ομάδα των Mouheb, Dalvi, Haidar, Muneer χρησιμοποίησε όλες τις παραπάνω μεθόδους, με πολύ υψηλά ποσοστά εντοπισμού μηνυμάτων bullying (Alduailaj, A.M.; Belghith,2022) Αυτό βέβαια – σε ένα άλλο επίπεδο- δημιουργεί, πολλά θέματα σε ό,τι αφορά τα προσωπικά δεδομένα και για τη ελευθερία του λόγου, καθώς απαιτείται η συναίνεση των χρηστών για την ανάλυση των αναρτήσεών τους από τον αλγόριθμο.

5.4 Οι ανακριτικές δυνατότητες κατά η Σύμβαση της Βουδαπέστης

Η Σύμβαση της Βουδαπέστης προβλέπει μια πλειάδα δικονομικών ενεργειών. Ειδικότερα, ορίζει ένα πλήθος πρωτότυπων ανακριτικών πράξεων κατάλληλων για την ανάκτηση και επεξεργασία ψηφιακών δεδομένων για τους σκοπούς της ποινικής διαδικασίας. Χαρακτηριστικό είναι ότι οι προβλεπόμενες στη Σύμβαση ενέργειες είναι δυνατές, όχι μόνο ειδικώς για τα εγκλήματα, τα οποία προβλέπει η ίδια, αλλά για το σύνολο των ποινικών εγκλημάτων. Επομένως, οι προβλεπόμενες ενέργειες διεξάγονται σε όλα τα κυβερνοεγκλήματα, γνήσια ή μη γνήσια, ακόμη και στα ηλεκτρονικά εγκλήματα που δεν διεξάγονται διαδικτυακά.

Ειδικότερα, στη Σύμβαση της Βουδαπέστης προβλέπονται μέτρα για:

1)την έρευνα και την κατάσχεση, όπως και για την απομακρυσμένη έρευνα και κατάσχεση ψηφιακών δεδομένων που είναι αποθηκευμένα σε υπολογιστή ή άλλο μέσο.

2) τη γνωστοποίηση στοιχείων συνδρομητών (επικοινωνιών)

3) τη διατήρηση, κοινοποίηση, διάθεση και γνωστοποίηση δεδομένων και των δεδομένων κίνησης και θέσης από τους παρόχους ηλεκτρονικών υπηρεσιών

4) τη συλλογή και αποθήκευση άμεσα από τις αρχές σε πραγματικό χρόνο των δεδομένων κίνησης και θέσης (επικοινωνιών)

5) τη συλλογή και καταγραφή άμεσα από τις αρχές δεδομένων περιεχομένου(επικοινωνιών)

Ωστόσο, οι σχετικές με τις ανακριτικές πράξεις διατάξεις δεν είναι άμεσα εκτελεστές και απαιτούν την ειδική εφαρμογή τους με εσωτερικούς νόμους. Όπως ορίζει η ίδια η Σύμβαση στο άρθρο 14(1): «κάθε συμβαλλόμενο μέρος λαμβάνει τα νομοθετικά και άλλα μέτρα που είναι αναγκαία για να θεσπίσει τις αρμοδιότητες και τις διαδικασίες που προβλέπονται στο παρόν τμήμα για τους σκοπούς συγκεκριμένων ποινικών ερευνών ή διώξεων». Ο Έλληνας νομοθέτης ωστόσο, παρά τη σαφήνεια των διατάξεων της Σύμβασης της Βουδαπέστης, δεν άδραξε την ευκαιρία και δεν θέσπισε εσωτερικές διατάξεις σύμφωνες με τα πρότυπά της. Μόνο δύο από τις προβλέψεις της Σύμβασης της Βουδαπέστης αντιστοιχούν μερικώς και μία καθ΄ ολοκληρίαν στο υφιστάμενο νομοθετικό πλαίσιο στην Ελλάδα: Αφενός, η ανακοίνωση δεδομένων συνδρομητών και η έρευνα και κατάσχεση ψηφιακών μέσων κατά τις γενικές διατάξεις του ΚΠΔ. Αφετέρου, η δέσμευση του περιεχομένου επικοινωνιών που είναι δυνατή μέσω των παρόχων, υπό τους τεχνολογικούς περιορισμούς. Έτσι λοιπόν, οι δικονομικές διατάξεις της Σύμβασης της Βουδαπέστης (άρθρα 15-21) προς το παρόν, παραμένουν

γράμμα κενό περιεχομένου για τον εφαρμοστή του εσωτερικού δικαίου. (Καργόπουλος,2018).

5.5 ΚΠΔ & ανακριτικές ενέργειες που αφορούν σε ψηφιακά δεδομένα

Η εφαρμογή των γενικών διατάξεων του ΚΠΔ περί των κατασχέσεων αντικειμένων και εγγράφων στα ψηφιακά δεδομένα δεν ανταποκρίνεται στις σύγχρονες ανάγκες και την πραγματικότητα, ούτε στις απαιτήσεις της νομολογίας του ΕΔΔΑ και του ΔΕΕ.

Επιπλέον, τα ψηφιακά δεδομένα είναι άυλα. Ο υλικός φορέας των δεδομένων (σκληρός δίσκος ή άλλο μέσο αποθήκευσης), στον οποίον αφορούν τα ψηφιακά δεδομένα, είναι διακριτός έναντι των ίδιων των δεδομένων. Επομένως, οι ρυθμίσεις του ΚΠΔ που αφορούν αποκλειστικά σε υλικά πειστήρια και έγγραφα δεν ανταποκρίνονται στην πραγματικότητα και τις ανάγκες των ψηφιακών δεδομένων. Επί παραδείγματι, οι ισχύουσες διατάξεις του ΚΠΔ δεν αντιμετωπίζουν τη βεβαίωση και την επαλήθευση της αυθεντικότητας των ψηφιακών δεδομένων και των ιδιοτήτων τους (πότε επεξεργάστηκαν, αντιγράφηκαν κλπ). Οι του ΚΠΔ διατάξεις δεν εκτείνονται ρητώς στα ψηφιακά δεδομένα, με αποτέλεσμα η οποιαδήποτε μορφή επεξεργασίας τους, όπως η αντιγραφή του, να μη διαθέτει νόμιμη βάση ή να διαθέτει ανεπαρκή νόμιμη βάση, κατά παράβαση των άρθρων 8 ΕΣΔΑ, 7 και 8, 52 του χάρτη.

Ως εκ τούτου, οι επιβαλλόμενες ενέργειες των αρχών, κατά τα διεθνή πρότυπα, δηλαδή η κατάσχεση υλικών φορέων, η αντιγραφή των αρχείων, η επεξεργασία των αρχείων και η αναπαραγωγή των αρχείων για τους σκοπούς της ποινικής δίκης, ως ορθώς μεν γίνονται στην πράξη, δεν έχουν κανένα έρεισμα στο νόμο. Δηλαδή, εφόσον η παραγγελία και η κατάσχεση κατά τον ΚΠΔ αφορά στα καθαυτά υλικά μέσα αποθήκευσης, οι ενέργειες των αρχών δεν μπορούν να αφορούν στα ψηφιακά δεδομένα, χωρίς σαφή νομική βάση. Επομένως, οι τυχόν ανακριτικές πράξεις που αφορούν σε ψηφιακά δεδομένα και γίνονται χωρίς νομική βάση, αποτελούν κατ' ουσίαν αυθαίρετες ενέργειες. Επίσης, διαδικαστικές ενέργειες που λαμβάνουν χώρα χωρίς ειδική και σαφή νομική βάση που να οριοθετεί επακριβώς το εύρος και τις δυνατότητες των αρχών είναι δεκτικές σε καταχρήσεις και αυθαιρεσία. Τούτων δοθέντων, ο νόμος πρέπει να ορίζει ειδικώς και συγκεκριμένα τις ανακριτικές πράξεις επί των ψηφιακών δεδομένων, σύμφωνα και με την ανωτέρω νομολογία του ΕΔΔΑ και

ΔΕΕ και την αρχή της νομιμότητας που αποτελεί αναπόσπαστο στοιχείο του κράτους δικαίου (Καργόπουλος,2018).

Επιπλέον, η κατάσχεση, κατά το ισχύον σύστημα, καταλαμβάνει μόνον τους υλικούς φορείς και δεν υπάρχει δυνατότητα, καίτοι εφικτό και αναγκαίο στην πράξη, να διενεργείται κατάσχεση (αντιγραφή και αποθήκευση) των ψηφιακών δεδομένων αυτοτελώς και όχι των υλικών τους φορέων. Κάτι τέτοιο όμως θα ήταν αναγκαίο, ιδίως στην περίπτωση που τα δεδομένα βρίσκονται αποθηκευμένα απομακρυσμένα εντός του ίδιου πληροφοριακού συστήματος, λ.χ. σε κάποιον server. Έτσι λοιπόν, οι αρχές αδυνατούν προς το παρόν, στα πλαίσια κατ΄ οίκον έρευνας, να δεσμεύσουν και να κατασχέσουν αυτοτελώς τα δεδομένα, στα οποία ο χρήστης έχει απομακρυσμένη πρόσβαση, παρότι τεχνικά εφικτό. Αυτό, όμως, περιπλέκει τις έρευνες και μπορεί να αποβεί επιζήμιο. Με τις ισχύουσες διατάξεις δεν μπορεί να γίνει κατάσχεση των δεδομένων αυτών, διότι δεν μπορεί να βρεθεί ο υλικός φορέας και είναι δυσαπόδεικτο το αδίκημα. Αντιθέτως, κατά τα πρότυπα της Σύμβασης της Βουδαπέστης αυτό θα είναι εφικτός και οι αρχές θα μπορούν να αντιγράψουν (κατασχέσουν) τα δεδομένα, χωρίς να κατασχέσουν τον ίδιο τον υλικό τους φορέα.

Η εν λόγω ρύθμιση θα είχε προδήλως αναγκαία εφαρμογή ιδίως σε επιχειρήσεις, οι οποίες διατηρούν τα δεδομένα αποθηκευμένα σε απομακρυσμένους υλικούς φορείς (servers) των ίδιων ή άλλων παρόχων που τους προσφέρουν τέτοιου είδους υπηρεσίες. Αξίζει, βέβαια, να σημειωθεί ότι τα ψηφιακά δεδομένα που είναι αποθηκευμένα και προσβάσιμα μέσω συστημάτων και υπηρεσιών νεφοϋπολογιστικής (cloud services) δε θεωρούνται αποθηκευμένα σε απομακρυσμένο σύστημα υπολογιστή ή σε απομακρυσμένο μέσο αποθήκευσης δεδομένων, στο οποίο ο χρήστης έχει πρόσβαση. Κατ΄ αποτέλεσμα ως προς αυτά να απαιτείται να ακολουθηθεί η διαδικασία που αφορά σε ανάκτηση δεδομένων επικοινωνιών.

Επιπροσθέτως, όπως ήδη αναφέρθηκε, η κατάσχεση των ψηφιακών δεδομένων κατά την Οδηγία 680/2016 και τη νομολογία, απαιτείται να περιβάλλεται με τις κατάλληλες εγγυήσεις κατά τυχόν αυθαιρεσιών. Τέτοιες είναι όπως προελέχθη η προηγούμενη δικαστική έγκριση, η τήρηση αρχείου καταγραφής, ο περιορισμός της πρόσβασης μόνο σε εξουσιοδοτημένο προσωπικό, μέτρα κατά της τυχαίας απώλειας και διαγραφής των ψηφιακών δεδομένων, κ.λ.π. Ελλείψει αυτών, η διαδικασία πάσχει και δεν διασφαλίζει την τήρηση των απαιτήσεων του άρθρου 8 της ΕΣΔΑ (και άρθρων 7 και 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων). Συνεπεία των ανωτέρω γεννάται ζήτημα απόλυτης ακυρότητας, ακόμη κι αν δεν έχουν διαπιστωθεί συγκεκριμένες

αυθαιρεσίες, διότι μόνο ο κίνδυνος επέλευσης αυτών αρκεί για τη διαπίστωση παράβασης των παραπάνω άρθρων της ΕΣΔΑ και του Χάρτη. Ως εκ τούτου επιβάλλεται να ορισθούν διατάξεις και στο ημεδαπό δίκαιο που να ορίζουν κατ΄ελάχιστο τη διαδικασία και τη η δυνατότητα κατάσχεσης ψηφιακών δεδομένων και τις απαραίτητες εγγυήσεις (Καργόπουλος,2018).

Σύμφωνα με την 6/2021 Γνωμοδότηση του Αντιεισαγγελέα του Αρείου Πάγου Χαρ. Βουρλιώτη : «Κατά τη διάταξη του άρθρου 265 του νέου Κώδικα Ποινικής Δικονομίας (που κυρώθηκε με το άρθρο πρώτο του ν. 4620/2019, ΦΕΚ Α` 96/11.6.2019 και άρχισε να ισχύει από την 1η Ιουλίου 2019) 1. Η κατάσχεση ψηφιακών δεδομένων μπορεί να επιβληθεί: α) Σε ένα σύστημα υπολογιστή στο σύνολό του ή σε μέρος αυτού και στα δεδομένα υπολογιστή που είναι αποθηκευμένα σε αυτόν, στα οποία έχει φυσική πρόσβαση εκείνος που διενεργεί την ανάκριση, β) σε ένα μέσο αποθήκευσης δεδομένων υπολογιστή στο οποίο υπάρχουν αποθηκευμένα δεδομένα υπολογιστή και έχει φυσική πρόσβαση εκείνος που διενεργεί την ανάκριση, γ) σε ένα απομακρυσμένο σύστημα υπολογιστή στο σύνολό του ή σε μέρος αυτού και στα δεδομένα υπολογιστή που είναι αποθηκευμένα σε αυτόν ή σε ένα απομακρυσμένο μέσο αποθήκευσης δεδομένων υπολογιστή και στα δεδομένα υπολογιστή που είναι αποθηκευμένα σε αυτό, τα οποία είναι διασυνδεδεμένα στο σύστημα υπολογιστή στο οποίο έχει φυσική πρόσβαση εκείνος που διενεργεί την ανάκριση. Στην τελευταία περίπτωση, τα ψηφιακά δεδομένα που είναι αποθηκευμένα και προσβάσιμα μέσω συστήματος και υπηρεσιών νεφοϋπολογιστικής (cloud services) δεν θεωρούνται αποθηκευμένα σε απομακρυσμένο σύστημα υπολογιστή ή σε απομακρυσμένο μέσο αποθήκευσης δεδομένων υπολογιστή τα οποία είναι διασυνδεδεμένα στο σύστημα υπολογιστή στο οποίο έχουν φυσική πρόσβαση οι αρχές. 2. Η κατά τα ανωτέρω κατάσχεση πραγματοποιείται αποκλειστικά με τη χρήση κατάλληλου εξοπλισμού που επιτρέπει σε εκείνον που τη διεξάγει: α) Την αφαίρεση και την κατάσχεση του υλικού φορέα των υπό στοιχείων α-γ της παρ. 1, στο οποίο βρίσκονται αποθηκευμένα τα δεδομένα και/ή β) την αντιγραφή και την αφαίρεση των αποθηκευμένων ψηφιακών δεδομένων των υπό στοιχείων α-γ της παρ. 1 σε μέσο αποθήκευσης δεδομένων και γ) την αναπαραγωγή και την επαλήθευση της αυθεντικότητας και της ακεραιότητας των κατασχεθέντων δεδομένων. 3. Η κατάσχεση που διενεργείται κατά τις παρ. 1 και 2, βεβαιώνεται με ειδική έκθεση, η οποία αναφέρει ειδικώς τις ενέργειες της παρ. 2 που πραγματοποιεί εκείνος που διεξάγει την ανάκριση. 4. Τα ψηφιακά δεδομένα που κατάσχονται διατηρούνται αποθηκευμένα καθ’ όλη τη διάρκεια της ποινικής

διαδικασίας σε ένα και μόνο υλικό μέσο αποθήκευσης που περιέχεται στη δικογραφία. Ασφαλές αντίγραφο αυτού ώστε να διασφαλίζεται η δυνατότητα ανάκτησης των δεδομένων που έχουν κατασχεθεί, σε περίπτωση απώλειας ή καταστροφής, σχηματίζεται κατά την κατάσχεσή τους και διατηρείται στο γραφείο πειστηρίων του πρωτοδικείου στο οποίο υποβάλλεται η δικογραφία και το οποίο παρέχει τις κατάλληλες εγγυήσεις φυσικής ασφάλειας και πρόσβασης σε εκείνους μόνο που ασκούν καθήκοντα στην υπόθεση. Η παρούσα ισχύει αναλόγως και στα ψηφιακά δεδομένα που αφορούν στα δεδομένα επικοινωνίας που περιλαμβάνονται στη δικογραφία. 5. Η πρόσβαση και η δυνατότητα αναπαραγωγής των ψηφιακών δεδομένων που κατάσχονται επιτρέπεται μόνο σε όσους ασκούν δικαστικά, εισαγγελικά και ανακριτικά καθήκοντα στην υπόθεση ή τους γραμματείς. Προς το σκοπό αυτό χρησιμοποιούνται τα κατάλληλα τεχνικά μέσα. Τέτοια μέσα είναι η κρυπτογράφηση και η χρήση κωδικών ασφαλείας για την πρόσβαση και αναπαραγωγή των κατασχεμένων ψηφιακών δεδομένων από το υλικό μέσο αποθήκευσης στο οποίο βρίσκονται αποθηκευμένα. Η παρούσα ισχύει αναλόγως και στα ψηφιακά δεδομένα που αφορούν στα δεδομένα επικοινωνίας που περιλαμβάνονται στη δικογραφία. 6. Απαγορεύεται η δημιουργία και η διατήρηση αντιγράφων των ψηφιακών δεδομένων για οποιονδήποτε άλλον λόγο εκτός αν ο αρμόδιος εισαγγελέας ή ανακριτής ή συμβούλιο ή το δικαστήριο κρίνουν ότι τα κατασχεμένα ψηφιακά δεδομένα είναι αναγκαίο να περιληφθούν σε άλλη δικογραφία. Η παρούσα ισχύει αναλόγως και στα ψηφιακά δεδομένα που αφορούν στα δεδομένα επικοινωνίας που περιλαμβάνονται στη δικογραφία. Με τη ρύθμιση της διάταξης αυτής, που συνιστά μια επιβεβλημένη νεωτεριστική αποτύπωση επενέργειας της σύγχρονης τεχνολογικής εξέλιξης στην ποινική δίκη, παρέχεται η απαραίτητη και δικαιοκρατικά επαρκής νομική βάση για τη διενέργεια της συγκεκριμένης ανακριτικής πράξης, αφού, ενόψει του ότι τα ψηφιακά δεδομένα είναι άυλα, οποιαδήποτε ρύθμιση του Κώδικα που αναφέρεται σε υλικά πειστήρια και έγγραφα, τα οποία είναι διακριτά έναντι των δεδομένων, δεν καταλαμβάνει την πραγματική φύση και τις ανάγκες αυτών, ενώ, παράλληλα, παρέχονται οι δέουσες εγγυήσεις και προϋποθέσεις για την αποτροπή τυχόν αυθαιρεσιών, προβλέποντας τη σύνταξη ειδικής έκθεσης, τη χρήση κατάλληλου εξοπλισμού κατάσχεσης, τον περιορισμό της πρόσβασης μόνο σε εξουσιοδοτημένο προσωπικό, αλλά και μέτρα κατά της τυχαίας απώλειας και διαγραφής των ψηφιακών δεδομένων (Αιτιολογική Έκθεση νέου ΚΠΔ). Εξάλλου, κατά το άρθρο 30 παρ. 22 εδ. α` και υποπερ. ζζ` του π.δ. 178/2014 "Το Τμήμα Εξέτασης Ψηφιακών Πειστηρίων της

Διεύθυνσης Εγκληματολογικών Ερευνών εξετάζει ή αναλύει ψηφιακά, ηλεκτρονικά ή ακουστικά μέσα και τα δεδομένα που περιέχονται σ' αυτά, τα οποία περισυλλέγονται από τον τόπο του εγκλήματος από το Τμήμα Εξερευνήσεων της Διεύθυνσης Εγκληματολογικών Ερευνών ή αποστέλλονται με σχετική παραγγελία από ανακριτική, εισαγγελική ή δικαστική αρχή, εφόσον επιδέχονται εργαστηριακές εξετάσεις και μπορούν να συμβάλουν στην εξιχνίαση εγκληματικής πράξης....συνεργάζεται με τις επιληφθείσες Υπηρεσίες για τη διασφάλιση της κατάσχεσης, ορθής διαχείρισης και ταχύτερης αποστολής των προς εξέταση πειστηρίων, παρέχοντας σε αυτές οδηγίες ασφαλούς μεταφοράς και φύλαξης, ενώ σε εξαιρετικά κρίσιμες περιπτώσεις παρέχει τεχνική συνδρομή στην κατάσχεση, δια της αποστολής εξειδικευμένου κλιμακίου". Με την κατάσχεση, η οποία είναι ανακριτική πράξη, αφαιρείται από ορισμένο πρόσωπο η κατοχή πραγμάτων που σχετίζονται με ορισμένο έγκλημα, ως αντικείμενα ή μέσα τέλεσης ή προϊόντα του εγκλήματος, προς εξυπηρέτηση των αναγκών της ανακριτικής διαδικασίας και μάλιστα της συλλογής και διατήρησης των αποδείξεων ή για τη διασφάλιση της προβλεπόμενης δήμευσης ή της επιβαλλόμενης από το νόμο καταστροφής τους. Προς τούτο συντάσσεται σχετική έκθεση, σύμφωνα με τη διάταξη του άρθρου 149 του ίδιου, ως άνω, Κώδικα, κατά την οποία "Η έκθεση πρέπει να συντάσσεται στον τόπο όπου γίνεται η πράξη ή η δήλωση που βεβαιώνεται σ' αυτήν και στον ίδιο το χρόνο της ενέργειας ή, αν αυτό είναι αδύνατο, αμέσως κατόπιν". Με τη διάταξη αυτή επιτάσσεται η άμεση σύνταξη της έκθεσης κατάσχεσης στον τόπο και τον αυτό χρόνο της ενέργειας, με σκοπό την ακριβέστερη πιστοποίηση των πράξεων ή δηλώσεων, χωρίς, όμως, λόγω του ανέφικτου, σε πολλές περιπτώσεις, της επίκαιρης, κατά τα άνω, σύνταξης έκθεσης, να απαγγέλλεται σχετική ακυρότητα. Περαιτέρω, τα (άϋλα) ψηφιακά δεδομένα που είναι αποθηκευμένα σε ένα σύστημα ή σε ένα μέσο αποθήκευσης δεδομένων ή σε ένα απομακρυσμένο σύστημα υπολογιστή στο σύνολό του ή σε μέρος αυτού ή σε ένα απομακρυσμένο μέσο αποθήκευσης δεδομένων υπολογιστή, αποτελούν μέρος του υλικού φορέα στον οποίο εμπεριέχονται, είτε πρόκειται για σύστημα υπολογιστή είτε για μέσο αποθήκευσης, από τη φύση δε του πράγματος και κατά λογική ακολουθία, τα ψηφιακά δεδομένα κατάσχονται ταυτόχρονα με τον περιέκτη υλικό φορέα, ανεξάρτητα από το είδος και τη μορφή του, χωρίς να συντρέχει περίπτωση διακριτής κατάσχεσής τους και σύνταξης σε μεταγενέστερο χρόνο και διαφορετικό τόπο ιδιαίτερης, εκτός αυτής που αφορά στον υλικό φορέα τους, σχετικής έκθεσης, συνακόλουθα δε ουδεμία ακυρότητα της συγκεκριμένης ανακριτικής πράξης, συναπτόμενη με τη νομιμότητα των κτηθέντων,

ως άνω, αποδεικτικών μέσων, υπόκειται. Η τεχνική υποστήριξη του ανωτέρω Τμήματος που παρέχεται με τη διάθεση προσωπικού ειδικών γνώσεων και κατάλληλου εξοπλισμού, για την συλλογή, εξαγωγή, ανάλυση, διατήρηση, αναπαραγωγή και επαλήθευση της αυθεντικότητας των κατασχεθέντων δεδομένων, συνιστά περίπτωση πραγματογνωμοσύνης, η οποία διέπεται από τις σχετικές δικονομικές διατάξεις, οι διαπιστώσεις δε και τα συμπεράσματα αυτής αποτελούν συνέχεια και αναπόσπαστο μέρος της οικείας, κατά κανόνα χρονικά προηγούμενης, έκθεσης κατάσχεσης του υλικού φορέα».

Με την επικείμενη αλλαγή του Ποινικού Κώδικα με τον Ν.5090/24: Για τη διασφάλιση της αυθεντικότητας και της ακεραιότητας των ψηφιακών δεδομένων που κατάσχονται, αυτά θα σφραγίζονται κατά τη διεξαγωγή αυτής. Επίσης, θα χρησιμοποιούνται τα κατάλληλα τεχνικά μέσα για τη διασφάλιση της ακεραιότητας των ψηφιακών δεδομένων. Τέτοια μέσα είναι η κρυπτογράφηση και η χρήση κωδικών ασφαλείας για την πρόσβαση και αναπαραγωγή των κατασχεμένων ψηφιακών δεδομένων από το υλικό μέσο αποθήκευσης στο οποίο βρίσκονται αποθηκευμένα.

5.6 Σοβαρά ζητήματά που προκύπτουν από ενδεχόμενη άρση απορρήτου-Δικονομικές απαγορεύσεις

Στην περίπτωση που θύτης μιας εξύβρισης, ή συκοφαντικής δυσφήμισης μέσω Διαδικτύου είναι γνωστός του θύματος, τα πράγματα είναι πολύ απλά ως προς το εναντίον ποιου θα στραφεί το θύμα. Είναι γεγονός, ότι το αδίκημα της συκοφαντικής δυσφήμισης τελείται όλο και συχνότερα μέσω του διαδικτύου. Η αδυναμία της ελληνικής έννομης τάξης να αναμορφώσει αποτελεσματικά τη νομοθεσία για την άρση του απορρήτου των επικοινωνιών για τη διακρίβωση εγκλημάτων έχει καταστήσει προβληματική την υπεράσπιση των κατηγορουμένων για συκοφαντική δυσφήμηση τελεσθείσα μέσω του διαδικτύου. Συγκεκριμένα:

Αν και σύμφωνα με το άρθρο 19 παρ. 1 του ισχύοντος Συντάγματος (1975/1986/2001/2008): «Νόμος ορίζει τις εγγυήσεις υπό τις οποίες η δικαστική αρχή δεν δεσμεύεται από το απόρρητο για λόγους εθνικής ασφάλειας ή για διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων», στην πράξη το σχετικό νομοθετικό πλαίσιο έχει τροποποιηθεί, ώστε πλέον περιλαμβάνει και πράξεις σε βαθμό πλημμελήματος, οι

οποίες, όπως τουλάχιστον προκύπτει από τις επαπειλούμενες από τον Νόμο ποινές, δεν μπορούν να θεωρηθούν ως ιδιαίτερα σοβαρά εγκλήματα, όπως ορίζει το Σύνταγμα (Μεταξάκης, 2018).

Πράγματι, η άρση του απορρήτου των επικοινωνιών για λόγους εθνικής ασφάλειας και για τη διακρίβωση εγκλημάτων ρυθμιζόταν μέχρι το 2022, από τους Ν 2225/1994 και 3115/2003 και από το ΠΔ 47/2005, το οποίο εκδόθηκε δυνάμει της εξουσιοδοτικής διάταξης του άρθρου 9 Ν 3115/2003.

Με το άρθρο 5 του Ν. 5002/2022, (ΦΕΚ Α`228/09.12.2022) με τον τίτλο « "Διαδικασία άρσης του απορρήτου των επικοινωνιών, κυβερνοασφάλεια καιπροστασία προσωπικών δεδομένων πολιτών", καταργήθηκαν τα άρθρα 3, 4, 5 και 7 του Ν. 2225/1994 περί άρσης του απορρήτου.

Συγκεκριμένα σύμφωνα με το άρθρο 6, Ν.5002/22 ,η άρση του απορρήτου των επικοινωνιών είναι επιτρεπτή για τη διακρίβωση των ακόλουθων κακουργημάτων:

α) των Κεφαλαίων Πρώτου, περί προσβολών του δημοκρατικού πολιτεύματος, Δεύτερου, περί προσβολών της διεθνούς υπόστασης της χώρας, Τέταρτου, περί εγκλημάτων κατά των πολιτειακών και πολιτικών οργάνων, Έκτου, περί εγκλημάτων κατά της δημόσιας τάξης, Ένατου, περί εγκλημάτων σχετικά με το νόμισμα, άλλα μέσα πληρωμής και ένσημα, Δέκατου Έκτου, περί εγκλημάτων κατά της σωματικής ακεραιότητας, Δέκατου Όγδοου, περί εγκλημάτων κατά της προσωπικής ελευθερίας, Δέκατου Ένατου, περί εγκλημάτων κατά της γενετήσιας ελευθερίας και εγκλημάτων οικονομικής εκμετάλλευσης της γενετήσιας ζωής, Εικοστού Δεύτερου, περί προσβολών ατομικού απορρήτου και επικοινωνίας, καθώς και των άρθρων 235, περί δωροληψίας υπαλλήλου, 236, περί δωροδοκίας υπαλλήλου, 237, περί δωροληψίας και δωροδοκίας δικαστικού λειτουργού, 264 περί εμπρησμού, 265 περί εμπρησμού σε δάση, 270 περί έκρηξης, 272 περί κατασκευής και κατοχής εκρηκτικών και εμπρηστικών υλών, 290 περί επικίνδυνων παρεμβάσεων στην οδική συγκοινωνία, 291 περί επικίνδυνων παρεμβάσεων στη συγκοινωνία μέσων σταθερής τροχιάς, πλοίων και αεροσκαφών, 299 περί ανθρωποκτονίας με δόλο, 374 περί διακεκριμένης κλοπής, 380 περί ληστείας, 385 περί εκβίασης, 386 περί απάτης και 386Α περί απάτης με υπολογιστή του Ειδικού Μέρους του Ποινικού Κώδικα (ν. 4619/2019, Α' 95),

β) του Πρώτου Κεφαλαίου, περί προσβολών κατά της ακεραιότητας της χώρας, καθώς και των άρθρων 46, περί στάσης, 47, περί ομαδικής απείθειας, 140, περί αποσφράγισης, υπεξαγωγής εγγράφων ή άλλων αντικειμένων και 144, περί μετάδοσης

στρατιωτικών μυστικών, του Ειδικού Μέρους του Στρατιωτικού Ποινικού Κώδικα (ν. 2287/1995, Α' 20),

γ) του ν. 4557/2018 (Α' 139), περί νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες και χρηματοδότησης της τρομοκρατίας, της περ. γ' της παρ. 1 του άρθρου 157 του Εθνικού Τελωνειακού Κώδικα (ν. 2960/2001, Α' 265), περί λαθρεμπορίας, των άρθρων 28 και 31 του ν. 4443/2016 (Α' 232), περί αξιόποινων πράξεων προσώπων που κατέχουν προνομιακές πληροφορίες και περί αξιόποινης χειραγώγησης της αγοράς, αντιστοίχως, του άρθρου 15 του ν. 2168/1993 (Α' 147), περί όπλων, πυρομαχικών, εκρηκτικών υλών και εκρηκτικών μηχανισμών, των άρθρων 20, 22 και 23 του ν. 4139/2013 (Α' 74), περί εξαρτησιογόνων ουσιών, του άρθρου 11 του ν. 3917/2011 (Α' 22), περί δεδομένων που διατηρούνται από τον πάροχο υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιου δικτύου επικοινωνιών, της παρ. 5 του άρθρου 38 του ν. 4624/2019 (Α' 137), περί πρόσβασης σε δεδομένα προσωπικού χαρακτήρα, του άρθρου 28 του ν. 1650/1986 (Α' 160), περί προστασίας του περιβάλλοντος, του ν. 4858/2021 (Α' 220), περί προστασίας των αρχαιοτήτων και εν γένει της πολιτιστικής κληρονομιάς, της παρ. 3 του άρθρου 66 του ν. 2121/1993 (Α' 25), περί προστασίας της πνευματικής ιδιοκτησίας και των συγγενικών δικαιωμάτων, της παρ. 4 του άρθρου 132 του ν. 2725/1999 (Α' 121), περί δωροδοκίας-δωροληψίας για αλλοίωση αποτελέσματος αγώνα και του άρθρου 30 του ν. 4251/2014 (Α' 80), περί μεταφοράς υπηκόων τρίτων χωρών που δεν έχουν δικαίωμα εισόδου στη χώρα.

Η απαρίθμηση των αδικημάτων αυτών είναι περιοριστική, πράγμα που σημαίνει, ότι δεν μπορεί να αρθεί το απόρρητο για άλλα αδικήματα.

Περαιτέρω, με τον ίδιο Ν. 5002/2022 στο μεν άρθρο 3 τίθενται οι ορισμοί που χρησιμοποιούνται για τους σκοπούς του Νόμου, και δη α) «Λόγοι εθνικής ασφάλειας» είναι ... β) «Πολιτικά πρόσωπα» είναι ... ενώ στο άρθρο 4 γίνεται εξαντλητική περιγραφή της διαδικασίας άρσης του απορρήτου των επικοινωνιών για λόγους εθνικής ασφάλειας. Ειδικότερα, προσδιορίζονται τα όργανα που υποβάλλουν το αίτημα της άρσης, το περιεχόμενο του αιτήματος και της διάταξης που επιβάλλει ή απορρίπτει την άρση του απορρήτου. Επιπλέον, θεσπίζονται ειδικές ασφαλιστικές δικλίδες για την άρση του απορρήτου για τα πολιτικά πρόσωπα. Τέλος, προβλέπεται η διαδικασία γνωστοποίησης της επιβολής του περιοριστικού μέτρου στον θιγόμενο, κατά τρόπο που, όπως αναφέρεται παραπάνω, συναρθρώνονται αφενός μεν η προστασία της

εθνικής ασφάλειας, αφετέρου τα δικαιώματα του θιγόμενου πολίτη (1/2023 ΓΝΜΔ ΕΙΣΑΠ Ισίδωρου Ντογιάκου).

Πέραν τούτων, στο άρθρο 6 του ιδίου νόμου προβλέπονται οι προϋποθέσεις άρσης του απορρήτου των επικοινωνιών για τη διακρίβωση εγκλημάτων και εξορθολογίζεται ο κατάλογος των αδικημάτων για τη διακρίβωση των οποίων είναι δυνατό να αρθεί το απόρρητο των επικοινωνιών, στο πλαίσιο της συνταγματικής επιταγής «για διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων» και παράλληλα προβλέπεται η διαδικασία γνωστοποίησης επιβολής του περιοριστικού μέτρου στον θιγόμενο, ενώ στο άρθρο 8 περιγράφεται η διαδικασία για την άρση του απορρήτου, τόσο για λόγους εθνικής ασφάλειας όσο και για τη διακρίβωση εγκλημάτων. Ως προς τη διάρκεια της άρσης του απορρήτου, διευκρινίζεται ότι αυτή δεν μπορεί να υπερβαίνει τους δύο (2) μήνες και σε κάθε περίπτωση τους δέκα (10) μήνες συνολικά, αν έχουν δοθεί περισσότερες από μια παρατάσεις. Κατ' εξαίρεση, επιτρέπεται η υπέρβαση του ως άνω ορίου μόνο για λόγους εθνικής ασφάλειας και υπό συγκεκριμένες προϋποθέσεις. (Αιτιολογική Έκθεση ν. 5002/9-12-2022 σελ.47 επ.,βλ και ΠΡΑΚΤΙΚΑ ΒΟΥΛΗΣ, ΣΥΝΟΔΟΣ Δ` ΣΥΝΕΔΡΙΑΣΗ ΜΒ` Παρασκευή 9 Δεκεμβρίου 2022)

Ούτε το αδίκημα της εξύβρισης, ούτε το αδίκημα της συκοφαντικής δυσφήμησης (άρθρο 363 σε συνδυασμό με το άρθρο 362 ΠΚ) περιέχονται στα αδικήματα, για τη διακρίβωση των οποίων προβλέπεται σύμφωνα με τις διατάξεις του άρθρου 4 Ν 2225/1994, ούτε περιλήφθηκε στα εγκλήματα τα οποία ορίζει ο Ν.5002/22, η άρση του απορρήτου των επικοινωνιών. Για τον λόγο αυτόν, στις περιπτώσεις που το αδίκημα της συκοφαντικής δυσφήμησης τελείται μέσω του διαδικτύου, οι διωκτικές αρχές για την απαραίτητη άρση του απορρήτου των επικοινωνιών επικαλούνται τις γνωμοδοτήσεις υπ' αριθ. 9/2009, 12/2009 και 9/2011 των Εισαγγελέων του Αρείου Πάγου, οι οποίες όμως έρχονται σε πλήρη αντίθεση με τις διατάξεις των Ν 2225/1994 και 3115/2003 και του ΠΔ 47/2005. Εδώ θα πρέπει να ειπωθεί, ότι η αρμοδιότητα του Εισαγγελέως του Αρείου Πάγου να γνωμοδοτεί προβλέπεται στο άρθρο 25 παρ.2 Ν 1756/1988. Η πρακτική αυτή των διωκτικών αρχών είναι άκρως προβληματική, επειδή, ως γνωστόν, οι γνωμοδοτήσεις των Εισαγγελέων του Αρείου Πάγου δεν περιλαμβάνονται καν στην ιεραρχία των κανόνων δικαίου, όπως αυτή διαμορφώνεται

στην ημεδαπή έννομη τάξη, και επομένως αυτές δεν δύνανται να αντικαταστήσουν τυπικούς νόμους, όπως είναι ο Ν 2225/1994 (Μεταξάκης, 2018).

Τίθεται ερώτημα αν τα στοιχεία, που προκύπτουν από την άρση απορρήτου των επικοινωνιών καθ'υπέρβαση του άρθρου 19 παρ. 1 του Συντάγματος, είναι απαγορευμένα αποδεικτικά μέσα διάταξης του άρθρου 19 παρ. 3 του Συντάγματος, η οποία προβλέπει ότι "Απαγορεύεται η χρήση αποδεικτικών μέσων που έχουν αποκτηθεί κατά παράβαση του άρθρου αυτού και των άρθρων 9 και 9Α.", της διάταξης του άρθρου 117 παρ. 2 ΚΠΔ, σύμφωνα με την οποία "Αποδεικτικά μέσα που έχουν αποκτηθεί με αξιόποινες πράξεις ή μέσω αυτών, δεν λαμβάνονται υπόψη στην ποινική διαδικασία", αλλά και του γεγονότος, ότι αποδεικτικά μέσα αποκτηθέντα με αξιόποινες πράξεις αποτελούν απαγορευμένα αποδεικτικά μέσα, η λήψη υπ'όψη των οποίων στην ποινική διαδικασία αποτελεί απόλυτη ακυρότητα αυτής κατ'άρθρο 171 παρ. 1 περ. δ' ΚΠΔ . Πρέπει λοιπόν να ειπωθεί περαιτέρω:

Οι διωκτικές αρχές επικαλούνται τις Γνωμοδοτήσεις υπ' αριθ. 9/2009, 12/2009 και 9/2011 των Εισαγγελέων του Αρείου Πάγου για την άρση του απορρήτου των επικοινωνιών για τη διακρίβωση του αδικήματος της συκοφαντικής δυσφήμισης που τελείται μέσω του διαδικτύου. Με τη δε γνωμοδότηση 9/2009 του Εισαγγελέως του Αρείου Πάγου, υποστηρίχθηκε χωρίς κανένα πειστικό επιχείρημα ότι "1) Το απόρρητο των επικοινωνιών δεν καλύπτει α) την επικοινωνία μέσω του διαδικτύου (Internet) και β) τα εξωτερικά στοιχεία της επικοινωνίας (ονοματεπώνυμα και λοιπά στοιχεία συνδρομητών, αριθμοί τηλεφώνων, χρόνος και τόπος κλήσεως, διάρκεια συνδιάλεξης κ.λπ.)". Στη λογική της γνωμοδότησης αυτής κινήθηκαν και οι γνωμοδοτήσεις υπ'αριθ. 12/2009 και 9/2011 των Εισαγγελέων του Αρείου Πάγου (Μεταξάκης,2018).

Παρόλο που στο συγκεκριμένο θέμα υπάρχουν γνωμοδοτήσεις εισαγγελέων ΑΠ αυτές, αυτές δεν μπορεί να είναι δεσμευτικές. Στη συγκεκριμένη περίπτωση το απόρρητο επικοινωνίας δεν καλύπτει το περιεχόμενο του μηνύματος διότι αυτό είναι ήδη δημοσιευμένο, αλλά τα εξωτερικά στοιχεία επικοινωνίας. Στην έννοια των εξωτερικών στοιχείων επικοινωνίας περιλαμβάνονται οι διευθύνσεις IP, τα ηλεκτρονικά ίχνη που βοηθούν στην ταυτοποίηση του χρήστη με τον εξοπλισμό του, όπως είναι το MacAdress. Σύμφωνα με την Οδηγία 2006/24, τα στοιχεία αυτά πρέπει να διατηρούνται υποχρεωτικά. Αυτό σημαίνει ότι η διάθεση των στοιχείων για την ταυτοποίηση bloggers επιτρέπεται μόνο με τους όρους που επιβάλλει το 19 Σ: απόφαση δικαστικής αρχής και ιδιαίτερα σοβαρά εγκλήματα ή λόγοι εθνικής ασφάλειας.

Η αμφιβολία σχετικά με το εάν η άρση του απορρήτου των επικοινωνιών καταλαμβάνει και τα εξωτερικά στοιχεία της επικοινωνίας, δηλαδή σύμφωνα με τη νεότερη ορολογία, τα δεδομένα κίνησης και θέσης, έχει λυθεί μετά τη θέσπιση του ΠΔ 47/2005 και του Ν 3471/2006 (άρθρο 4 παρ. 1), από τις διατάξεις των οποίων προκύπτει αβιάστως ότι τα εν λόγω δεδομένα καλύπτονται από το απόρρητο των επικοινωνιών, για την άρση του οποίου πρέπει να τηρούνται οι τιθέμενες από το Ν 2225/1994 προϋποθέσεις, οι οποίες δεν έχουνε μεταβληθεί με τον Ν5002/22.

Δυστυχώς, και μετά τη θέσπιση των ανωτέρω νομοθετημάτων που έλυσαν τη σχετική αμφιβολία για τα δεδομένα κίνησης και θέσης, η αρεοπαγιτική νομολογία επιμένει ότι με την αρχή του άρθρου 18 του Συντάγματος "προστατεύεται το περιεχόμενο της επικοινωνίας και όχι η ύπαρξη αυτής και τα εξωτερικά της στοιχεία" .

Από όλα τα παραπάνω προκύπτει ότι η πρακτική των διωκτικών αρχών να αιτούνται την άρση του απορρήτου των επικοινωνιών παρακάμπτοντας την ισχύουσα νομοθεσία είναι όχι μόνο αξιόποινη, αλλά και ευθέως αντισυνταγματική. Για τον λόγο αυτόν και τα στοιχεία που προκύπτουν από την άρση απορρήτου των επικοινωνιών καθ'υπέρβαση του άρθρου 19 παρ. 1 του Συντάγματος είναι πράγματι απαγορευμένα αποδεικτικά μέσα και ως τέτοια, δεν μπορούν να ληφθούν υπ'όψιν στην ποινική διαδικασία, όπως ακριβώς ορίζει το άρθρο 177 παρ. 2 ΚΠΔ. Σε περίπτωση που παρά ταύτα ληφθεί υπ'όψη απαγορευμένο αποδεικτικό μέσο, θα υπάρχει, όπως προειπώθηκε, απόλυτη ακυρότητα κατ'άρθρο 171 παρ. 1 περ. δ' ΚΠΔ

-Οι στρεβλώσεις :

Ο συνδρομητής, τα στοιχεία του οποίου θα προκύψουν από την προπεριγραφείσα παράνομη άρση του απορρήτου των επικοινωνιών, πολλές φορές αιφνιδιάζεται, παραπεμπόμενος με απευθείας κλήση του στο ακροατήριο του καθ'ύλιν αρμοδίου μονομελούς πλημμελειοδικείου (άρθρα 53 παρ. 1 και 114 παρ. 1 ΚΠΔ) και εξ αυτού του λόγου εκμηδενίζεται το περιθώριο αντίδρασής του στην περιγραφείσα ανωτέρω απόλυτη ακυρότητα της προδικασίας (Μεταξάκης, 2018).

Πράγματι, η ανωτέρω ακυρότητα αποτελεί αναμφιβόλως ακυρότητα της προδικασίας, η οποία μπορεί να προταθεί μέχρι την αμετάκλητη παραπομπή του κατηγορουμένου στο ακροατήριο (άρθρο 173 παρ. 2 ΚΠΔ), δηλαδή εν προκειμένω

μέχρι την επίδοση σε αυτόν του κλητηρίου θεσπίσματος, άλλως αυτή καλύπτεται, όπως ορίζει το άρθρο 174 παρ. 1 ΚΠΔ, και ο κατηγορούμενος χάνει το δικαίωμα να προτείνει την ακυρότητα της προδικασίας στο αρμόδιο δικαστικό συμβούλιο κατ'άρθρο 176 παρ. 1 ΚΠΔ (Μεταξάκης, 2018).

Άλλωστε, υπάρχει δημοσιευμένο το ΒουλΣυμβΠλημΚεφαλ 84/2008: Στην προκείμενη περίπτωση, η εγκαλούσα ....., στις 23.12.2003, κατέθεσε απευθείας στον Εισαγγελέα Πλημμελειοδικών Κεφαλληνίας την από ίδια ημερομηνία (23.12.2003) έγκληση της, με την οποία ζητούσε τη διακρίβωση των στοιχείων ταυτότητας του αγνώστου, ο οποίος ισχυρίστηκε γι` αυτήν ψευδή γεγονότα, που μπορούσαν να βλάψουν την τιμή και την υπόληψη της, ενώ γνώριζε ότι τα γεγονότα αυτά δεν ήταν αληθινά, και την άσκηση ποινικής δίωξης σε βάρος αυτού για την αξιόποινη πράξη της συκοφαντικής δυσφήμησης. Ειδικότερα, στην ως άνω έγκλησή της, η εγκαλούσα εξέθεσε ότι άγνωστος, χρησιμοποιώντας τις υπηρεσίες του διαδικτύου, διακινούσε κείμενο, το οποίο, αναφερόμενο στο πρόσωπο της ανωτέρω εγκαλούσας, η οποία υπηρετούσε τότε ως αγροτικός ιατρός στη .... Κεφαλληνίας, είχε το ακόλουθο περιεχόμενο: «Προσοχή στη γιατρό του ...., ... Της έχουν αφαιρέσει την άδεια άσκησης επαγγέλματος στο ..... Ιταλίας από όπου την πήρε και έχουν γίνει μηνύσεις εναντίον της για τον τρόπο που πήρε την άδεια και το πτυχίο της (με μέσο). Το υπουργείο Υγείας δεν έχει ακόμη ενημερωθεί. Έχει αναλάβει το ελληνικό προξενείο του ..... Μέχρι να παρθούν μέτρα, ειδοποιήστε δικούς σας ανθρώπους στο Δήμο ..... Υπάρχουν ήδη καταγγελίες για θανάτους εφτά ανθρώπων από την περιοχή, γιατί δεν ήξερε τι να κάνει. Είναι επικίνδυνη». Η Εισαγγελέας Πλημμελειοδικών Κεφαλληνίας, κ. ....., αμέσως μόλις έλαβε την παραπάνω έγκληση, άσκησε (αυθημερόν), με την με ΑΒΜ ...../...../23.12.2003 παραγγελία της για διενέργεια προανάκρισης, ποινική δίωξη για την αξιόποινη πράξη της συκοφαντικής δυσφήμησης (άρθρα 1,14,16,17,18,26 παρ. 1 εδ. α`, 27,51,53,57,79,80 και 363 σε συνδυασμό με 362 ΠΚ), δηλαδή για πλημμέλημα αρμοδιότητας του Τριμελούς Πλημμελειοδικείου, χωρίς όμως προηγουμένως να έχουν ενεργηθεί προκαταρκτική εξέταση ή προανακριτικές πράξεις κατά την παρ. 2 του άρθρου 243 ή ένορκη διοικητική εξέταση. Σύμφωνα όμως και με όσα προεκτέθηκαν στη μείζονα σκέψη της παρούσας, η κίνηση ποινικής δίωξης στα πλημμελήματα αρμοδιότητας του Τριμελούς Πλημμελειοδικείου, χωρίς προηγουμένως να έχουν ενεργηθεί προκαταρκτική εξέταση ή προανακριτικές πράξεις κατά την παρ. 2 του άρθρου 243 ή ένορκη διοικητική εξέταση, είναι απολύτως άκυρη, κατ` άρθρο 171 παρ. 1 περ. β` ΚΠΔ, αφού υφίσταται περίπτωση μη τήρησης των διατάξεων που καθορίζουν

την κίνηση της ποινικής δίωξης από τον Εισαγγελέα. Στη συνέχεια δε και στα πλαίσια των παραγγελιών που δόθηκαν κατά τη διάρκεια της διενεργηθείσας προανά- κρισης, έλαβαν χώρα: 1) η από 12.3.2004 ένορκη εξέταση της εγκαλούσας ....., κατά την οποία προσκόμισε αυτή: α`) Το με αριθμ. πρωτ.... /24.7.2002 έγγραφο του Πανεπιστημίου του .., β`) το με αριθμ. πρωτ. .../25.7.2002 έγγραφο του Πανεπιστημίου του ..., γ`) το από 23.9.2002 έγγραφο του Υπουργείου Υγείας - τμήμα Υγειονομικού Κανονισμού,Έρευνας και Οργάνωσης του υπουργείου - Γενική Διεύθυνση Ανθρωπίνων Πόρων και Ιατρικών Επαγγελμάτων - Γραφ. /...../..... και δ`) η με αριθμ. πρωτ. .../29.10.2002 απόφαση περί χορήγησης άδειας άσκησης ιατρικού επαγγέλματος. 2) Η από 2.8.2004 συμπληρωματική ένορκη εξέταση της ίδιας ως άνω (εγκαλούσας). 3) Η από 13.3.2004 ένορκη εξέταση του ..... 4) Η από 15.6.2004 συμπληρωματική ένορκη εξέταση του ίδιου ως άνω μάρτυρα (.....). 5) Η από 21.8.2004 έκθεση εργαστηριακής εξέτασης του τομέα Εξέτασης Ψηφιακών Πειστηρίων του Εργαστηρίου Δικαστικής Γραφολογίας, Πλαστότητας Εντύπων και Αξιών της Διεύθυνσης Αστυνομίας. 6) Η με αριθμ. πρωτ. .../13.4.2005 αίτηση δικαστικής συνδρομής προς τις αρμόδιες δικαστικές αρχές της Ιταλίας και η με αριθμ. πρωτ. .../13.4.2005 αίτηση προς το τμήμα Ειδικών Ποινικών Υποθέσεων και Διεθνούς Δικαστικής Συνεργασίας της Διεύθυνσης Απονομής Χάριτος και Διεθνούς Δικαστικής Συνεργασίας της Γενικής Διεύθυνσης Διοίκησης Δικαιοσύνης του Υπουργείου Δικαιοσύνης. 7) Το με αριθμ. πρωτ. .../30.5.2008 έγγραφο του τμήματος Ειδικών Ποινικών Υποθέσεων και Διεθνούς Δικαστικής Συνεργασίας της Διεύθυνσης Απονομής Χάριτος και Διεθνούς Δικαστικής Συνεργασίας της Γενικής Διεύθυνσης Διοίκησης Δικαιοσύνης του υπουργείου Δικαιοσύνης περί περαίωσης αιτήματος δικαστικής συνδρομής των Ελληνικών Αρχών (Πταισματοδικείο Σάμης) από τις ιταλικές αρχές, με το με αριθμ..... /4.5.2006 έγγραφο του Υπουργείου Δικαιοσύνης της Ιταλίας και τα συνημμένα σε αυτό έγγραφα, από τα οποία προκύπτει ότι το αίτημα δικαστικής συνδρομής περαιώθηκε. 8) Η από 5.9.2008 εξέταση κατηγορουμένου (απολογία) του ....., κατοίκου ..... Αττικής (οδός.., αριθμ....), με τα συνημμένα σ` αυτήν έγγραφα. Κατ` ακολουθία, πρέπει να κηρυχθούν άκυρες τόσο η ασκηθείσα ποινική δίωξη (με ΑΒΜ ...../...../23.12.2003) για την αξιόποινη πράξη της συκοφαντικής δυσφήμησης, που φέρεται ότι τέλεσε το Δεκέμβριο του έτους 2003 (4.9.2003), ο ....., κάτοικος .....Αττικής, οδός.., αριθμ..., όσο και οι ανωτέρω, με αριθμούς 1 έως 8, εξαρτημένες από αυτήν μεταγενέστερες πράξεις της ποινικής διαδικασίας ως συνιστώσες το αναγκαίο αποτέλεσμα της άκυρης ποινικής

δίωξης, αφού παρήχθησαν συνεπεία αυτής (άκυρης ποινικής δίωξης), η οποία και αποτέλεσε δικονομική προϋπόθεση και λογικό νόμιμο όρο των μεταγενέστερων αυτών πράξεων.

Ενδιαφέρουσα είναι η ΑΠ 1411/2003, η οποία έκρινε ότι δεν υπάρχει απόλυτη ακυρότητα στην περίπτωση που αξιοποιείται εις βάρος του κατηγορούμενου κατάθεση με υφαρπαγείσες υφαρπαγές συνομιλίας συγκατηγορουμένων του και τηλεφωνικές υποκλοπές μέσω πομπού, χωρίς να τηρηθούν οι νόμιμες διατυπώσεις. «Από την επιτρεπτή επισκόπηση της καταθέσεως του εν λόγω μάρτυρα, προκειμένου να ελεγχθεί η βασιμότητα του ως άνω λόγω ακυρότητας, δεν προκύπτει τίνος συνομιλία επικαλέσθηκε ο εν λόγω μάρτυρας από τον πομπό ανοιχτής ακροάσεως, συγκατηγορουμένων ή ατόμων που συνεργαζόταν με την αστυνομία και επέβαιναν του αυτοκινήτου, ενόψει του ότι το αυτοκινήτου στο οποίο είχε τοποθετηθείο ανοικτός πομπός ήταν των ανθρώπων που συνεργαζόταν με την αστυνομία και προφανώς τελούσαν εν γνώσει αυτού και η παρακολούθηση των συνομιλιών τους γινόταν εν γνώσει τους και δεν συνέτρεχε περίπτωση παράνομης παρακολουθήσεως».

Αντιθέτως, σύμφωνα με την ΑΠ 1568/2004: Αποδεικτικά μέσα που έχουν αποκτηθεί με αξιόποινες πράξεις ή μέσω αυτών δεν λαμβάνονται υπόψη από το δικαστήριο, εκτός αν πρόκειται για κακουργήματα που τιμωρούνται με ισόβια κάθειρξη. Δημιουργήθηκε απόλυτη ακυρότητα, αφού το δικαστήριο καταδικάζοντας τον κατηγορούμενο για απάτη σχετικά με τις ασφάλειες έλαβε υπόψη του ένορκη κατάθεση μάρτυρα, η οποία ανέφερε ότι ο μάρτυρας όσα γνωρίζει ήταν αντικείμενο παρακολούθησης συνομιλίας του κατηγορουμένου (στην προκείμενη περίπτωση της προσβαλλόμενης απόφασης για την κήρυξη της ενοχής του ελήφθη υπόψη και η ένορκη κατάθεση της μάρτυρος στην κατάθεσή της ενώπιον του πρωτοβάθμιου δικαστηρίου, που βεβαιώνεται στην προσβαλλόμενη απόφαση ότι αναγνώσθηκε στο ακροατήριο, στην οποία αυτή αναφέρει ότι «άκουγε τις συνομιλίες του αναιρεσείοντος, της ....., του ..... κ.λ.π. από 100 μέτρα απόσταση με ειδικό μηχάνημα που διαθλά τη φωνή» ήτοι έλαβε υπόψη της απαγορευμένο αποδεικτικό μέσο).

Επίσης, σύμφωνα με το 50/2022 βούλευμα του Συμβουλίου Πλημμελειοδικών Κω:

«Προς υλοποίηση της λεπτής αυτής στάθμισης, ο νομοθέτης θέσπισε με τις ως άνω παρατιθέμενες διατάξεις του Ν. 2225/94 κανόνες για τη νόμιμη κτήση αποδεικτικών μέσων που ανάγονται στην σφαίρα του απορρήτου επικοινωνιών και ταυτόχρονα αποδεικτικές απαγορεύσεις. Ειδικότερα, διά των ως άνω αναφερομένων διατάξεων ο νομοθέτης ρυθμίζει τις περιπτώσεις νόμιμης κτήσης και νόμιμης αξιοποίησης νομίμως κτηθέντων αποδεικτικών μέσων, με κάμψη του δικαιώματος του απορρήτου των επικοινωνιών και ταυτόχρονα, με τις ίδιες διατάξεις, υπό την αντίστροφη όψη τους, προβλέπονται αποδεικτικές απαγορεύσεις δύο ειδών. Απαγορεύσεις κτήσης και απαγορεύσεις αξιοποίησης ήδη κτηθέντων αποδεικτικών μέσων. Πιο συγκεκριμένα, στο άρθρο 4 του Ν. 2225/94 προβλέπονται περιοριστικά οι προϋποθέσεις νόμιμης κτήσης αποδεικτικών μέσων που εμπίπτουν στο πεδίο του απορρήτου των επικοινωνιών. Εξ αντιδιαστολής, προκύπτει ότι η κτήση τέτοιων αποδεικτικών μέσων, χωρίς να πληρούνται οι προϋποθέσεις που οι διατάξεις του άρθρου αυτού προβλέπουν, απαγορεύεται, και η κτήση τους κατά παράβαση αυτών τα καθιστά παράνομα αποδεικτικά μέσα. Στην περίπτωση, όμως, που το αποδεικτικό μέσο αποκτηθεί υπό της προϋποθέσεις που προβλέπουν οι διατάξεις του άρθρου 4 Ν. 2225/1994, τότε αυτό έχει το χαρακτήρα του νομίμως κτηθέντος αποδεικτικού μέσου και μπορεί κατ' αρχήν ελεύθερα να αξιοποιηθεί σε κάθε ποινική διαδικασία, εκτός αν από το νόμο προβλέπεται κάποια ρητή απαγόρευση αξιοποίησής του. Εξάλλου, στο άρθρο 5 παρ. 10 του Ν. 2225/1994 προβλέπεται τέτοια ρητή απαγόρευση αξιοποίησης νομίμως κτηθέντος αποδεικτικού μέσου. Κρίσιμη είναι η οριοθέτηση του πεδίου εφαρμογής της εν λόγω απαγόρευσης, καθώς για κάθε περίπτωση που εμπίπτει στη διάταξη αυτή απαγορεύεται η αξιοποίηση ενός αποδεικτικού μέσου παρά το γεγονός ότι αυτό αποκτήθηκε νομίμως, ενώ για κάθε περίπτωση που εκφεύγει του πεδίου εφαρμογής της συνεχίζει να ισχύει ο κανόνας ότι το νομίμως αποκτηθέν αποδεικτικό μέσο νομίμως αξιοποιείται ελεύθερα. Από τη διατύπωση της διάταξης του άρθρου 5 παρ. 10 του Ν. 2225/1994, στην οποίαν ορίζεται ότι: "Το περιεχόμενο της ανταπόκρισης ή επικοινωνίας, το οποίο έγινε γνωστό λόγω της άρσης του απορρήτου, καθώς και κάθε άλλο σχετικό με αυτή στοιχείο απαγορεύεται, με ποινή ακυρότητας, να χρησιμοποιηθεί και να ληφθεί υπόψη ως άμεση ή έμμεση απόδειξη σε άλλη ποινική, πολιτική, διοικητική και πειθαρχική δίκη και διοικητική διαδικασία για σκοπό διαφορετικό από εκείνον που είχε καθορισθεί με τη

διάταξη. [...]" προκύπτει ότι η απαγόρευση αξιοποίησης θεμελιώνεται όταν συντρέχουν σωρευτικά οι εξής προϋποθέσεις: α) το αποδεικτικό μέσο πρόκειται να αξιοποιηθεί σε άλλη ποινική δίκη και β) το αποδεικτικό μέσο πρόκειται να αξιοποιηθεί για σκοπό διαφορετικό από εκείνον που είχε καθορισθεί με τη διάταξη».

Σε πολλές περιπτώσεις κατά τις οποίες εντοπίζεται μια ποινικώς ενδιαφέρουσα ηλεκτρονική επικοινωνία και δεν υπάρχει το νομιμοποιητικό βούλευμα του για την άρση του απορρήτου, η παρανόμως κτηθείσα πληροφορία από την παρακολούθηση της ηλεκτρονικής επικοινωνίας, παρουσιάζεται στο αιτιολογικό της δικαστικής απόφασης ως αποδεικτική πληροφορία που αποκτήθηκε όχι με τον πραγματικό τρόπο που περιγράφηκε, αλλά μέσα από την κατάθεση του αστυνομικού που έκανε την έρευνα, νομιμοποιείται δηλαδή η υποκλαπείσα ηλεκτρονική επικοινωνία, δίνοντας κιόλας την ψευδαίσθηση ότι η κατάθεση είναι δικονομικά συνεπής. Με αυτόν τον τρόπο έχουμε μια πολυεπίπεδη προσβολή των ατομικών δικαιωμάτων του κατηγορουμένου, τόσο σε δικονομικό επίπεδο (καθώς πλήττεται το δικαίωμα υπεράσπισης του), όσο και σε αυτό των ατομικών ελευθεριών και των προσωπικών δεδομένων (Παπαδόπουλος, 2020).

Υπάρχει και η άποψη ότι το εγκληματικό περιεχόμενο, εφόσον είναι το ίδιο εγκληματικό, δεν μπορεί να είναι αντικείμενο προστασίας από το 19 παρ. 3 Σ, αλλά αυτό δεν είναι ορθό διότι δεν μπορεί να θεωρηθεί από την αρχή αξιόποινη μια επικοινωνία, μόνο επειδή την έχει καταγγείλει κάποιος, καθώς καταλύει κάθε έννοια δικαστικής κρίσης και λειτουργεί εις βάρος του τεκμηρίου αθωότητας (Παπαδόπουλος, 2020).

Ο γενικός κανόνας που επικρατεί είναι ότι η απαγόρευση του 19 παρ 3 Σ, είναι καταρχήν απόλυτη, χωρίς εξαιρέσεις, άρα κάθε αντίθετη διάταξη νόμου είναι αντισυνταγματική. Με βάση όμως την αρχή της αναλογικότητας του 25 παρ 1 Σ για την προστασία της αξίας του ατόμου, μπορεί να επιτραπεί μόνο στην περίπτωση που το παράνομο αποδεικτικό μέσο είναι ο μόνος τρόπος για την απόδειξη αθωότητας του κατηγορουμένου.

Σχεδόν κατά κανόνα η ποινική δίωξη μπορεί να προσωποποιηθεί μόνο μετά την επιτυχή άρση του απορρήτου των επικοινωνιών, καθώς πολλές εγκλήσεις για συκοφαντική δυσφήμιση μέσω του διαδικτύου υποβάλλονται κατ' αγνώστων. Επομένως, τα στοιχεία που προκύπτουν από την άρση του απορρήτου των

επικοινωνιών δεν είναι απλά αποδεικτικά μέσα, αλλά απολύτως ουσιώδη αποδεικτικά μέσα, αφού βάσει αυτών κατονομάζονται οι φερόμενοι ως δράστες.

Περαιτέρω, αρκετά συχνά, οι πραγματικοί δράστες του υπό εξέταση αδικήματος να αξιοποιούν ασύρματα δίκτυα, να αποκτούν σύνδεση σε αυτά, να διαπράττουν την αξιόποινη πράξη της συκοφαντικής δυσφήμισης μέσω του διαδικτύου ενόσω είναι συνδεδεμένοι με το ασύρματο δίκτυο ξένου και αμέτοχου στην αξιόποινη πράξη συνδρομητή, έτσι ώστε, όταν πραγματοποιηθεί η άρση απορρήτου των τηλεπικοινωνιών, να εμφανίζεται η διεύθυνση διαδικτυακού πρωτοκόλλου [αγγλ. Internet protocol (IP) address] του αμέτοχου αυτού συνδρομητή, συνήθως κάποιου επαγγελματία, ο οποίος παρέχει δωρεάν σύνδεση στο διαδίκτυο στους πελάτες της επιχείρησής του (Μεταξάκης, 2018).

Όπως είναι απολύτως φυσικό, σε τέτοιες περιπτώσεις ο αμέτοχος συνδρομητής, τα στοιχεία του οποίου θα προκύψουν από την άρση του απορρήτου των επικοινωνιών, σε περίπτωση απευθείας παραπομπής του στο ακροατήριο θα απωλέσει όχι μόνο τη δυνατότητα να προτείνει την εμφιλοχωρήσασα στην ποινική διαδικασία προπεριγραφείσα απόλυτη ακυρότητα, αλλά και να εκθέσει τους ισχυρισμούς του, όπως σε περίπτωση ενέργειας προκαταρκτικής εξέτασης. (Μεταξάκης, 2018).

Για να εξαλειφθούν οι προεκτεθείσες στρεβλώσεις ως προς την αντιμετώπιση του αδικήματος της συκοφαντικής δυσφήμισης, όταν αυτό τελείται μέσω του διαδικτύου, είναι επιβεβλημένη: α) η τροποποίηση του Ν.5002/22, ώστε να περιλαμβάνει και το αδίκημα του άρθρου 363 ΠΚ και β) η διενέργεια προκαταρκτικής εξέτασης, ώστε να μην παραπέμπονται δίχως άλλο στο ακροατήριο όλοι όσων τα στοιχεία προκύπτουν από την άρση του απορρήτου των επικοινωνιών.

Καλό θα ήταν να ληφθεί σοβαρά υπόψιν σε μελλοντική αναθεώρηση του Συντάγματος, το οποίο στο άρθρο 19 παρ. 1 αυτού προβλέπει ότι "Νόμος ορίζει τις εγγυήσεις υπό τις οποίες η δικαστική αρχή δεν δεσμεύεται από το απόρρητο για λόγους εθνικής ασφάλειας ή για διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων." και για τον λόγο αυτόν εμφανίζεται άκρως προβληματική η συμπερίληψη στο άρθρο 4 Ν 2225/1994 αξιόποινων πράξεων όχι μόνο ιδιαίτερα σοβαρών, ήτοι σε βαθμό κακουργήματος, αλλά και ήσσονος σοβαρότητας, ήτοι σε βαθμό πλημμελήματος. (Μεταξάκης, 2018)

Οι αποδεικτικές απαγορεύσεις συνιστούν τόσο νομοθετικό, όσο και νομολογιακό διακύβευμα. Συνδέονται άμεσα με τη δίκαιη δίκη. Με βάση τις σύγχρονες δικαιοπολιτικές αντιλήψεις η αναζήτηση της αλήθειας στην ποινική δίκη δεν μπορεί να προωθείται άνευ ορίων και με κάθε μέσο. Η ανάγκη προστασίας υπέρτερων αξιών και εννόμων αγαθών, νομιμοποιεί τη θέσπιση περιορισμών στην ανάγκη δικαστικής διερεύνησης και στην εν γένει αποδεικτική διαδικασία που εισάγονται με τη θέσπιση και αναγνώριση των αποδεικτικών απαγορεύσεων. Οι αποδεικτικές απαγορεύσεις συνιστούν δικαιϊκούς περιορισμούς που αφορούν την απόκτηση και την αξιοποίηση των αποδείξεων, ενώ εκτείνονται σε όλο το φάσμα της αποδεικτικής διαδικασίας. Επίσης, θεωρούνται ως ενσάρκωση του φιλελευθέρου χαρακτήρα της ποινικής δίκης που αξιώνει να υπάρχει ένα δομημένο δικανικό σχήμα με δικονομικούς τύπους, διαδικαστικούς ρόλους, δικονομικές λειτουργίες, αλλά και όρια επεμβάσεων. Σε αντίθεση με το γερμανικό νομικό σύστημα, στην Ελλάδα οι αποδεικτικές απαγορεύσεις τίθενται νομοθετικά. Υπάρχει πλέον μια τάση εξίσωσης, να γίνονται δεκτά παράνομα αποδεικτικά μέσα, όχι μόνο όταν είναι το μοναδικό μέσο για να αποδειχθεί η αθωότητα του κατηγορούμενου, αλλά και όταν είναι το μόνο μέσο για να αποδειχθεί η ενοχή (Δαλακούρας, 2024).

Το «κακό» είναι ότι ο Έλληνας συνταγματικός νομοθέτης με το 19 παρ.3 Σ θέσπισε εξαρτημένη αποδεικτική απαγόρευση, την εξάρτηση από την απαγόρευση των 9, 9^{A} και 19Σ. Η διάταξη του 19 παρ3 Σ βαρύνεται με τη μορφή της απολυτότητας και της διάσπασης της άτυπης αξιακής συνταγματικής κλίμακας. Η παράλειψη της κυρωτικής δομής της και η παράκαμψη της συνταγματικής λειτουργίας της με τη θέσπιση εξαιρέσεων του κοινού νόμου, βαρύνεται με αυθαιρεσία και μπορεί να οδηγήσει σε ύβρη κατά του Συντάγματος. Τα κριτήρια της αρχής της αναλογικότητας υπερισχύουν πάντα θέτοντας σε προτεραιότητα το 19 παρ 3 Σ. Γενικά, όσο περισσότερο οχυρώνεται και εμπεδώνεται η αξία των αποδεικτικών απαγορεύσεων, τόσο πιο πολύ οχυρώνεται το δικονομικό σύστημα, ώστε να πάρει έτσι το κύρος που του αρμόζει (Δαλακούρας, 2024)

Ο νόμος που προβλέπει την άρση του απορρήτου επικοινωνιών πρέπει να είναι εξειδικευμένος και σαφής αναφορικά με τον προσδιορισμό των αδικημάτων για τα οποία χορηγείται η δυνατότητα της άρσης. Αν ο νόμος είναι γενικόλογος ως προς τις προϋποθέσεις άρσης του απορρήτου τότε δεν έχει να απαιτούμενη σαφήνεια και προβλεψιμότητα που επιβάλλεται να έχει ένας κανόνας δικαίου για να θεωρηθεί ως

νόμος θεμιτός περιορίζων δικαίωμα κατοχυρωμένο μάλιστα τόσο από την ΕΣΔΑ όσο και από το ίδιο το Σύνταγμα. Κατ' ακολουθίαν ένας τέτοιος νόμος δεν είναι συμβατός με την αρχή της ασφαλείας του δικαίου, που αποτελεί βασική αρχή της έννοιας του κράτους δικαίου (Μαργελής, 2022).

Υπάρχουν επίσης και κάποια άλλα τεχνικά ζητήματα, όπως το αν θα βρεθεί αποδεικτικό υλικό στο server. Δεν πρέπει να λησμονούμε ότι η IP διεύθυνση περιορίζει τον χώρο αναζήτησης, δε σχετίζεται απαραίτητα με την ταυτότητα, ποτέ δεν μπορούμε να είμαστε σίγουροι για το ποιος είναι κρυμμένος πίσω από μια οθόνη υπολογιστή, ακόμα και αν εντοπίσουμε την IP (τι κάνουμε άραγε στην περίπτωση που εντοπίζεται η IP, αλλά ζουν 3 άτομα σε ένα νοικοκυριό με κοινόχρηστο υπολογιστη;). Επίσης, όταν γίνεται η εξύβριση δια των μέσων κοινωνικής δικτύωσης όπως το Facebook, καθώς το τελευταίο διέπεται από το αμερικάνικο δίκαιο, δε γνωρίζουμε αν θα δώσει ποτέ τα στοιχεία του αυτουργού, καθώς στο Αμερικάνικο Δίκαιο, δεν αποτελούν ποινικά αδικήματα τα εγκλήματα κατά της τιμής.

6 Μέτρα προστασίας από bullying

6.1 Μέτρα που λαμβάνουν τα ίδια τα ΜΚΔ για αντιμετώπιση εκφοβισμού

Το ίδιο το Facebook έχει δημιουργήσει το Κέντρο πρόληψης του εκφοβισμού, https://www.facebook.com/safety/bullying/ το οποίο αποτελεί πηγή πληροφοριών για εφήβους, γονείς και εκπαιδευτικούς που χρειάζονται υποστήριξη για θέματα που αφορούν τον εκφοβισμό και άλλες διενέξεις. Παρέχει αναλυτική καθοδήγηση, όπως μεταξύ άλλων πληροφορίες για το πως μπορεί κανείς να ανοίξει σημαντικές συζητήσεις για τον εκφοβισμό.

Παγκόσμια μέτρα προστασίας για όλους:

Όλοι προστατεύονται από ανεπιθύμητη επικοινωνία που μπορεί να είναι:

- Επαναλαμβανόμενη
- Σεξουαλική παρενόχληση
- Απευθύνεται σε έναν μεγάλο αριθμό ατόμων χωρίς να έχει εξασφαλιστεί εκ των προτέρων η άδειά τους
- Ευχές για τον αυτοτραυματισμό ή την αυτοκτονία ενός συγκεκριμένου ατόμου ή μιας ομάδας ατόμων.

- Επιθέσεις με βάση την εμπειρία του ατόμου σχετικά με τη σεξουαλική επίθεση, τη σεξουαλική εκμετάλλευση, τη σεξουαλική παρενόχληση ή την ενδοοικογενειακή βία.
- Δηλώσεις για πρόθεση εμπλοκής σε σεξουαλική δραστηριότητα ή υποστήριξη εμπλοκής σε σεξουαλική δραστηριότητα.
- Έντονα σεξουαλικά σχόλια.
- Υποτιμητικές επεξεργασμένες εικόνες ή σχέδια με σεξουαλικό περιεχόμενο
- Επιθέσεις σε κάποιον με προσβλητικούς όρους που σχετίζονται με τη σεξουαλική δραστηριότητα
- Ισχυρισμοί άρνησης κάποιας βίαιας τραγωδίας.
- Ισχυρισμοί ότι τα θύματα κάποιας βίαιας τραγωδίας ή τρομοκρατικής επίθεσης ψεύδονται για την ιδιότητά τους, συμπεριλαμβανομένων ισχυρισμών ότι τα άτομα αυτά: Παριστάνουν ότι είναι θύματα κάποιου συγκεκριμένου συμβάντος, ή έχουν πληρωθεί ή προσληφθεί από τρίτους για να παραπλανήσουν το κοινό σχετικά με τον ρόλο τους στο συμβάν.
- Απειλές κοινοποίησης του προσωπικού αριθμού κινητού, της διεύθυνσης κατοικίας, της διεύθυνσης email ή του ιατρικού φακέλου κάποιου ατόμου (όπως ορίζεται στην πολική για τις Παραβιάσεις απορρήτου).
- Παρότρυνση τρίτων να προβούν σε πράξεις εκφοβισμού ή/και παρενόχλησης ή δήλωση της πρόθεσης συμμετοχής σε τέτοιου είδους πράξεις.
- Περιεχόμενο που υποβιβάζει ή εκφράζει αηδία απέναντι σε άτομα που απεικονίζονται σε διαδικασία έμμηνου ρύσης, ούρησης, εμετού ή αφόδευσης, ή αμέσως μετά από αυτές τις διαδικασίες.

Όλοι προστατεύονται από τις ακόλουθες περιπτώσεις, εξαιρουμένων των ενήλικων δημόσιων προσώπων που πρέπει να εκτίθενται σκοπίμως σε:

-Ευχές για θάνατο, προσβολή από ασθένεια ή εμφάνιση ιατρικής πάθησης.

- Εορτασμό ή χλευασμό για τον θάνατο ή για κάποια ιατρική πάθηση.

-Ισχυρισμούς για σεξουαλικά μεταδιδόμενα νοσήματα.

-Υποτιμητικοί υβριστικοί όροι που σχετίζονται με το γυναικείο φύλο.

-Δηλώσεις κατωτερότητας με βάση την εξωτερική εμφάνιση.

Σχεδόν ταυτόσημη πολιτική ακολουθεί και το Instagram, το οποίο πλέον ανήκει στον ίδιο όμιλο Meta του Facebook. Το Instagram μάλιστα τώρα τελευταία, διαθέτει μια ρύθμιση, η οποία ονομάζεται Restrict (Περιορισμός) και επιτρέπει στους χρήστες να διαβάζουν τα DM (προσωπικά μηνύματα) χωρίς να το γνωρίζει ο αποστολέας (με αυτόν τον τρόπο, ο θύτης εκνευρίζεται που το θύμα δεν αντιδρά και έτσι το πιθανότερο σταματά την όποια προσπάθεια παρενόχλησης). Αυτή η ρύθμιση όμως δε θεωρείται και πολύ επιτυχημένη, γιατί επηρεάζει όλες τις επαφές που έχει ο χρήστης, τόσο ως προς τα εισερχόμενα, όσο και ως προς τα εξερχόμενα μηνύματα.

Πολιτική ανάλογη με του Facebook για τη ρητορική μίσους, διαθέτει και το X/Twitter (https://help.twitter.com/en/rules-and-policies/abusive-behavior)

6.2 Τι μπορούμε να κάνουμε γενικά όταν ερχόμαστε αντιμέτωποι με τους «νταήδες» του Διαδικτύου

Βήματα που πρέπει να ακολουθούνται όταν αντιμετωπίζουμε έναν διαδικτυακό εκφοβισμό

-Να έχουμε τη δύναμη να αντιμετωπίσουμε οποιονδήποτε στο Διαδίκτυο δε μας σέβεται.

-Επειδή μπορεί να είναι δύσκολο για τους εφήβους να ειδοποιήσουν κάποιον ενήλικα για βοήθεια σχετικά με τον διαδικτυακό εκφοβισμό, πρέπει οι ίδιοι να είναι προετοιμασμένοι να αντιμετωπίσουν το θέμα μόνοι τους. Όταν αντιμετωπίζουμε έναν διαδικτυακό εκφοβισμό, πρέπει να χρησιμοποιούμε την κοινή λογική: Παρόλο που είναι δύσκολο να αγνοηθούν τα προσβλητικά σχόλια, η τυχόν απάντηση μόνο θα ενθαρρύνει τη συμπεριφορά του εκφοβιστή. Πρέπει να αγνοούμε τον διαδικτυακό «νταή» που είναι αγενής.

-Διατηρούμε ένα σωστό αρχείο με όλα τα διαδικτυακά μηνύματα εκφοβισμού, σχόλια και άλλες μορφές παρενόχλησης με στιγμιότυπα οθόνης. Εάν πρέπει να αναφέρουμε τον εκφοβισμό στις αρχές, η τεκμηρίωση του περιστατικού είναι ζωτικής σημασίας.

Οι μεγαλύτεροι σε ηλικία, καλό είναι να σκέφτονται, ότι συνήθως ο έφηβος, δεν αναζητά εύκολα βοήθεια. Καλό είναι σε περίπτωση που υποψιαστούν ότι κάτι

συμβαίνει, να μιλήσουν άμεσα με το θύμα και να που ότι είναι σε θέση να προσφέρουν την οποιαδήποτε βοήθεια (Nikolaou, 2022).

6.3 Γενική προληπτική προστασία από παρενοχλήσεις

1. Επιλέγουμε ένα ουδέτερο όνομα χρήστη, e-mail κλπ. Αποφεύγουμε οτιδήποτε χαριτωμένο ή σεξουαλικό.
2. Διατηρούμε τη βασική μας διεύθυνση ηλεκτρονικού ταχυδρομείου μυστική. Να τη χρησιμοποιούμε μόνο με ανθρώπους που γνωρίζουμε και εμπιστευόμαστε.
3. Δημιουργούμε έναν άλλο λογαριασμό ηλεκτρονικής αλληλογραφίας τον οποίο χρησιμοποιούμε στις μη επαγγελματικές/εκπαιδευτικές on-line δραστηριότητές μας
4. Δε δίνουμε προσωπικές μας πληροφορίες απλά επειδή τις ζητάνε. Πολλοί δικτυακοί τύποι ζητάνε το πλήρες όνομά μας, ημερομηνία γέννησης, διεύθυνση, αριθμό τηλεφώνου, e-mail, κ.α. Το αποφεύγουμε όσο μπορούμε
5. Όταν συνομιλούμε σε ένα chat, μπλοκάρουμε χρήστες που ενοχλούν ρυθμίζοντας τους παραμέτρους του προγράμματος συνομιλίας που χρησιμοποιούμε.
6. Δεν επιτρέπουμε στους άλλους να δημιουργούν συγκρούσεις. Είναι προτιμότερο να μην ανοίξουμε διάλογο με κάποιον που επιτίθεται. Όταν αντιληφθεί ότι δεν αντιδρά το υποψήφιο θύμα, θα αναζητήσει άλλο στόχο.
7. Πριν λάβουμε μέρος σε οποιαδήποτε on-line δραστηριότητα, παρακολουθούμε για αρκετό χρονικό διάστημα το περιεχόμενο των συζητήσεων.
8. Εάν χρειαστεί αλλάζουμε το όνομα χρήστη για να αποφύγουμε κάποιον που παρενοχλεί, να φροντίζουμε ώστε το νέο όνομα να μην έχει καμιά σχέση με αυτό που χρησιμοποιούσαμε πριν.
9. Ποτέ δε χρησιμοποιούμε τα στοιχεία της εταιρείας που εργαζόμαστε (διεύθυνση, τηλέφωνο κ.λπ.) σε μια δημόσια συζήτηση στο διαδίκτυο
10. Ποτέ δε δίνουμε τον κωδικό πρόσβασης σε κανέναν.

(Βλαχόπουλος, 2007)

7 Επίλογος

Συμπερασματικά θα μπορούσαμε να πούμε: παρά το γεγονός ότι το φαινόμενο του διαδικτυακού εκφοβισμού έχει λάβει διαστάσεις επιδημίας την τελευταία δεκαετία, ο Έλληνας νομοθέτης δεν έχει ακόμη προβεί στην πρόβλεψη μιας ρητής νομοθετικής διάταξης που να ποινικοποιεί το cyberbullying. Δεν προβλέπεται ούτε με τον καινούριο Ποινικό Κώδικα. Μια τέτοια νομοθετική πρόβλεψη, κατά πολλές απόψεις, θα μπορούσε να λειτουργήσει αποτρεπτικά για τους «υποψήφιους δράστες» για τη διάπραξη του αδικήματος, καθώς αυτό θα τυποποιούνταν νομοθετικά, άρα θα είχαν και τον φόβο της τιμωρίας. Όμως, καθημερινά βλέπουμε στην πράξη ότι έχουμε τέλεση εγκλημάτων, παρόλο που είναι τυποποιημένα σε άρθρα του Ποινικού Κώδικα. Επίσης, το αντικείμενο του διαδικτυακού εκφοβισμού είναι όπως έχει διαφανεί και με όσα εκτέθηκαν στην εργασία αχανές, άρα είναι δύσκολο να τυποποιηθεί και η αντικειμενική του υπόσταση ως έγκλημα. Επίσης, κατά άποψη πολλών, θα πρέπει να υπάρξει μια τροποποίηση στον Νόμο περί άρσης απορρήτου επικοινωνιών, ώστε να αφορά η άρση και στις περιπτώσεις εγκλημάτων κατά της τιμής, καθώς με το παρόν καθεστώς, οδηγούμαστε εύκολα σε παραβίαση του δικαιώματος προστασίας επικοινωνίας με εντολή για άρση απορρήτου χωρίς νόμο, αλλά μόνο με τις υφιστάμενες γνωμοδοτήσεις. Η υπέρμετρη επίσης άρση απορρήτου επικοινωνιών, για «ελαφρά» αδικήματα, όπως αυτό της προσβολής τιμής, μπορεί να οδηγήσει και σε επικίνδυνα μονοπάτια του περιορισμού της ελευθερίας έκφρασης. Επιπλέον, θα πρέπει να γίνει συνείδηση όλων, ότι όσο λιγότερο εκθέτουμε την προσωπική μας ζωή στα διαδίκτυο, τόσες λιγότερες πιθανότητες υπάρχουν να είμαστε θηράματα κακόβουλων συμπεριφορών.

Βιβλιογραφία

Ελληνικές

Αντωνιάδου Ν. και Κόκκινος Μ., 2013, *Κυβερνο-εκφοβισμός και κυβερνοθυματοποίηση σε παιδιά και εφήβους: Συχνότητα εμφάνισης και παράγοντες επικινδυνότητας. Προσχολική & Σχολική Εκπαίδευση*

Βλαχόπουλος Κ., 2007, *Ηλεκτρονικό έγκλημα: μορφές, πρόληψη, αντιμετώπιση*, Νομική Βιβλιοθήκη

Δαγτόγλου Π., 2005, *Συνταγματικό Δίκαιο* , Σάκκουλας

Δαλακούρας Θ. 2019, *Ηλεκτρονικό Έγκλημα (Κεφάλαια: Δαλακούρας, Καργόπουλος, Μοροζίνης)*, Νομική Βιβλιοθήκη

Ιγγλεζάκης Ι., 2018, *Δίκαιο και Πληροφορική* , Σάκκουλας

Καστανίδου Ε., 1999,*Ποινικό Δίκαιο*, Σάκκουλας

Κοτσαλής Λ.,2018 ,*Γενικός Κανονισμός για την προστασία Δεδομένων (Κεφάλαιο Βλαχόπουλος)* , Νομική Βιβλιοθήκη

Λάζος Γ.,2001,*Πληροφορική και έγκλημα* , Νομική Βιβλιοθήκη

Μαργαρίτης Μ., 2020, *Ποινικός Κώδικας (Ερμηνεία)* , Σάκκουλας

Παπαδόπουλος Θ., 2020, *Ηλεκτρονικά εγκλήματα. Η ανακριτική διερεύνηση υπό το φως των ατομικών δικαιωμάτων και της νομολογίας του ΕΔΔΑ*, Νομική Βιβλιοθήκη

Παραράς Π, 2001, *Σύνταγμα και Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου,* Σάκκουλας

Φράγκος Κ, 2020, *Ποινικός Κώδικας(Ερμηνεία),* Νομική Βιβλιοθήκη

Αρθρογραφία

Δαλακούρας*, Οι αποδεικτικές απαγορεύσεις ως σύγχρονο νομοθετικό και νομολογιακό διακύβευμα,* Ποινικά Χρονικά, 1/2024

Καραγκούνης, *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;,* ΔιΜΕΕ 3/2018

Ξένες

Alduailaj A, 2022, *Detecting Arabic Cyberbullying Tweets Using Machine Learning*

Ferrara P, 2014, *Childhood maltreatment and cyberbullying victimization: roles of maladaptive self-cognition and gender*

Kao DY,2008, *The IP address and time in cyber-crime investigation*

Kowalski R, 2014, *Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth*

Langos C., 2012, *Cyberbullying: The Challenge to Define*
, http://dx.doi.org/10.1089/cyber.2011.0588

Li S, 2022, *Childhood maltreatment and cyberbullying victimization: roles of maladaptive self-cognition and gender*

Macit, H. B., Macit, G., & Güngör, O., (2018), A Research on Social Media Addiction and Dopamine Driven Feedback. Doi https://dergipark.org.tr/en/pub/makuiibf/issue/41626/435845

Mc Quade, 2008, *Cyber bullying: protecting kids and adults from online bullies,* ,

Morales-Arjona M.,2022, *Characterization of Cyberbullying Victimization and Perpetration Before and During the COVID-19 Pandemic in Spain,* , DOI: 10.1089/cyber.2022.0041

Nikolaou D, 2021, *Bullying Cyberbullying and Young Health Behaviors*

Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S. and Tippett, N., 2008, *Cyberbullying: Its nature and impact in secondary school pupils*

Willard N.E.,2007, *Cyberbullying and cyberthreats: Responding to the challenge of online social aggression, threats, and distress*

Νομοθετήματα

Γενικός Κανονισμός για την Προστασία Δεδομένων

Ποινικός Κώδικας

Σύνταγμα της Ελλάδος

ΕΣΔΑ

Νομολογία

ΠολΠρΑθ 3667/2020

Τριμ.Εφ.Θες 2116/2020

ΜΠλημΒόλου 1456/2018

ΑΠ 509/2014

ΑΠ 1411/2003

ΑΠ 1568/2004

ΣυμβΠλημΚω 50/2022

ΑΠ 858/2020

ΑΠ 509/2014

ΒουλΣυμβΠλημΚεφαλ 84/2008

ΜονΠρΑθηνών 497/2017

Ιστοσελίδες

http://www.indeepanalysis.gr/koinwnia/kybernoekfobismos-mia-nea-morfi-bias

https://psychoedu.gr/o-kouloxeris-pou-exeis-panta-mazi-sou

https://ischool.uw.edu/news/2016/12/too-much-screen-time-could-lead-popcorn-brain

https://www.protothema.gr/world/article/1453523/i-lista-me-ti-simasia-ton-emojis-poia-boroun-na-se-steiloun-akoma-kai-fulaki/

https://www.coe.int/en/web/cyberviolence

https://www.constitutionalism.gr/2021-01-sotirelis-ap858-2020-misallodoxos-logos/

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

https://lawnet.gr/

https://www.facebook.com/safety/bullying

https://help.twitter.com/en/rules-and-policies/abusive-behavior

Άλλες πηγές

Μαργέλης Α., 2022, *Η άρση του απορρήτου των επικοινωνιών και η δικονομική αξιοποίηση των ευρημάτων*, Διπλωματική εργασία ΑΠΘ

Διαδικτυακό σεμινάριο CSI institute «Ψηφιακή Ακαδημία-Γίνε άνθρωπος»

Google form

https://docs.google.com/forms/d/1a1XDbavOsqSOeJ2ysSfcKIbfF76uFalerfQ2YltsbjM/edit?pli=1