ΠΑΝΤΕΙΟΝ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

PANTEION UNIVERSITY OF SOCIAL AND POLITICAL SCIENCES

ΣΧΟΛΗ ΚΟΙΝΩΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΚΟΙΝΩΝΙΟΛΟΓΙΑΣ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

«ΕΓΚΛΗΜΑΤΟΛΟΓΙΑ»

Το αδίκημα της έμμονης διαδικτυακής παρενοχλητικής παρακολούθησης («Cyberstalking») και η παραβίαση των ατομικών δικαιωμάτων που προκύπτει από τη διάπραξή του

The offense of online stalking (“Cyberstalking”) and the violation of individual rights resulting from its commission

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Μαρία-Νίκη Κ. Σκουφή

Αθήνα, 2023

Τριμελής Επιτροπή

Εριφύλη Μπακιρλή, Διδάκτωρ Εγκληματολογίας Παντείου Πανεπιστημίου (Επιβλέπουσα)

Χρήστος Τσουραμάνης, Ομότιμος Καθηγητής Πανεπιστημίου Πατρών

Γρηγόρης Λάζος, Καθηγητής Παντείου Πανεπιστημίου

Συντομογραφίες

Ελληνόγλωσσες

ΑΔΑΕ: Αρχή Διασφάλισης Απορρήτου Επικοινωνιών

ΑΚ: Αστικός Κώδικας

ΑΠΔΠΧ: Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

άρ.: άρθρο

ΓΚΠΔ: Γενικός Κανονισμός για την Προστασία των Δεδομένων

ΔΣΑΠΔ: Διεθνές Σύμφωνο για τα Ατομικά και Πολιτικά Δικαιώματα

εδ.: εδάφιο

ΕΔΔΑ: Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων

ΕΕ: Ευρωπαϊκή Ένωση

ΕλλΠΚ: Ελληνικός Ποινικός Κώδικας

ΕλλΣ: Ελληνικό Σύνταγμα

ΕΣΔΑ: Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου

ΗΕ: Ηνωμένα Έθνη

ΗΠΑ: Ηνωμένες Πολιτείες Αμερικής

Η/Υ: Ηλεκτρονικός Υπολογιστής

κ.ά.: και άλλα

ΚτΠ: Κοινωνία της Πληροφορίας

μ.ό.: μέσος όρος

ΟΗΕ: Οργανισμός Ηνωμένων Εθνών

ΟΟΣΑ: Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης

παρ.: παράγραφος

π.χ.: παραδείγματος χάριν

ΣΑΠΔ: Σύστημα Απονομής Ποινικής Δικαιοσύνης

ΣΛΕΕ: Συνθήκη Λειτουργίας της Ευρωπαϊκής Ένωσης

ΤΠΕ: Τεχνολογίες Πληροφοριών και Επικοινωνίας

ΧΘΔΕΕ: Χάρτης Θεμελιωδών Δικαιωμάτων Ευρωπαϊκής Ένωσης

Ξενόγλωσσες

CMC: Computer Mediated Communication

ICTs: Information and Communication Technologies

IM: Instant Messaging

ISP: Internet Service Provider

Περιεχόμενα

Περίληψη

Σκοπός της παρούσας διπλωματικής εργασίας είναι η ανάδειξη της έμμονης διαδικτυακής παρενοχλητικής παρακολούθησης («Cyberstalking») ως μια σχετικά πρόσφατη μορφή εγκληματικής συμπεριφοράς, η οποία προσβάλλει σημαντικά έννομα αγαθά, δικαιώματα και ελευθερίες του ατόμου. Η μεθοδολογία που ακολουθήθηκε στην παρούσα μελέτη περιλαμβάνει δευτερογενή έρευνα και συγκεκριμένα επισκόπηση της σχετικής βιβλιογραφίας/αρθρογραφίας, νομικών διατάξεων και πηγών του Διαδικτύου. Στο πρώτο μέρος του παρόντος πονήματος παρουσιάζονται τα χαρακτηριστικά και οι ειδικότερες μορφές εκδήλωσης της εξεταζόμενης συμπεριφοράς, όπως και το προφίλ δραστών και θυμάτων. Επίσης, μέσω της συγκριτικής προσέγγισης της συμπεριφοράς με την παραδοσιακή μορφή εκδήλωσής της και της θεωρητικής της πλαισίωσης επιτυγχάνεται η θεμελίωσή της ως νέα και διακριτή από την παραδοσιακή της μορφή εγκληματική συμπεριφορά που εκδηλώνεται στο Διαδίκτυο. Ακολούθως, το δεύτερο μέρος της εργασίας περιλαμβάνει τα ατομικά δικαιώματα που παραβιάζονται από το «cyberstalking», μέσω της χρήσης Τεχνολογιών Πληροφοριών και Επικοινωνίας (ΤΠΕ) και του σύγχρονου «συμμετοχικού» Διαδικτύου, και δίνεται έμφαση στην προστασία τους στο εικονικό περιβάλλον (ψηφιακά δικαιώματα). Τέλος, το γενικότερο συμπέρασμα που εξάγεται από την παρούσα εργασία είναι η ανάγκη περαιτέρω εμπειρικής διερεύνησης και ολιστικής προσέγγισης του «cyberstalking», ώστε να επιτευχθεί ένα υψηλό επίπεδο προστασίας των δικαιωμάτων και ελευθεριών των χρηστών του Διαδικτύου.

Λέξεις - κλειδιά: έμμονη διαδικτυακή παρενοχλητική παρακολούθηση, Τεχνολογίες Πληροφοριών και Επικοινωνίας, ατομικά δικαιώματα, πληροφοριακός αυτοκαθορισμός, ολιστική προσέγγιση

The offense of online stalking ("Cyberstalking") and the violation of individual rights resulting from its commission

Maria-Niki K. Skoufi

Abstract

The purpose of this dissertation is to highlight "cyberstalking" as a relatively recent form of criminal behavior, which infringes on important legal goods, rights, and freedoms of the human. The methodology followed in this study includes secondary research and specifically a review on relevant literature/articles, legal provisions, and Internet sources. The first part of this paper presents the characteristics and the most specific forms of manifestation of the behavior under consideration, as well as the profile of the perpetrators and the victims. Also, through the comparative approach of the behavior with its traditional form of manifestation and its theoretical framing, its establishment is achieved as a new and distinct from its traditional form criminal behavior manifested on the Internet. Subsequently, the second part of the paper includes the individual rights violated by "cyberstalking", using Information and Communication Technologies (ICTs) and the modern "participatory" Internet, and emphasis is placed on their protection in the virtual environment (digital rights). Finally, the most general conclusion drawn from this work is the need for further empirical investigation and a holistic approach to "cyberstalking", in order to achieve a high level of protection of the rights and freedoms of Internet users.

Keywords: "cyberstalking", Information and Communication Technologies, individual rights, informational self-determination, holistic approach

Εισαγωγή

Το έγκλημα, σύμφωνα με τον E. Durkheim, Γάλλο φιλόσοφο και κοινωνιολόγο, αποτελεί κοινωνικό φαινόμενο και συστατικό στοιχείο κάθε υγιούς κοινωνίας[1]. Εμφανίζεται ως χρήσιμο και αναγκαίο, αφού κατά τους K.T. Erikson και A. Cohen, συμβάλλει στην επαναβεβαίωση των ορίων των κοινωνικών συστημάτων δοκιμάζοντας τους κανόνες ρύθμισης της κοινωνικής συμβίωσης. Εφόσον, λοιπόν, το έγκλημα εμφανίζεται αναπόφευκτα σε κάθε κοινωνία, είναι φυσιολογικό να ακολουθεί τους ρυθμούς των κοινωνικών μεταβολών που λαμβάνουν χώρα με την πάροδο του χρόνου. Η εξέλιξη των κοινωνιών ακολουθείται ταυτόχρονα από την εξέλιξη του εγκλήματος[2].

Οι μετασχηματισμοί στη δομή και τη λειτουργία των κοινωνιών, ιδίως μετά τη Βιομηχανική Επανάσταση και την άνοδο του καπιταλισμού, οδήγησαν στις σύγχρονες, μετα-νεωτερικές, μεταβιομηχανικές κοινωνίες, οι οποίες χαρακτηρίζονται από ραγδαία τεχνολογική ανάπτυξη και επιστημονική πρόοδο[3]. Η φύση τους συναρτάται άμεσα με την ανάπτυξη των ηλεκτρονικών επικοινωνιών, την χρήση της τεχνολογίας της πληροφορίας και της τεχνολογίας δικτύωσης με την ολοένα και αυξανόμενη χρήση του Διαδικτύου (Internet). Τα νέα δεδομένα που δημιούργησε η τεχνολογική πρόοδος οδήγησαν σε μια νέα εποχή που βασίζεται στη διαχείριση και την ανταλλαγή της πληροφορίας. Πρόκειται για κοινωνίες της γνώσης και της πληροφορίας (ΚτΠ)[4], αφού όλες οι πτυχές της ανθρώπινης ζωής και δραστηριότητας εξαρτώνται από την Τεχνολογία της Πληροφορίας (Information Technology/IT)[5].

Παρόλα αυτά, η εξάρτηση των σύγχρονων κοινωνιών από τις Τεχνολογίες Πληροφοριών και Επικοινωνίας/ΤΠΕ (Information and Communication Technologies/ICTs)[6] και την ευρεία εξάπλωση της χρήσης του Διαδικτύου καθιστούν τις ΚτΠ ευάλωτες σε κινδύνους, μιας και η τεχνολογία, ο Η/Υ και το Διαδίκτυο χρησιμοποιούνται ως εργαλεία – μέσα διάπραξης εγκλημάτων. Η Τεχνολογία της

---

[1] Βλ. Ι. Φαρσεδάκης, *Στοιχεία Εγκληματολογίας*, Αθήνα, Νομική Βιβλιοθήκη, 2005, σ. 24

[2] Στο ίδιο, σ. 25-26

[3] Βλ. St. Furnell, *ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ: Καταστρέφοντας την κοινωνία της πληροφορίας* (επιμ. Χρ. Ε. Τσουραμάνης μτφρ Φωτ. Α. Μηλιώνη), Αθήνα, εκδ. Παπαζήση, 2006, σ. 2-4

[4] Στο ίδιο, σ. 3

[5] Τα μέλη των Κοινωνιών της Πληροφορίας χαρακτηρίζονται στην ξενόγλωσση βιβλιογραφία ως «Generation X», «Millenials», ή «Digital Natives», βλ. Λ. Μήτρου, Μια σύντομη εισαγωγή, Στο: Μ. Καρύδα, Σπ. Κοκολάκης, Λ. Μήτρου, Μ. Πισκοπάνη & Σπ. Τάσσης (επιμ.), *facebook, blogs και δικαιώματα*, Αθήνα, εκδ. Σάκκουλα, 2016, σ. 14 (υποσημείωση 18)

[6] Βλ. M. Nuth, Crime and technology - Challenges or solutions? Taking advantage of new technologies: For and against crime, *Computer Law & Security Report*, 24, 2008, σ. 439, doi: https://doi.org/10.1016/j.clsr.2008.07.003

Πληροφορίας και το Διαδίκτυο χρησιμοποιούνται για τη διάπραξη παραδοσιακών εγκλημάτων με διαφορετικό τρόπο τέλεσης (modus operandi), ενώ παράλληλα δυσχεραίνουν τον εντοπισμό και τη σύλληψη των δραστών, διαμέσου της ανωνυμίας που προσφέρουν[7].

Το ηλεκτρονικό έγκλημα προϋποθέτει την χρήση Η/Υ και του Διαδικτύου και αναδεικνύεται ως μείζον πρόβλημα για τις διωκτικές και δικαστικές αρχές αναφορικά με την πρόληψη και την καταστολή του[8].

Τα πλεονεκτήματα και οι δυνατότητες που προσφέρουν οι ΤΠΕ και το Διαδίκτυο επέφεραν την αύξηση του αριθμού των ατόμων που παραμένουν συνδεδεμένοι (online) σε καθημερινή βάση και τη μεταφορά των δραστηριοτήτων τους στο εικονικό περιβάλλον, χωρίς, ωστόσο, να είναι εξοικειωμένοι με την τεχνολογία δικτύωσης και την επίγνωση των κινδύνων που ελλοχεύουν από την χρήση της. Έτσι, λοιπόν, η αύξηση του ηλεκτρονικού εγκλήματος δε συναρτάται μόνο με την τεχνολογική κατάρτιση των επίδοξων κυβερνοεγκληματιών (cybercriminals), αλλά και την άγνοια των «αθώων» χρηστών του Διαδικτύου για τους κινδύνους του ψηφιακού περιβάλλοντος και του Κυβερνοχώρου (Cyberspace) σχετικά με τα δικαιώματα και τις ελευθερίες τους.

Εν προκειμένω, η παρούσα εργασία πραγματεύεται την εμφάνιση της έμμονης διαδικτυακής παρενοχλητικής παρακολούθησης («online stalking» ή «cyberstalking»)[9], η οποία συνιστά την παρακολούθηση ενός ατόμου από κάποιο άλλο άτομο ή ομάδα ατόμων στο Διαδίκτυο. Οι άξονες στους οποίους στηρίζεται η εργασία είναι οι εξής: η εξέταση της εν λόγω συμπεριφοράς ως μια νέα μορφή ηλεκτρονικής εγκληματικότητας, η οποία διαφοροποιείται από την παραδοσιακή της μορφή, η απουσία ενός κοινά αποδεκτού ορισμού λόγω της δυσχέρειας κατανόησής της ως κοινωνικό φαινόμενο, γεγονός που απορρέει από την περιορισμένη μέχρι τώρα εμπειρική της διερεύνηση, καθώς και η διαφοροποίηση στη νομοθέτηση και την ποινική της αντιμετώπιση στις επιμέρους έννομες τάξεις. Ακόμη, αναλύονται οι ειδικότερες μορφές εμφάνισης του φαινομένου και συγκεκριμένα διαμέσου Η/Υ,

[7] Βλ. Furnell, ό.π., σ. 20

[8] Στο ίδιο, σ. 25

[9] Βλ. Μ. Κατσογιάννου, Η δυστοπική πραγματικότητα της κρίσης ως θρυαλλίδα έκπτυξης αντικοινωνικής συμπεριφοράς και ανάδυσης αθέατης θυματοποίησης: Η περίπτωση της «έμμονης διαδικτυακής παρενοχλητικής παρακολούθησης» (“Cyberstalking”), στο Μ. Γασπαρινάτου (επιμ.), *Έγκλημα και Ποινική Καταστολή σε Εποχή Κρίσης*, Τιμ. Τόμος Ν. Κουράκη, Αθήνα, εκδ. Σάκκουλα, 2016, σ. 1423

ηλεκτρονικού ταχυδρομείου (email) και Διαδικτύου, το προφίλ δραστών και θυμάτων και οι προσπάθειες, παρά τις δυσκολίες, ανάπτυξης στρατηγικών αποτελεσματικής πρόληψης και αντιμετώπισης στο πλαίσιο μιας ευρύτερης συνεργασίας μεταξύ των διωκτικών αρχών, των ιδιωτικών εταιρειών παροχής υπηρεσιών Διαδικτύου και της Κοινωνίας των Πολιτών.

Ακολούθως, στο δεύτερο μέρος της εργασίας επιχειρείται η σύνδεση του αδικήματος με τη μεταβολή του χαρακτήρα των σύγχρονων ανθρώπινων σχέσεων, οι οποίες στις ΚτΠ αναπτύσσονται ηλεκτρονικά με την χρήση ΤΠΕ και με τη συμβολή των υπηρεσιών κοινωνικής δικτύωσης που προσφέρει το Διαδίκτυο.

Η ψηφιοποίηση, όμως, αυτή της ανθρώπινης επικοινωνίας και δραστηριότητας γεννά κινδύνους για την προστασία των χρηστών στο Διαδίκτυο. Η κουλτούρα διαμοιρασμού προσωπικών πληροφοριών, ιδίως στα μέσα κοινωνικής δικτύωσης, που διαδραματίζουν σημαντικό ρόλο στο «cyberstalking», συντελεί στην απώλεια του ελέγχου επί των προσωπικών δεδομένων και την εν αγνοία των υποκειμένων τους ηλεκτρονική τους επεξεργασία και διάδοση. Αυτό, όμως, έχει ως αποτέλεσμα την παραβίαση της ιδιωτικότητάς τους και άλλων ατομικών τους δικαιωμάτων.

Καταληκτικά, μετά την ανάλυση των παραβιαζόμενων ατομικών δικαιωμάτων από το «cyberstalking», παρουσιάζεται η προσπάθεια που γίνεται σε νομοθετικό επίπεδο για την ενίσχυση της προστασίας των ήδη υπαρχόντων ατομικών δικαιωμάτων και τη θέσπιση νέων, ανταποκρινόμενων στις ιδιαιτερότητες του ψηφιακού περιβάλλοντος, των «ψηφιακών δικαιωμάτων» ή δικαιωμάτων στο Διαδίκτυο («Internet Rights»)[10]. Ακόμη, επιχειρείται η ενίσχυση της προστασίας των ατομικών δικαιωμάτων μέσω της ανάπτυξης τεχνολογιών φιλικών προς τα ανθρώπινα δικαιώματα που θα συμβάλουν στην προστασία τους από κακόβουλες προσβολές. Επιπλέον, στην προσπάθεια ολιστικής προσέγγισης των ηλεκτρονικών εγκλημάτων εντάσσεται η συνεργασία τεχνολογίας και δικαίου με τη συμπερίληψη των νέων μορφών εγκληματικότητας και των τεχνολογικών εργαλείων που χρησιμοποιούνται πλέον από τους εγκληματίες στη διάπραξη των εγκλημάτων. Εκτός αυτών, η ασφάλεια στο εικονικό περιβάλλον μπορεί να επιτευχθεί με την ευαισθητοποίηση και δραστηριοποίηση όλων των ενδιαφερόμενων μερών για την αποτροπή και καταπολέμηση των ηλεκτρονικών εγκλημάτων, αλλά και την παροχή ενός ενισχυμένου

[10] Βλ. Introduction of The Charter of Human Rights and Principles for the Internet, Ανακτήθηκε από: https://internetrightsandprinciples.org/charter/ (επίσκεψη την 18-10-2022)

πλέγματος προστασίας των χρηστών του Διαδικτύου και των δικαιωμάτων τους μέσω της ελαχιστοποίησης των κινδύνων για την ιδιωτική τους ζωή, τα προσωπικά τους δεδομένα και την προσωπικότητά τους.

Μέρος Πρώτο

1. Εννοιολογική προσέγγιση του αδικήματος της έμμονης διαδικτυακής παρενοχλητικής παρακολούθησης («Cyberstalking»)

1.1. Το «cyberstalking» ως ειδική μορφή ηλεκτρονικού εγκλήματος

Το «cyberstalking» ή εναλλακτικά «online stalking», όροι που στην ελληνική γλώσσα αποδίδονται ως έμμονη διαδικτυακή παρενοχλητική παρακολούθηση, αποτελεί νέα μορφή εγκληματικής συμπεριφοράς, η οποία σχετίζεται άμεσα με την χρήση επικοινωνιακών τεχνολογιών και ιδίως του Η/Υ και του Διαδικτύου. Πρόκειται για αδίκημα που εκδηλώνεται στον Κυβερνοχώρο με εργαλείο το Διαδίκτυο. Εκ των ανωτέρω, συνάγεται το συμπέρασμα πως η εγκληματική αυτή συμπεριφορά με τις ειδικότερες μορφές τέλεσής της υπάγονται στην ευρύτερη κατηγορία των ηλεκτρονικών εγκλημάτων[11].

Λόγω της απουσίας ενός κοινά αποδεκτού ορισμού για το ηλεκτρονικό έγκλημα[12] ένεκα του δυναμικού του χαρακτήρα, της ταχύτατης εξέλιξης και των διαφορετικών τρόπων προσέγγισής του, η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος του Αρχηγείου της Ελληνικής Αστυνομίας το ορίζει ως «*όλες τις αξιόποινες πράξεις που τελούνται με την χρήση Η/Υ και συστημάτων επεξεργασίας δεδομένων και τιμωρούνται με συγκεκριμένες ποινές από την ελληνική νομοθεσία*». Στη βιβλιογραφία χρησιμοποιείται και ο όρος «πληροφορικό έγκλημα»[13] προκειμένου να αναδειχθεί η σχέση αλληλεπίδρασης με την πληροφορική τεχνολογία, η αξιοποίηση της οποίας οδήγησε στην εδραίωση του εν λόγω αδικήματος (information technology crime)[14]. Σύμφωνα με τον ορισμό που δόθηκε το 1976 από τον Donn Parker, ερευνητή στον τομέα της ασφάλειας των πληροφοριών, στη μελέτη του με τίτλο «Crime by Computer», ως πληροφορικό έγκλημα λογίζεται «*κάθε αδίκημα που σχετίζεται με την*

[11] Βλ. Κατσογιάννου, ό.π., σ. 1465
[12] Βλ. Γρ. Λάζος, *ΠΛΗΡΟΦΟΡΙΚΗ & ΕΓΚΛΗΜΑ*, Αθήνα, Νομική Βιβλιοθήκη, 2001, σ. 45
[13] Στο ίδιο, σ. 13
[14] ό.π.

πληροφορική τεχνολογία, στο οποίο το θύμα υπέστη ή θα μπορούσε να υποστεί ζημία και ο δράστης σκόπιμα πραγματοποίησε ή θα μπορούσε να πραγματοποιήσει κέρδος»[15].

Ακολούθως, ο Parker διέκρινε το ηλεκτρονικό έγκλημα περαιτέρω σε έγκλημα μέσω Η/Υ (computer crime) και σε κυβερνοέγκλημα (cybercrime) προσδιορίζοντας το πρώτο ως το έγκλημα στο οποίο ο δράστης χρησιμοποιεί ειδικές γνώσεις γύρω από την τεχνολογία των Η/Υ και το δεύτερο ως το έγκλημα στο οποίο ο δράστης χρησιμοποιεί ειδικές γνώσεις γύρω από τον Κυβερνοχώρο[16]. Μάλιστα, όσον αφορά το έγκλημα μέσω Η/Υ προσδιόρισε πως ο Η/Υ μπορεί να αποτελεί είτε το αντικείμενο της πληροφορικής προσβολής, καθώς επίσης, και οι ηλεκτρονικές πληροφορίες που είναι αποθηκευμένες σε αυτόν, ή να χρησιμοποιηθεί ως εργαλείο για την τέλεση εγκλημάτων[17].

Μεταξύ πολλών ακόμη ορισμών ο ΟΟΣΑ προσεγγίζει το πληροφορικό έγκλημα ως «*παράνομη και ανήθικη συμπεριφορά που περιλαμβάνει την αυτόματη και χωρίς την έγκριση του κατόχου επεξεργασία ή/και μετάδοση δεδομένων*»[18], εστιάζοντας στην σκόπιμη συμπεριφορά του δράστη, ενώ ο Ulrich Sieber, Γερμανός νομικός που ασχολήθηκε με το δίκαιο της πληροφορίας, προβαίνει στην εξής κατηγοριοποίηση: πληροφορικά οικονομικά εγκλήματα (π.χ. απάτη), πληροφορικά εγκλήματα κατά των προσωπικών δικαιωμάτων (κυρίως κατά της ιδιωτικότητας) και υπερ-ατομικά πληροφορικά εγκλήματα (π.χ. κατά της εθνικής ασφάλειας)[19], δίνοντας έμφαση στο προσβαλλόμενο ή απειλούμενο έννομο αγαθό.

Όσον αφορά τα κυβερνοεγκλήματα ή διαδικτυακά εγκλήματα αξίζει να σημειωθεί πως έπονται χρονικά των εγκλημάτων που τελούνται μέσω Η/Υ και διαφοροποιούνται ποιοτικά από αυτά λόγω των ιδιαίτερων χαρακτηριστικών του Διαδικτύου[20]. Ο χώρος δραστηριοποίησης των κυβερνοεγκληματιών είναι ο Κυβερνοχώρος, ο οποίος είναι ευρύτερος του Διαδικτύου, και περιλαμβάνει το Διαδίκτυο, τις ΤΠΕ, που υποστηρίζουν τη λειτουργία του, και τα συνδεόμενα με αυτόν δίκτυα Η/Υ για την αποθήκευση, τροποποίηση και ανταλλαγή δεδομένων μέσω δικτυωμένων συστημάτων και φυσικών υποδομών[21]. Με άλλα λόγια, αποτελεί το

[15] Στο ίδιο, σ. 38
[16] Βλ. Furnell, ό.π., σ. 25
[17] Βλ. Λάζος, ό.π., σ. 39
[18] Στο ίδιο, σ. 51
[19] Στο ίδιο, σ. 52
[20] Βλ. Γ. Γερμάνος και Α. Παπαθανασίου, Εξέλιξη και ανάπτυξη νέων μορφών ψηφιακής εγκληματικότητας στον Κυβερνοχώρο σε εποχές κρίσης, Στο Μ. Γασπαρινάτου (επιμ.), *Έγκλημα και Ποινική Καταστολή σε Εποχή Κρίσης*, Τιμ. Τόμος Ν. Κουράκη, Αθήνα, εκδ. Σάκκουλα, 2016, σ. 1308
[21] Βλ. https://cyberalert.gr/cybercrime/ (επίσκεψη την 09-08-2022)

εικονικό περιβάλλον στο οποίο διευκολύνεται η διασύνδεση και επικοινωνία των ατόμων διαμέσου δικτύων Η/Υ και τηλεπικοινωνιών χωρίς γεωγραφικούς περιορισμούς[22]. Ωστόσο, δεδομένης της ανοικτής πρόσβασης στους χρήστες και της σχετικά ανεμπόδιστης επικοινωνίας και μετάδοσης πληροφοριών, το Διαδίκτυο έχει καταστεί ως κυρίαρχο μέσο επικοινωνίας με μεγάλη ποικιλία περιεχομένου και ακριβώς αυτό είναι που διευκολύνει την χρήση του για εγκληματικούς σκοπούς[23].

Συνοψίζοντας, η διάκριση των ηλεκτρονικών εγκλημάτων σε εγκλήματα που διαπράττονται μονάχα σε περιβάλλον Η/Υ (χωρίς την ύπαρξη δικτύωσης) και σε αυτούσια εγκλήματα του Κυβερνοχώρου, βοηθά στην κατανόηση της φύσης του αδικήματος του «cyberstalking», το οποίο συνιστά ιδιαίτερη μορφή ηλεκτρονικού εγκλήματος που συνδυάζει την χρήση Η/Υ και Διαδικτύου.

1.2. Η προβληματική του ορισμού του «cyberstalking» και οι προσπάθειες κατανόησής του ως κοινωνικό φαινόμενο

Όπως στο ηλεκτρονικό έγκλημα εν γένει, έτσι και στο αδίκημα του «cyberstalking» αλλά και στο παραδοσιακό έγκλημα της έμμονης παρενοχλητικής παρακολούθησης («offline stalking/conventional stalking») απουσιάζει ενός καθολικά αποδεκτός ορισμός[24]. Γενικά, ο όρος «cyberstalking» αποτελεί νεολογισμό και κρίθηκε πρόσφορος για να περιγράψει την εμφάνιση συμπεριφορών που προσιδιάζουν στην παραδοσιακή μορφή του αδικήματος της έμμονης παρενοχλητικής παρακολούθησης στο περιβάλλον του Διαδικτύου[25]. Γι' αυτόν τον λόγο, οι ακριβείς όροι που συναντώνται στη βιβλιογραφία για την περιγραφή της νέας αυτής μορφής εγκληματικής συμπεριφοράς, είναι «έμμονη διαδικτυακή παρενοχλητική παρακολούθηση» («cyberstalking» ή «online stalking») και εναλλακτικά «ηλεκτρονική stricto sensu έμμονη παρακολούθηση»[26].

Οι δυσχέρειες στην εξεύρεση ενός κοινά αποδεκτού ορισμού για την περιγραφή της εν λόγω συμπεριφοράς οφείλονται στη διαφοροποίηση του νομικού πλαισίου μεταξύ των επιμέρους εθνικών έννομων τάξεων, στις οποίες έχει τυποποιηθεί ως

[22] ό.π.
[23] Βλ. Λάζος, ό.π., σ. 164
[24] Βλ. M. Pittaro, Cyber stalking: An Analysis of Online Harassment and Intimidation, *International Journal of Cyber Criminology (IJCC)*, Vol. 1, Issue 2, 2007, σ. 181, Ανακτήθηκε από: https://www.researchgate.net/publication/241843583_Cyber_stalking_An_Analysis_of_Online_Harassment_and_Intimidation
[25] Βλ. Κατσογιάννου, ό.π., σ. 1469
[26] Στο ίδιο, σ. 1465

αυτοτελές έγκλημα το «cyberstalking», αλλά και στη διαφοροποίηση των δικαιϊκών συστημάτων[27]. Ακόμη, η πολυ-επιστημονική προσέγγιση του φαινομένου, ο έντονα περιπτωσιολογικός του χαρακτήρας, η ευρηματικότητα, η πολυπλοκότητα και η πληθώρα των αξιοποιούμενων από τους δράστες μεθόδων εκδήλωσης της συμπεριφοράς συνιστούν παράγοντες που καθιστούν δύσκολο το εγχείρημα εύρεσης ενός κοινά αποδεκτού ορισμού[28]. Επίσης, το γεγονός πως δεν έχουν αποκρυσταλλωθεί ακόμη τα βασικά και προσδιοριστικά χαρακτηριστικά της εν λόγω συμπεριφοράς, τα μοτίβα (patterns) της αλλά και το προστατευόμενο έννομο αγαθό που επαπειλείται από την εκδήλωσή της, αποτελεί τροχοπέδη στη δημιουργία ενός ενιαίου ερμηνευτικού και νομικού πλαισίου για την κατανόηση του φαινομένου[29]. Ανακύπτουν, λοιπόν, ζητήματα σχετικά με το πότε και υπό ποιες συνθήκες μια συμπεριφορά αποτελεί έμμονη διαδικτυακή παρενοχλητική παρακολούθηση, τη συχνότητα και τη διάρκεια των περιστατικών (αλληλουχία δράσεων - course of conduct) πριν τα θύματα ζητήσουν προστασία από τις αρμόδιες Αρχές, κ.ά.[30]

Η έλλειψη όμως ενός καθολικά αποδεκτού ορισμού έχει αντίκτυπο στην κατανόηση και την ερμηνεία του φαινομένου και κατ' επέκταση στην εμπειρική του προσέγγιση[31]. Η απουσία ενός συνεκτικού ορισμού εμποδίζει τη νομοθετική αποτύπωση της αποδοκιμαστέας συμπεριφοράς σε κυρωτικούς κανόνες και την εγκληματολογική της διερεύνηση, διότι για να αποτελέσει μια συμπεριφορά αντικείμενο μελέτης στο πλαίσιο της εγκληματολογικής έρευνας, πρέπει να είναι σαφώς και ρητώς ορισμένη, ενώ παράλληλα, δυσχεραίνεται η αποτελεσματική αντιμετώπιση του φαινομένου και η προστασία των θυμάτων[32].

Η επιστημονική ενασχόληση με το «cyberstalking» ξεκίνησε με την αύξηση της θυματοποίησης από το συγκεκριμένο αδίκημα από τα μέσα της δεκαετίας του '90[33],

---

[27] Στο ίδιο, σ. 1472
[28] ό.π.
[29] Στο ίδιο, σ. 1473
[30] Βλ. P. Bocij, Chapter 1: What Is Cyberstalking?, Στο P. Bocij (επιμ.), *Cyberstalking: Harassment in the Internet Age and How to Protect Your Family*, Westport, Connecticut London, Praeger Publishers, 2004, σ. 8, Ανακτήθηκε από: https://books.google.gr/books?id=q8NZLBE0sm0C&printsec=frontcover&hl=el#v=onepage&q&f
[31] Βλ. Κατσογιάννου, ό.π., σ. 1436
[32] Βλ. P. Bocij & L. McFarlane, Online harassment: towards a definition of cyberstalking, *Prison Service Journal*, Issue 139, 2002, σ. 32, Ανακτήθηκε από: https://www.researchgate.net/publication/284807346_Online_harassment_Towards_a_definition_of_cyberstalking
[33] Βλ. E. Spence-Diehl, Stalking and Technology: The Double-Edged Sword, *Journal of Technology in Human Services*, Vol. 22, Issue 1, 2003, σ. 6, Ανακτήθηκε από:

ενώ η μεγάλη προβολή του φαινομένου από τα ΜΜΕ συνέτεινε στην ανάγκη της εμπειρικής του διερεύνησης[34], χωρίς, ωστόσο, να έχουν διεξαχθεί ακόμη πολλές εμπειρικές έρευνες γύρω από το αδίκημα αυτό. Ως εκ τούτου, η γνώση μας σχετικά με το «online stalking» προέρχεται από τα πορίσματα των ερευνών που έχουν διεξαχθεί για το παραδοσιακό έγκλημα του «offline stalking». Κάτι τέτοιο όμως ελλοχεύει κινδύνους για την αξιοπιστία των πορισμάτων αυτών, καθώς το «cyberstalking» διακρίνεται ουσιωδώς από την παραδοσιακή μορφή του φαινομένου[35].

Από τα ανωτέρω προκύπτει η ανάγκη δημιουργίας ενός κοινά αποδεκτού και ενιαίου ορισμού για το αδίκημα του «cyberstalking» που να ικανοποιεί αφενός τις ανάγκες των Αρχών επιβολής του νόμου ώστε να νομιμοποιούνται στη σύλληψη των δραστών, και αφετέρου των ερευνητών προκειμένου να μελετήσουν τη φύση του φαινομένου, το προφίλ των θυμάτων αλλά και τον ρόλο των παρόχων υπηρεσιών Διαδικτύου (Internet Service Providers/ISPs) σχετικά με την παροχή ασφαλούς περιβάλλοντος πλοήγησης και χρήσης των υπηρεσιών Διαδικτύου στους πελάτες τους[36].

Οι Paul Bocij - συγγραφέας και ερευνητής που ειδικεύεται στα πληροφορικά συστήματα και τις ΤΠΕ και Leroy McFarlane, ψυχολόγος που ασχολήθηκε με τη μελέτη της διαδικτυακής παρενόχλησης (cyberharassment ή online harassment), όρισαν το «cyberstalking» ως[37]:

> *το σύνολο συμπεριφορών με τις οποίες ένα άτομο, μια ομάδα ατόμων ή ένας οργανισμός χρησιμοποιεί ΤΠΕ για να παρενοχλήσει ένα ή περισσότερα άτομα. Οι συμπεριφορές αυτές μπορεί να περιλαμβάνουν, χωρίς να περιορίζονται αποκλειστικά σε αυτές, μετάδοση απειλών ή αβάσιμων κατηγοριών, κλοπή ταυτότητας, υποκλοπή δεδομένων, καταστροφή δεδομένων ή εξοπλισμού, παρακολούθηση μέσω Η/Υ αλλά και προσέγγιση ανηλίκων για σεξουαλικούς σκοπούς. Ως παρενόχληση νοούνται εκείνες οι ενέργειες, τις οποίες αν τις υφίσταντο ένα φυσιολογικό και λογικό άτομο, θα του προκαλούσαν συναισθηματική δυσφορία.*

https://www.researchgate.net/publication/254377993_Stalking_and_Technology_The_Double-Edged_Sword

[34] Βλ. P. Bocij & L. McFarlane, An Exploration of Predatory Behaviour in Cyberspace: Towards a Typology of Cyberstalkers, *First Monday (Peer-Reviewed Journal on the Internet)*, Vol. 8, Number 9, 2003, σ. 2, Ανακτήθηκε από: https://www.researchgate.net/publication/220167750_An_exploration_of_predatory_behaviour_in_cyberspace_Towards_a_typology_of_cyberstalkers

[35] Βλ. Κατσογιάννου, ό.π., σ. 1474

[36] Βλ. Bocij, Chapter 1 What Is Cyberstalking?, Στο P. Bocij (επιμ.), *Cyberstalking: Harassment in the Internet Age and How to Protect Your Family*, ό.π., σ. 5

[37] Βλ. Bocij & McFarlane, ό.π., σ. 2

Επιπλέον, η δικηγόρος Μαριλένα Κατσογιάννου, προσεγγίζοντας εννοιολογικά το αδίκημα υποστήριξε πως πρόκειται για[38]:

> *δια της χρήσεως οιουδήποτε πρόσφορου διαδικτυακού μέσου – απρόκλητη, σταθερή, έντονη και επανειλημμένη προσπάθεια προσέγγισης ενός ατόμου, παρά την αντίθετη θέλησή του, και, εν γένει, η κατά τρόπο επίμονο και διαρκή – αυθαίρετη επιδίωξη επικοινωνίας και επίτευξης μακρόθεν επαφής με αυτό, συνοδευόμενη δυνητικώς με εξαπόλυση απειλών συμπεριφορά, η οποία, ορώμενη εν συνόλω, εμποιεί δικαιολογημένα το φόβο στον υποστάντα αυτή για την ασφάλεια του ίδιου ή των οικείων του προσώπων.*

Οι προσπάθειες που γίνονται για την οριοθέτηση του «cyberstalking» αποσκοπούν στην κατανόησή του ως υπαρκτό κοινωνικό φαινόμενο, δυναμικά μεταβαλλόμενο στο ιστορικό και κοινωνικο-οικονομικό και πολιτιστικό πλαίσιο εμφάνισής του. Άλλωστε, η τυποποίησή του ως αυτοτελές ποινικό αδίκημα στο εσωτερικό δίκαιο πολλών έννομων τάξεων αποδεικνύει πως εκλαμβάνεται και αντιμετωπίζεται ως έγκλημα, το οποίο διαπράττεται εξαιτίας της ραγδαίας τεχνολογικής προόδου και της παρείσφρησης των νέων τεχνολογιών και του Διαδικτύου σε κάθε πτυχή της ανθρώπινης ζωής και δραστηριότητας. Αποτελεί ένα κοινωνικό φαινόμενο των μετα-νεωτερικών, παγκοσμιοποιημένων, καπιταλιστικών και ανεπτυγμένων κοινωνιών, στις οποίες κυριαρχούν οι ηλεκτρονικές επικοινωνίες, οι ΤΠΕ και το Διαδίκτυο[39].

Οι τεχνολογίες της πληροφορίας δημιούργησαν νέα δεδομένα και συνθήκες, οδηγώντας αναπόφευκτα στην αναπροσαρμογή της κοινωνικής πραγματικότητας, της οποίας αναπόσπαστο κομμάτι αποτελεί και το έγκλημα. Οι ποιοτικές αυτές διαφοροποιήσεις αποτυπώνονται στην εξέλιξη των τρόπων διάπραξης των παραδοσιακών εγκλημάτων με την χρήση της πληροφορικής τεχνολογίας και την εμφάνιση νέων μορφών εγκληματικής συμπεριφοράς, των οποίων η ορθή κατανόηση και αντιμετώπιση οφείλουν να λαμβάνουν χώρα υπό το πρίσμα των συντρεχουσών κοινωνικο-οικονομικών και πολιτιστικών μεταβολών[40].

Για τους λόγους αυτούς, το «cyberstalking» δύναται να κατανοηθεί υπό το πρίσμα της αναζήτησης εναλλακτικών τρόπων σύναψης σχέσεων στη σύγχρονη εποχή, των εικονικών διαπροσωπικών σχέσεων (cyber-relationships), μέσω της ευρύτατης χρήσης των ανάλογων υπηρεσιών του Διαδικτύου[41]. Όμως, η μεταφορά της

[38] Βλ. Κατσογιάννου, ό.π., σ. 1475
[39] Στο ίδιο, σ. 1485
[40] Στο ίδιο, σ. 1438
[41] Στο ίδιο, σ. 1429

ανθρώπινης αλληλεπίδρασης στο ψηφιακό περιβάλλον έχει ως συνέπεια αφενός την εικονική κοινωνικοποίηση, και αφετέρου την ταυτόχρονη φυσική αποξένωση, απομόνωση και από-κοινωνικοποίηση, αλλά και την αύξηση του κινδύνου θυματοποίησης από νέες εγκληματικές συμπεριφορές, επαληθεύοντας κατά αυτόν τον τρόπο τη θεώρηση του Ulrich Beck για τις κοινωνίες της διακινδύνευσης (risk societies)[42].

1.3. Η εγκληματοποίηση της συμπεριφοράς – Νομικό πλαίσιο

Η αλλαγή της φυσιογνωμίας του εγκλήματος εξαιτίας της τεχνολογικής προόδου οδήγησε στην εμφάνιση σύγχρονων μορφών εγκληματικής συμπεριφοράς, πιο «εκλεπτυσμένων», απρόσωπων, κεκαλυμμένων και δυσαπόδεικτων, για τις οποίες απαιτείται υψηλό επίπεδο εξοικείωσης με την πληροφορική τεχνολογία και το Διαδίκτυο. Η διαδικτυακή μορφή που απέκτησαν πλήθος παραδοσιακών εγκλημάτων και η εμφάνιση νέων τεχνολογικά προηγμένων, επιτάσσει την τυποποίησή τους ως αυτοτελή ποινικά αδικήματα, ώστε να μπορεί το δίκαιο να συμβαδίσει, στο μέτρο του δυνατού, με τη ραγδαία τεχνολογική πρόοδο[43].

Η έμμονη διαδικτυακή παρενοχλητική παρακολούθηση αποτελεί μια πολυδιάστατη συμπεριφορά με ποικιλομορφία στους τρόπους εκδήλωσής της, που προκαλεί έντονο εγκληματολογικό ενδιαφέρον. Ωστόσο, υπάρχει και έντονο ποινικό ενδιαφέρον στο να απαντηθεί εάν αποτελεί μια συμπεριφορά που συνιστά απλή μορφή παρέμβασης στην ιδιωτική ζωή των παρακολουθούμενων ή αν προσβάλλει σημαντικά έννομα αγαθά (π.χ. ιδιωτικότητα, προσωπικότητα) και χρήζει ποινικής αντιμετώπισης. Τα ζητήματα που εγείρονται αφορούν το βαθμό ανοχής που πρέπει να επιδείξουν τα θύματα, τα όρια που θα πρέπει να «αγγίζει» η συμπεριφορά ώστε να χαρακτηριστεί ως «cyberstalking», τη χρονική διάρκεια αυτής, κ.ά.[44]

Η εγκληματοποίηση της συμπεριφοράς είναι προβληματική αφενός διότι δεν έχει ακόμη κατανοηθεί πλήρως η φύση του φαινόμενου και υπάρχουν ελλιπή στοιχεία λόγω του περιορισμένου αριθμού εμπειρικών ερευνών που έχουν διεξαχθεί γύρω από αυτό, και αφετέρου διότι πεδίο εκδήλωσης της εν λόγω συμπεριφοράς είναι ο Κυβερνοχώρος και οι ηλεκτρονικές επικοινωνίες. Η ανωνυμία και η απόκρυψη της ταυτότητας που προσφέρει το Διαδίκτυο, αλλά και η υπερεθνική του διάσταση με την

[42] Στο ίδιο, σ. 1432-1434
[43] Βλ. Κατσογιάννου, ό.π., σ. 1434
[44] Στο ίδιο, σ. 1481

κατάργηση των φυσικών συνόρων, εντείνουν ακόμη περισσότερο το πρόβλημα της αποτελεσματικής θεσμοθέτησης και εφαρμογής της νομοθεσίας στο εικονικό περιβάλλον. Ακόμη, ζητήματα προκύπτουν και από την ανάγκη προστασίας συνταγματικά κατοχυρωμένων ελευθεριών που διέπουν τη λειτουργία του Διαδικτύου, όπως είναι η ελευθερία λόγου, έκφρασης, πληροφόρησης και επικοινωνίας, και στάθμισής τους σε περίπτωση μεταξύ τους σύγκρουσης[45].

Ποια συμπεριφορά, όμως, είναι αυτή που πρέπει να καταστεί ποινικά κολάσιμη; Αρχικά, απαιτείται υπαιτιότητα και πιο συγκεκριμένα δόλος για την επίτευξη του επιδιωκόμενου αποτελέσματος, αφού ο δράστης πρέπει να πράττει σκόπιμα, γνωρίζοντας πως η απειλητική ή παρενοχλητική συμπεριφορά του δύναται να προκαλέσει φόβο ή συναισθηματική δυσφορία στο θύμα. Συνακόλουθα, πρέπει η απειλή για την ασφάλεια του θύματος να είναι αξιόπιστη (credible threat) και ικανή να προκαλέσει τα ανωτέρω δυσάρεστα συναισθήματα. Επιπρόσθετα, η συμπεριφορά αυτή πρέπει να είναι ικανή να προκαλέσει φόβο για την προσωπική του ασφάλεια στο μέσο συνετό άνθρωπο (reasonable person), ενώ δύσκολα προσδιορίζεται και το όριο (threshold) ανοχής της συμπεριφοράς από το θύμα, κάτι το οποίο σχετίζεται άμεσα με την χρονική της διάρκεια και τον επαναλαμβανόμενο χαρακτήρα των συντονισμένων ενεργειών του δράστη μέχρις ότου επιτύχει τον σκοπό του[46].

Αν και η ενασχόληση με το αδίκημα του «cyberstalking» είναι εντονότερη τις τελευταίες δεκαετίες, η ποινική του τυποποίηση δεν ακολουθεί τους ίδιους ρυθμούς[47]. Υπάρχουν κράτη που έχουν συμπεριλάβει στην εθνική τους νομοθεσία το αδίκημα του «cyberstalking» θεσπίζοντας ειδικό ποινικό νόμο. Η πλειοψηφία, όμως, των κρατών δεν το αντιμετωπίζει ως αυτοτελές έγκλημα, τροποποιώντας μονάχα τις ισχύουσες διατάξεις που αφορούν το «offline stalking» και τυποποιώντας την χρήση ηλεκτρονικών επικοινωνιών ή ηλεκτρονικού ταχυδρομείου ως νέων τρόπων διάπραξης του αδικήματος αυτού, κάτι που έχει ως αποτέλεσμα τη μη επαρκή και αποτελεσματική προστασία των θυμάτων.

---

[45] Βλ. Y. Akdeniz & L. Ellison, Cyber-stalking: the Regulation of Harassment on the Internet, *Criminal Law Review*, December Special Edition: Crime, Criminal Justice, and the Internet, 1998, σ. 38, Ανακτήθηκε από: https://www.academia.edu/943428/Cyber_stalking_the_Regulation_of_Harassment_on_the_Internet

[46] Βλ. N. Goodno, Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws, *Federal Laws*, Vol. 72, Issue 1, 2007, σ. 133-140, Ανακτήθηκε από: https://scholarship.law.missouri.edu/mlr/vol72/iss1/7/

[47] Βλ. Bocij & McFarlane, Online harassment: towards a definition of cyberstalking, ό.π., σ. 34

Αμέσως μετά, παρουσιάζεται αρκετά συνοπτικά η ποινική αντιμετώπιση του φαινομένου στις ΗΠΑ και την Ελλάδα.

1.3.1. Η ποινική αντιμετώπιση του «cyberstalking» στις ΗΠΑ. Το 1999 τυποποιήθηκε για πρώτη φορά αυτοτελώς ως αδίκημα το «cyberstalking» στην πολιτεία της California με ειδική διάταξη στον Ποινικό της Κώδικα (Cal. Penal Code §649.9), ενώ είχε προηγηθεί η εγκληματοποίηση του αδικήματος στην παραδοσιακή του μορφή (Anti-stalking Legislation) ήδη από το 1990 με αφορμή τη δολοφονία της ηθοποιού Rebecca Schaeffer από θαυμαστή της το 1989 (περίπτωση celebrity stalking)[48]. Το παράδειγμα της Πολιτείας της California για την εγκληματοποίηση του «offline stalking» ακολούθησαν 48 ακόμη πολιτείες[49] και του «cyberstalking» 38 πολιτείες[50], εισάγοντας σχετική ειδική ρύθμιση για τη διαδικτυακή μορφή της συγκεκριμένης παραδοσιακής εγκληματικής συμπεριφοράς. Σε όσες πολιτείες δεν έχει κατοχυρωθεί νομοθετικά το αδίκημα εφαρμόζονται οι σχετικές διατάξεις για τη διαδικτυακή παρενόχληση, η οποία όμως διακρίνεται από το «cyberstalking», καθότι περιλαμβάνει την χρήση ηλεκτρονικών συσκευών για την απειλή και παρενόχληση συγκεκριμένου στόχου, χωρίς όμως συγκεκριμένη απειλή επικείμενου κινδύνου ή φόβου για το θύμα ή τους οικείους του. Άρα, απουσιάζει η ύπαρξη σοβαρής απειλής πρόκλησης φόβου ή συναισθηματικής δυσφορίας στο θύμα από την επαναλαμβανόμενη παρενοχλητική επικοινωνία, που αποτελεί συστατικό στοιχείο του «cyberstalking»[51].

1.3.2. Η ποινική αντιμετώπιση του «cyberstalking» στην Ελλάδα. Στο άρ. 333 παρ. 1 εδ. β΄ ΕλλΠΚ έχει τυποποιηθεί η παραδοσιακή μορφή της επίμονης καταδίωξης ή παρακολούθησης που προκαλεί τρόμο ή ανησυχία στο θύμα δίχως την απειλή βίας ή άλλης παράνομης πράξης αναφέροντας διαζευκτικά τους τρόπους τέλεσης μεταξύ των οποίων συγκαταλέγεται η χρήση τηλεπικοινωνιακών ή ηλεκτρονικών μέσων. Ωστόσο,

[48] Βλ. Κατσογιάννου, ό.π., σ. 1492

[49] Βλ. L. Roberts, Jurisdictional and definitional concerns with computer-mediated interpersonal crimes: Analysis on Cyber Stalking, *International Journal of Cyber Criminology*, Vol. 2, Issue 1, 2008, σ. 274, Ανακτήθηκε από: https://www.researchgate.net/publication/242074185_Jurisdictional_and_Definitional_Concerns_with_Computer-mediated_Interpersonal_Crimes_An_Analysis_on_Cyber_Stalking

[50] Βλ. Κατσογιάννου, ό.π., σ. 1492-1494

[51] Βλ. J. Clarke, E. Davies & A-L Roden, Self-Reports of Adverse Health Effects Associated with Cyberstalking and Cyberharassment: A Thematic Analysis of Victims' Lived Experiences, *Faculty Articles & Research*, 1, 2016, σ. 4, Ανακτήθηκε από: https://dc.swosu.edu/cas_act_articles/

δεν υπάρχει στην ελληνική νομοθεσία ad hoc ρύθμιση του «cyberstalking»[52]. Σε αντιστοιχία με τις λοιπές ευρωπαϊκές χώρες η προστασία από την εν λόγω συμπεριφορά παρέχεται από τη συνδυαστική εφαρμογή πλήθους συναφών διατάξεων[53]. Πιο συγκεκριμένα, η Ελλάδα έχει επικυρώσει με τον Ν. 4411/2016 (Φ.Ε.Κ. 142/03.08.2016) τη Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο και το Πρόσθετο Πρωτόκολλό της, με τον οποίο προστέθηκε το άρ. 292Β ΕλλΠΚ για την παρακώλυση λειτουργίας πληροφοριακών συστημάτων, το άρ. 370 ΕλλΠΚ για την παραβίαση του απορρήτου των εγγράφων και το άρ. 370Α ΕλλΠΚ για το απόρρητο της τηλεφωνικής επικοινωνίας και προφορικής συνομιλίας, αδικήματα που τελούνται με την χρήση Η/Υ. Ωστόσο, οι εν λόγω διατάξεις τυγχάνουν εφαρμογής και στις περιπτώσεις εκείνες που οι συμπεριφορές τελούνται στο Διαδίκτυο. Επίσης, με τον Ν. 4624/2019 εναρμονίστηκε η εσωτερική μας νομοθεσία με τις επιταγές του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27-04-2016 επικυρώνοντας τον νέο Γενικό Κανονισμό για την Προστασία Δεδομένων (General Data Protection Regulation/GDPR) σχετικά με την προστασία των φυσικών προσώπων από την επεξεργασία των δεδομένων προσωπικού χαρακτήρα που τα αφορούν.

2. Το «cyberstalking» ως μια νέα διακριτή εγκληματική συμπεριφορά σε σχέση με την παραδοσιακή έμμονη παρενοχλητική παρακολούθηση («offline stalking/conventional stalking»)

2.1. Συγκλίσεις και αποκλίσεις του «cyberstalking» και του «offline stalking»

Τα χαρακτηριστικά που πρέπει να έχει μια συμπεριφορά για να χαρακτηριστεί ως «cyberstalking» είναι τα ακόλουθα: α) να είναι έμμονη, β) να είναι διαδικτυακή, δηλαδή πρόκειται για επικοινωνία που πραγματοποιείται μέσω Η/Υ (Computer Mediated Communication/CMC) ή με την χρήση συσκευής κινητής τηλεφωνίας, η οποία δύναται να επιτελέσει την ίδια λειτουργία με τον Η/Υ, εφόσον υπάρχει σύνδεση στο Διαδίκτυο, γ) να είναι παρενοχλητική και δ) να συνιστά παρακολούθηση[54].

[52] Στο ίδιο, υποσημείωση 132, σ. 1489-1492

[53] Σε ευρωπαϊκό επίπεδο πληθώρα ευρωπαϊκών χωρών έχουν σχετική πρόβλεψη του παραδοσιακού «offline stalking», ενώ η αντιμετώπιση του «cyberstalking» προκύπτει είτε από τον συνδυασμό διατάξεων συναφών νομοθεσιών, είτε με την επέκταση της υφιστάμενης νομοθεσίας για το «offline stalking», ώστε να συμπεριλάβει τις τηλεπικοινωνίες ή άλλα μέσα επικοινωνίας (π.χ. email) χωρίς, ωστόσο, να γίνεται ρητή αναφορά στο Διαδίκτυο, βλ. Κατσογιάννου, ό.π., σ. 1494-1497

[54] Στο ίδιο, σ. 1444

Συμπεραίνεται, λοιπόν, πως η συμπεριφορά πρέπει να είναι επίμονη, σταθερή, επαναλαμβανόμενη και με διάρκεια, με τον δράστη να εξακολουθεί να εκδηλώνει τις ενέργειές του μέχρι την επέλευση του επιδιωκόμενου αποτελέσματος. Ακόμη, η εγκληματική δράση πρέπει να λαμβάνει χώρα στο Διαδίκτυο, γεγονός που την διαφοροποιεί ποιοτικά από την παραδοσιακή «εξω-διαδικτυακή» της μορφή. Επιπλέον, η συμπεριφορά πρέπει να συνιστά παρακολούθηση. Από την ετυμολογία του όρου γίνεται κατανοητό πως πρόκειται για παράπλευρη κίνηση, με τον δράστη να ακολουθεί από πολύ κοντά το θύμα με μεγάλη προσοχή ώστε να μη γίνει αντιληπτός, έχοντας ως απώτερο σκοπό τη συλλογή πληροφοριών για τη ζωή και τις δραστηριότητές του. Τέλος, η παρακολούθηση πρέπει να εκλαμβάνεται ως παρενοχλητική από το θύμα[55].

Στην περίπτωση που ο παρακολουθούμενος ενοχλείται από την εν λόγω συμπεριφορά του δράστη και αισθάνεται δυσφορία, γίνεται λόγος για τη διάπραξη του αδικήματος του «online stalking», και αυτό διότι συνιστά επέμβαση στην ιδιωτική ζωή του θύματος, από τη στιγμή που δεν υπάρχει συναίνεση στην επικοινωνία είτε επειδή δεν ήταν ποτέ ηθελημένη ή επειδή ο παρακολουθούμενος επιθυμεί τη διακοπή της. Αυτός είναι ακριβώς ο επιδιωκόμενος σκοπός του συνόλου των σταθερά επαναλαμβανόμενων ενεργειών του δράστη, δηλαδή η διατάραξη της ηρεμίας της ιδιωτικής ζωής του θύματος ή η πρόκληση φόβου και ανησυχίας[56].

Μολονότι το «cyberstalking» αποτελεί νέα μορφή εγκληματικής συμπεριφοράς, δεν παύει να σχετίζεται με την παραδοσιακή του μορφή. Το αδίκημα του «offline stalking» ή «conventional stalking» ή «terrestrial stalking»[57], όπως το χαρακτηρίζει ο Lucks (2001), αποδίδεται ακριβέστερα με τους όρους παρακολούθηση (following) και καταδίωξη (pursuit)[58]. Συνίσταται στην παρακολούθηση ενός ατόμου - στόχου με τέτοιο τρόπο που συνιστά σφοδρή επέμβαση στην ιδιωτική του ζωή, προκαλώντας στο άτομο το αίσθημα της καταδίωξης, χωρίς να μπορεί να κάνει κάτι για να την σταματήσει. Κατά τον Αμερικανό ψυχολόγο J. Reid Meloy, το «offline stalking» αποτελεί έμμονη παρακολούθηση (obsessional following)[59] υπό την έννοια πως πρόκειται για ένα μη φυσιολογικό ή μακρόχρονο μοτίβο απειλών ή παρενόχλησης προς συγκεκριμένο άτομο - στόχο, μια απροκάλυπτη και αθέμιτη καταδίωξη που

[55] Στο ίδιο, σ. 1470
[56] ό.π.
[57] Βλ. Spens-Diehl, ό.π., σ. 6
[58] Βλ. Bocij, Chapter 1 What Is Cyberstalking?, Στο P. Bocij (επιμ.), *Cyberstalking: Harassment in the Internet Age and How to Protect Your Family*, ό.π., σ. 5
[59] Στο ίδιο, σ. 6

εκλαμβάνεται ως παρενοχλητική από τον παρακολουθούμενο, σημείο στο οποίο συγκλίνουν το «cyberstalking» και το «offline stalking» ως προς τον θυματοκεντρικό τους χαρακτήρα[60]. Επίσης, οι Mullen, Pathe και Purcell (2000) ορίζουν το «offline stalking» ως ένα σύνολο συμπεριφορών με τις οποίες ένα άτομο επιβάλλει σε ένα άλλο επαναλαμβανόμενες αθέμιτες παρεμβάσεις στην ιδιωτική του ζωή και επικοινωνία[61].

Οι όροι «offline» και «cyber» αναφέρονται στο περιβάλλον εκδήλωσης των δύο αυτών αδικημάτων, χωρίς, ωστόσο, να αποκλείεται και η κλιμάκωση της συμπεριφοράς από το περιβάλλον του Διαδικτύου στο «εξω-διαδικτυακό» περιβάλλον και αντίστροφα[62].

Τα σημεία στα οποία συγκλίνουν το «cyberstalking» και το «offline stalking» είναι ο επαναλαμβανόμενος χαρακτήρας, η επίγνωση του δράστη ως προς τις αρνητικές σωματικές ή ψυχολογικές επιπτώσεις που επιφέρουν οι πράξεις του στο θύμα, η πρόκληση έντονης παρενόχλησης και αρνητικών συναισθημάτων ως επακόλουθα της παρακολούθησης στο θύμα, το κίνητρο - επιθυμία του δράστη για δύναμη, έλεγχο, επιβολή και επιρροή στη ζωή του θύματος, και τέλος, η πιθανότητα ύπαρξης προηγούμενης σχέσης οποιασδήποτε φύσης μεταξύ δράστη και θύματος[63].

Ωστόσο, οι δύο αυτές συμπεριφορές διαφοροποιούνται μεταξύ τους, ενώ σύμφωνα με τον Bocij (2004), υπάρχουν ορισμένοι «μύθοι» που μένει να καταρριφθούν σχετικά με τα αδικήματα αυτά. Πιο συγκεκριμένα:

α) Το «cyberstalking» αποτελεί επέκταση του «offline stalking». Υπάρχει διχογνωμία μεταξύ των ερευνητών για το εάν το «cyberstalking» αποτελεί μια νέα και διακριτή εγκληματική συμπεριφορά σε σχέση με το «offline stalking» ή όχι. Μεταξύ άλλων οι Ogilvie (2000), Petherick (2001) και Burgess & Baker (2002) υποστηρίζουν πως το «cyberstalking» αποτελεί επέκταση του παραδοσιακού «offline stalking» στον Κυβερνοχώρο και πως πρόκειται για μία ακόμη μέθοδο παρενόχλησης των θυμάτων από τους επίδοξους δράστες[64]. Ωστόσο, η θέση αυτή απορρίπτεται από την πλειοψηφία των ερευνητών με τους Bocij και McFarlane (2004) να υποστηρίζουν πως πρόκειται

[60] Βλ. J. Dickinson, The phenomenon of cyberstalking on the RIT campus: Definitions, behaviors and normalization, *Thesis,* Rochester Institute of Technology, 2006, σ. 14, Ανακτήθηκε από: https://scholarworks.rit.edu/theses/index.49.html
[61] Βλ. Bocij, ό.π., σ. 6
[62] Στο ίδιο, σ. 15
[63] Βλ. Goodno, ό.π., σ. 128, Pittaro, ό.π., σ. 182 και Roberts, ό.π., σ. 274
[64] Βλ. Bocij & McFarlane, An Exploration of Predatory Behaviour in Cyberspace: Towards a Typology of Cyberstalkers, ό.π., σ. 1

για μια νέα διακριτή εγκληματική συμπεριφορά με την χρήση ΤΠΕ, την οποία αναγνωρίζουν ως τέτοια τόσο τα θύματα, όσο και οι διωκτικές αρχές[65]. Επίσης, οι δράστες του «cyberstalking» παρενοχλούν τα θύματά τους αποκλειστικά μέσω Διαδικτύου, επομένως δεν είναι δυνατόν το «cyberstalking» να αποτελεί επέκταση του «offline stalking», το οποίο τελείται πλήρως εκτός διαδικτυακού περιβάλλοντος[66]. Τέλος, η εν λόγω συμπεριφορά άρχισε να εμφανίζεται μετά τη δεκαετία του '80, περίοδο που έλαβαν χώρα καινοτόμα τεχνολογικά επιτεύγματα, με αποτέλεσμα την εμφάνιση νέων μορφών εγκληματικότητας, ενώ προϋπήρχαν περιστατικά «offline stalking»[67].

β) Οι «cyberstalkers» είναι εμμονικοί. Στην βιβλιογραφία υποστηρίζεται από κάποιους ερευνητές (π.χ. Spitzberg & Veksler, 2007 και McEwan *et al.*, 2009) πως επειδή το «offline stalking» συνδέεται με προβλήματα ψυχοπαθολογίας και πιο συγκεκριμένα με διαταραχές προσωπικότητας και διάθεσης του δράστη, η σύνδεση αυτή μπορεί να επεκταθεί και στους δράστες «cyberstalking», χωρίς, ωστόσο, να υπάρχουν ασφαλή και αξιόπιστα πορίσματα από τις έως τώρα διεξαχθείσες έρευνες και χωρίς να υποστηρίζεται κάτι τέτοιο από μεγάλο αριθμό ερευνητών[68]. Όπως ακριβώς οι «offline stalkers», έτσι και οι «cyberstalkers» δεν διαγιγνώσκονται στο σύνολό τους με ψυχικές νόσους, επομένως η σύνδεση με την ψυχοπαθολογία δεν μπορεί να είναι απόλυτη[69]. Ενώ το «offline stalking» χαρακτηρίζεται ως εμμονική συμπεριφορά, ιδίως όταν αυτή συνεχιστεί μετά την απόρριψη που βιώνει ο δράστης από τον παρακολουθούμενο, οι «cyberstalkers» δεν παίρνουν το ρίσκο στις περισσότερες περιπτώσεις να κλιμακώσουν τη συμπεριφορά τους και να την επεκτείνουν στο «εξω-διαδικτυακό» περιβάλλον, δηλαδή σε εκ του σύνεγγυς παρακολούθηση, διότι δεν θέλουν να αποκαλύψουν την ταυτότητά τους. Ως εκ τούτου, εκμεταλλεύονται την ανωνυμία που προσφέρει το Διαδίκτυο, καθώς και τις δυσκολίες εντοπισμού των ψηφιακών τους ιχνών από τις Αρχές[70].

---

[65] Βλ. Bocij, Chapter 2: Stalking or Cyberstalking?, Στο P. Bocij (επιμ.), *Cyberstalking: Harassment in the Internet Age and How to Protect Your Family*, ό.π., σ. 21-22

[66] ό.π.

[67] ό.π.

[68] Βλ. N. Al Mutawa, J. Bryce, V. Franqueira & A. Marrington, Forensic investigation of cyberstalking cases using Behavioural Evidence Analysis, *Digital Investigation*, 16, 2016, σ. 97, https://doi.org/10.1016/j.diin.2016.01.012

[69] Βλ. Bocij, ό.π., σ. 22-23

[70] ό.π.

γ) Οι «cyberstalkers» γνωρίζουν τα θύματά τους. Αν και για το «offline stalking» υποστηρίζεται πως τα θύματα σχετίζονταν με τους δράστες με οποιοδήποτε είδος σχέσης (ερωτική, επαγγελματική, απλή γνωριμία κ.λπ.) πριν από την εκδήλωση της συμπεριφοράς, εντούτοις στο «cyberstalking» κάτι τέτοιο δεν είναι απόλυτο, καθώς υπάρχουν αρκετές περιπτώσεις στις οποίες δράστης και θύμα είναι τελείως άγνωστοι μεταξύ τους[71]. Δεν είναι λίγες οι φορές, όπου οι «cyberstalkers» επιλέγουν τυχαία το θύμα βάσει των πληροφοριών, της εικόνας ή του online προφίλ που παρουσιάζει σε ιστότοπους κοινωνικών γνωριμιών ή ψηφιακές πλατφόρμες μέσων κοινωνικής δικτύωσης. Οι προσωπικές πληροφορίες που εκθέτει ο ίδιος ο χρήστης στο Διαδίκτυο είναι επαρκείς για τη δημιουργία μιας εικόνας που θα προσελκύσει το ενδιαφέρον του επίδοξου «cyberstalker». Στην περίπτωση που διαπιστώσει πως η εικόνα του θύματος δεν ανταποκρίνεται στην πραγματικότητα, και ματαιωθούν οι προσδοκίες του ή εάν λάβει απόρριψη από το θύμα ή αισθανθεί υποτίμηση ή περιφρόνηση, μπορεί να αντιδράσει επιθετικά και να προβεί σε ενέργειες που εμπίπτουν στο «cyberstalking»[72].

δ) Οι «cyberstalkers» σπάνια παρενοχλούν μέσω άλλου προσώπου («cyberstalking by proxy» - παρακολούθηση δι' αντιπροσώπου). Το Διαδίκτυο ενθαρρύνει τη συμμετοχή και δραστηριοποίηση σε ομάδες στο πλαίσιο των οποίων είναι δυνατός ο διαμοιρασμός υλικού και η προσφορά υπηρεσιών. Έτσι λοιπόν, οι «cyberstalkers» είναι δυνατό να προσελκύσουν άλλα άτομα να τους βοηθήσουν στις ενέργειές τους ή να οργανωθούν σε ομάδες που από κοινού θα προβαίνουν σε διαδικτυακή παρακολούθηση του στόχου - θύματος[73] ή ακόμη και να προσλάβουν ιδιωτικούς ερευνητές επί πληρωμή για τη συλλογή πληροφοριών για το θύμα[74]. Το Διαδίκτυο προσφέρει, άλλωστε, τη δυνατότητα «στρατολόγησης» τελείως αγνώστων ατόμων που ενδεχομένως να μοιράζονται τον ίδιο σκοπό με τον επίδοξο «cyberstalker» ή απλά να

---

[71] Βλ. P. Bocij, Victims of Cyberstalking: An Explanatory Study of Harassment Perpetrated via the Internet, *First Monday* (Peer-Reviewed Journal on the Internet), Vol. 8, Number 10, 2003, σ. 8, Ανακτήθηκε από: https://firstmonday.org/ojs/index.php/fm/article/view/1086/1006

[72] Βλ. Bocij, Chapter 2 Stalking or Cyberstalking?, στο P. Bocij (επιμ.), *Cyberstalking: Harassment in the Internet Age and How to Protect Your Family*, ό.π., σ. 23-24, Pittaro, ό.π., σ. 182 και Κατσογιάννου, ό.π., σ. 1456

[73] Πρόκειται για την περίπτωση του «group cyberstalking». Οι ομάδες αυτές είναι πολύ πιθανό να συμφωνήσουν στο να παρενοχλήσουν μια ομάδα ατόμων βάσει των χαρακτηριστικών που παρουσιάζουν στο Διαδίκτυο. Στην περίπτωση αυτή συγκαταλέγονται οι σεξουαλικοί παραβάτες (sexual offenders) και οι παιδόφιλοι που οργανώνονται σε διαδικτυακές ομάδες, μοιράζονται υλικό κυρίως σεξουαλικής εκμετάλλευσης και κακοποίησης ανηλίκων, και αναζητούν ανήλικα θύματα, τα οποία προσεγγίζουν επιδιώκοντας δια ζώσης συνάντηση για την ικανοποίηση των εγκληματικών τους σκοπών, βλ. Κατσογιάννου, ό.π., σ. 1516-1517

[74] ό.π.

ενθαρρύνθηκαν από αυτόν για να συνεχίσουν ή να υποστηρίξουν το έργο του (π.χ. σε ένα δωμάτιο συζητήσεων/chatroom μπορεί ο «cyberstalker» να ξεκινήσει να δυσφημεί το θύμα του με αποτέλεσμα να ενθαρρυνθούν και άλλοι, άγνωστοι στον «cyberstalker» χρήστες, και να ξεκινήσουν τα υβριστικά σχόλια στο άγνωστο προς εκείνους θύμα)[75].

ε) Οι «cyberstalkers» δεν παρενοχλούν σοβαρά το θύμα. Κοινό χαρακτηριστικό και των δύο εγκλημάτων είναι ο παρενοχλητικός χαρακτήρας της συμπεριφοράς. Οι ενέργειες του δράστη πρέπει να είναι ικανές να προκαλέσουν στο θύμα ενόχληση λόγω της επέμβασης στην ιδιωτική του σφαίρα, καθώς επίσης, φόβο ή συναισθηματική δυσφορία. Σοβαρή παρενόχληση μπορεί να υπάρξει τόσο στο «offline stalking», όσο και στο «cyberstalking» παρόλο που το τελευταίο εκδηλώνεται σε εικονικό περιβάλλον[76]. Να σημειωθεί πως στο «offline stalking» η παρενόχληση γίνεται πολύ πιο εύκολα αντιληπτή, εξαιτίας της εκ του σύνεγγυς προσέγγισης του θύματος από τον δράστη, ενώ και ο «cyberstalker» μπορεί να παρενοχλήσει εξίσου σοβαρά το θύμα διαμέσου των ΤΠΕ ανεξαρτήτως της γεωγραφικής εγγύτητας μεταξύ τους. Κατά τον Bocij (2002) οι προσβολές στο Διαδίκτυο φαίνεται να έχουν σοβαρότερο αντίκτυπο στα θύματα, διότι αφορούν την τιμή και την υπόληψή τους και δημοσιοποιούνται σε ένα ευρύ και άγνωστο κοινό[77], ενώ αντιθέτως κατά την άποψη του Petherick (1999) στην πλειοψηφία των περιπτώσεων «cyberstalking» απουσιάζει εντελώς η άσκηση σωματικής βίας από τον δράστη, επιφέροντας μικρότερη βλάβη στα θύματα (κυρίως ψυχολογική ή κοινωνική βλάβη)[78].

στ) Οι «cyberstalkers» *έχουν* τα ίδια κίνητρα με τους «offline stalkers». Από τις τυπολογίες για τους «offline stalkers» που υπάρχουν στη βιβλιογραφία υποστηρίζεται πως το έναυσμα για την έναρξη της συμπεριφοράς μπορεί να είναι η απόρριψη του δράστη από το θύμα ή η διακοπή της επικοινωνίας μεταξύ τους. Έγκειται δηλαδή στην ύπαρξη προηγούμενης σχέσης μεταξύ δράστη και θύματος, ο τερματισμός της οποίας μπορεί να αποτελέσει εφαλτήριο, ώστε ο δράστης να αναζητήσει εκδίκηση ή να προβεί σε αντίποινα. Καθίσταται, έτσι, εμφανές πως το ερωτικό πάθος, ο θυμός, τα αντίποινα, η εκδίκηση, η επιθυμία για κυριαρχία και έλεγχο στη ζωή του θύματος, αλλά και η

[75] Στο ίδιο, σ. 25
[76] Στο ίδιο, σ. 24-26
[77] Βλ. Bocij, Victims of Cyberstalking: An Explanatory Study of Harassment Perpetrated via the Internet, ό.π., σ. 9
[78] Στο ίδιο, σ. 2

ψυχοπαθολογία του δράστη, μπορούν να αποτελέσουν κίνητρα για την εκδήλωση μιας τέτοιας συμπεριφοράς[79].

Τα κίνητρα αυτά συναντώνται και στις περιπτώσεις του «cyberstalking» αλλά όχι περιοριστικά. Πιο συγκεκριμένα, δεν έχουν όλοι οι «cyberstalkers» προβλήματα ψυχικής υγείας, όπως έχει ειπωθεί προηγουμένως, ενώ είναι πολύ πιθανό να εκδηλώσουν τη συμπεριφορά τους απλά και μόνο για να τραβήξουν την προσοχή ή για να διασκεδάσουν σερφάροντας στο Διαδίκτυο ή ακόμη για να ξεγελάσουν το θύμα και τις Αρχές εκμεταλλευόμενοι τα πλεονεκτήματα του Διαδικτύου αναφορικά με την απόκρυψη της ταυτότητας και τις δυσχέρειες εντοπισμού τους.[80] Επιπρόσθετα, κίνητρο μπορεί να αποτελέσει η ιδεολογία που συναντάται στις περιπτώσεις της κυβερνοτρομοκρατίας (cyber-terrorism) και του χακτιβισμού (hactivism)[81], που περιλαμβάνουν επιθέσεις - αλλοιώσεις σε επίσημες ιστοσελίδες στο όνομα ενός πολιτικού ή κοινωνικού σκοπού ή προκειμένου να υποστηριχτούν αιτήματα ακτιβιστών[82]. Ακόμη, κίνητρο μπορεί να αποτελέσει το κέρδος και ο ανταγωνισμός ιδίως στην περίπτωση που δράστης ή/και θύμα αποτελούν επιχειρήσεις ή οργανισμούς (περιπτώσεις «corporate cyberstalking»)[83], αλλά και η προσέλκυση ανηλίκων από παιδόφιλους για σεξουαλική κακοποίηση και εκμετάλλευση[84].

Εκτός από τα ανωτέρω αναφερόμενα σημεία στα οποία παρατηρείται διάσταση των απόψεων των ερευνητών στη βιβλιογραφία για το θέμα αυτό, από τις μέχρι τώρα διεξαχθείσες μελέτες για το «cyberstalking», έχει διαπιστωθεί πως δεν απαιτείται γεωγραφική εγγύτητα μεταξύ δράστη και θύματος, αφού παρενόχληση μπορεί να

---

[79] Βλ. Bocij & McFarlane, An Exploration of Predatory Behaviour in Cyberspace: Towards a Typology of Cyberstalkers, ό.π., σ. 2-3

[80] Βλ. Bocij, Chapter 2 Stalking or Cyberstalking?, στο P. Bocij (επιμ.), *Cyberstalking: Harassment in the Internet Age and How to Protect Your Family*, ό.π., σ. 28-29

[81] Πρόκειται για τον ακτιβισμό του Διαδικτύου και πιο συγκεκριμένα για την χρήση τεχνικών που βασίζονται σε Η/Υ (π.χ. hacking) ως μια μορφή πολιτικής ανυπακοής για την προώθηση μιας πολιτικής ατζέντας ή κοινωνικής αλλαγής, βλ. https://en.wikipedia.org/wiki/Hacktivism επίσκεψη την 26-01-2023

[82] Βλ. Bocij, Chapter 2 Stalking or Cyberstalking?, στο P. Bocij (επιμ.), *Cyberstalking: Harassment in the Internet Age and How to Protect Your Family*, ό.π., σ. 28 και Furnell, ό.π., σ. 52

[83] Στην περίπτωση αυτή το θύμα μπορεί να είναι ένας οργανισμός και ο δράστης ένας ιδιώτης, πιθανόν απολυμένος που αναζητά δικαίωση αναρτώντας στο Διαδίκτυο δυσφημιστικά ή ψευδή σχόλια με σκοπό να πλήξει την αξιοπιστία και το κύρος του οργανισμού και να προκαλέσει οικονομική ζημία. Επίσης, όταν το κίνητρο είναι ιδεολογικό, τότε ένα άτομο ή ομάδα ατόμων μπορεί να προβεί σε κυβερνοτρομοκρατία ή χακτιβισμό, ώστε να ασκήσει πίεση σε έναν οργανισμό για να συμμορφωθεί. Ακόμη, αν το «cyberstalking» χρησιμοποιείται ως στρατηγική ανταγωνισμού, τότε δράστης και θύμα είναι οργανισμοί και χρησιμοποιούνται ιστοσελίδες (websites) για τη δημοσιοποίηση παραπόνων ώστε να πληγεί το κύρος του οργανισμού – στόχου, βλ. P. Bocij, Corporate Cyberstalking: An Invitation to Build Theory, *First Monday* Peer-Reviewed Journal on the Internet, Vol. 7, No. 11, 2002, σ. 2-4, Ανακτήθηκε από: https://firstmonday.org/

[84] Βλ. Bocij, Chapter 2 Stalking or Cyberstalking?, στο P. Bocij (επιμ.), *Cyberstalking: Harassment in the Internet Age and How to Protect Your Family*, ό.π., σ. 28

υπάρξει ανάμεσα σε άτομα που βρίσκονται σε διαφορετικές χώρες, μιας και στο Διαδίκτυο τα σύνορα καταργούνται, δημιουργώντας προβλήματα στον εντοπισμό του δράστη, τη δικαιοδοσία και την εφαρμογή της εκάστοτε νομοθεσίας[85]. Επίσης, σύμφωνα με τον ορισμό των Bocij και McFarlane (2002), δράστης «cyberstalking» μπορεί να είναι είτε ένα άτομο ή μια ομάδα ατόμων ή ένας οργανισμός που παρενοχλεί άλλο άτομο ή άλλο οργανισμό. Ενώ, λοιπόν, στο «offline stalking» ο δράστης προβαίνει στην παρακολούθηση ενός μονάχα συγκεκριμένου ατόμου - στόχου, ο «cyberstalker» μπορεί να παρενοχλεί διαδικτυακά ταυτόχρονα περισσότερα από ένα άτομα[86].

Ακόμη, η χρονική διάρκεια της συμπεριφοράς διαφοροποιεί τα δύο αδικήματα μεταξύ τους, διότι από τα πορίσματα των μελετών έχει προκύψει πως η διάρκεια του «cyberstalking» κυμαίνεται από 2 εβδομάδες έως 38 μήνες με μ.ό. τους 6 μήνες, ενώ το «offline stalking» διαρκεί περισσότερο και κυμαίνεται από 1 χρόνο έως 3 χρόνια ή και παραπάνω. Αυτό ενδεχομένως συμβαίνει, διότι ο απαιτούμενος χρόνος προετοιμασίας για την εκδήλωση της συμπεριφοράς μειώνεται δραστικά στο Διαδίκτυο εξαιτίας της ταχύτητας, της ευκολίας και της άνεσης στην αναζήτηση των πληροφοριών[87].

Τέλος, μεταξύ των «offline stalkers» και των «cyberstalkers» παρατηρούνται διαφορές ως προς τον τρόπο που λαμβάνουν ικανοποίηση από τις πράξεις τους. Ο «cyberstalker» δεν μπορεί να αντιληφθεί άμεσα τις επιπτώσεις της συμπεριφοράς του στη ζωή του θύματος όπως συμβαίνει με τον «offline stalker», ο οποίος βλέπει το θύμα να φοβάται και να τροποποιεί το πρόγραμμα των καθημερινών του δραστηριοτήτων. Άρα, ο «cyberstalker» λαμβάνει έμμεση ευχαρίστηση βλέποντας π.χ. το θύμα - στόχο να αποχωρεί από κάποιο δωμάτιο συζήτησης κατόπιν υβριστικών ή προσβλητικών σχολίων σε βάρος του. Η ικανοποίηση είναι πολύ μικρότερη και λιγότερο διεγερτική για τον «cyberstalker» με αποτέλεσμα είτε τη διακοπή της συμπεριφοράς, ή την κλιμάκωσή της σε φυσική παρακολούθηση ή την αναζήτηση νέου θύματος[88].

[85] Βλ. Goodno, ό.π., σ. 129-130
[86] Βλ. Bocij & McFarlane, An Exploration of Predatory Behaviour in Cyberspace: Towards a Typology of Cyberstalkers, ό.π., σ. 2
[87] Βλ. Bocij, Victims of Cyberstalking: An Explanatory Study of Harassment Perpetrated via the Internet, ό.π., σ. 9
[88] Στο ίδιο, σ. 9-10

3. Περιγραφή της συμπεριφοράς και οι ειδικότερες μορφές εκδήλωσής της

3.1. Τα χαρακτηριστικά και τα μέσα τέλεσης του αδικήματος

Σύμφωνα με το CyberAngels[89], μια online πλατφόρμα για την ασφαλή πλοήγηση στο Διαδίκτυο και την παροχή βοήθειας, συνδρομής και υποστήριξης σε θύματα «cyberstalking», μια συμπεριφορά που εμπίπτει σε αυτή τη μορφή ηλεκτρονικού εγκλήματος χαρακτηρίζεται από δόλο (malice), προσχεδιασμό (premeditation), επανάληψη (repetition), εμμονή (obsession), απουσία νόμιμου σκοπού (no legitimate purpose), παρενόχληση (harassment), απειλές (threats), ενώ εκδηλώνεται σε βάρος συγκεκριμένου θύματος - στόχου (personally directed) και το θύμα έχει προηγουμένως απευθύνει προειδοποιήσεις στο δράστη να την σταματήσει και εκείνος τις έχει αγνοήσει[90].

Επίσης, οι Bocij και McFarlane (2002) επιχειρώντας να ορίσουν τι είναι το «cyberstalking» υποστήριξαν πως η συμπεριφορά περιλαμβάνει απειλές σε βάρος του θύματος ή των οικείων του μέσω ηλεκτρονικού ταχυδρομείου ή της τεχνολογίας άμεσης ανταλλαγής μηνυμάτων (Instant Messaging/IM)[91], μετάδοση ψευδών κατηγοριών με στόχο την πρόκληση βλάβης στην τιμή και υπόληψη του θύματος σε διαδικτυακούς ιστότοπους, δωμάτια συζητήσεων, πίνακες ανακοινώσεων (bulletin boards), ιστολόγια (blogs) κ.ά., αποστολή υβριστικών, προσβλητικών ή με άσεμνο περιεχόμενο μηνυμάτων μέσω email ή της υπηρεσίας άμεσης ανταλλαγής μηνυμάτων, επιθέσεις στον εξοπλισμό ή τα δεδομένα του θύματος με την αποστολή ιού και την εγκατάσταση κακόβουλου λογισμικού (malware) στον Η/Υ με σκοπό την καταστροφή τους ή την παρακολούθηση - καταγραφή των δραστηριοτήτων του θύματος, συλλογή προσωπικών πληροφορίων για το θύμα αξιοποιώντας τις δυνατότητες της ευρείας και ταχύτατης αναζήτησης πληροφοριών στο Διαδίκτυο (π.χ. Παγκόσμιος Ιστός και μηχανές αναζήτησης όπως η Google), προσλαμβάνοντας ιδιωτικό ερευνητή ή προσεγγίζοντας διαδικτυακά το θύμα με το πρόσχημα της φιλίας ή της σύναψης σχέσης[92].

---

[89] Βλ. https://www.cyberangels.org/cyber-security/ (επίσκεψη την 11-08-2022)

[90] Βλ. Bocij & McFarlane, Online harassment: towards a definition of cyberstalking, ό.π., σ. 36

[91] Πρόκειται για έναν τύπο διαδικτυακής συνομιλίας που επιτρέπει την ανταλλαγή μηνυμάτων σε πραγματικό (άμεσο) χρόνο μέσω του Διαδικτύου ή άλλου δικτύου Η/Υ χωρίς να περιμένει ο αποστολέας πολλή ώρα να φτάσει το μήνυμα στον αποδέκτη (π.χ. Facebook Messenger), βλ. https://en.wikipedia.org/wiki/Instant_messaging επίσκεψη την 26-01-2023

[92] Βλ. Bocij, Chapter 1 What Is Cyberstalking?, στο P. Bocij (επιμ.), *Cyberstalking: Harassment in the Internet Age and How to Protect Your Family*, ό.π., σ. 12-14

Επιπλέον, ο «cyberstalker» ενδέχεται να υποδύεται το θύμα με σκοπό να το εξευτελίσει ή να προβεί σε ακριβές αγορές προϊόντων ή υπηρεσιών μέσω Διαδικτύου εξ ονόματός του, αλλά και να ενθαρρύνει τρίτους να συνεχίσουν την παρενοχλητική συμπεριφορά αναρτώντας αγγελίες στο Διαδίκτυο με τα προσωπικά στοιχεία του θύματος (π.χ. για παροχή σεξουαλικών υπηρεσιών) με αποτέλεσμα άλλοι ανυποψίαστοι χρήστες να ενοχλούν το θύμα[93].

Κατά τους Mansourabadi και Salimi (2014) η παρενόχληση, η απειλή και ο εκφοβισμός του θύματος από τον δράστη μπορεί να επιτευχθεί με τους ακόλουθους τρόπους: 1) παρακολουθώντας κρυφά το θύμα σε όλες τις διαδικτυακές κοινότητες που συμμετέχει καθώς και τις δημοσιεύσεις και τις online δραστηριότητες τόσο του ίδιου όσο και των οικείων του προσώπων, 2) συλλέγοντας φωτογραφίες του θύματος - στόχου από τα προφίλ που διατηρεί στα μέσα κοινωνικής δικτύωσης και χρήση τους, κατόπιν επεξεργασίας, για παράνομους σκοπούς (π.χ. πορνογραφίας ή δυσφήμισης), 3) δημιουργώντας ψεύτικο προφίλ με τα προσωπικά στοιχεία του θύματος και στέλνοντας αιτήματα φιλίας σε προσφιλή του άτομα (οικογενειακό, κοινωνικό, επαγγελματικό περιβάλλον) επιτυγχάνοντας να παρακολουθεί και τις δραστηριότητες των προσώπων που σχετίζονται στενά με το θύμα - στόχο (phishing), 4) αποκτώντας παράνομη και μη εξουσιοδοτημένη πρόσβαση στο προφίλ του θύματος και αξιοποιώντας τις προσωπικές του πληροφορίες με κακόβουλη πρόθεση (hacking), 5) αποστέλλοντας κατ' επανάληψη email ή αιτήματα φιλίας στα διατηρούμενα από το θύμα προφίλ σε μέσα κοινωνικής δικτύωσης με σκοπό τη γελοιοποίησή του ή τον εκφοβισμό του τόσο στο προφίλ του όσο και στις διαδικτυακές ομάδες στις οποίες συμμετέχει (cyberbullying - vituperation), 6) αποκλείοντας την έκφραση προσωπικής άποψης του θύματος σε διαδικτυακές κοινότητες των οποίων είναι μέλος ή forums (blocking a user and preventing him/her from expressing his/her views)[94].

Τα μέσα που χρησιμοποιεί ο «cyberstalker» εντάσσονται στον ευρύτερο τομέα των ΤΠΕ, των υπηρεσιών Διαδικτύου και του Κυβερνοχώρου. Τα κοινωνικά δίκτυα (social networks) και τα μέσα κοινωνικής δικτύωσης (social media) βοηθούν μεν στην κοινωνικοποίηση ιδίως των ανηλίκων και των νεότερων ηλικιακά ατόμων, αλλά αυξάνουν και τον κίνδυνο της θυματοποίησης από «cyberstalking». Από πορίσματα

[93] ό.π.

[94] Βλ. A. Mansourabadi και E. Salimi, The Criminology of Cyber stalking: Investigating the Crime, Offenders and Victims of Cyber Stalking, *International Journal of Criminology and Sociological Theory*, Vol. 7, No. 2, 2014, σ. 2-3, Ανακτήθηκε από: https://ijcst.journals.yorku.ca/index.php/ijcst/issue/view/2266

ερευνών έχει επιβεβαιωθεί πως οι γυναίκες είναι πιο ευάλωτοι στόχοι των κυβερνοεγκλημάτων και καθίστανται πιο συχνά θύματα «cyberstalking» σε σχέση με τους άνδρες[95]. Τα μέσα κοινωνικής δικτύωσης είναι περισσότερο ελκυστικά για τα έφηβα κορίτσια και τις γυναίκες, διότι πιστεύουν πως στο ψηφιακό περιβάλλον είναι μικρότερος ο κίνδυνος να πέσουν θύματα σεξουαλικής παρενόχλησης και πως απειλείται λιγότερο η ιδιωτικότητά τους σε σχέση με τον πραγματικό κόσμο. Ταυτόχρονα, ωστόσο, ελλοχεύουν οι κίνδυνοι χρήσης των προσωπικών δεδομένων των χρηστών σε παράνομες δραστηριότητες, κλοπής της ταυτότητας (identity theft) και διαδικτυακής σεξουαλικής παρενόχλησης (sexual online harassment)[96]. Επίσης, σύμφωνα με αποτελέσματα ερευνών έχει αποδειχθεί πως το ηλεκτρονικό ταχυδρομείο χρησιμοποιείται πολύ περισσότερο από άλλες ηλεκτρονικές επικοινωνιακές τεχνολογίες για την παρενόχληση ή τον εκφοβισμό, διότι επιτρέπει την εύκολη, άμεση και μαζική αποστολή μηνυμάτων με προσβλητικό, άσεμνο ή απαράδεκτο περιεχόμενο[97].

Ακόμη, τα δωμάτια συζήτησης, οι πίνακες ανακοινώσεων και οι ομάδες/χώροι συζητήσεων (discussion groups/forums) προσφέρουν πρόσφορο έδαφος για την εμφάνιση παρενοχλητικής συμπεριφοράς από τους χρήστες του Διαδικτύου. Επιπρόσθετα, η ανταλλαγή άμεσων μηνυμάτων σε πραγματικό χρόνο και οι ιστοσελίδες που επιτρέπουν την ελεύθερη έκφραση θυμού και αγανάκτησης, την ανταλλαγή πληροφοριών και υλικού μεταξύ των χρηστών (που μπορεί να περιλαμβάνει π.χ. προσβλητικά σχόλια για γυναίκες από τους πρώην συντρόφους τους, αποστολή υλικού με άσεμνο περιεχόμενο σε όλους τους χρήστες, κ.ο.κ.), αποτελούν ορισμένα από τα εργαλεία του «cyberstalking». Πρόκειται για τις «crime-stimulating websites» με πιο διαδεδομένη την www.myspace.com[98].

[95] Στο ίδιο, σ. 7
[96] Στο ίδιο, σ. 3-5
[97] Σχετική με το ηλεκτρονικό ταχυδρομείο είναι η υπηρεσία των «anonymous remailers» για την επαναποστολή ενός συγκεκριμένου email στον αποδέκτη - στόχο μέσω της χρήσης της υπηρεσίας αυτής με την οποία παραμένει άγνωστη στον αποδέκτη η διεύθυνση ηλεκτρονικού ταχυδρομείου από την οποία εστάλη, βλ. ό.π.
[98] ό.π. και Spence-Diehl, ό.π., σ. 10 και Μήτρου, ό.π., σ. 12

3.2. Ειδικότερες μορφές εκδήλωσης του «cyberstalking»

3.2.1. Το «email stalking». Πρόκειται για την παρακολούθηση μέσω ηλεκτρονικού ταχυδρομείου και αποτελεί μια επιμέρους μορφή διάπραξης του αδικήματος του «cyberstalking». Σύμφωνα με τον Ogilvie (2000) το «email stalking» αποτελεί την ιδιωτική διάσταση του «cyberstalking», καθώς η επικοινωνία μέσω της χρήσης του ηλεκτρονικού ταχυδρομείου λαμβάνει χώρα μεταξύ του αποστολέα και συγκεκριμένου ατόμου, και όχι απροσδιόριστου αριθμού αποδεκτών[99]. Ως περισσότερο εκλεπτυσμένος τρόπος παρέμβασης στην ιδιωτική ζωή του θύματος αποτελεί εκείνη τη μορφή ηλεκτρονικής επικοινωνίας που επιτρέπει την τάχιστη αποστολή μηνυμάτων από έναν Η/Υ ή άλλη ηλεκτρονική συσκευή συνδεδεμένη στο Διαδίκτυο σε πολλά δίκτυα Η/Υ ή συσκευές συνδεδεμένες στο Διαδίκτυο[100].

Από πορίσματα ερευνών έχει προκύψει πως πρόκειται για την ευχερέστερη και περισσότερο συχνά χρησιμοποιούμενη μέθοδο ηλεκτρονικής επικοινωνίας από τους «cyberstalkers», διότι επιτρέπει την αποστολή μηνυμάτων με προσβλητικό, άσεμνο, απειλητικό ή απαράδεκτο περιεχόμενο, αλλά και υλικού πρόσφορου για παρενόχληση ή εκφοβισμό δεδομένης της απουσίας λογοκρισίας στο Διαδίκτυο και της ελεύθερης αποστολής μηνυμάτων[101].

Μέσω ηλεκτρονικού ταχυδρομείου ο «cyberstalker» αποστέλλει κατά τρόπο συνεχή, επίμονο και πιεστικό γραπτά μηνύματα, φωτογραφίες, οπτικο-ακουστικό υλικό στο θύμα (email bombing) προβαίνοντας έτσι σε λεκτική ή μη παρενόχληση (email harassment)[102]. Εκτός από αυτό, ο δράστης μπορεί να προβαίνει σε μαζική αποστολή ηλεκτρονικών μηνυμάτων ή εξωτερικών συνδέσμων σε απεριόριστο αριθμό αποδεκτών για εμπορικούς συνήθως σκοπούς (spamming), χωρίς να έχουν δείξει ανάλογο ενδιαφέρον, «γεμίζοντας» κατ' αυτόν τον τρόπο το ηλεκτρονικό τους ταχυδρομείο (electronic junk mail)[103]. Ακόμη, το ηλεκτρονικό ταχυδρομείο προσφέρεται για την αποστολή κακόβουλου λογισμικού με κρυμμένους ιούς σε αρχεία με σκοπό την καταστροφή των αρχείων του θύματος ή τη μετάδοση ιού στους Η/Υ των

---

[99] Βλ. Roberts, ό.π., σ. 275

[100] Βλ. E. Ross, E-Mail Stalking: Is Adequate Legal Protection Available?, *J. Marshall Journal of Computer & Information Law 405*, Vol. 13, Issue 3, 1995, σ. 410, Ανακτήθηκε από: "E-Mail Stalking: Is Adequate Legal Protection Available?, 13 J. Marsha" by Eileen S. Ross (uic.edu)

[101] Βλ. Κατσογιάννου, ό.π., σ. 1497 και Mansourabadi και Salimi, ό.π., σ. 4

[102] Στο ίδιο, σ. 1498

[103] Βλ. E. Ogilvie, Cyberstalking, *Trends and Issues in Crime and Criminal Justice*, Australian Institute of Criminology, No. 166, 2000, σ. 2, Ανακτήθηκε από: https://www.aic.gov.au/publications/tandi/tandi166 και https://cyberalert.gr/spamming/ (επίσκεψη την 12-08-2022)

χρηστών, που είναι αποθηκευμένοι στη λίστα επαφών του θύματος[104]. Στις ανωτέρω ενέργειες προβαίνει χρησιμοποιώντας τις δυνατότητες των «anonymous remailers», που αναφέρθηκαν στο αμέσως προηγούμενο υπο-κεφάλαιο, ώστε να αποπροσανατολίσει το θύμα[105].

3.2.2. Το «computer stalking». Απαιτείται εξοικείωση με τον Η/Υ και το Διαδίκτυο, καθώς περιλαμβάνει την χρήση κακόβουλου λογισμικού και την παράνομη και μη εξουσιοδοτημένη πρόσβαση στον Η/Υ, τα αρχεία και τα δεδομένα του θύματος με σκοπό την καταστροφή ή τη δυσλειτουργία τους. Αυτή η μορφή εμμονικής παρακολούθησης εμφανίζεται συνήθως συνδυαστικά με το «internet stalking», που περιλαμβάνει την χρήση του Διαδικτύου και θα αναλυθεί αμέσως πιο κάτω[106].

Ειδικότερα, ο «computer cyberstalker» χρησιμοποιεί λογισμικό κατασκοπίας (spyware) για να συνδεθεί στον Η/Υ του θύματος και να παρακολουθεί χωρίς να γίνεται αντιληπτός τις κινήσεις και τις δραστηριότητές του. Μπορεί, επίσης, να προβεί στην χρήση δούρειων ίππων (trojan horses) και ιών (viruses), οι οποίοι εγκαθιστούν στον Η/Υ του θύματος κακόβουλο λογισμικό - προγράμματα «κερκόπορτας» (backdoor trojan), με τα οποία ο δράστης μπορεί να παρακολουθεί τις συσκευές εισόδου, να ελέγχει, αλλά και να χειρίζεται το πληκτρολόγιο και τον κέρσορα της οθόνης. Δημιουργείται έτσι κίνδυνος υποκλοπής κωδικών πρόσβασης και δεδομένων προσωπικού χαρακτήρα του θύματος, αριθμών πιστωτικών καρτών, περιεχομένου των επικοινωνιών του, που μπορεί να αξιοποιήσει ο «cyberstalker» για να υποδυθεί το θύμα και να «οικειοποιηθεί» την ταυτότητά του (identity theft) προβαίνοντας ακολούθως σε αγορές προϊόντων ή υπηρεσιών στο Διαδίκτυο, ανάρτηση αγγελιών, διαφημίσεων, σχολίων κ.λπ.[107] Τέλος, η μέθοδος του «ratting» δίνει στον επίδοξο «cyberstalker» τη δυνατότητα απομακρυσμένης και εκ του ασφαλούς οπτικής επαφής με το θύμα μέσω κάμερας (webcam). Το λογισμικό (remote access trojan) εγκαθίσταται στον Η/Υ του θύματος είτε από τον δράστη ή από το ίδιο το θύμα, χωρίς να το γνωρίζει. Κατ' αυτόν τον τρόπο, εγκαθίσταται ιός που επιτρέπει στον δράστη να έχει πρόσβαση στην επιφάνεια εργασίας και τα αρχεία του Η/Υ του θύματος και να καταγράφει σε οπτικά

[104] Βλ. Κατσογιάννου, ό.π., σ. 1498 και Pittaro, ό.π., σ. 186-187
[105] Βλ. Mansourabadi και Salimi, ό.π., σ. 4
[106] Βλ. Κατσογιάννου, ό.π., σ. 1498-1499
[107] Στο ίδιο, σ. 1499-1500

μέσα τις κινήσεις του συλλέγοντας πληροφορίες και παραβιάζοντας την ιδιωτική του ζωή[108].

3.2.3. Το «internet stalking». Πρόκειται για το «cyberstalking» που πραγματοποιείται μέσω του Διαδικτύου με στενή έννοια ή διαφορετικά για την έμμονη παρενοχλητική κυβερνοπαρακολούθηση[109]. Μαζί με το «computer stalking» περιγράφουν τη δημόσια διάσταση του «cyberstalking» λόγω της χρήσης του ανοιχτά προσβάσιμου Διαδικτύου[110]. Οι δυνατότητες που προσφέρει το Διαδίκτυο διευκολύνουν τους δράστες για εύκολη, γρήγορη και χαμηλού κόστους παροχή υπηρεσιών και αναζήτηση πληροφοριών. Μετατρέπονται δηλαδή σε ψηφιακούς ιχνηλάτες της ζωής των θυμάτων αξιοποιώντας σε μεγάλο βαθμό τα μέσα κοινωνικής δικτύωσης για να αντλήσουν προσωπικές πληροφορίες από τα προφίλ τους στα ψηφιακά κοινωνικά δίκτυα που προσφέρονται για τη σύναψη σχέσεων, ομάδες συζητήσεων, δωμάτια συζητήσεων, πίνακες ανακοινώσεων κ.ά.[111].

Επίσης, οι δυνατότητες που παρέχει το Διαδίκτυο για ανταλλαγή μηνυμάτων σε πραγματικό και άμεσο χρόνο[112] και για έκφραση της ψυχολογικής ή συναισθηματικής κατάστασης των χρηστών με την χρήση emoticons χαρακτηρίζουν την εν γένει ηλεκτρονική επικοινωνία και μάλιστα, σύμφωνα με πορίσματα μελετών, η ανταλλαγή μηνυμάτων σε πραγματικό χρόνο αποτελεί τη δεύτερη πιο συχνά χρησιμοποιούμενη μέθοδο των δραστών μετά το ηλεκτρονικό ταχυδρομείο για την επιλογή και προσέγγιση των θυμάτων[113].

Η διαδικτυακή επιθετικότητα που χαρακτηρίζει και το «email stalking», εκδηλώνεται στο «internet stalking» με τη διατύπωση προκλητικών ή εσφαλμένων απόψεων για το θύμα με σκοπό να προκληθεί η αντίδρασή του (μέθοδος trolling)[114]. Η μέθοδος αυτή περιλαμβάνει την αποστολή μηνυμάτων, κυρίως μέσω ηλεκτρονικού ταχυδρομείου, στο θύμα με υβριστικό, προσβλητικό ή απειλητικό περιεχόμενο ή

[108] Στο ίδιο, σ. 1500-1501
[109] Στο ίδιο, σ. 1501
[110] Βλ. Roberts, ό.π., σ. 275
[111] Βλ. Κατσογιάννου, ό.π., σ. 1440
[112] Βλ. Σπ. Τάσσης, Ό,τι πεις θα χρησιμοποιηθεί εναντίον σου; Η χρήση ψηφιακών δικτύων κοινωνικής δικτύωσης και ιστολογίων, Στο: Μ. Καρύδα, Σπ. Κοκολάκης, Λ. Μήτρου, Μ. Πισκοπάνη & Σπ. Τάσσης (επιμ.), *facebook, blogs και δικαιώματα*, Αθήνα, εκδ. Σάκκουλα, 2013, σ. 94-95
[113] Το μειονέκτημα της υπηρεσίας άμεσης ανταλλαγής μηνυμάτων είναι πως τα μηνύματα δεν επιδέχονται κρυπτογράφησης, μπορούν να διαβαστούν και από τρίτα άτομα πέραν του παραλήπτη και είναι ευάλωτα σε ιούς, βλ. ό.π.
[114] Βλ. Κατσογιάννου, ό.π., σ. 1504

αισχρολογώντας σε βάρος του (τακτική «flaming»)[115] και αντιστοιχεί στα «δηλητηριώδη γράμματα» («poison pen letters») που συναντώνται στο «offline stalking». Σκοπός της τακτικής αυτής ως λεκτικής κακοποίησης (verbal abuse) είναι η παρενόχληση μέσω συνομιλίας (chat harassment), η υποτίμηση και ο εξευτελισμός του θύματος[116].

Περαιτέρω, μέθοδοι που χρησιμοποιούνται στο «internet stalking» και ομοιάζουν με αυτές του «email stalking» είναι η ανάρτηση ανακριβών, εξευτελιστικών, ντροπιαστικών ή δυσφημιστικών σε βάρος του θύματος σχολίων ή φημών ή ψευδών υπαινιγμών ή κατηγοριών (false accusations) με σκοπό την βλάβη του κύρους, της τιμής και της υπόληψής του ή η έκφραση ψευδών (συνήθως) σεξουαλικών υπονοούμενων από τον δράστη σχετικά με τις προτιμήσεις του θύματος. Πρόκειται για την τακτική της διαδικτυακής δυσφήμισης (cyber defamation ή άλλως «cybersmearing»)[117]. Η τακτική αυτή περιλαμβάνει επίσης την αποστολή άσεμνων ή τροποποιημένων φωτογραφιών (morphing) του θύματος μέσω email σε οικείους ή συναδέλφους του και τη δημοσίευση άσεμνων ή τροποποιημένων φωτογραφιών του σε ιστότοπους ψηφιακής κοινωνικής δικτύωσης. Τέλος, στη μέθοδο του «trolling» συγκαταλέγεται η δημοσίευση στο Διαδίκτυο βίντεο με προσωπικές στιγμές του θύματος, τις οποίες έχει στη διάθεσή του ο δράστης εξαιτίας προηγούμενης σχέσης μαζί του, καθώς και η ανάρτηση προσωπικών στοιχείων του αναγνωριστικών της ταυτότητάς του σε αγγελίες ή διαφημίσεις σεξουαλικού κυρίως περιεχομένου[118].

4. Θεωρητική προσέγγιση του φαινομένου του «cyberstalking»

4.1. Ψυχολογικές θεωρίες

4.1.1. Η θεωρία της κοινωνικής συμπεριφοράς (The Social Conduct Theory). Ο Gattiker (2001) προσπαθώντας να ερμηνεύσει την εκδηλούμενη στο πλαίσιο των διαδικτυακών ομάδων και κοινοτήτων συμπεριφορά βασίστηκε στη θεωρία της κοινωνικής συμπεριφοράς (social conduct theory)[119]. Όπως στο εξωτερικό περιβάλλον έτσι και στο ψηφιακό, οι ομάδες δομούνται και λειτουργούν στη βάση συγκεκριμένων

[115] ό.π.
[116] Βλ. Pittaro, ό.π., σ. 187
[117] Βλ. Κατσογιάννου, ό.π., σ. 1504
[118] ό.π.
[119] Βλ. Dickinson, ό.π., σ. 13

κανόνων και ηθικής που τα μέλη τους οφείλουν να σεβαστούν και να υιοθετήσουν προκειμένου να εξασφαλιστεί η συνοχή της ομάδας. Συνδυαστικά και με τη θεωρία της γνωστικής ανάπτυξης (cognitive development theory), την οποία αξιοποίησε ο Gattiker για να εξηγήσει τα πρότυπα συμπεριφοράς στις διαδικτυακές ομάδες (online codes of conduct), η ικανότητα να διακρίνει το άτομο το σωστό από το λάθος εξαρτάται από το πόσο αντικειμενικά μπορεί να δει τις καταστάσεις. Αυτό πρακτικά σημαίνει πως στο Διαδίκτυο κάθε χρήστης μπορεί να αντιδράσει διαφορετικά σε μια δεδομένη κατάσταση και κάτι που μπορεί να θεωρείται ασήμαντο για κάποιον άλλον να θεωρείται κατάφορη παραβίαση των κανόνων της συμπεριφοράς και ως εκ τούτου μη αποδεκτή συμπεριφορά, σύμφωνα με το δικό του αξιακό σύστημα και τους κανόνες που έχει ενστερνιστεί. Όταν, λοιπόν, επέρχονται συγκρούσεις μεταξύ των μελών της διαδικτυακής ομάδας και δεδομένης της απουσίας οπτικής επαφής και φυσικής αλληλεπίδρασης, εμφανίζονται δυσπροσαρμοστικές και υπερ-αντισταθμιστικές συμπεριφορές λόγω του διαφορετικού επιπέδου αντικειμενικής αντίληψης και των διαφορετικών ιδεών σχετικά με τους κανόνες και τα πρότυπα συμπεριφοράς[120].

Υπό αυτό το πρίσμα, η online συμπεριφορά ενός χρήστη ως κοινωνική συμπεριφορά διαμορφώνεται τόσο από τις διαφορές μεταξύ των χρηστών, που μπορούν να οδηγήσουν σε λανθασμένους τρόπους συμπεριφοράς (misbehaviors), με το άτομο να μη συμμορφώνεται με τους κανόνες της ομάδας και να τους παραβιάζει (αντικοινωνική συμπεριφορά), όσο και από την ατομική συμπεριφορά[121]. Το μοντέλο αυτό του Gattiker επιχειρήθηκε να χρησιμοποιηθεί για να δείξει αν η συμπεριφορά του «cyberstalking» αποτελεί μια διαφαινόμενη απειλή ή τείνει να αντιμετωπιστεί ως μια «κανονικοποιημένη» παρενόχληση και συμπεριφορά στο Διαδίκτυο (normalized conduct)[122].

4.2. Θεωρίες της επικοινωνίας

4.2.1. Η θεωρία της αποατομίκευσης (The Deindividuation Theory) και το μοντέλο κοινωνικής ταυτότητας που προκύπτει από τις συνέπειες της αποατομίκευσης (The Social Identity Model of Deindividuation Effects/SIDE Theory). Η θεωρητική προσέγγιση του «cyberstalking» δε θα μπορούσε να μην

[120] ό.π.
[121] Στο ίδιο, σ. 9
[122] Στο ίδιο, σ. 13

περιλαμβάνει τις θεωρίες της επικοινωνίας από την στιγμή που αποτελεί συμπεριφορά και τρόπο επικοινωνίας που πραγματοποιείται διαμέσου Η/Υ. Η θεωρία που έχει χρησιμοποιηθεί για να πλαισιώσει την προβληματική του αν το «cyberstalking» τείνει να «κανονικοποιηθεί» ή αν εκλαμβάνεται ως μια μορφή αντικοινωνικής διαδικτυακής συμπεριφοράς είναι η θεωρία της αποατομίκευσης (deindividuation theory) και το μοντέλο της κοινωνικής ταυτότητας που προκύπτει από της συνέπειές της (social identity model of deindividuation effects/SIDE theory)[123].

Η θεωρία της αποατομίκευσης χρησιμοποιείται για τη μελέτη της συμπεριφοράς του πλήθους και την απώλεια της αυτογνωσίας που παρατηρείται στις ομάδες. Ειδικότερα, η θεωρία στοχεύει να εξηγήσει τις συλλογικές και αντικοινωνικές ενέργειες των ατόμων μέσα σε πλήθος/όχλο κάνοντας λόγο για μια ψυχολογική κατάσταση μειωμένης αυτοαξιολόγησης και ανησυχίας για την αντίδραση που προκαλεί μια αντικανονική και απαγορευμένη συμπεριφορά. Ωστόσο, εξαιτίας της ανάγκης εξήγησης των αντικοινωνικών συμπεριφορών που εμφανίζονται στο διαδικτυακό περιβάλλον και ειδικά στις διαδικτυακές κοινότητες η θεωρία επεκτάθηκε και στην διαδικτυακή επικοινωνία[124].

Υποστηρίζεται, λοιπόν, πως τα άτομα όταν δραστηριοποιούνται σε μεγάλες ομάδες και όχλους, βιώνουν την απώλεια της αίσθησης του εαυτού τους και της ατομικότητάς τους, με αποτέλεσμα να μειώνονται οι εσωτερικοί περιορισμοί και να εμφανίζονται συχνότερα συμπεριφορές που υπό άλλες συνθήκες θα είχαν αποτραπεί. Επίσης, η διάχυση της ευθύνης και η ανωνυμία συμβάλλουν στο να χάνουν τα άτομα την ιδιότητα να αξιολογούν τη συμπεριφορά τους και να συμμορφώνονται με τις ενέργειες της ομάδας συμμετέχοντας σε αντικοινωνικές και αντικανονικές συμπεριφορές. Μολονότι η θεωρία αρχικά χρησιμοποιήθηκε για την ανάλυση των αρνητικών συμπεριφορών που εκδηλώνονται στο πλαίσιο των ομάδων (π.χ. βία του όχλου), μια μετα-ανάλυση των Postmes και Spears το 1998 θεμελίωσε ακριβώς το αντίθετο, δηλαδή τη θετική επίδραση της αποατομίκευσης, όπως είναι η μεγαλύτερη τήρηση και συμμόρφωση του ατόμου προς τους κανόνες στο πλαίσιο των μεγάλων ομάδων[125].

Έτσι λοιπόν, η καταλληλότητα της θεωρίας της αποατομίκευσης για την πλαισίωση της online συμπεριφοράς οδήγησε στη δόμηση της θεωρίας για την

[123] Στο ίδιο, σ. 9
[124] Στο ίδιο, σ. 10
[125] ό.π.

κοινωνική ταυτότητα που διαμορφώνεται εξαιτίας των συνεπειών της αποατομίκευσης. Η θεωρία αυτή διατυπώθηκε από τους Postmes, Spears και Lea και αποτελεί ένα συνδυασμό των θεωριών της κοινωνικής ταυτότητας (social identity theory) και της αποατομίκευσης. Χρησιμοποιήθηκε για την προσέγγιση της διαδικτυακής συμπεριφοράς όπως το «cyberstalking», είτε ως κανονικότητα, ή ως λανθασμένος τρόπος συμπεριφοράς[126].

Οι θεμελιωτές της θεωρίας υποστήριξαν πως μέσα στις μεγάλες ομάδες η κοινωνική ταυτότητα εμφανίζεται ως απόρροια της αποατομίκευσης του ατόμου χωρίς να απαιτείται η οπτική επαφή και η δια ζώσης επικοινωνία με άλλα άτομα, κάτι που αποτελεί κυρίαρχο χαρακτηριστικό του Διαδικτύου. Η δραστηριοποίηση στις ομάδες και η συνακόλουθη αποατομίκευση προκαλεί την εμφάνιση συμπεριφορών που υπό άλλες συνθήκες δε θα εκδήλωναν τα άτομα, εξαιτίας του αισθήματος της ντροπής, της ατομικής ηθικής και ευσυνειδησίας που τα διακατέχουν[127].

Επεκτείνοντας την εν λόγω θεωρία στο Διαδίκτυο η συμμετοχή σε διαδικτυακές κοινότητες οδηγεί σε συμμόρφωση των χρηστών σε ήδη υπάρχοντες και προεπιλεγμένους κανόνες που καθορίζουν τα όρια της συμπεριφοράς τους[128]. Επιπλέον, αναγκάζει τους χρήστες να ενστερνίζονται πρότυπα συμπεριφοράς που προβάλλονται μέσα στην ομάδα, δίνοντας έτσι την εντύπωση πως η αλληλεπίδραση στο Διαδίκτυο είναι τόσο πραγματική όσο και η κοινωνικοποίηση στο «εξω-διαδικτυακό» περιβάλλον[129]. Αν το άτομο υιοθετήσει την κοινωνική ταυτότητα που έχει αποδοθεί και στα υπόλοιπα μέλη της ομάδας στην οποία ανήκει στο Διαδίκτυο, τότε θα συμμορφωθεί και θα ακολουθήσει τους κανόνες που διέπουν τη λειτουργία της, ενώ αν διατηρήσει την ατομική του ταυτότητα, μολονότι βιώνει τις συνέπειες της αποατομίκευσης, θα απομακρυνθεί από αυτούς[130].

Με άλλα λόγια, η SIDE theory εξηγεί πώς οι διαδικτυακές ομάδες διαμορφώνουν τους δικούς τους κανόνες, στη βάση των οποίων επιτυγχάνεται η συνοχή, ενώ όσο μεγαλύτερη είναι η επίδραση της αποατομίκευσης, τόσο πιθανότερο είναι το άτομο να τηρήσει αυστηρά τους κανόνες της ομάδας. Τέλος, όσον αφορά το «cyberstalking», τείνει να εκλαμβάνεται ως μια «κανονικοποιημένη» συμπεριφορά στο

[126] Στο ίδιο, σ. 10-11
[127] ό.π.
[128] Π.χ. η τακτική του «flaming» συναντάται σε δωμάτια ή ομάδες συζητήσεων (chatrooms ή discussion groups) για βιντεοπαιχνίδια αλλά δε θα χρησιμοποιηθεί από τα μέλη μιας ομάδας συζήτησης περί μητρότητας, βλ. στο ίδιο, σ. 11
[129] ό.π.
[130] Στο ίδιο, σ. 12-13

Διαδίκτυο, την οποία είναι πιο πιθανό να αποδεχτούν οι χρήστες - θύματα λόγω του ότι δεν έχουν άλλη επιλογή, ώστε να μπορέσουν να επικοινωνούν με άλλους χρήστες ηλεκτρονικά[131].

4.3. Εγκληματολογικές θεωρίες

4.3.1. Η θεωρία της ορθολογικής επιλογής (The Rational Choice Theory). Όπως έχει ήδη αναφερθεί, η τεχνολογική πρόοδος και η ευρύτατη χρήση των ΤΠΕ και του Διαδικτύου δημιούργησαν νέες εγκληματικές ευκαιρίες στο ψηφιακό περιβάλλον, οι οποίες συνδυαστικά με το κίνητρο των δραστών και τα διαθέσιμα ηλεκτρονικά μέσα οδήγησαν στην εμφάνιση ποικίλων μορφών ηλεκτρονικής εγκληματικότητας. Λαμβάνοντας υπόψη τη σημαντικότητα του περιβάλλοντος για τη δόμηση των εγκληματικών ευκαιριών στο πλαίσιο της περιβαλλοντικής εγκληματολογίας (environmental ή green criminology) αναπτύχθηκαν νέες θεωρίες/προσεγγίσεις για τις εγκληματικές ευκαιρίες (new crime opportunity theories/approaches), που πλαισιώνουν θεωρητικά τα ηλεκτρονικά εγκλήματα και κατ' επέκταση και το «cyberstalking»[132].

Η θεωρία της ορθολογικής επιλογής (The Rational Choice Theory) εστιάζει στη διαδικασία λήψης απόφασης για τη διάπραξη του εγκλήματος από τον εγκληματία. Βασιζόμενη στις απόψεις του Beccaria περί ελεύθερης βούλησης και επιλογής του ατόμου, εξηγεί πως η ανθρώπινη συμπεριφορά εξαρτάται από τις καταστάσεις και η τροποποίηση των ευκαιριών μπορεί να οδηγήσει σε μείωση της εγκληματικότητας. Περαιτέρω, οι Clarke και Felson το 1986 επικεντρώθηκαν στην ικανότητα του ατόμου να ελέγχει τη συμπεριφορά του και πως οι ενέργειες του εγκληματία συνιστούν ορθολογικές επιλογές, ώστε να ικανοποιηθούν οι ανάγκες και οι επιθυμίες του. Εστιάζοντας στον εγκληματία εξηγούν πως η απόφαση περί διάπραξης ή μη ενός εγκλήματος λαμβάνεται κατόπιν στάθμισης του οφέλους και των ρίσκων από την τέλεσή του. Η εγκληματική συμπεριφορά είναι επομένως σκόπιμη προς αποκόμιση οφέλους (κίνητρο), βασίζεται στη λογική του εγκληματία και για τη λήψη της απόφασης συνυπολογίζονται η ποιότητα των διαθέσιμων πληροφοριών και η άνεση

---

[131] ό.π.

[132] Βλ. R. Clarke & M. Felson, Opportunity Makes The Thief – Practical theory for crime prevention, *Police Research Series*, Paper 98, Policing and Reducing Crime Unit and Research, Development and Statistics Directorate of the Home Office, 1998, σ. 4, Ανακτήθηκε από: https://popcenter.asu.edu/sites/default/files/opportunity_makes_the_thief.pdf

χρόνου. Με άλλα λόγια, ο επίδοξος δράστης θα σταθμίσει ορθολογικά τα επιδιωκόμενα οφέλη και τα ρίσκα τέλεσης ενός συγκεκριμένου εγκλήματος (π.χ. πιθανότητα σύλληψης και καταδίκης κ.λπ.) και είτε θα αποφασίσει τη διάπραξή του σε άμεσο χρόνο ή θα το αποφύγει[133].

Όσον αφορά το «cyberstalking» η θεωρία της ορθολογικής επιλογής εξηγεί τη συμπεριφορά του «cyberstalker», ο οποίος ενεργεί κατά τον ίδιο τρόπο, σταθμίζοντας τα οφέλη (π.χ. αντίποινα, εκδίκηση, κέρδος, ανταγωνισμός) και τα ρίσκα (π.χ. ανακάλυψη ταυτότητας μέσω του εντοπισμού των ψηφιακών ιχνών και σύλληψη) από την εκδήλωση της συμπεριφοράς. Ωστόσο, λόγω των ιδιαιτεροτήτων του διαδικτυακού περιβάλλοντος ο κίνδυνος εντοπισμού είναι μικρότερος, όπως και λιγότερες είναι οι πιθανότητες ταυτοποίησης, σύλληψης, απαγγελίας κατηγοριών και καταδίκης με αποτέλεσμα να καθίσταται το «cyberstalking» μια ελκυστική επιλογή για τους επίδοξους δράστες[134].

4.3.2. Η θεωρία των καθημερινών δραστηριοτήτων (The Routine Activity Theory). Η θεωρία των καθημερινών δραστηριοτήτων (The Routine Activity Theory) διατυπώθηκε από τους Cohen και Felson το 1979. Χρησιμοποιείται για να εξηγήσει πως η διάπραξη ενός εγκλήματος εξαρτάται από τη συνδρομή τριών σωρευτικών προϋποθέσεων: 1) την ύπαρξη ενός επίδοξου δράστη με κίνητρο (motivated offender), 2) την ύπαρξη ενός κατάλληλου στόχου (suitable target) και 3) την απουσία ικανού φύλακα για την προστασία του στόχου (absence of capable guardian). Όταν δεν υπάρχει ικανός φύλακας, τότε ο κατάλληλος στόχος καθίσταται ευάλωτος σε πιθανή εγκληματική επίθεση, κάτι το οποίο εξαρτάται από τη θέση του στο χώρο και τον χρόνο και συναρτάται με την αξία (Value), την αδράνεια (Inertia), την ορατότητα (Visibility) και την πρόσβαση (Access) σε αυτόν. Η επιλογή του κατάλληλου στόχου από τον επίδοξο δράστη επί απουσίας ικανού φύλακα εξαρτάται σε μεγάλο βαθμό από την καθημερινή ρουτίνα των ατόμων και τις επαναλαμβανόμενες δραστηριότητές τους στην καθημερινή τους ζωή[135].

Η θεωρία αυτή συνδυαστικά με τη θεωρία της έκθεσης (δημοσιοποίησης) του τρόπου ζωής (The Lifestyle Exposure Theory), για την οποία θα γίνει λόγος στην αμέσως επόμενη ενότητα, χρησιμοποιούνται για να πλαισιώσουν θεωρητικά τη δόμηση

[133] Στο ίδιο, σ. 7-8
[134] Βλ. Pittaro, ό.π., σ. 189
[135] Βλ. Clarke & Felson, ό.π., σ. 4-6

των εγκληματικών ευκαιριών στο ψηφιακό περιβάλλον και τη διαδικτυακή θυματοποίηση (cyber-victimization). Δεδομένης της απουσίας χρονικής και τοπικής εγγύτητας μεταξύ δράστη και θύματος, η θεωρία μεταλλάσσεται έτσι ώστε οι προϋποθέσεις που πρέπει να συντρέχουν σωρευτικά για τη δημιουργία της εγκληματικής ευκαιρίας να είναι η διαδικτυακή έκθεση σε κινητοποιημένους δράστες (online exposure to motivated offenders), η διαδικτυακή εγγύτητα με κινητοποιημένους δράστες (online proximity to motivated offenders), η απουσία διαδικτυακής φύλαξης του στόχου (absence of online guardianship), η διαδικτυακή ελκυστικότητα του στόχου (online target attractiveness) και η εμπλοκή σε επικίνδυνες ή αποκλίνουσες διαδικτυακές δραστηριότητες (participation in risky or deviant online activities)[136].

Από μελέτη που διεξήχθη σχετικά με τη θυματοποίηση από το «cyberstalking» προέκυψε πως η διαδικτυακή έκθεση σε κινητοποιημένους δράστες μπορεί να γίνει κατανοητή μέσα από τον χρόνο που οι χρήστες παραμένουν συνδεδεμένοι στο Διαδίκτυο καθημερινά, τον αριθμό των προφίλ που διατηρούν στα κοινωνικά δίκτυα, τη συχνότητα επικαιροποίησης των προσωπικών τους πληροφοριών κάθε μέρα στους λογαριασμούς που διαθέτουν στα κοινωνικά δίκτυα, τον αριθμό των φωτογραφιών που αναρτούν σε καθημερινή βάση και την χρήση ή όχι της υπηρεσίας ανταλλαγής άμεσων μηνυμάτων. Η διαδικτυακή εγγύτητα με κινητοποιημένους δράστες μπορεί να γίνει αντιληπτή ως την επιλογή που έχει ο χρήστης να επιτρέπει σε αγνώστους να έχουν πρόσβαση σε προσωπικά προφίλ, φωτογραφίες και προσωπικές πληροφορίες που διατηρεί σε κοινωνικά δίκτυα, του αριθμού των διαδικτυακών του φίλων στα μέσα κοινωνικής δικτύωσης, καθώς και της χρήσης διαδικτυακών υπηρεσιών που θα τον βοηθήσουν να αποκτήσει διαδικτυακούς φίλους στις πλατφόρμες κοινωνικής δικτύωσης. Όσον αφορά τη διαδικτυακή φύλαξη του στόχου αυτή περιλαμβάνει τείχη προστασίας (firewalls), προγράμματα ασφαλείας (security programs), προεπιλογή ρυθμίσεων για το ποιος θα έχει πρόσβαση στο προφίλ του χρήστη ή και χρήση διαδικτυακής υπηρεσίας για τον εντοπισμό των χρηστών που έχουν επισκεφθεί το προφίλ του στα κοινωνικά δίκτυα. Ακολούθως, η διαδικτυακή ελκυστικότητα του στόχου αφορά στόχους που έχουν μεγαλύτερη αξία για τον επίδοξο δράστη ή είναι ευκολότερο να θυματοποιηθούν. Στην κατηγορία αυτή εμπίπτουν τα κοινωνικο-δημογραφικά χαρακτηριστικά και οι προσωπικές πληροφορίες των πιθανών θυμάτων

[136] Βλ. B. Fisher & B. Henson, Being Pursued Online: Applying Cyberlifestyle – Routine Activities Theory to Cyberstalking Victimization, *Criminal Justice and Behavior*, Vol. 38, No. 11, 2011, σ. 1151-1153, doi: http://dx.doi.org/10.1177/0093854811421448

όπως είναι το φύλο, τα ενδιαφέροντα, η οικογενειακή κατάσταση, φωτογραφίες και βίντεο που έχουν αναρτηθεί στα προφίλ τους στα κοινωνικά δίκτυα, κ.ά.[137].

4.4. Θυματολογικές θεωρίες

4.4.1. Η θεωρία της έκθεσης (δημοσιοποίησης) του τρόπου ζωής (The Lifestyle Exposure Theory). Συνδυαστικά με τη θεωρία των καθημερινών δραστηριοτήτων συγκροτούν το θεωρητικό πλαίσιο προσέγγισης του «cyberstalking» υπό το πρίσμα των θυματολογικών θεωριών (Lifestyle/Routine Activity theory/LRAT). Το χαρακτηριστικό τους είναι πως εστιάζουν κυρίως στο θύμα, το οποίο διευκολύνει, έστω και ακούσια, τις ενέργειες του δράστη, με αποτέλεσμα να γίνεται λόγος στη βιβλιογραφία για μετατόπιση της ευθύνης θυματοποίησης στο ίδιο το θύμα, καθώς συμβάλλει στην ψηφιακή αυτοέκθεσή του και συνεπώς και στην ψηφιακή θυματοποίησή του[138].

Οι Hinderlang, Gottfredson και Garofalo (1978) υποστήριξαν πως οι εγκληματικές ευκαιρίες δημιουργούνται μέσα από την καθημερινή ρουτίνα και τον τρόπο ζωής των ατόμων, που τους εκθέτουν σε κίνδυνο. Πέρα όμως από την εξήγηση της παραδοσιακής εγκληματικότητας και θυματοποίησης οι θεωρίες αυτές χρησιμοποιήθηκαν για την θεωρητική τεκμηρίωση του εγκλήματος στον Κυβερνοχώρο, αφού τα πιθανά θύματα μπορούν να έρθουν σε επαφή με εν δυνάμει δράστες χωρίς να απαιτείται φυσική αλληλεπίδραση και χρονική εγγύτητα, κάτι το οποίο ισχύει στο Διαδίκτυο. Επομένως, η θεωρία της έκθεσης (δημοσιοποίησης) αφορά και τον διαδικτυακό τρόπο ζωής (cyber-lifestyle) και μαζί με τις παραμέτρους που εκτέθηκαν πιο πάνω σχετικά με την θεωρία των καθημερινών δραστηριοτήτων παρέχουν επαρκές θεωρητικό πλαίσιο για τη διαδικτυακή θυματοποίηση[139].

Οι χρήστες του Διαδικτύου και των μέσων κοινωνικής δικτύωσης, διαμέσου των προφίλ και λογαριασμών που διατηρούν, δημοσιοποιούν πληροφορίες που αφορούν την ιδιωτική τους σφαίρα και τις καθιστούν με τον τρόπο αυτό προσιτές σε ένα ευρύ και συχνά άγνωστο μεταξύ τους αριθμό προσώπων. Επακόλουθο της αυτοέκθεσης των χρηστών του Διαδικτύου είναι η διευκόλυνση των επίδοξων κυβερνοεγκληματιών, άρα και των «cyberstalkers», στη συλλογή πληροφοριών τόσο για τους ίδιους τους χρήστες, όσο και για το συγγενικό, φιλικό ή επαγγελματικό τους

[137] Στο ίδιο, σ. 1153-1160
[138] Βλ. Κατσογιάννου, ό.π., σ. 1457
[139] Βλ. Fisher & Henson, ό.π., σ. 1150

περιβάλλον, η ευχερέστερη και κεκαλυμμένη δράση τους, αλλά και η εν αγνοία των θυμάτων θυματοποίησή τους, αφού οι χρησιμοποιούμενες από τους δράστες πληροφορίες συλλέχθηκαν κατόπιν δικής τους διάθεσης[140].

5. Το «προφίλ» των δραστών του «cyberstalking»

Ο μικρός αριθμός ερευνών που έχουν διεξαχθεί μέχρι τώρα για το «cyberstalking» έχουν κατά κύριο λόγο ως αντικείμενο μελέτης τα χαρακτηριστικά των δραστών και των θυμάτων, την ύπαρξη ή μη προηγούμενης σχέσης μεταξύ τους, τη δυσκολία ανάπτυξης διαπροσωπικών σχέσεων από πλευράς των δραστών, την χρήση του Διαδικτύου και των ψηφιακών κοινωνικών δικτύων, τα κίνητρα των δραστών, καθώς και τον κίνδυνο και τις επιπτώσεις της θυματοποίησης. Πολλά από τα δεδομένα που έχουν συλλεχθεί για το αδίκημα προέρχονται είτε από τις αφηγήσεις των ίδιων των θυμάτων σχετικά με την εμπειρία θυματοποίησής τους, ή από τις περιγραφές δραστών μετά την απαγγελία σχετικών σε βάρος τους κατηγοριών[141].

5.1. Χαρακτηριστικά προσωπικότητας και κοινωνικο-δημογραφικά χαρακτηριστικά των δραστών

Προκειμένου να σχηματισθεί πλήρης εικόνα για το «προφίλ» των δραστών του «cyberstalking» έχουν μελετηθεί εμπειρικά τόσο τα χαρακτηριστικά της προσωπικότητας, όσο και τα κοινωνικο-δημογραφικά τους χαρακτηριστικά.

Σύμφωνα με τα αποτελέσματα των έως τώρα διεξαχθεισών μελετών, οι δράστες «cyberstalking» εμφανίζουν τα ακόλουθα χαρακτηριστικά προσωπικότητας: επιθυμία επιβολής και κυριαρχίας στη ζωή του θύματος, σαδισμό, ναρκισσισμό, έλλειψη αυτοελέγχου, ψυχικές διαταραχές, ανάγκη προσκόλλησης στο θύμα μέσω εκφοβισμού του, σωματική και σεξουαλική επιθετικότητα, θυμό, δυσκολία σύναψης διαπροσωπικών σχέσεων, επιθυμία για άμεση ικανοποίηση των αναγκών τους, βιωματικές - τραυματικές εμπειρίες, εμπειρία σεξουαλικής κακοποίησης και ιστορικό κατάχρησης αλκοόλ και εξαρτησιογόνων ουσιών[142].

---

[140] Βλ. Κατσογιάννου, ό.π., σ. 1458-1459

[141] Βλ. A. Abohassan, E. Alzeiby, A. Dhir, P. Kaur & A. Tandon, A systematic literature review on cyberstalking. An analysis of past achievements and future promises, *Technological Forecasting & Social Change, 163, 2021,* σ. 2, doi: https://doi.org/10.1016/j.techfore.2020.120426 και Spence-Diehl, ό.π., σ. 8

[142] Στο ίδιο, σ. 5-6

Τα κοινωνικο-δημογραφικά χαρακτηριστικά των δραστών «cyberstalking» έχουν αποτελέσει, επίσης, αντικείμενο μελέτης περισσότερων ερευνών και φαίνεται πως οι «cyberstalkers» δημογραφικά ταιριάζουν περισσότερο με το στερεοτυπικό προφίλ του εγκληματία του λευκού κολάρου (white-collar criminal) παρά με εκείνο του εγκληματία του δρόμου (street-crime offender/criminal)[143]. Πιο ειδικά, από πορίσματα μελετών για τα κοινωνικο-δημογραφικά χαρακτηριστικά των δραστών «cyberstalking» έχουν προκύψει τα ακόλουθα συμπεράσματα:

Φύλο

Δράστες «cyberstalking» μπορεί να είναι τόσο άνδρες όσο και γυναίκες με την πλειοψηφία των περιπτώσεων να αντιστοιχεί σε άνδρα δράστη και γυναίκα θύμα[144]. Πιο συγκεκριμένα, από τα αποτελέσματα της μελέτης των Al Mutawa, Bryce, Franqueira και Marrington, που πραγματοποιήθηκε στο Dubai το 2016 σε δείγμα 20 θυμάτων περιπτώσεων «cyberstalking», προέκυψε πως το 80% των δραστών ήταν άνδρες και το 20% γυναίκες. Μάλιστα, το 60% των περιπτώσεων αφορούσε διαδικτυακή παρενοχλητική συμπεριφορά από άνδρα σε βάρος γυναίκας, το 20% από άνδρα σε άνδρα, το 15% από γυναίκα σε γυναίκα και το 5% από γυναίκα σε άνδρα[145].

Με τα πορίσματα της ανωτέρω μελέτης συγκλίνει και η ποιοτική μελέτη των Bocij και McFarlane (2003), η οποία πραγματοποιήθηκε μέσω ημι-δομημένου ερωτηματολογίου σε 24 θύματα «cyberstalking» σχετικά με τα δημογραφικά χαρακτηριστικά τόσο των ίδιων όσο και των δραστών, την μορφή και τη διάρκεια της παρενοχλητικής συμπεριφοράς και τον τύπο της επικοινωνίας τους με τους δράστες, καθώς προέκυψε ότι το 84,6% των δραστών ήταν άνδρες και το 15,4% γυναίκες[146].

Με τα συμπεράσματα αυτά συμφωνεί και η μελέτη των Abohassan, Alzeiby, Dhir, Kaur και Tandon (2021), η οποία αφορά την βιβλιογραφική ανασκόπηση των εμπειρικών μελετών που είχαν διεξαχθεί για το αδίκημα της έμμονης διαδικτυακής παρενοχλητικής παρακολούθησης κατά το χρονικό διάστημα 2009-2019. Σύμφωνα με τα αποτελέσματα της έρευνας αυτής, στην πλειονότητα των περιπτώσεων οι δράστες είναι άνδρες, οι οποίοι και κρίνονται δυνητικά περισσότερο επικίνδυνοι σε σχέση με τις γυναίκες δράστιδες[147].

[143] Βλ. Pittaro, ό.π., σ. 182
[144] Βλ. Mansourabadi και Salimi, ό.π., σ. 7
[145] Βλ. Al Mutawa, Bryce, Franqueira και Marrington, ό.π., σ. 98-99
[146] Βλ. Bocij και McFarlane, An Exploration of Predatory Behaviour in Cyberspace: Towards a Typology of Cyberstalkers, ό.π., σ. 3-5
[147] Βλ. Abohassan, Alzeiby, Dhir, Kaur & Tandon, ό.π., σ. 3&6

Επιπρόσθετα, οι Mansourabadi και Salimi (2014) υποστήριξαν πως οι άνδρες «cyberstalkers» παρενοχλούν τα θύματά τους για σεξουαλικούς και μη σκοπούς, ενώ οι γυναίκες παρενοχλούν άλλες γυναίκες εξαιτίας διαφορετικών απόψεων, μίσους και εκδίκησης. Επίσης, οι γυναίκες «cyberstalkers» τείνουν να χρησιμοποιούν περισσότερο έμμεσους τρόπους παρενόχλησης και εκφοβισμού, όπως είναι η δυσφήμιση και ο κοινωνικός σχολιασμός (gossip) του θύματος[148].

Ηλικία

Κατά τους D' Ovidio και Doyle (2003) οι δράστες του «cyberstalking» έχουν μ.ό. ηλικίας τα 40 έτη [149]. Στην ίδια κατεύθυνση κυμαίνονται και τα αποτελέσματα της έρευνας των Abohassan, Alzeiby, Dhir, Kaur και Tandon (2021)[150]. Ακόμη, σύμφωνα με τα αποτελέσματα της μελέτης των Bocij και McFarlane (2003), το 42,3% των δραστών είχε ηλικία μεγαλύτερη των 41 ετών, το 34,6% βρισκόταν μεταξύ των ηλικιών 31 έως 40 ετών και το 23,1% μεταξύ 18 και 30 ετών[151]. Αντιστοίχως, σύμφωνα με την έρευνα των Al Mutawa, Bryce, Franqueira και Marrington (2016), το 45% των δραστών ανήκε στην ηλικιακή ομάδα άνω των 41 ετών, το 35% ανήκε στην ηλικιακή ομάδα από 31 έως 40 ετών και το 20% στην ηλικιακή ομάδα από 21 έως 30 ετών[152].

Επίπεδο εκπαίδευσης

Με βάση τα πορίσματα της πλειοψηφίας των μελετών που έχουν διεξαχθεί για το φαινόμενο και αναφέρθηκαν πιο πάνω (όπως των Abohassan, Alzeiby, Dhir, Kaur και Tandon του 2021, D' Ovidio και Doyle του 2003 και G. Higgins, C. Marcum, J. Navarro και M. Ricketts του 2016) οι «cyberstalkers» έχουν υψηλό επίπεδο εκπαίδευσης[153]. Το ίδιο προκύπτει και από την έρευνα των Bocij και McFarlane (2003), με βάση τα αποτελέσματα της οποίας το 27,3% των δραστών ήταν κάτοχοι πτυχίου, το 22,7% απόφοιτοι κολεγίου, το 9,1% απόφοιτοι λυκείου, ενώ το 4,5% δεν είχε λάβει τη βασική εκπαίδευση[154].

---

[148] Βλ. Mansourabadi και Salimi, ό.π., σ. 7
[149] Βλ. Roberts, ό.π., σ. 278
[150] Βλ. Abohassan, Alzeiby, Dhir, Kaur & Tandon, ό.π., σ. 6
[151] Βλ. Bocij και McFarlane, ό.π., σ. 5
[152] Βλ. Al Mutawa, Bryce, Franqueira & Marrington, ό.π., σ. 99
[153] Βλ. Abohassan, Alzeiby, Dhir, Kaur & Tandon, ό.π., σ. 6, Roberts, ό.π., σ. 278 και G. Higgins, C. Marcum, J. Navarro & M. Ricketts, Addicted to the Thrill of the Virtual Hunt: Examining the Effects of Internet Addiction on the Cyberstalking Behaviors of Juveniles, *Deviant Behavior*, 37, 8, 2016, σ. 8, doi: https://psycnet.apa.org/doi/10.1080/01639625.2016.1153366
[154] Βλ. Bocij και McFarlane, ό.π., σ. 6

Επαγγελματική απασχόληση

Στη μελέτη των Bocij και McFarlane (2003) το 50% των δραστών είχε κάποια επαγγελματική απασχόληση και το 10% περίπου ήταν φοιτητές[155]. Στη μελέτη των Al Mutawa, Bryce, Franqueira και Marrington (2016) το 80% του δείγματος, στο οποίο συμπεριλαμβάνονταν και δράστες και θύματα «cyberstalking», είχε κάποια επαγγελματική απασχόληση με το 70% να διαθέτει επαγγελματική θέση μεσαίου κοινωνικού στάτους και το 20% χαμηλού κοινωνικού στάτους[156].

Φυλετική καταγωγή

Από τα αποτελέσματα των έως τώρα μελετών που έχουν πραγματοποιηθεί για το φαινόμενο του «cyberstalking», προέκυψε ότι τόσο οι δράστες όσο και τα θύματα είναι λευκοί (αυτό αφορά περισσότερο τις ανεπτυγμένες δυτικές κοινωνίες και λιγότερο τις αναπτυσσόμενες)[157].

Οικογενειακή κατάσταση

Στη μελέτη των Bocij και McFarlane (2003) το 52,3% των δραστών ήταν ανύπαντροι, το 21,7% παντρεμένοι, το 13% χωρισμένοι και το 13% σε διάσταση[158].

Τεχνολογική κατάρτιση

Οι περισσότεροι «cyberstalkers» είναι εξοικειωμένοι με την χρήση του Η/Υ και του Διαδικτύου[159]. Από τη μελέτη των Bocij και McFarlane (2003) προέκυψε πως το 50% των δραστών είχε υψηλό έως αρκετά υψηλό βαθμό εξοικείωσης με τις νέες τεχνολογίες και το 40% μέτριο βαθμό αντίστοιχα[160]. Η εξοικείωση με τις υπηρεσίες του Διαδικτύου αφορά την χρήση του ηλεκτρονικού ταχυδρομείου, ιστότοπων κοινωνικής δικτύωσης, ιστοσελίδων γνωριμιών, ομάδων και δωματίων συζητήσεων και πινάκων ανακοινώσεων[161].

Ύπαρξη προηγούμενης σχέσης μεταξύ δράστη και θύματος

Στη μελέτη των Bocij και McFarlane (2003) το 33,3% των δραστών είχε πρόσφατη ή πολύ πρόσφατη επικοινωνία με το θύμα μέσω ΤΠΕ, το 22% ήταν εντελώς άγνωστοι,

[155] Στο ίδιο, σ. 5
[156] Βλ. Al Mutawa, Bryce, Franqueira & Marrington, ό.π., σ. 99
[157] Βλ. Abohassan, Alzeiby, Dhir, Kaur & Tandon, ό.π., σ. 6, Roberts, ό.π., σ. 278 και Higgins, Marcum, Navarro & Ricketts, ό.π., σ. 4-5, Al Mutawa, Bryce, Franqueira & Marrington, ό.π., σ. 99 και Bocij και McFarlane, ό.π., σ. 5
[158] ό.π.
[159] Βλ. Abohassan, Alzeiby, Dhir, Kaur & Tandon, ό.π., σ. 6
[160] Βλ. Bocij και McFarlane, ό.π., σ. 5
[161] ό.π. και Al Mutawa, Bryce, Franqueira & Marrington, ό.π., σ. 100

το 16,7% είχε μια απλή γνωριμία με το θύμα και το 12% ήταν πρώην σύντροφοι ή συνάδελφοι[162]. Στη μελέτη των Al Mutawa, Bryce, Franqueira και Marrington (2021) το 40% των δραστών ήταν συνάδελφοι του θύματος, το 35% πρώην σύντροφοι, το 20% απλή γνωριμία και σε ποσοστό 5% τελείως άγνωστοι με το θύμα[163].

Διάρκεια της παρενοχλητικής συμπεριφοράς

Σύμφωνα με τη μελέτη των Bocij και McFarlane (2003) η διάρκεια της συμπεριφοράς μπορεί να εκτείνεται από 1 μέρα έως 5 έτη, με μ.ό. τους 12 μήνες[164]. Στη μελέτη των Al Mutawa, Bryce, Franqueira και Marrington (2021) στο 60% των περιπτώσεων η παρενόχληση διήρκησε έως 6 μήνες, στο 20% από 7 μήνες έως 1 χρόνο, στο 5% έως 2 χρόνια, ενώ το υπόλοιπο 15% των ερωτηθέντων δεν μπορούσε να προσδιορίσει τη διάρκεια της παρενόχλησης[165].

Τέλος, όσον αφορά τη συσχέτιση προγενέστερου ιστορικού επιθετικής συμπεριφοράς, εγκλεισμού σε ψυχιατρείο ή προηγούμενων καταδικών με την εκδήλωση έμμονης διαδικτυακής παρενοχλητικής παρακολούθησης δεν προέκυψαν ασφαλή συμπεράσματα, καθότι δεν υπήρχαν επαρκή δεδομένα, κάτι το οποίο χρήζει περαιτέρω εμπειρικής διερεύνησης[166].

5.2. Τυπολογίες δραστών

Αν και στην υπάρχουσα βιβλιογραφία για το «offline stalking» υπάρχει υλικό σχετικά με τις τυπολογίες των δραστών, εντούτοις είναι ένα θέμα που χρήζει περαιτέρω εμπειρικής διερεύνησης προκειμένου να διαπιστωθεί αν οι τυπολογίες των «offline stalkers» ισχύουν και στους «cyberstalkers» αντίστοιχα. Ο Petherick (2001) χρησιμοποίησε την τυπολογία των Zona *et al.* (1993), σύμφωνα με την οποία οι «offline stalkers» διακρίνονται σε ερωτομανείς (erotomaniacs), εμμονικούς με την αγάπη (love obsessionals) και απλούς εμμονικούς (simple obsessionals), και στην περίπτωση των «cyberstalkers». Ωστόσο, από την στιγμή που πρόκειται για διακριτές μεταξύ τους εγκληματικές συμπεριφορές με τα κίνητρα και τα χαρακτηριστικά των δραστών να διαφοροποιούνται, δεν αποτυπώνουν όλες οι τυπολογίες των «offline stalkers» τη

[162] ό.π.
[163] Βλ. Al Mutawa, Bryce, Franqueira & Marrington, ό.π., σ. 99
[164] Βλ. Bocij και McFarlane, ό.π., σ. 5
[165] Βλ. Al Mutawa, Bryce, Franqueira & Marrington, ό.π., σ. 100
[166] Βλ. Bocij και McFarlane, An Exploration of Predatory Behaviour in Cyberspace: Towards a Typology of Cyberstalkers, ό.π., σ. 6

δυναμική των δραστών του «cyberstalking», με αποτέλεσμα κάποιες συμπεριφορές «cyberstalking» να μην συναντώνται στο «offline stalking»[167].

Οι Bocij και McFarlane (2003) στη μελέτη τους για τους δράστες του «cyberstalking» ανέπτυξαν τυπολογία με βάση τις περιγραφές της συμπεριφοράς που βίωσαν τα θύματα που συμμετείχαν στην έρευνα, και είναι η εξής:

α) Ο «εκδικητικός» (vindictive) «cyberstalker». Μπορεί να χαρακτηριστεί και ως κακόβουλος (malicious) εξαιτίας της βαναυσότητας των απειλών και της παρενόχλησης των θυμάτων του, συγκριτικά με τις υπόλοιπες κατηγορίες δραστών «cyberstalking». Η χρησιμοποιούμενη τακτική αφορά σκληρή και επαναλαμβανόμενη παρενόχληση, η οποία μπορεί να ξεκινήσει από μια ασήμαντη αφορμή (π.χ. από μια συζήτηση που πήγε στραβά ή ως επακόλουθο μιας ενεργούς διαμάχης μεταξύ δράστη και θύματος). Ο εκδικητικός «cyberstalker» χαρακτηρίζεται από υψηλό επίπεδο τεχνολογικής κατάρτισης και εξοικείωσης με την χρήση του Η/Υ και του Διαδικτύου, δεδομένου ότι προβαίνει σε εκτεταμένη χρήση των ΤΠΕ και προσφεύγει συχνότερα στις πρακτικές του «email bombing», του «spamming» και της «οικειοποίησης» της ταυτότητας. Είναι ο μόνος που χρησιμοποιεί κακόβουλο λογισμικό και πιο συγκεκριμένα δούρειους ίππους για να αποκτήσει απομακρυσμένη πρόσβαση στον Η/Υ του θύματος και να παρακολουθεί ηλεκτρονικά τις κινήσεις του ή για να τον «μολύνει» μέσω της εγκατάστασης κάποιου «ιού». Ακόμη, δεν αποκλείεται να γίνεται ταυτόχρονα «εξω-διαδικτυακή» παρακολούθηση, δηλαδή «offline stalking». Τέλος, δεν αποκλείεται οι δράστες αυτής της κατηγορίας να έχουν προηγούμενο ποινικό παρελθόν και ιστορικό θυματοποίησης των ίδιων, ενώ δεν έχει αποδειχθεί η σύνδεση της εν λόγω κατηγορίας δραστών με προβλήματα ψυχικής υγείας.[168]

β) Ο «ήρεμος» (composed) «cyberstalker». Ο δράστης αυτής της κατηγορίας στοχεύει τα θύματά του με ηρεμία και τον χαρακτηρίζει η ετοιμότητα στο σύνολο των ενεργειών του. Σκοπός του δεν είναι η σύναψη σχέσης με το θύμα - στόχο αλλά η πρόκληση διαρκούς ενόχλησης, δυσφορίας, αγωνίας και εκνευρισμού του θύματος. Η τακτική της παρενόχλησης περιλαμβάνει ποικιλία απειλητικών συμπεριφορών, που καταδεικνύουν εξοικείωση με την χρήση της πληροφορικής τεχνολογίας αν όχι σε υψηλό, σίγουρα σε μέτριο επίπεδο. Όπως και στην προηγούμενη κατηγορία δραστών

[167] Στο ίδιο, σ. 3
[168] Στο ίδιο, σ. 6-7

δεν αποκλείεται να γίνεται ταυτόχρονα «offline stalking». Τέλος, όσον αφορά την ύπαρξη προηγούμενου ποινικού παρελθόντος, ιστορικού θυματοποίησης ή προβλημάτων ψυχικής υγείας δεν έχουν εξαχθεί ασφαλή και αντιπροσωπευτικά συμπεράσματα.[169]

γ) Ο «οικείος» (intimate) «cyberstalker». Ο δράστης της κατηγορίας αυτής προσπαθεί να κεντρίσει το ενδιαφέρον και την προσοχή του θύματος – στόχου αναζητώντας και συλλέγοντας πληροφορίες γύρω από αυτό. Πρόκειται για άτομο που είναι εξοικειωμένο με την χρήση Η/Υ και του Διαδικτύου και προβαίνει σε ευρύτατη χρήση των ΤΠΕ για να παρενοχλήσει το θύμα είτε μέσω ηλεκτρονικού ταχυδρομείου, ή ομάδων συζητήσεων ή ιστοσελίδων γνωριμιών[170].

Η κατηγορία αυτή διακρίνεται σε δύο υπο-κατηγορίες. Η πρώτη αφορά τους «πρώην οικείους» (ex-intimates) «cyberstalkers». Πρόκειται για πρώην συντρόφους, που αποζητούν την εκ νέου σύναψη σχέσης με το θύμα. Η παρενόχληση συμβαίνει αποκλειστικά στο Διαδίκτυο και περιλαμβάνει απειλές, επαναλαμβανόμενα μηνύματα προς το θύμα και «οικειοποίηση» της ταυτότητας, με το δράστη να υποδύεται το θύμα σε δωμάτια συζητήσεων ή να προβαίνει σε αγορές προϊόντων ή υπηρεσιών στο Διαδίκτυο εξ ονόματος του πραγματικού θύματος.[171]

Η δεύτερη υπο-κατηγορία περιλαμβάνει τους «ερωτευμένους - ξετρελαμένους» (infatuates) «cyberstalkers», οι οποίοι επιδιώκουν να δημιουργήσουν στενότερη σχέση με το θύμα. Η επικοινωνία είναι στην αρχή φιλική έως ότου απορριφθούν από το θύμα, οπότε και εκδηλώνονται απειλητικές συμπεριφορές. Η παρενόχληση, όπως και στους «ex-intimates cyberstalkers», λαμβάνει χώρα αποκλειστικά στο Διαδίκτυο.[172]

δ) Ο «συλλογικός» (collective) «cyberstalker». Στην κατηγορία αυτή εμπίπτουν δράστες που εκδηλώνουν τη συμπεριφορά τους είτε σε συνεργασία με κάποιο άλλο άτομο ή στο πλαίσιο της συμμετοχής τους σε κάποια διαδικτυακή κοινότητα. Ο βαθμός εξοικείωσής τους με την χρήση πληροφορικής τεχνολογίας είναι από υψηλός έως αρκετά υψηλός και χρησιμοποιούν ευρύτατα τις ΤΠΕ για να παρενοχλήσουν τα θύματά τους. Οι μέθοδοι που αξιοποιούν είναι οι απειλές, η πρόκληση φόβου, η συνεχόμενη

[169] Στο ίδιο, σ. 7 και Pittaro, ό.π., σ. 188
[170] ό.π.
[171] ό.π.
[172] ό.π.

αποστολή μηνυμάτων μέσω ηλεκτρονικού ταχυδρομείου, η «οικειοποίηση» της ταυτότητας και η αναζήτηση και συλλογή πληροφοριών για το θύμα[173].

5.3. Παράγοντες κινδύνου εκδήλωσης της συμπεριφοράς και υποτροπής

Στην υπάρχουσα βιβλιογραφία έχει επιχειρηθεί η σύνδεση του «offline stalking» με συγκεκριμένους παράγοντες κινδύνου (Stalking Risk Profile/SRP), που θα συμβάλλει στην κατανόηση της συμπεριφοράς, την πρόληψή της μέσω της εύστοχης και έγκαιρης παρέμβασης και την αποτελεσματική αντιμετώπισή της (Stalking Assessment and Management)[174].

Όσον αφορά το «cyberstalking» έχει επιχειρηθεί η σύνδεσή του με κάποιους προγνωστικούς παράγοντες κινδύνου, οι οποίοι ισχύουν και για το «offline stalking» με κάποιες, ωστόσο, διαφοροποιήσεις[175]. Η ψυχική υγεία του δράστη, για παράδειγμα, υποστηρίζεται πως αποτελεί παράγοντα κινδύνου, αν και από τα πορίσματα των μελετών για το «offline stalking» δεν έχει αποκρυσταλλωθεί ακόμη κάποια συσχέτιση μεταξύ του συγκεκριμένου αδικήματος και της ψυχικής διαταραχής[176]. Παρόλα αυτά, υπάρχουν συγκεκριμένα είδη ψυχικών ασθενειών που σχετίζονται με την έμμονη παρακολούθηση σύμφωνα με τη βιβλιογραφία. Αυτές είναι η σχιζοφρένεια, οι διαταραχές προσωπικότητας, οι παραληρηματικές διαταραχές, η διπολική διαταραχή και η ιδεοψυχαναγκαστική σχεσιακή παρείσδυση (Obsessive Relational Intrusion/ ORI)[177] ως μορφή ιδεοψυχαναγκαστικής διαταραχής που περιλαμβάνει την επαναλαμβανόμενη και αυθαίρετη διείσδυση στην ιδιωτική ζωή ενός ατόμου γνωστού ή άγνωστου στο δράστη, με σκοπό τη δημιουργία στενής και συνήθως ερωτικής σχέσης μαζί του[178].

---

[173] ό.π.

[174] Βλ. Κατσογιάννου, ό.π., σ. 1504-1505

[175] Πιο συγκεκριμένα, έχει μελετηθεί η σύνδεση του «offline stalking» με τη βία και την επιθετικότητα, Ως παράγοντες κινδύνου έχουν αναδειχθεί η ύπαρξη προηγούμενης σχέσης μεταξύ δράστη και θύματος, με τους πρώην συντρόφους να έχουν αυξημένες πιθανότητες εκδήλωσης επιθετικής συμπεριφοράς, οι απειλητικές συμπεριφορές, η εμπλοκή του δράστη με το ΣΑΠΔ, το ποινικό του παρελθόν, το ιστορικό επιθετικής συμπεριφοράς και προηγούμενης θυματοποίησης, η κατάχρηση ουσιών, προβλήματα ψυχικής υγείας και κοινωνικο-δημογραφικοί παράγοντες, βλ. T. McEwan, P. Mullen και R. Purcell, Identifying risk factors in stalking: A review of current research, *International Journal of Law, and Psychiatry*, 30, 1, 2007, σ. 2-5, doi: http://dx.doi.org/10.1016/j.ijlp.2006.03.005

[176] Βλ. Κατσογιάννου, ό.π., σ. 1506-1507

[177] Βλ. Κατσογιάννου, ό.π., σ. 1507

[178] Επίσης, το σύνδρομο de Clerambault υποστηρίζεται πως συνδέεται με την έμμονη παρακολούθηση. Πρόκειται για παραληρηματική διαταραχή που σχετίζεται με την ερωτομανία και εμπίπτει στην κατηγορία των ψυχικών διαταραχών. Όσοι πάσχουν από αυτό το σύνδρομο πιστεύουν πραγματικά πως έχουν στενή σχέση με το θύμα και εκδηλώνουν εμμονικές και ψυχαναγκαστικές συμπεριφορές, βλ. Pittaro, ό.π., σ. 188

Επιπρόσθετα, υποστηρίζεται από μερίδα ερευνητών πως το φύλο μπορεί να αποτελέσει παράγοντα κινδύνου, αν και η πλειοψηφία τάσσεται υπέρ της έμφυλα ουδέτερης διάστασης της συμπεριφοράς. Όσοι υποστηρίζουν πως το φύλο αποτελεί προγνωστικό παράγοντα βασίζονται στα αυξημένα ποσοστά γυναικείας θυματοποίησης που έχουν προκύψει από τις έρευνες. Από την άλλη, οι υπέρμαχοι της έμφυλα ουδέτερης φύσης του αδικήματος επικαλούνται πορίσματα μελετών βάσει των οποίων τα ποσοστά γυναικείας και ανδρικής θυματοποίησης είναι παρεμφερή. Σε αυτό θα πρέπει βέβαια να συνυπολογιστεί και η διάσταση του σκοτεινού αριθμού του φαινομένου, που επηρεάζει την ακρίβεια των ποσοτικών δεδομένων[179].

Επιπλέον, ο υψηλός βαθμός εξοικείωσης και χρήσης των ΤΠΕ, του Διαδικτύου και των ψηφιακών κοινωνικών δικτύων συνδέεται πολύ στενά με την πιθανότητα εκδήλωσης συμπεριφοράς που να εμπίπτει στο «cyberstalking». Έχει προκύψει εμπειρικά πως οι δεξιότητες χρήσης της πληροφορικής τεχνολογίας αποτελούν κυρίαρχο χαρακτηριστικό των «cyberstalkers», οι οποίοι αξιοποιούν την ανωνυμία και ψευδωνυμοποίηση που προσφέρει το Διαδίκτυο, τα μέσα κοινωνικής δικτύωσης και τους ιστότοπους ηλεκτρονικής επικοινωνίας για να επιλέξουν τα θύματά τους, να συλλέξουν πληροφορίες γι' αυτά και να ξεκινήσουν τη διαδικτυακή παρενόχληση[180].

Σχετικά με το ιστορικό χρήσης ουσιών, προηγούμενης θυματοποίησης, ποινικού παρελθόντος και της ύπαρξης προηγούμενης σχέσης μεταξύ δράστη και θύματος, δεν έχουν εξαχθεί ακόμη ασφαλή συμπεράσματα σχετικά με το εάν μπορούν να λειτουργήσουν ως προγνωστικοί παράγοντες στο «cyberstalking»[181].

Τέλος, όσον αφορά την σχέση μεταξύ «cyberstalking» και υποτροπής (recidivism), κυρίαρχη στα ερευνητικά δεδομένα είναι η εμπειρική έρευνα που διεξήγαγε ο Rosenfeld το 2003 για την σχέση του «offline stalking» και της υποτροπής, τα αποτελέσματα της οποίας μπορούν να επεκταθούν και στο «cyberstalking»[182]. Σύμφωνα με την έρευνα αυτή, το 49% του δείγματος εκδήλωσε ξανά εγκληματική συμπεριφορά κατά τη διάρκεια της περιόδου παρακολούθησης (follow-up period) με το 80% να παρουσιάζει υποτροπή μέσα στον πρώτο χρόνο μετά την πρώτη σύλληψη[183]. Οι παράγοντες που επιδρούν στην υποτροπή των δραστών «cyberstalking»

[179] Βλ. Κατσογιάννου, ό.π., σ. 1508-1511
[180] Στο ίδιο, σ. 1505-1506
[181] ό.π.
[182] Βλ. Pittaro, ό.π., σ. 190
[183] Βλ. B. Rosenfeld, Recidivism in stalking and obsessional harassment, *Law and Human Behavior*, Vol. 27, No. 3, 2003, σ. 257, doi: https://doi.org/10.1023/a:1023479706822

συναντώνται και σε άλλες κατηγορίες εγκληματιών και σχετίζονται με την ύπαρξη ψυχικής ασθένειας και ειδικότερα διαταραχής της προσωπικότητας (ναρκισσιστική ή αντικοινωνική συμπεριφορά) και προηγούμενου ιστορικού κατάχρησης ουσιών[184].

6. Το «προφίλ» των θυμάτων «cyberstalking»

6.1. Κοινωνικο-δημογραφικά χαρακτηριστικά

Όπως έχει ήδη αναφερθεί, το «cyberstalking» έχει θυματοκεντρικό χαρακτήρα (victim-defined crime), διότι ο παρενοχλητικός χαρακτήρας της συμπεριφοράς βιώνεται αποκλειστικά και μόνο από το θύμα, ενώ ανάλογα με το εάν έχει αποδεχθεί ή όχι τη θυματοποίησή του αποφασίζει να το αντιμετωπίσει ενεργητικά ή παθητικά αντιστοίχως.

Τα χαρακτηριστικά των θυμάτων και οι επιπτώσεις της θυματοποίησης από το «cyberstalking» έχουν αποτελέσει αντικείμενο εγκληματολογικών ερευνών, ενώ έχει αποδειχθεί πως οι γυναίκες, οι νέοι και οι μη εξοικειωμένοι με την χρήση του Διαδικτύου κρίνονται ως περισσότερο ευάλωτοι (vulnerable) σε πιθανή θυματοποίηση[185].

Εξετάζοντας τα εμπειρικά δεδομένα γύρω από τα κοινωνικο-δημογραφικά χαρακτηριστικά των θυμάτων «cyberstalking» έχουν προκύψει τα εξής:

Φύλο

Υπάρχει συμφωνία μεταξύ των αποτελεσμάτων των ερευνών πως τα ποσοστά της γυναικείας θυματοποίησης είναι υψηλότερα από εκείνα της ανδρικής. Οι γυναίκες και ειδικότερα οι άγαμες γυναίκες θυματοποιούνται από το «cyberstalking» οχτώ φορές περισσότερο σε σχέση με τους άνδρες, σύμφωνα με τους Hutton και Haantz (2003)[186].

Σύμφωνα με την ποιοτική μελέτη των Bocij και McFarlane (2003), το 91% του δείγματος το οποίο αποτελούνταν από θύματα «cyberstalking», ήταν γυναίκες με μόλις το 9% να είναι άνδρες[187]. Επίσης, στην ποσοτική μελέτη του Bocij (2003) για τον αντίκτυπο που έχει το «cyberstalking» στα θύματα, το 56,3% του δείγματος ήταν γυναίκες - θύματα και το 43,7% άνδρες - θύματα[188]. Περαιτέρω, τα αποτελέσματα της

[184] Στο ίδιο, σ. 258-259
[185] Βλ. Mansourabadi και Salimi, ό.π., σ. 7
[186] Στο ίδιο, σ. 8
[187] Βλ. Bocij και McFarlane, An Exploration of Predatory Behaviour in Cyberspace: Towards a Typology of Cyberstalkers, ό.π., σ. 5
[188] Βλ. Bocij, Victims of Cyberstalking: An Explanatory Study of Harassment Perpetrated via the Internet, ό.π., σ. 2-3

συστηματικής βιβλιογραφικής ανασκόπησης των Abohassan, Alzeiby, Dhir, Kaur και Tandon (2021) έδειξαν πως ο δημογραφικός παράγοντας του φύλου επηρεάζει την εμπειρία θυματοποίησης και την προθυμία καταγγελίας από πλευράς των θυμάτων, με τις γυναίκες να έχουν αυξημένες πιθανότητες θυματοποίησης από το «cyberstalking», να βιώνουν εντονότερα τις αρνητικές του συνέπειες στην προσωπική, επαγγελματική και κοινωνική τους ζωή, να εκλαμβάνουν τη συμπεριφορά ως περισσότερο επιβλαβή, και ως εκ τούτου, να εκδηλώνουν μεγαλύτερη προθυμία καταγγελίας της θυματοποίησής τους στις διωκτικές Αρχές σε σχέση με τους άνδρες[189].

Ηλικία

Σύμφωνα με τους Abohassan, Alzeiby, Dhir, Kaur και Tandon (2021) τα πορίσματα των ερευνών είναι αντιφατικά, διότι θυματοποιούνται εξίσου νεότεροι, όσο και μεγαλύτεροι ηλικιακά, γι' αυτό και ο συγκεκριμένος δημογραφικός παράγοντας πρέπει να εξετάζεται συνδυαστικά και με άλλα κοινωνικο-δημογραφικά χαρακτηριστικά των θυμάτων. Η ηλικία επηρεάζει τον τρόπο με τον οποίο το άτομο αντιλαμβάνεται το «cyberstalking» και κατ' επέκταση τη θυματοποίησή του από αυτό. Οι νέες γενιές αν και είναι περισσότερο εξοικειωμένες με την χρήση της πληροφορικής τεχνολογίας και του Διαδικτύου, δεν αντιλαμβάνονται απόλυτα τους κινδύνους που ελλοχεύουν από την χρήση αυτή (όπως είναι η αυτοδιάθεση των προσωπικών τους πληροφοριών σε άγνωστο αριθμό αποδεκτών και η δυσχέρεια ελέγχου περαιτέρω διάδοσης και επεξεργασίας τους). Από την άλλη πλευρά, οι μεγαλύτεροι ηλικιακά, και κυρίως οι άγαμοι ή διαζευγμένοι, και όσοι χρησιμοποιούν εκτεταμένα ιστοσελίδες κοινωνικής δικτύωσης ή/και συμμετέχουν σε διαδικτυακές ομάδες, οι οποίοι όμως δεν είναι εξοικειωμένοι με την χρήση του Διαδικτύου, διατρέχουν τον ίδιο κίνδυνο θυματοποίησης[190].

Σύμφωνα με τη μελέτη των Bocij και McFarlane (2003), ο μ.ό. ηλικίας των θυμάτων «cyberstalking» ήταν τα 32 έτη, με το 50% περίπου του δείγματος να ανήκει στην ηλικιακή ομάδα 18-30 ετών και το υπόλοιπο ποσοστό να μοιράζεται ισομερώς μεταξύ των ηλικιακών ομάδων 31-40 και άνω των 41 ετών αντίστοιχα[191].

Στην ποσοτική έρευνα του Bocij (2003) για τις συνέπειες της θυματοποίησης από την έμμονη διαδικτυακή παρενοχλητική παρακολούθηση το ηλικιακό εύρος των

[189] Βλ. Abohassan, Alzeiby, Dhir, Kaur & Tandon, ό.π., σ. 1&5
[190] Βλ. Κατσογιάννου, ό.π., σ. 1519 και Abohassan, Alzeiby, Dhir, Kaur & Tandon, ό.π., σ. 6
[191] Βλ. Bocij και McFarlane, An Exploration of Predatory Behaviour in Cyberspace: Towards a Typology of Cyberstalkers, ό.π., σ. 5

θυμάτων κυμαινόταν από 16-84 ετών. Ο μ.ό. ηλικίας ήταν τα 35 έτη και περίπου το 61% των γυναικών θυμάτων ήταν άνω των 30 ετών και το υπόλοιπο ποσοστό ήταν ισομερώς καταμερισμένο μεταξύ της ηλικιακής ομάδας 21-30 και κάτω των 20 ετών[192].

Τέλος, στη μελέτη των Al Mutawa, Bryce, Franqueira και Marrington (2016) το ηλικιακό εύρος των θυμάτων κυμαινόταν μεταξύ 23-48 ετών με το 40% να ανήκει στην ηλικιακή ομάδα 21-30, το 30% στην ηλικιακή ομάδα 31-40 και το υπόλοιπο 30% να είναι άνω των 41 ετών[193].

Οικογενειακή κατάσταση

Τα αποτελέσματα της μελέτης των Abohassan, Alzeiby, Dhir, Kaur και Tandon (2021) έδειξαν αυξημένες πιθανότητες θυματοποίησης για άτομα που βρίσκονται σε σχέση[194], ενώ οι Bocij και McFarlane (2003) στη μελέτη τους υποστήριξαν πως το 60% του δείγματος ήταν έγγαμοι, το 30% άγαμοι και το υπόλοιπο ποσοστό διαζευγμένοι[195]. Προς την ίδια κατεύθυνση με τα αποτελέσματα των παραπάνω μελετών στράφηκαν τα αποτελέσματα της μελέτης του Bocij (2003) για τη θυματοποίηση, σύμφωνα με τα οποία το 77% του δείγματος ήταν παντρεμένοι ή συζούσαν με τον/την σύντροφό τους[196].

Επίπεδο εκπαίδευσης

Στην έρευνα των Bocij και McFarlane (2003) το 70% των θυμάτων ήταν απόφοιτοι κολεγίου, το 25% πτυχιούχοι και το υπόλοιπο ποσοστό ανήκε σε όσους δεν είχαν λάβει τη βασική εκπαίδευση[197].

Στη μελέτη του Bocij (2003) η συντριπτική πλειοψηφία των θυμάτων είχε λάβει υψηλό επίπεδο εκπαίδευσης (σε ποσοστό 92%)[198], ενώ σύμφωνα με τη μελέτη των Fisher, Fox, Nobles και Reyns (2014) τα θύματα «cyberstalking» εμφανίζουν υψηλότερο επίπεδο εκπαίδευσης σε σύγκριση με τα θύματα «offline stalking»[199].

---

[192] Βλ. Bocij, Victims of Cyberstalking: An Explanatory Study of Harassment Perpetrated via the Internet, ό.π., σ.3&6&8
[193] Βλ. Al Mutawa, Bryce, Franqueira & Marrington, ό.π., σ. 99
[194] Βλ. Abohassan, Alzeiby, Dhir, Kaur & Tandon, ό.π., σ. 6
[195] Βλ. Bocij και McFarlane, ό.π., σ. 5
[196] Βλ. Bocij, ό.π., σ. 6
[197] Βλ. Bocij και McFarlane, ό.π., σ. 6
[198] Βλ. Bocij, ό.π., σ. 8
[199] Βλ. B. Fisher, K. Fox, M. Nobles και B. Reyns, Protection Against Pursuit: A Conceptual and Empirical Comparison of Cyberstalking and Stalking Victimization Among a National Sample, *Justice Quarterly*, Vol. 31, No. 6, 2014, σ.1003, doi: http://dx.doi.org/10.1080/07418825.2012.723030

Επαγγελματική απασχόληση

Με βάση τα αποτελέσματα της μελέτης των Bocij και McFarlane (2003) το 38% του δείγματος είχε αποκατασταθεί επαγγελματικά, το 21% ήταν φοιτητές και σε ίδιο ποσοστό κληρικοί, και το 5% ήταν χειρώνακτες[200]. Ακολούθως, το δείγμα της μελέτης του Bocij (2003) αποτελούνταν κατά 27% από μαθητές και φοιτητές, κατά 11% από εργαζόμενους στον πρωτογενή τομέα παραγωγής, κατά 8,4% από εργαζόμενους σε επαγγέλματα που χρησιμοποιούν Η/Υ, κατά 7% από αυτο-απασχολούμενους και στο υπολειπόμενο ποσοστό από συνταξιούχους και άνεργους[201]. Τέλος, στη μελέτη των Al Mutawa, Bryce, Franqueira και Marrington (2016) το 85% του δείγματος των θυμάτων είχε αποκατασταθεί επαγγελματικά, το 10% ήταν άνεργοι και το 5% ήταν μαθητές - φοιτητές[202].

Ύπαρξη προηγούμενης σχέσης με τον δράστη

Με βάση τα αποτελέσματα της μελέτης των Bocij και McFarlane (2003) στην πλειοψηφία των περιπτώσεων «cyberstalking» (78%) υπήρχε κάποια σχέση ανάμεσα στον δράστη και το θύμα[203], ενώ στη μελέτη των Al Mutawa, Bryce, Franqueira και Marrington (2016) το 95% του δείγματος αφορούσε πρώην συντρόφους, συναδέλφους και απλή γνωριμία δράστη – θύματος[204].

Τεχνολογική κατάρτιση

Σύμφωνα με τα αποτελέσματα των διεξαχθεισών μελετών γύρω από το φαινόμενο, θύματα της έμμονης διαδικτυακής παρενοχλητικής παρακολούθησης φαίνεται να είναι τόσο οι εξοικειωμένοι χρήστες Η/Υ και μέσων κοινωνικής δικτύωσης, όσο και οι τελείως άπειροι χρήστες του Διαδικτύου, οι οποίοι έχουν πλήρη άγνοια των κινδύνων που ελλοχεύουν. Ενδεικτικά να αναφέρουμε πως σύμφωνα με τα αποτελέσματα της μελέτης των Bocij και McFarlane (2003) το 21% του δείγματος είχε αρκετά χαμηλό επίπεδο εξοικείωσης με τους Η/Υ και το Διαδίκτυο, το 29,2% είχε μέτριο επίπεδο, το 21% αρκετά υψηλό επίπεδο και το 16,7% είχε υψηλό επίπεδο αντίστοιχα[205].

Στην έρευνα του Bocij (2003) το 95% του δείγματος κατείχε δικό του Η/Υ και συνδυαστικά με την εμπειρία στην πλοήγηση στο Διαδίκτυο το 44% είχε ένα μέτριο

[200] Βλ. Bocij και McFarlane, ό.π., σ. 5
[201] Βλ. Bocij, ό.π., σ. 4
[202] Βλ. Al Mutawa, Bryce, Franqueira & Marrington, ό.π., σ. 99
[203] Βλ. Bocij και McFarlane, ό.π., σ. 6
[204] Βλ. Al Mutawa, Bryce, Franqueira & Marrington, ό.π., σ. 99
[205] Βλ. Bocij και McFarlane, ό.π., σ. 5

επίπεδο εξοικείωσης με τις ΤΠΕ, το 34% ήταν αρχάριοι και το υπόλοιπο ποσοστό είχε λίγες γνώσεις στην χρήση τους[206].

Η χρήση του Διαδικτύου και των μέσων κοινωνικής δικτύωσης έχει μεγάλη σημασία για τον κίνδυνο θυματοποίησης, διότι σχετίζεται με τη δημοσιοποίηση προσωπικών πληροφοριών και την έντονη παρουσία των θυμάτων στο Διαδίκτυο. Από τις αντίστοιχες έρευνες έχει προκύψει πως οι γυναίκες χρησιμοποιούν περισσότερο τα μέσα κοινωνικής δικτύωσης, στα οποία επικρατούν η εικόνα, οι φωτογραφίες και τα βίντεο (π.χ. Instagram), ενώ για το Facebook δεν έχει παρατηρηθεί ουσιαστική διαφοροποίηση μεταξύ ανδρών και γυναικών[207].

Τα αποτελέσματα της έρευνας του Bocij (2003) έδειξαν πως πάνω από το 80% των ερωτώμενων χρησιμοποιούσε το Διαδίκτυο και την υπηρεσία άμεσης ανταλλαγής μηνυμάτων σε καθημερινή βάση, το 60% διέθετε προφίλ σε μέσα κοινωνικής δικτύωσης, ενώ συνδυαστικά με την ηλικία και την εξοικείωση με την χρήση Η/Υ προέκυψε πως άτομα άνω των 31 ετών με μέσο ή υψηλό επίπεδο τεχνολογικής κατάρτισης χρησιμοποιούσαν το Διαδίκτυο καθημερινά και συμμετείχαν περισσότερο σε ομάδες συζητήσεων[208].

Επίσης, σύμφωνα με τα αποτελέσματα της ίδιας έρευνας, όσο περισσότερο εξοικειωμένο είναι το θύμα με την χρήση Η/Υ και Διαδικτύου τόσο λιγότερη δυσφορία αισθάνεται από την παρενοχλητική συμπεριφορά λόγω της πεποίθησης πως οι γνώσεις του το καθιστούν ικανό να αναγνωρίσει μια παρενοχλητική συμπεριφορά και να ανακαλύψει την ταυτότητα του δράστη αξιοποιώντας τα ψηφιακά ίχνη στο Διαδίκτυο. Επιπλέον, οι περισσότερο εξοικειωμένοι με την χρήση ΤΠΕ είναι πιο πιθανό να θυματοποιηθούν με περισσότερο εξελιγμένες τεχνολογικά μεθόδους, όπως είναι η παρακολούθηση με την εγκατάσταση λογισμικού κατασκοπίας στον Η/Υ ή η καταστροφή του εξοπλισμού και των δεδομένων τους[209].

Ωστόσο, οι απόψεις διίστανται σχετικά με το εάν οι άπειροι χρήστες του Διαδικτύου θυματοποιούνται περισσότερο από τους εξοικειωμένους χρήστες, διότι αγνοούν τους κινδύνους που υπάρχουν στο εικονικό περιβάλλον. Η εκτεταμένη χρήση των ιστοσελίδων κοινωνικής δικτύωσης έχει συνδεθεί με την αύξηση των περιστατικών «cyberstalking», διότι οι επίδοξοι «cyberstalkers» εκμεταλλεύονται τόσο

[206] Βλ. Bocij, ό.π., σ. 4-5
[207] Βλ. Κατσογιάννου, ό.π., σ. 1518-1519
[208] Βλ. Bocij, ό.π., σ. 5
[209] Στο ίδιο, σ. 7-8

την υπερβολική και διαρκή αυτοδιάθεση προσωπικών δεδομένων των ατόμων στο Διαδίκτυο, όσο και την ανωνυμία που αυτό προσφέρει[210].

Διάρκεια της παρενοχλητικής συμπεριφοράς

Με βάση τα αποτελέσματα ερευνών που αφορούν την εμπειρία θυματοποίησης από την έμμονη διαδικτυακή παρενοχλητική παρακολούθηση η διάρκεια της παρενοχλητικής συμπεριφοράς έτσι όπως βιώθηκε από τα θύματα κυμαίνεται από 2 εβδομάδες έως 38 μήνες. Η πλειοψηφία, ωστόσο, των θυμάτων αναφέρει πως η εις βάρος της παρενοχλητική συμπεριφορά είχε διάρκεια έως 6 μήνες[211].

Συγκεφαλαιωτικά, καταλήγουμε στο συμπέρασμα πως κοινωνικές ομάδες με συγκεκριμένα κοινωνικο-δημογραφικά χαρακτηριστικά είναι περισσότερο ευάλωτες στη θυματοποίηση από «cyberstalking», χωρίς όμως από τη μέχρι τώρα ερευνητική εμπειρία να είναι δυνατή η γενίκευση των πορισμάτων, με αποτέλεσμα να κρίνεται αναγκαία η περαιτέρω εξέταση αυτών των παραγόντων στο πλαίσιο της αλληλεπίδρασής τους με άλλους παράγοντες κινδύνου θυματοποίησης (όπως π.χ. η συμμετοχή σε διαδικτυακές κοινότητες, η ανάγκη προβολής και δημοφιλίας που συναντάται κυρίως στις νεότερες ηλικιακές ομάδες κ.λπ.).

6.2. Επιπτώσεις της θυματοποίησης

Ο αντίκτυπος που έχει η εμπειρία της θυματοποίησης από το «cyberstalking» έχει αποτελέσει αντικείμενο μελέτης των ερευνητών με τον Spitzberg (2002) να υποστηρίζει την εμφάνιση επιπτώσεων στο θύμα «cyberstalking», ανάλογων με εκείνων που βιώνει το θύμα «offline stalking». Πρόκειται για μια τυπολογία συμπτωμάτων που περιλαμβάνει κατάθλιψη, άγχος, αγωνία, μετατραυματικό στρες, απώλεια οικονομικών εσόδων λόγω διακοπής της εργασίας, απροθυμία αντιμετώπισης της θυματοποίησης, αλλά και επιπτώσεις στη σωματική και γνωστική υγεία αλλά και την κοινωνική ζωή του θύματος.[212]

Η ψυχολογική πίεση που ασκείται στα θύματα από την παρενοχλητική συμπεριφορά προκαλεί φόβο και τα οδηγεί στο να περιέλθουν σε μια κατάσταση γενικής αδυναμίας να αντιδράσουν και να αντιμετωπίσουν την κατάσταση, με αποτέλεσμα να τροποποιούν τις δραστηριότητες και τις συνήθειές τους στο Διαδίκτυο προκειμένου να αποφύγουν την εξακολουθητική συμπεριφορά των δραστών. Επίσης,

[210] Βλ. Abohassan, Alzeiby, Dhir, Kaur & Tandon, ό.π., σ. 6
[211] Βλ. Bocij και McFarlane, ό.π., σ. 7
[212] Βλ. Clarke, Davies & Roden, ό.π., σ. 9

η ψυχολογική βία που υφίστανται μπορεί να συνοδεύεται και από συναισθητική βία (affective violence), «αρπακτική» βία (predatory violence)[213] και ενίοτε σωματική βία[214].

Οι επιπτώσεις στη σωματική υγεία των θυμάτων περιλαμβάνουν, ανάμεσα σε άλλα, διαταραχές ύπνου, όρεξης, διάθεσης και διατροφικών συνηθειών, εναλλαγές βάρους, πονοκεφάλους, υπερβολική κόπωση ή αδυναμία, ναυτία, εφιάλτες, οξείες αγχώδεις διαταραχές, διαρκή αγωνία και φόβο, αλλά και σωματοποίηση (somatization) της ψυχικής πίεσης (ψυχοσωματικές αντιδράσεις)[215].

Οι επιπτώσεις στη συναισθηματική υγεία των θυμάτων περιλαμβάνουν θυμό, ντροπή, ενόχληση, δυσφορία, απογοήτευση, αίσθηση παραίτησης και φόβο που προκαλείται από τις απειλές του δράστη, και την πιθανή βλάβη της υπόληψής τους που μπορεί να επέλθει από τη δημοσιοποίηση φωτογραφιών ή προσωπικών τους στιγμών[216]. Περαιτέρω, οι επιπτώσεις στην ψυχολογική υγεία των θυμάτων σχετίζονται με την πνευματική και συναισθηματική δυσφορία, τη διαρκή και διάχυτη αγωνία, το φόβο, τη μείωση της διάθεσης, την ευερεθιστότητα, την κατάθλιψη, το άγχος, την αίσθηση αβοηθησίας και ανικανότητας να αντιδράσει, αλλά και τον αυτοκτονικό ιδεασμό. Ακόμη, το θύμα περιέρχεται σε κατάσταση υπερεγρήγορσης και διαρκούς επαγρύπνησης, εγκλωβίζεται σε μια διαρκώς επιδεινούμενη συμπεριφορά και μπορεί να στραφεί ακόμη και στην χρήση αλκοόλ, φαρμάκων ή εξαρτησιογόνων ουσιών. Επιπλέον, είναι σύνηθες τα θύματα να παρουσιάζουν Διαταραχή Μετατραυματικού Στρες (Posttraumatic Stress Disorder/PTSD), που περιλαμβάνει την επαναλαμβανόμενη επαναβίωση (πραγματική ή φανταστική) του τραύματος στο οποίο εκτέθηκε το θύμα και συνοδεύεται από εκρήξεις θυμού, κρίσεις πανικού, αισθήματα ενοχής, κατάθλιψη, αυξημένη υπερδιέγερση που διαρκούν τουλάχιστον ένα μήνα μετά την τραυματική εμπειρία[217].

Η θυματοποίηση, επίσης, επιδρά στην κοινωνική και επαγγελματική ζωή του θύματος. Πρόκειται για λειτουργικές επιπτώσεις που αφορούν μειωμένες ακαδημαϊκές

[213] Η «αρπακτική» βία (predatory violence) περιλαμβάνει ένταση, με τη συμπεριφορά του δράστη να κλιμακώνεται σταδιακά από ήπια παρέμβαση στην ιδιωτική ζωή του θύματος σε συστηματική προσβολή της προσωπικότητάς του, της ανθρώπινης αξιοπρέπειας, της ιδιωτικής ζωής, της αυτονομίας και του αυτοπροσδιορισμού του αλλά και σε περιορισμό της ελεύθερης ανάπτυξης της προσωπικότητάς του, βλ. Κατσογιάννου, ό.π., σ. 1480-1481

[214] Βλ. Κατσογιάννου, ό.π., σ. 1478-1479

[215] Βλ. Clarke, Davies & Roden, ό.π., σ. 12&21 και Pittaro, ό.π., σ. 191

[216] Βλ. Clarke, Davies & Roden, ό.π., σ. 17-19

[217] Βλ. Κατσογιάννου, ό.π., σ. 1484-1485 και Abohassan, Alzeiby, Dhir, Kaur & Tandon, ό.π., σ. 7 και Clarke, Davies & Roden., ό.π., σ. 10-11

και επαγγελματικές επιδόσεις, επιφυλακτικότητα και καχυποψία προς άλλους, απόσυρση από την κοινωνική ζωή και απομόνωση, εσωστρέφεια, τροποποίηση της καθημερινότητας, του τρόπου ζωής και των διαδικτυακών συνηθειών (π.χ. μείωση της εκτεταμένης χρήσης του Διαδικτύου, αποχώρηση από διαδικτυακές ομάδες, forums και κοινότητες) προς αποφυγή της επαφής με το δράστη, απροθυμία καταγγελίας στις διωκτικές Αρχές, παθητική αντιμετώπιση της τραυματικής εμπειρίας και γενικότερα περιορισμό της ατομικής ελευθερίας ένεκα του φόβου μελλοντικής επαναθυματοποίησης[218].

7. Αντιμετώπιση του φαινομένου του «cyberstalking»

7.1. Δυσκολίες στη δίωξη και εξιχνίαση των περιστατικών

Η εξιχνίαση των κυβερνοεγκλημάτων αποτελεί πρόκληση για το σύνολο των έννομων τάξεων και κρίνεται ολοένα και πιο επιτακτική η ανάγκη αντιμετώπισης του φαινομένου εξαιτίας της ταχύτατης τεχνολογικής εξέλιξης των Η/Υ και του Διαδικτύου[219]. Το «cyberstalking» ως μορφή ηλεκτρονικού εγκλήματος εγείρει ανάλογες δυσκολίες στη δίωξη και την εξιχνίασή του με τον εκσυγχρονισμό των μεθόδων αντιμετώπισης να αποτελεί το «κλειδί» στις προσπάθειες διαχείρισης του φαινομένου.

Αρχικά, η δίωξη του «cyberstalking» καθίσταται προβληματική λόγω των ζητημάτων που αναφέρθηκαν σε προηγούμενο κεφάλαιο σχετικά με την ποινική του τυποποίηση, αλλά και την εφαρμογή της νομοθεσίας σε κάθε χώρα. Η τυποποίησή του ως αυτοτελές ποινικό αδίκημα στο εκάστοτε ποινικό δίκαιο δεν συμβαίνει σε όλες τις χώρες διεθνώς, κάτι το οποίο δυσχεραίνει το έργο των διωκτικών αρχών, ενώ σε ορισμένες έννομες τάξεις το αδίκημα της έμμονης διαδικτυακής παρενοχλητικής παρακολούθησης εκλαμβάνεται ως ήπια παρέμβαση του δράστη στην ιδιωτική ζωή του παρακολουθούμενου[220]. Ακόμη όμως και στις έννομες τάξεις που έχει ποινικοποιηθεί η εν λόγω συμπεριφορά, δεν αξιολογείται ως εξαιρετικά σοβαρή προσβολή στη ζωή του θύματος, διότι εκλαμβάνεται ως μια εν δυνάμει επικίνδυνη συμπεριφορά με τον κίνδυνο για την προσωπική ασφάλεια και τη σωματική ακεραιότητα του

[218] Στο ίδιο
[219] Βλ. Furnell, ό.π., σ. 268
[220] Βλ. Κατσογιάννου, ό.π., σ. 1455

παρακολουθούμενου ή των οικείων του να μην είναι άμεσος και παρών, αλλά ελλοχεύων (π.χ. κλιμάκωση σε «offline stalking»)[221].

Ας μην ξεχνάμε πως το «cyberstalking» αποτελεί μια σειρά ενεργειών που διαπράττονται κατά τρόπο διαρκή και επίμονο. Επίσης, η συμπεριφορά μπορεί να μην εκλαμβάνεται ως παρενοχλητική από τα θύματα, διότι ενδέχεται να θεωρούν πως αποτελεί πτυχή της σχέσης τους με το δράστη. Επιπρόσθετα, δεν έχουν αποκρυσταλλωθεί ακόμη επιστημονικά τα χαρακτηριστικά και το «προφίλ» των «cyberstalkers», αλλά και οι παράγοντες κινδύνου εκδήλωσης της συμπεριφοράς ή πρόβλεψης της κλιμάκωσής της σε «offline stalking». Ακόμη, η απροθυμία καταγγελίας των περιστατικών και το γεγονός ότι αυτά τελούνται εξ αποστάσεως χωρίς να υπάρχει εκ του σύνεγγυς παρακολούθηση (όπως στο «offline stalking»), εντείνουν περισσότερο το πρόβλημα δίωξής τους[222].

Εκτός αυτών, οι «cyberstalkers» χρησιμοποιούν τις ΤΠΕ και το Διαδίκτυο για να παρακολουθήσουν και να παρενοχλήσουν τα θύματά τους και λαμβάνουν μέτρα για την απόκρυψη της ταυτότητάς τους δυσχεραίνοντας, έτσι, τον εντοπισμό τους (αφού δεν αφήνουν ψηφιακά ίχνη). Οι «cyberstalkers» φαίνεται πως είναι περισσότερο εξοικειωμένοι με την πληροφορική τεχνολογία σε σχέση με τα θύματα και τις Αρχές επιβολής του νόμου. Επίσης, οι πάροχοι υπηρεσιών Διαδικτύου (ISPs), που παρέχουν στους συνδρομητές τους έναντι αντιτίμου διάφορες υπηρεσίες που σχετίζονται με το Διαδίκτυο (π.χ. πρόσβαση σε ιστοσελίδες), δυσχεραίνουν την εξιχνίαση των υποθέσεων, διότι πολλές φορές δεν παρέχουν έγκαιρα τις απαιτούμενες πληροφορίες που θα βοηθήσουν τις διωκτικές αρχές στην ανακάλυψη της ταυτότητας των δραστών (π.χ. δεν επιτρέπουν την είσοδο σε αρχεία τους που αφορούν τις δραστηριότητες πελατών τους). Τέλος, η εκπαίδευση των διωκτικών Αρχών (όπως π.χ. των αστυνομικών) στην χρήση ΤΠΕ κρίνεται ως ελλιπής, λαμβάνοντας υπόψη πως η εξιχνίαση των ηλεκτρονικών εγκλημάτων απαιτεί την τεχνολογική αξιοποίηση των ψηφιακών αποδείξεων μέσω της ύπαρξης κατάλληλης τεχνογνωσίας, προγραμμάτων και λογισμικών Η/Υ και του εν γένει υλικοτεχνικού εξοπλισμού[223].

Παρόλα αυτά, δεν πρέπει να παραβλεφθεί και το γεγονός πως αμφισβητείται η εγκληματοπροληπτική λειτουργία των ποινών που επιβάλλονται για το αδίκημα του «cyberstalking», καθώς φαίνεται να μην είναι ικανές να αποτρέψουν τους

[221] Στο ίδιο, σ. 1477 και Roberts, ό.π., σ. 280
[222] Βλ. Pittaro, ό.π., σ. 185 και Roberts, ό.π., σ. 280
[223] ό.π.

μεμονωμένους δράστες από την επανάληψη του αδικήματος, ούτε το σύνολο του πληθυσμού από τη διάπραξή του. Δεν είναι λίγες οι περιπτώσεις που δεν έχει καταδικασθεί ο «cyberstalker» λόγω των «κενών» που υπάρχουν στην δικογραφία και της αδυναμίας αξιοποίησης των ψηφιακών αποδείξεων[224].

Μία ακόμη δυσκολία στην εξιχνίαση και αποτελεσματική αντιμετώπιση του φαινομένου είναι οι διαφορετικές ποινικές δικαιοδοσίες στις οποίες πιθανώς να υπάγονται δράστης και θύμα, δεδομένου πως δεν έχει διευκρινιστεί πλήρως η έννοια της δικαιοδοσίας στον Κυβερνοχώρο. Οι Brenner και Koops (2004) έθεσαν τον προβληματισμό σχετικά με τα κριτήρια καθορισμού της δικαιοδοσίας άσκησης ποινικής δίωξης σε βάρος του «cyberstalker» και αν θα είναι η χώρα καταγωγής του δράστη ή του θύματος, ή αν θα είναι η χώρα που διαπράττεται το σύνολο των ενεργειών του δράστη ή εκείνη όπου εμφανίζονται οι συνέπειες των πράξεών του, δηλαδή ο τόπος διαμονής του θύματος[225].

7.2. Παράγοντες απροθυμίας καταγγελίας

Τα ποσοτικά δεδομένα των εμπειρικών μελετών σχετικά με το «cyberstalking» δεν είναι ακριβή λόγω του ότι δεν καταγγέλλονται όλα τα περιστατικά από τα θύματα, ούτε εξιχνιάζονται όλες οι υποθέσεις ώστε να ταυτοποιηθεί ο δράστης και να του απαγγελθούν κατηγορίες. Ο παράγοντας της απροθυμίας καταγγελίας επιδρά στην αποτύπωση των πραγματικών διαστάσεων του φαινομένου και εντείνει ακόμη περισσότερο το πρόβλημα του *σκοτεινού αριθμού* αυτής της μορφής εγκληματικότητας[226].

Η απροθυμία καταγγελίας, όπως έχει ήδη αναφερθεί, δυσχεραίνει τη δίωξη και την εξιχνίαση των υποθέσεων «cyberstalking». Τα θύματα ενδέχεται να μην καταγγείλουν στις Αρχές την σε βάρος τους παρενοχλητική συμπεριφορά, διότι έχουν την πεποίθηση πως δεν είναι αρκετά σοβαρή και επιβλαβής, παρά μόνο σε περιπτώσεις που ο βαθμός και η ένταση του άγχους, της δυσφορίας και του φόβου που βιώνουν από την παρακολούθηση δεν είναι πλέον ανεκτά. Να ληφθεί υπόψη, πως πολλά από τα θύματα δεν γνωρίζουν τη νέα αυτή μορφή εγκληματικής συμπεριφοράς με αποτέλεσμα ακόμη και αν την υφίστανται, να μην την αναγνωρίζουν ως τέτοια και ως εκ τούτου να

[224] Βλ. Furnell, ό.π., σ. 275-277
[225] Βλ. Roberts, ό.π., σ. 281
[226] Βλ. Pittaro, ό.π., σ. 182

μην την καταγγέλλουν στις Αρχές[227]. Κυριαρχεί δε η αντίληψη πως οι αστυνομικές αρχές δε θα λάβουν σοβαρά υπόψη την καταγγελία, αν δεν προσκομιστούν από τα ίδια τα θύματα αποδεικτικά της σε βάρος τους συμπεριφοράς στοιχεία (π.χ. συνομιλίες από το «MSN messenger» ή μέσω email) ή αν αυτή δεν κλιμακωθεί σε δια ζώσης παρακολούθηση[228]. Ακόμη, πιθανή είναι η αποθάρρυνση των θυμάτων να εμπλακούν στο σύστημα απονομής ποινικής δικαιοσύνης (ΣΑΠΔ) από τους ανακριτικούς υπαλλήλους, με σκοπό την εξωδικαστική μεταχείριση της υπόθεσης[229].

Επιπρόσθετα, πολλά από τα θύματα δεν είναι επαρκώς ενημερωμένα για το νομικό πλαίσιο προστασίας ούτε για την ύπαρξη εθελοντικών οργανώσεων στο Διαδίκτυο και τη λειτουργία online πλατφορμών (π.χ. «WHO@», «CyberAngels» αντίστοιχα) που δραστηριοποιούνται στον τομέα της καθοδήγησης, της υποστήριξης και της παροχής νομικών συμβουλών σε θέματα κυβερνοασφάλειας και προστασίας των πολιτών από κυβερνοεγκλήματα. Επικρατεί δε η αντίληψη πως οι πάροχοι υπηρεσιών Διαδικτύου έχουν μερίδιο ευθύνης στην εκδήλωση εγκληματικών συμπεριφορών από τους πελάτες τους, καθώς δεν ελέγχουν τις δραστηριότητές τους και δεν απενεργοποιούν άμεσα τους λογαριασμούς των δραστών σε περίπτωση εμφάνισης παράνομης συμπεριφοράς παρά μόνο όταν υποβληθεί σχετικό αίτημα από τα θύματα[230].

Το κλίμα της δυσπιστίας των θυμάτων απέναντι στις διωκτικές Αρχές εντείνεται ακόμη περισσότερο από την ελλιπή εξειδίκευση και εκπαίδευση των αρμόδιων υπαλλήλων στον χειρισμό υποθέσεων ηλεκτρονικών εγκλημάτων, όπως αναφέρθηκε στο αμέσως προηγούμενο υποκεφάλαιο. Επίσης, το θύμα «cyberstalking» μπορεί να αποθαρρυνθεί να καταγγείλει επίσημα το περιστατικό, διότι γίνεται αποδέκτης των στάσεων των διωκτικών αρχών σχετικά με το ότι και τα θύματα φέρουν μερίδιο ευθύνης για τη θυματοποίησή τους από την στιγμή που τα ίδια καθιστούν προσιτά στο ευρύ κοινό του Διαδικτύου προσωπικά τους δεδομένα και λόγω του ότι δε λαμβάνουν τεχνικά μέτρα αυτοπροστασίας από τους κινδύνους στον Κυβερνοχώρο[231].

Ακόμη, η απροθυμία καταγγελίας δεν οφείλεται μόνο στις στάσεις των θυμάτων για την αναποτελεσματικότητα των αστυνομικών, αλλά και των δικαστικών αρχών. Τα μικρά ποσοστά καταδίκης των «cyberstalkers» και η εν γένει επιείκεια με

[227] Στο ίδιο, σ. 191
[228] ό.π.
[229] ό.π.
[230] ό.π.
[231] ό.π.

την οποία αντιμετωπίζονται από τη δικαιοσύνη, αυξάνουν την απροθυμία καταγγελίας περιστατικών έμμονης διαδικτυακής παρενοχλητικής παρακολούθησης από τα θύματα, ενώ η κατάρριψη του κατηγορητηρίου λόγω ελλιπούς αποδεικτικής δύναμης ως απόρροια του έργου των αστυνομικών αρχών μπορούν να συντελέσουν στο να αποθαρρυνθούν τα θύματα από το να καταγγείλουν τις σε βάρος τους αξιόποινες πράξεις[232].

7.3. Διαχείριση καταγγελιών και αξιοποίηση των ψηφιακών αποδείξεων από τις Αρχές

Η αξιοποίηση των ψηφιακών αποδείξεων για την εξιχνίαση των υποθέσεων ηλεκτρονικών εγκλημάτων και κυβερνοεγκλημάτων (Digital Forensics)[233] και η μετέπειτα Συμπεριφορική Ανάλυση των Αποδείξεων (Behavioural Evidence Analysis/BEA), η οποία αποτελεί στρατηγική έρευνας που βασίζεται στην ανάλυση των αποδείξεων και εστιάζει σε συγκεκριμένα χαρακτηριστικά συμπεριφοράς και προσωπικότητας του πιθανού δράστη, βοηθούν στην κατανόηση του κινήτρου και του τρόπου δράσης του, καθώς επίσης, αυξάνουν τις πιθανότητες αναγνώρισης και άλλων πιθανών θυμάτων[234].

Η διερεύνηση ενός περιστατικού «cyberstalking» ξεκινά με την καταγγελία του στις διωκτικές Αρχές και την προσκόμιση ή ανεύρεση από το θύμα ψηφιακών αποδείξεων (cyber/digital evidence) σχετικά με την καταγγελλόμενη αξιόποινη συμπεριφορά. Οι ψηφιακές αποδείξεις στην περίπτωση του «cyberstalking» αφορούν κυρίως πληροφορίες σχετικά με την online επικοινωνία του θύματος με το δράστη. Ζητείται, λοιπόν, από το θύμα να προσκομίσει αντικειμενικά στοιχεία που αποδεικνύουν την έκνομη συμπεριφορά, όπως συνομιλίες μέσω της υπηρεσίας άμεσης ανταλλαγής μηνυμάτων ή ηλεκτρονικού ταχυδρομείου που περιέχουν το απειλητικό ή υβριστικό ή προσβλητικό περιεχόμενο ή ακόμη και αγγελίες που είναι αναρτημένες στο Διαδίκτυο με προσωπικά του δεδομένα[235].

---

[232] Βλ. Bocij, Chapter 1: What Is Cyberstalking?, στο P. Bocij (επιμ.), *Cyberstalking: Harassment in the Internet Age and How to Protect Your Family*, ό.π., σ. 10

[233] Βλ. C. Brown, Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice, *International Journal of Cyber Criminology*, 9, 1, 2015, σ. 65, Ανακτήθηκε από: https://www.researchgate.net/publication/282161204_Investigating_and_Prosecuting_Cyber_Crime_Forensic_Dependencies_and_Barriers_to_Justice

[234] Βλ. Al Mutawa, Bryce, Franqueira & Marrington, ό.π., σ. 97

[235] Βλ. Roberts, ό.π., σ. 280

Μέσω αυτών των αποδεικτικών στοιχείων μπορούν οι διωκτικές Αρχές να εξάγουν συμπεράσματα σχετικά με κάποια αναγνωριστικά χαρακτηριστικά του δράστη στη σύνταξη και την ορθογραφία, καθώς και πληροφορίες για την ταυτότητα και τα ενδιαφέροντά του. Επίσης, μπορεί να προκύψει το κίνητρο από το περιεχόμενο της επικοινωνίας (π.χ. σεξουαλικό, εκδικητικό, άλλο), αλλά και η ύπαρξη προηγούμενης σχέσης με το θύμα ή η φύση της σχέσης που επιθυμεί να έχει ο δράστης με το θύμα, χωρίς τη συναίνεση του τελευταίου[236].

Εκτός όμως από τις συνομιλίες μεταξύ δράστη και θύματος, οι αστυνομικές αρχές μπορούν να προβούν στην εξέταση του Η/Υ του θύματος και του υπόπτου/ πιθανού δράστη. Εξετάζοντας τα αρχεία, τους φακέλους και το ιστορικό περιήγησης σε διάφορους ιστότοπους στο Διαδίκτυο μπορούν να εξαχθούν συμπεράσματα σχετικά με τη διαδικτυακή συμπεριφορά του θύματος, τα ενδιαφέροντα και τον τρόπο ζωής του, τον χρόνο που αφιερώνει για περιήγηση στο Διαδίκτυο, αλλά και τις δραστηριότητες εκείνες που ενδεχομένως να συνέβαλαν στη θυματοποίησή του (π.χ. τακτικές επισκέψεις σε συγκεκριμένες ιστοσελίδες γνωριμιών, υψηλός βαθμός αυτο-έκθεσης στα μέσα κοινωνικής δικτύωσης κ.ο.κ.)[237]. Στην περίπτωση που υπάρχουν ένας ή περισσότεροι ύποπτοι ή έχει συλληφθεί ο δράστης, οι αστυνομικές αρχές μπορούν να εξετάσουν κατασχεμένους Η/Υ ή άλλες ηλεκτρονικές συσκευές προκειμένου να αποδείξουν τη σύνδεση του κατόχου τους με την αξιόποινη συμπεριφορά απέναντι στο θύμα. Βέβαια, η εξέταση του Η/Υ του υπόπτου μπορεί να οδηγήσει και στην απαλλαγή από τις κατηγορίες, στην περίπτωση που δεν ανευρεθούν ψηφιακές αποδείξεις που να τον συνδέουν με το θύμα και τις καταγγελλόμενες πράξεις[238].

7.4. Αποτελεσματική αντιμετώπιση του φαινομένου του «cyberstalking»

Για την αποτελεσματική παρέμβαση και αντιμετώπιση του φαινομένου του «cyberstalking» χρησιμοποιείται από τις διωκτικές Αρχές το μοντέλο «OVIAR» (Online Victimization Intervention and Reduction), το οποίο αποτυπώνει τη δυναμική

[236] Βλ. Al Mutawa, Bryce, Franqueira & Marrington, ό.π., σ. 101-102
[237] ό.π.
[238] ό.π.

πορεία ενός περιστατικού «cyberstalking» και μπορεί να χρησιμοποιηθεί και σε άλλες μορφές διαδικτυακής θυματοποίησης (π.χ. στο «cyberbullying»)[239].

Κάθε περιστατικό «cyberstalking» αποτελείται από διακριτά στάδια που επαναλαμβάνονται, το καθένα εκ των οποίων παρέχει ευκαιρίες αποτροπής του δράστη μέσω της κατάλληλης παρέμβασης που προσφέρει το μοντέλο «OVIAR». Σημασία για το μοντέλο αυτό έχει η διαδικασία λήψης απόφασης από τον «cyberstalker» για τον περιορισμό ή την κλιμάκωση των ενεργειών του. Η διαδικασία αυτή επηρεάζεται από πλήθος παραγόντων και κυρίως από την εξωγενή ανατροφοδότηση (extrinsic feedback)[240] που λαμβάνει ο «cyberstalker» από τις αντιδράσεις του θύματός του, η οποία μπορεί αν τον ενθαρρύνει ή να τον αποθαρρύνει στη συνέχιση της συμπεριφοράς του[241].

Η δομή του μοντέλου είναι τέτοια ώστε να απεικονίζει την εξέλιξη ενός τυπικού περιστατικού «cyberstalking», καθώς όλα τα περιστατικά τείνουν να εξελίσσονται με παρόμοιο τρόπο ανεξάρτητα από τη σοβαρότητά τους. Βασίζεται στο έργο του Αμερικανού οικονομολόγου, κοινωνιολόγου και πολιτικού επιστήμονα Herbert Simon «Administrative Behavior» (1947) αναφορικά με τις νοητικές διαδικασίες με τις οποίες λαμβάνονται οι ορθολογικές αποφάσεις («bounded rationality») και την σκοπιμότητα των ενεργειών προς επίτευξη συγκεκριμένων αποτελεσμάτων, και εμπλουτίστηκε με την ιδέα της επανάληψης (repetition), αφού το «cyberstalking» συνιστά μια σειρά επαναλαμβανόμενων από το δράστη συμπεριφορών[242].

Το μοντέλο δημιουργήθηκε με βάση τον ορισμό των Bocij και McFarlane (2002) για το «cyberstalking» (που παρατέθηκε πιο πάνω στο 1.2. υποκεφάλαιο) και δομήθηκε στη βάση έξι σταδίων: της Έναρξης (Initiation Stage), της Νοημοσύνης (Intelligence Stage), του Σχεδιασμού (Planning Stage), της Δράσης (Action Stage), της Ανατροφοδότησης και Αξιολόγησης (Feedback and Evaluation Stage) και της Επίλυσης - Ανάλυσης (Resolution)[243].

Στο πρώτο στάδιο της Έναρξης αναζητείται το συμβάν πυροδότησης (trigger event) του ενδιαφέροντος του «cyberstalker», πώς επιλέχθηκε δηλαδή το θύμα και

---

[239] Βλ. P. Bocij, OVIAR: Towards a Model for Cyberstalking Intervention and Reduction, *International Journal of Emerging Trends in Social Sciences*, 4, 2, 2018, σ. 58, Ανακτήθηκε από: https://www.researchgate.net/publication/329165349_OVIAR_Towards_a_Model_for_Cyberstalking_Intervention_and_Reduction

[240] Στο ίδιο, σ. 58&61

[241] Στο ίδιο, σ. 59&60.

[242] ό.π.

[243] ό.π.

λήφθηκε η απόφαση για διαδικτυακή παρακολούθηση και παρενόχληση. Στο δεύτερο στάδιο της Νοημοσύνης ο «cyberstalker» συλλέγει πληροφορίες για το θύμα είτε με νόμιμα ή με παράνομα μέσα ώστε να σχεδιάσει στη συνέχεια τις ενέργειές του[244]. Στο επόμενο στάδιο του Σχεδιασμού επιλέγει σε ποιες ενέργειες θα προβεί συνεκτιμώντας τη διαθεσιμότητα των πληροφοριών, των πόρων, της τεχνογνωσίας, τον φόβο της ανακάλυψης και σύλληψης κ.λπ.. Στο στάδιο της Δράσης θέτει σε εφαρμογή το σχέδιό του αντιδρώντας στις απαντήσεις των θυμάτων ανάλογα. Στο στάδιο της Ανατροφοδότησης και της Αξιολόγησης ο «cyberstalker» αξιολογεί τα αποτελέσματα των ενεργειών του και λαμβάνει την ικανοποίηση από τις αντιδράσεις του θύματος. Αν αυτή είναι η επιδιωκόμενη, τότε θα συνεχίσει την παρενόχληση εμπλουτίζοντας ενδεχομένως τις επιτυχημένες πλέον τακτικές του. Αν όμως η ευχαρίστηση είναι λιγότερη από αυτή που προσδοκούσε, τότε είναι πολύ πιθανό να χάσει το ενδιαφέρον του για το συγκεκριμένο θύμα και να αναζητήσει κάποιο καινούριο ή να κλιμακώσει (escalate) τη συμπεριφορά του μέχρι να αποκομίσει την ευχαρίστηση που προσδοκά[245]. Τέλος, το στάδιο της Επίλυσης – Ανάλυσης αφορά είτε τη λήξη της παρενόχλησης ή την μείωσή της σε τέτοιο βαθμό ώστε να μη διαταράσσεται η ζωή του θύματος. Η λήξη της παρενόχλησης μπορεί να είναι οριστική αν ο δράστης συλληφθεί ή αναζητήσει καινούριο θύμα, ή προσωρινή λόγω καταδίκης ή απώλειας ενδιαφέροντος ή επιλογής καινούριου θύματος ή λόγω ενεργειών του θύματος που τον καθυστερούν ή τον αποτρέπουν προκειμένου να μην εντοπιστεί εκ νέου[246].

Η πρακτική εφαρμογή του μοντέλου «OVIAR» εστιάζει στα στάδια της Έναρξης, της Νοημοσύνης και της Ανατροφοδότησης και Αξιολόγησης. Στο πρώτο στάδιο της Έναρξης δίνεται έμφαση στην αποφυγή του να καταστεί το θύμα το επίκεντρο της προσοχής του δράστη. Πρόκειται για προληπτικά μέτρα που πρέπει να λαμβάνονται από τους χρήστες του Διαδικτύου για την ασφάλειά τους στον Κυβερνοχώρο και για την εκπαίδευση που πρέπει να έχουν σχετικά με τους κινδύνους που ελλοχεύουν. Η παρέμβαση στο στάδιο της Νοημοσύνης περιλαμβάνει τον περιορισμό της αυτοδιάθεσης προσωπικών πληροφοριών του θύματος στο Διαδίκτυο, ώστε να δυσχεραίνεται η συλλογή τους από επίδοξους δράστες. Τέλος, στο στάδιο της Ανατροφοδότησης και της Αξιολόγησης το ενδιαφέρον εστιάζεται κυρίως στην ανατροφοδότηση και ικανοποίηση που λαμβάνουν οι δράστες από τις αντιδράσεις των

[244] ό.π.
[245] ό.π.
[246] Στο ίδιο, σ. 60-61

θυμάτων τους, με την προτιμώμενη μέχρι στιγμής αντίδραση του θύματος στην αποθάρρυνση του δράστη να είναι η παθητική[247].

Εκτός από το μοντέλο «OVIAR», η αντιμετώπιση του «cyberstalking» απαιτεί την ολιστική (multi-layered) προσέγγιση και κατανόησή του ως κοινωνικό φαινόμενο. Επομένως, όλα τα ενδιαφερόμενα μέρη μπορούν να συμβάλλουν στην αποτελεσματική διαχείρισή του τόσο σε επίπεδο πολιτείας, όσο και σε επίπεδο ιδιωτικών φορέων, ερευνητών και θυμάτων, κάτι με το οποίο θα ασχοληθούμε αμέσως παρακάτω[248].

α) Σε επίπεδο πολιτείας

Η τροποποίηση της υπάρχουσας νομοθεσίας, ώστε να τυποποιείται αυτοτελώς ως ποινικό αδίκημα το «cyberstalking», με σαφή και ενιαία εννοιολόγηση της συμπεριφοράς που θα προσανατολίζεται περισσότερο στην αποτελεσματική προστασία των θυμάτων, η έμφαση στη γενική και ειδική πρόληψη, η αυστηροποίηση των ποινών και η ταχύτερη εκδίκαση των υποθέσεων «cyberstalking» αποτελούν πρωτοβουλίες καίριας παρέμβασης και ποινικής αντιμετώπισης του φαινομένου από μέρους της πολιτείας[249].

Επιπλέον, η πληροφόρηση και ευαισθητοποίηση του κοινού σχετικά με το «online stalking» και τον αντίκτυπο που έχει στη ζωή του θύματος αποτελεί έναν ακόμη άξονα της ολιστικής προσέγγισης της συμπεριφοράς, καθώς ένα ενημερωμένο κοινωνικό σύνολο είναι πιο εύκολο να αναγνωρίσει την παρενοχλητική συμπεριφορά και να προβεί στην καταγγελία της ή προκειμένου να αποτρέψει τη θυματοποίησή του θα λάβει τα κατάλληλα μέτρα αυτοπροστασίας στο Διαδίκτυο. Διοργανώνοντας, λοιπόν, εκστρατείες ενημέρωσης, καμπάνιες και ημερίδες και ενθαρρύνοντας τη συμμετοχή και την ανάληψη πρωτοβουλιών από αρμόδιους ιδιωτικούς φορείς σε θέματα κυβερνοασφάλειας, επιτυγχάνεται η υπευθυνοποίηση της Κοινωνίας της Πολιτών, η οποία απαρτίζεται από ενήμερους, ευαισθητοποιημένους ενεργούς πολίτες και ιδιωτικούς φορείς που συμβάλλουν στην πρόληψη της εγκληματικής αυτής συμπεριφοράς στο πλαίσιο ενός συμμετοχικού μοντέλου αντεγκληματικής πολιτικής[250].

---

[247] Στο ίδιο, σ. 63-64

[248] Βλ. Akdeniz και Ellison, ό.π., σ. 16,

[249] Βλ. C. Challa, G. Dhillon και K. Smith, Defining Objectives for Preventing Cyberstalking. *International Federation for Information Processing.* 2016, σ. 81, Ανακτήθηκε από: https://link.springer.com/article/10.1007%2Fs10551-017-3697-x

[250] ό.π.

Επιπρόσθετα, οι Αρχές επιβολής του νόμου (όπως η αστυνομία) πρέπει να προτρέπουν τα θύματα να καταγγέλλουν επίσημα τη θυματοποίησή τους συμβάλλοντας έτσι στη μείωση του σκοτεινού αριθμού αυτής της μορφής εγκληματικότητας. Δεδομένων των δυσκολιών στη δίωξη και εξιχνίαση των υποθέσεων της έμμονης διαδικτυακής παρενοχλητικής παρακολούθησης, πρέπει να ληφθεί μέριμνα για την εκπαίδευση των στελεχών των αστυνομικών αρχών σε θέματα κυβερνοασφάλειας, αναγνώρισης εγκληματικών συμπεριφορών στο ψηφιακό περιβάλλον, αρωγής προς τα θύματα και χρήσης της πληροφορικής τεχνολογίας. Ακόμη, κρίνεται αναγκαίος ο εφοδιασμός με τον απαραίτητο υλικο-τεχνικό εξοπλισμό προκειμένου να είναι σε θέση να χειριστούν υποθέσεις ηλεκτρονικών εγκλημάτων και κυβερνοεγκλήματων. Ακόμη, η χρηματοδότηση και η διάθεση πόρων για τη δημιουργία νέων υπηρεσιών που θα εξειδικεύονται στη διαχείριση ηλεκτρονικών εγκλημάτων και η στελέχωσή τους με καταρτισμένο στην τεχνολογία προσωπικό θα συντελούσε στην αποτελεσματική εξιχνίαση υποθέσεων «cyberstalking». Εκτός αυτών, η ανταλλαγή καλών πρακτικών και τεχνογνωσίας αλλά και η συνεργασία μεταξύ των συναρμόδιων φορέων και υπηρεσιών τόσο σε εθνικό όσο και σε υπερεθνικό επίπεδο αποτελεί ενθαρρυντική προοπτική για την αντιμετώπιση του αδικήματος[251].

β) Ερευνητές - Εγκληματολόγοι

Οι έρευνες γύρω από το «cyberstalking» θα μπορούσαν να εστιάσουν στην εξέταση των κοινωνικών, οικονομικών και πολιτιστικών παραγόντων που αλληλεπιδρούν στην εμφάνιση του φαινομένου, των παραγόντων απροθυμίας καταγγελίας από πλευράς των θυμάτων και των στάσεων των πολιτών σχετικά με την αποτελεσματικότητα ή μη των φορέων του επίσημου κοινωνικού ελέγχου στην εδραίωση ενός κλίματος ασφάλειας στο Διαδίκτυο. Περαιτέρω, θα μπορούσαν να διερευνηθούν τα ψυχολογικά και κοινωνικο-δημογραφικά χαρακτηριστικά των θυμάτων, ορισμένα από τα οποία ενδεχομένως να εντείνουν την ευαλωτότητά τους απέναντι στις απειλές, τρόποι ουσιαστικής υποστήριξης και προστασίας τους, καθώς και οι δυσάρεστες συνέπειες της θυματοποίησης στην καθημερινότητά τους. Επίσης, αντικείμενα εμπειρικής διερεύνησης θα μπορούσαν να είναι τα χαρακτηριστικά της συμπεριφοράς και της προσωπικότητας του δράστη, όπως και η σχέση του «cyberstalking» με άλλες μορφές

[251] Βλ. Abohassan, Alzeiby, Dhir, Kaur & Tandon, ό.π., σ. 12 και Dickinson, ό.π., σ. 25

εγκληματικής συμπεριφοράς στο Διαδίκτυο και ο ρόλος που διαδραματίζουν τα μέσα κοινωνικής δικτύωσης στην εμφάνιση της συμπεριφοράς[252].

γ) Ιδιωτικοί φορείς

Οι πάροχοι υπηρεσιών Διαδικτύου μπορούν να επιτελέσουν σημαντικό ρόλο στην αντιμετώπιση του «cyberstalking». Η αποτελεσματική παρέμβαση και πρόληψη του φαινομένου βασίζονται στην υπευθυνοποίηση των παρόχων σχετικά με την προστασία των προσωπικών δεδομένων και της ιδιωτικότητας των πελατών τους και την υποβόηθηση του έργου των διωκτικών αρχών παρέχοντας απρόσκοπτα τις πληροφορίες που αιτούνται στο πλαίσιο της διερεύνησης μιας υπόθεσης. Επίσης, στους ISPs μπορούν να απευθυνθούν τα θύματα για να ζητήσουν να «κλείσουν» το λογαριασμό πελάτη τους που τα παρενοχλεί. Ακόμη, είναι υποχρέωση των παρόχων να λάβουν ρυθμιστικά και τεχνικά μέτρα για την ασφαλή πλοήγηση στο Διαδίκτυο (π.χ. φίλτρα για το «μπλοκάρισμα» των ανεπιθύμητων συμπεριφορών, μηχανισμοί ελέγχου πρόσβασης, κ.ά.) και να καθιερώσουν διαδικασίες ασφάλειας και προστασίας από το «cyberstalking» (όπως είναι η αυθεντικοποίηση της ταυτότητας των χρηστών με χρήση ψηφιακών πιστοποιητικών/authentication schemes)[253].

Επιπλέον, οι εταιρείες που διαχειρίζονται τα μέσα κοινωνικής δικτύωσης έχουν την υποχρέωση να εκπονούν πολιτικές ασφαλείας – απορρήτου (privacy policies) για τη διαφύλαξη της ιδιωτικότητας των χρηστών τους. Η αυτορρύθμιση από τους ίδιους τους διαχειριστές των ιστοσελίδων και των πλατφορμών χωρίς κρατική παρέμβαση δίνει τη δυνατότητα επιβολής περιορισμών στο περιεχόμενο που αντίκειται στις πολιτικές ασφαλείας τους και συμβάλλει στον εντοπισμό έκνομων συμπεριφορών[254].

Τέλος, έχουν συσταθεί και λειτουργούν εθελοντικές οργανώσεις στο Διαδίκτυο για την παροχή νομικής υποστήριξης και αρωγής σε θύματα «cyberstalking» και γενικότερα ηλεκτρονικών εγκλημάτων όπως το «WHO@» (Working to Halt Online Abuse - https://www.haltabuse.org/). Επίσης, λειτουργούν online πλατφόρμες όπως το «CyberAngels» (https://www.cyberangels.org/), στις οποίες τα θύματα κυβερνοεγκλημάτων μπορούν να αναζητήσουν βοήθεια, ενώ λειτουργεί και το

[252] Βλ. Abohassan, Alzeiby, Dhir, Kaur & Tandon, ό.π., σ. 8-11

[253] Βλ. Μ. Καρύδα και Σπ. Κοκολάκης, Ψηφιακά κοινωνικά δίκτυα: Ζητήματα ιδιωτικότητας και η τεχνολογική αντιμετώπισή τους, Στο: Μ. Καρύδα, Σπ. Κοκολάκης, Λ. Μήτρου, Μ. Πισκοπάνη & Σπ. Τάσσης (επιμ.), *facebook, blogs και δικαιώματα*, Αθήνα, εκδ. Σάκκουλα, 2013, σ. 133-134

[254] Βλ. Α. Μ. Πισκοπάνη, Η ελευθερία της έκφρασης στο «ιδιωτικοποιημένο» δημόσιο δίκτυο του Facebook, Στο: Μ. Καρύδα, Σπ. Κοκολάκης, Λ. Μήτρου, Μ. Πισκοπάνη & Σπ. Τάσσης (επιμ.), *facebook, blogs και δικαιώματα*, Αθήνα, εκδ. Σάκκουλα, 2013, σ. 39&42&45

National Centre For Cyberstalking Research/NCCR (https://www.beds.ac.uk/nccr/) στο Πανεπιστήμιο του Bedfordshire στο Ηνωμένο Βασίλειο.

δ) Θύματα και χρήστες του Διαδικτύου

Τα θύματα του «cyberstalking» μπορούν να συμβάλλουν καταρχήν στην αντιμετώπιση του φαινομένου μέσω της καταγγελίας των περιστατικών. Η προσωπική υπευθυνότητα, η αυξημένη εποπτεία των προσωπικών πληροφοριών που δημοσιεύονται, η ενημέρωση σχετικά με τους κινδύνους που ελλοχεύουν στο Διαδίκτυο και η σωστή διαδικτυακή συμπεριφορά στη βάση ενός κώδικα δεοντολογίας μπορούν να συμβάλλουν στην πρόληψη της θυματοποίησης από το «cyberstalking». Η χρήση ονομάτων (usernames) και ψευδωνύμων που δεν προσδιορίζουν το φύλο και την ηλικία του χρήστη, η αποφυγή δημοσιοποίησης απόρρητων προσωπικών πληροφοριών, η ενημέρωση σχετικά με τις πολιτικές ασφαλείας των ISPs, η χρήση τεχνικών κρυπτογράφησης (encryption) στις ιδιωτικές συνομιλίες προκειμένου να διασφαλιστεί η ακεραιότητα, η εμπιστευτικότητα και η αυθεντικότητα των ανταλλασσόμενων πληροφοριών, και η αγορά προγραμμάτων προστασίας από ιούς Η/Υ και «τειχών προστασίας» από κακόβουλες επιθέσεις στο Διαδίκτυο, μπορούν να συμβάλλουν καθοριστικά στη μείωση της θυματοποίησης των αθώων χρηστών. Τέλος, η αποθήκευση του περιεχομένου των ηλεκτρονικών επικοινωνιών που θα μπορούσαν να αποτελέσουν αποδεικτικά στοιχεία της παρενοχλητικής συμπεριφοράς και η επικοινωνία με τους ISPs σε περίπτωση παραβίασης των πολιτικών ασφαλείας από τον πελάτη – δράστη, αποτελούν ατομικές ενέργειες που μπορούν να συμβάλλουν στη μείωση των περιστατικών «cyberstalking»[255].

Μέρος Δεύτερο

8. Η προστασία των ανθρωπίνων δικαιωμάτων

8.1. Εννοιολογική προσέγγιση των ανθρωπίνων δικαιωμάτων

Τα ανθρώπινα δικαιώματα αποτελούν ηθικές αρχές που θέτουν συγκεκριμένα πρότυπα συμπεριφοράς και προστατεύονται ως νόμιμα δικαιώματα λόγω της δικαιϊκής τους πρόβλεψης τόσο σε υπερεθνικό όσο και σε εθνικό επίπεδο, καθώς θεωρούνται έμφυτα της ανθρώπινης ύπαρξης, σύμφωνα με τη θεωρία του Άγγλου φιλόσοφου John

[255] Βλ. Challa, Dhillon και Smith, ό.π., σ. 81-83 και Pittaro, ό.π., σ. 193-194

Locke[256]. Τα θεμελιώδη ανθρώπινα δικαιώματα είναι οικουμενικά, λόγω της παγκόσμιας αποδοχής, αναγνώρισης, αποτύπωσής τους σε διεθνή και εθνικά κείμενα και εφαρμογής τους, και δεν μεταβάλλονται σύμφωνα με τους κοινωνικούς σχηματισμούς που παρατηρούνται στις κοινωνίες[257].

Ο όρος «δικαίωμα» ενέχει την έννοια της εξουσίας και η κατοχύρωσή του προϋποθέτει την ύπαρξη κράτους[258]. Ωστόσο, η κρατική εξουσία πολλές φορές θέτει σε κίνδυνο τα έννομα αγαθά που προστατεύουν τα ανθρώπινα δικαιώματα, γι' αυτό είναι απαραίτητη η νομική κατοχύρωσή τους ως θεμελιώδη δικαιώματα του ανθρώπου, που εδράζονται στις σχέσεις αλληλεπίδρασης μεταξύ κράτους και κοινωνίας είτε σε συλλογικό, είτε σε ατομικό επίπεδο[259].

Τα ανθρώπινα δικαιώματα καθιερώθηκαν διεθνώς μετά τον Β΄ Παγκόσμιο Πόλεμο με την υπογραφή διεθνών νομικών κειμένων και την ίδρυση δικαιοδοτικών οργάνων για την τήρηση και προστασία τους, αλλά και σε εθνικό επίπεδο με τον δικαστικό έλεγχο και τη λειτουργία Ανεξάρτητων Αρχών[260]. Στο πλαίσιο του ΟΗΕ το 1948 υπεγράφη η *Οικουμενική Διακήρυξη των Ανθρωπίνων Δικαιωμάτων* και ακολούθησαν πλήθος ακόμη διεθνών συμβάσεων και συμφώνων όπως το *Διεθνές Σύμφωνο για τα Ατομικά και Πολιτικά Δικαιώματα* (ΔΣΑΠΔ) και το *Διεθνές Σύμφωνο για τα οικονομικά, κοινωνικά και πολιτιστικά δικαιώματα* το 1966, καθώς και το *Διεθνές Σύμφωνο κατά των βασανιστηρίων και άλλων τρόπων σκληρής, απάνθρωπης ή ταπεινωτικής μεταχείρισης ή τιμωρίας* το 1984. Στο πλαίσιο του Συμβουλίου της Ευρώπης σημαντικά κείμενα αποτελούν η *Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου* (ΕΣΔΑ) του 1950, όπως τροποποιήθηκε και συμπληρώθηκε έκτοτε με μια σειρά πρόσθετων Πρωτοκόλλων, ο *Ευρωπαϊκός Κοινωνικός Χάρτης* του 1961, αλλά και η *Ευρωπαϊκή Σύμβαση για την πρόληψη των βασανιστηρίων και της απάνθρωπης ή εξευτελιστικής μεταχείρισης ή ποινής* του 1987. Σε ενωσιακό επίπεδο, το πρωτογενές και δευτερογενές δίκαιο της ΕΕ αποτελούν πηγές ατομικών και κοινωνικών

[256] Βλ. Β. Βλαχόπουλος και Κ. Χρυσόγονος, *Ατομικά και Κοινωνικά Δικαιώματα,* 4η αναθεωρημένη έκδοση, Αθήνα, Νομική Βιβλιοθήκη, 2017, σ. 28

[257]Από σημειώσεις μαθήματος Π.Μ.Σ. «ΕΓΚΛΗΜΑΤΟΛΟΓΙΑ» Β' Εξαμήνου «Διεθνοποίηση της αντεγκληματικής πολιτικής και δικαιώματα του ανθρώπου»

[258] Βλ. Π. Δαγτόγλου, *Συνταγματικό Δίκαιο-Ατομικά Δικαιώματα*, Τόμος Α΄, Δεύτερη Αναθεωρημένη Έκδοση, Αθήνα, εκδ. Αντ. Ν. Σάκκουλα, 2005, σ. 4

[259] Βλ. Ι. Κοϊμτζόγλου, *Στοιχεία Δημοσίου Δικαίου*, Συνταγματικό και Διοικητικό Δίκαιο σε συνδυασμό με Διεθνές και Κοινοτικό Δίκαιο, πρόλογος Καθηγητή Α. Ι. Τάχου, Γ΄ Έκδοση, Αθήνα, εκδ. Σάκκουλα, 2005, σ. 81

[260] Βλ. Βλαχόπουλος και Χρυσόγονος, ό.π., σ. 51-60

δικαιωμάτων, όπως και ο *Χάρτης των Θεμελιωδών Δικαιωμάτων της ΕΕ* (ΧΘΔΕΕ) του 2000.

Εκτός, όμως, από τη ρύθμιση των κάθετων σχέσεων μεταξύ κράτους και κοινωνίας, τα ανθρώπινα δικαιώματα αναπτύσσουν την ισχύ τους και έναντι τρίτων (τριτενέργεια) και πιο συγκεκριμένα στις οριζόντιες σχέσεις μεταξύ ιδιωτών, διότι οι θεμελιώδεις αρχές που θέτουν, αφορούν το σύνολο της κοινωνικής και οικονομικής ζωής και πρόκειται για την υποχρέωση του κράτους να προστατεύει την σφαίρα ελευθερίας ενός πολίτη από τις προσβολές τρίτων[261]. Η τριτενέργεια των ανθρωπίνων δικαιωμάτων είναι συνταγματικά κατοχυρωμένη στο άρ. 25 παρ. 1 εδ. γ΄ ΕλλΣ και βρίσκει έρεισμα στα φαινόμενα της παγκοσμιοποίησης, της ιδιωτικοποίησης των κρατικών δραστηριοτήτων και της ραγδαίας τεχνολογικής προόδου, που θέτουν σε κίνδυνο το δίκαιο υπό το πρίσμα του σύγχρονου ψηφιακού κράτους και της ολοένα και αυξανόμενης εξουσίας που αποκτούν ιδιωτικοί φορείς και επιχειρήσεις που δραστηριοποιούνται στους τομείς της επικοινωνίας και της πληροφορίας[262].

Στην βιβλιογραφία τα ανθρώπινα δικαιώματα συναντώνται εναλλακτικά με τους όρους «θεμελιώδη δικαιώματα» ή «ατομικά δικαιώματα», όροι που αναδεικνύουν τη σημασία τους στην προστασία της έμφυτης ατομικότητας και αυθυπαρξίας του ατόμου[263].

8.2. Οι διακρίσεις των ανθρωπίνων δικαιωμάτων – Οι «3 γενιές»

Οι «3 γενιές» των ανθρωπίνων δικαιωμάτων εμφανίστηκαν σε διαφορετικό στάδιο κοινωνικο-οικονομικής και πολιτιστικής εξέλιξης των μετανεωτερικών κοινωνιών[264]. Κάθε επόμενη γενιά δικαιωμάτων φαίνεται πως προκύπτει από την προηγούμενη δημιουργώντας μεταξύ τους αμοιβαία σχέση αλληλεπίδρασης και παραπληρωματικότητας[265]. Διακρίνονται σε ατομικά, κοινωνικά, πολιτικά και δικαιώματα αλληλεγγύης και η διάκρισή τους αυτή βρίσκει θεμελίωση στη γερμανική θεωρία των «status» του 20ου αιώνα[266].

---

[261] Βλ. Α. Γέροντας, Η αρχή της αναλογικότητας και η τριτενέργεια των θεμελιωδών δικαιωμάτων μετά την αναθεώρηση του 2001, Στο Ξ. Ι. Κοντιάδης (επιμ.), *Πέντε Χρόνια Μετά τη Συνταγματική Αναθεώρηση του 2001*, Πρόλογοι: Άννα Μπενάκη-Ψαρούδα & Δημήτρης Θ. Τσάτσος, Επίμετρο: Ευάγγελος Βενιζέλος & Ιωάννης Βαρβιτσιώτης, Αθήνα, εκδ. Αντ. Ν. Σάκκουλα, 2006, σ. 499

[262] Στο ίδιο, σ. 509-511

[263] Βλ. Δαγτόγλου, ό.π., σ. 5-6

[264] Από σημειώσεις μαθήματος Π.Μ.Σ. «ΕΓΚΛΗΜΑΤΟΛΟΓΙΑ» Β' Εξαμήνου «Διεθνοποίηση της αντεγκληματικής πολιτικής και δικαιώματα του ανθρώπου», σ. 4

[265] Βλ. Κοϊμτζόγλου, ό.π., σ. 84

[266] Βλ. Βλαχόπουλος και Χρυσόγονος, ό.π., σ. 68

Στην «πρώτη γενιά» δικαιωμάτων υποστηρίζεται πως ανήκουν τα ατομικά και πολιτικά δικαιώματα (civil/individual rights, political rights) και η εξαγγελία τους συμπίπτει χρονικά με την οικονομική και πολιτική ισχυροποίηση της αστικής τάξης με τη βαθμιαία επικράτηση του καπιταλιστικού τρόπου παραγωγής και της «οικονομίας της αγοράς». Καταγράφηκαν για πρώτη φορά σε επίσημα κείμενα προς τα τέλη του 18ου αιώνα[267].

Τα ατομικά δικαιώματα ή άλλως αμυντικά - αποθετικά έχουν «αρνητικό» περιεχόμενο (status negativus) και προστατεύουν την ελευθερία του ατόμου έναντι της κρατικής εξουσίας[268]. Η κατοχύρωσή τους συνεπάγεται την κατοχύρωση ενός χώρου ελευθερίας του ανθρώπου (status libertatis)[269] και την υποχρέωση του κράτους προς ανοχή της ασκήσεως των δικαιωμάτων αυτών, με την επιφύλαξη του νόμου και χωρίς να θίγεται ο πυρήνας του δικαιώματος, καθότι η άσκησή τους αποτελεί εκδήλωση της ελευθερίας του ατόμου να διαμορφώνει ελεύθερα και κατά βούληση τη ζωή του και ιδίως την ιδιωτική. Παραδείγματα ατομικών δικαιωμάτων που προβλέπονται στο Ελληνικό Σύνταγμα είναι το δικαίωμα στην προσωπική ελευθερία (άρ. 5 παρ. 3), στην προστασία της ιδιωτικής και οικογενειακής ζωής και στο άσυλο της κατοικίας (άρ. 9 παρ. 1&2), στην προστασία των προσωπικών δεδομένων (άρ. 9Α) και στο απόρρητο των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας (άρ. 19).

Τα πολιτικά δικαιώματα έχουν «ενεργητικό» περιεχόμενο (status activus) και εκφράζουν την αναγνώριση και προστασία της συμμετοχής του πολίτη στην πολιτειακή δράση. Αποτελούν έκφανση της δημοκρατικής αρχής με τη μορφή των αξιώσεων των ατόμων για συμμετοχή στην άσκηση της δημόσιας εξουσίας και τη διαμόρφωση της πολιτικής ζωής της χώρας[270]. Στην ελληνική έννομη τάξη πρόκειται για το δικαίωμα συμμετοχής στην πολιτική ζωή της χώρας (άρ. 5 παρ. 1 ΕλλΣ), το εκλογικό δικαίωμα (άρ. 51 παρ. 3 ΕλλΣ), το δικαίωμα του εκλέγεσθαι (άρ. 55 ΕλλΣ) και το δικαίωμα ίδρυσης πολιτικού κόμματος (άρ. 29 ΕλλΣ).

Στη «δεύτερη γενιά» ανθρωπίνων δικαιωμάτων συγκαταλέγονται τα οικονομικά, κοινωνικά και πολιτιστικά δικαιώματα (economic, social and cultural

[267] Από σημειώσεις μαθήματος Π.Μ.Σ. «ΕΓΚΛΗΜΑΤΟΛΟΓΙΑ» Β' Εξαμήνου «Διεθνοποίηση της αντεγκληματικής πολιτικής και δικαιώματα του ανθρώπου», σ. 5
[268] Βλ. Δαγτόγλου, ό.π., σ. 67
[269] Βλ. Μ. Σπυριδάκης, *Ατομικά και Κοινωνικά Δικαιώματα*, Επιτομή, Μ. Ι. Σπυριδάκης (επιμ.), Αθήνα, εκδ. Αντ. Ν. Σάκκουλα, 2011, σ. 8
[270] Στο ίδιο, ό.π., σ. 73-74

rights) και η εμφάνισή τους τοποθετείται χρονικά στις βιομηχανικές κοινωνίες του 19ου αιώνα[271].

Τα κοινωνικά δικαιώματα έχουν «θετικό» περιεχόμενο (status positivus) και αποτελούν έκφραση του κοινωνικού κράτους ως συνταγματικά αναγνωριζόμενες και προστατευόμενες αξιώσεις των πολιτών έναντι του κράτους για παροχή, υπό προϋποθέσεις, αγαθών ή υπηρεσιών[272]. Τα κοινωνικά δικαιώματα κατοχυρώνονται στο Ελληνικό Σύνταγμα στα άρ. 4 έως 25 και κάποια εξ αυτών είναι το δικαίωμα στην τέχνη, την επιστήμη και την παιδεία (άρ. 16) καθώς και το δικαίωμα στην προστασία της οικογένειας, της μητρότητας, της υγείας (άρ. 21).

Τέλος, η «τρίτη γενιά» δικαιωμάτων περιλαμβάνει τα δικαιώματα «αλληλεγγύης» (rights of solidarity), τα οποία θεμελιώνονται στη βάση των ιδεών της αλληλεγγύης μεταξύ των ανθρώπων και επιχειρούν να τοποθετήσουν τον άνθρωπο στο κοινωνικό, οικονομικό και πολιτιστικό πλαίσιο της ζωής του και των μεταβολών που επιφέρουν οι σύγχρονες τεχνολογικές και επιστημονικές εξελίξεις ιδίως στον τομέα της βιοϊατρικής και της γενετικής. Παραδείγματα αυτών είναι το δικαίωμα στο φυσικό και πολιτιστικό περιβάλλον, στην αειφόρο ανάπτυξη και την ειρήνη[273].

Τέλος, νέα δικαιώματα που εμφανίζονται λόγω της ραγδαίας τεχνολογικής και επιστημονικής προόδου, όπως είναι τα δικαιώματα που σχετίζονται με τη γενετική μηχανική, αλλά και τα ψηφιακά δικαιώματα που σχετίζονται με τις νέες τεχνολογίες, τίθενται υπό αμφισβήτηση σχετικά με το αν μπορούν να θεμελιώσουν θεωρητικά την καθιέρωση της «τέταρτης» γενιάς ανθρωπίνων δικαιωμάτων[274].

9. Η χρήση των νέων τεχνολογιών και του Διαδικτύου στις σύγχρονες Κοινωνίες της Πληροφορίας (ΚτΠ) και η παραβίαση των ατομικών δικαιωμάτων

9.1. Τα χαρακτηριστικά των Τεχνολογιών Πληροφοριών και Επικοινωνίας (ΤΠΕ) και του «συμμετοχικού» Διαδικτύου ή WEB 2.0

Η οικονομική αξία που απέκτησαν οι ηλεκτρονικά διακινούμενες πληροφορίες καθώς και η εμπορευματοποίησή τους στις σύγχρονες ΚτΠ είχαν ως αποτέλεσμα την

[271] Από σημειώσεις μαθήματος Π.Μ.Σ. «ΕΓΚΛΗΜΑΤΟΛΟΓΙΑ» Β' Εξαμήνου «Διεθνοποίηση της αντεγκληματικής πολιτικής και δικαιώματα του ανθρώπου»
[272] Βλ. Δαγτόγλου, ό.π., σ. 70-73
[273] Βλ. Μ. Σπυριδάκης, ό.π., σ. 81-82
[274] Βλ. Βλαχόπουλος και Χρυσόγονος, ό.π., σ. 82

εμφάνιση της «πληροφοριακής (έννομης) τάξης»[275] για τη ρύθμιση της ροής της πληροφορίας ανάμεσα στο κράτος και τους πολίτες, αλλά και στις σχέσεις μεταξύ ιδιωτών και την εξασφάλιση της ελεύθερης συμμετοχής των πολιτών στην «ηλεκτρονική κοινωνικότητα»[276].

Η ηλεκτρονική διακίνηση της πληροφορίας συντελείται με την χρήση των ΤΠΕ, οι οποίες δεν περιορίζονται μόνο στο Διαδίκτυο, αλλά περιλαμβάνουν κάθε τεχνολογία που βοηθά στην παραγωγή, αποθήκευση, μετάδοση, επικοινωνία και/ή διάδοση πληροφοριών με κάθε μορφή είτε ήχου, κειμένου, δεδομένων, γραφικών είτε βίντεο, ανεξαρτήτως εδαφικών συνόρων και εθνικών δικαιοδοσιών. Εξελίσσονται τάχιστα και χαρακτηρίζονται από παγκοσμιότητα, έχοντας μειώσει δραστικά το κόστος της φυσικής επικοινωνίας[277].

Από την άλλη, το Διαδίκτυο επιτρέπει τη διασύνδεση και δικτύωση συστημάτων Η/Υ σε όλο τον κόσμο, έχοντας πλέον αναχθεί σε κυρίαρχο μέσο επικοινωνίας. Η επέκταση της χρήσης του έχει επιφέρει την ανάπτυξη του ηλεκτρονικού εμπορίου, τη βελτίωση των υπηρεσιών επικοινωνίας και πληροφόρησης, ενώ χρησιμοποιείται για διασκέδαση, ψυχαγωγία και για άλλους σκοπούς, όπως για παράδειγμα στους τομείς της εκπαίδευσης και της τηλεργασίας. Είναι ένας χώρος που κυριαρχούν η ελευθερία της έκφρασης, της επικοινωνίας και της πληροφόρησης, και οι χρήστες του μπορούν να ανταλλάσσουν ελεύθερα απόψεις και γνώμες και να σχολιάζουν επίκαιρα θέματα χωρίς περιορισμούς, στο πλαίσιο μιας ορθής διαδικτυακής συμπεριφοράς, που υιοθετούν οι ίδιοι κατά βούληση[278].

Αυτή η εκτεταμένη χρήση των υπηρεσιών του Διαδικτύου και του Παγκόσμιου Ιστού έχουν θεμελιώσει ένα «νέο» δικαίωμα, αυτό της πρόσβασης στο Διαδίκτυο. Είναι τέτοια η δόμησή του που επιτρέπει τόσο την ιδιωτική επικοινωνία, όσο και τη δημόσια συζήτηση. Η πρόσβαση στο Διαδίκτυο επιτυγχάνεται από οποιοδήποτε μέρος στον κόσμο, οποιαδήποτε στιγμή, έχει χαμηλό κόστος και είναι σχετικά εύκολο στην χρήση.

---

[275] Βλ. Τ. Βιδάλης, Λ. Μήτρου και Α. Τάκης, Συνταγματική πρόσληψη των τεχνολογικών εξελίξεων και «νέα» δικαιώματα, Στο: Ξ. Ι. Κοντιάδης (επιμ.), *Πέντε χρόνια μετά τη συνταγματική αναθεώρηση του 2001*, Πρόλογοι: Άννα Μπενάκη-Ψαρούδα & Δημήτρης Τσάτσος, Επίμετρο: Ευάγγελος Βενιζέλος & Ιωάννης Βαρβιτσιώτης, Τόμος Πρώτος, Αθήνα, εκδ. Αντ. Ν. Σάκκουλα, 2006, σ. 302

[276] Στο ίδιο, σ. 296

[277] Βλ. Nuth, ό.π., σ. 444-445

[278] Βλ. Η. Καστανάς, Το Internet και η προστασία της ιδιωτικής ζωής και της ελευθερίας έκφρασης: σε αναζήτηση έξυπνων ρυθμίσεων, Στο: Χ. Σαββάκης, Π. Δόνος, Ηλ. Καστανάς, Δ. Χριστόπουλος, Κ. Τσιτσελίκης, Αν. Τάκης, Β. Βουτσάκης, Ευ. Μάλλιος, Φ. Βασιλόγιαννης, Τ. Βιδάλης, Γ. Κτιστάκις (επιμ.), *Νέες τεχνολογίες και συνταγματικά δικαιώματα*, Πρόλογος: Ν. Αλιβιζάτος, Δίκαιο & Κοινωνία στον 21ο αιώνα, Αθήνα, εκδ. Σάκκουλα, 2004, σ. 29

Χαρακτηρίζεται από παγκοσμιότητα και δεν γνωρίζει φυσικά όρια εγείροντας ταυτόχρονα ζητήματα δικαιοδοσίας ένεκα των υπερεθνικών του προοπτικών. Ενθαρρύνει την προσωπική έκφραση και ο χρήστης μπορεί να επιλέξει και να διαμορφώσει το προφίλ - εικόνα που θα παρουσιάσει στους άλλους χρήστες, ασκώντας το δικαίωμα του αυτοπροσδιορισμού του[279].

Επιπλέον, ο Παγκόσμιος Ιστός και οι διάφορες μηχανές αναζήτησης καθιστούν ακώλυτη την αναζήτηση, συλλογή και διάδοση πληροφοριών και την πρόσβαση σε ποικιλόμορφο περιεχόμενο. Η ελευθερία της έκφρασης που χαρακτηρίζει τη λειτουργία του Διαδικτύου ενθαρρύνει τη διάδραση και την ενεργό συμμετοχή του χρήστη. Ακόμη, πέρα από την ελευθερία έκφρασης και πληροφόρησης η λειτουργία του διέπεται από την ελεύθερη ανταπόκριση, η οποία ενθαρρύνεται από τις δυνατότητες της ανωνυμοποίησης (anonymization) και της ψευδωνυμοποίησης (pseudonymization). Πολλοί χρήστες επιθυμούν να αποκρύπτουν ή να συγκαλύπτουν την ταυτότητά τους στις ηλεκτρονικές επικοινωνίες. Η ανώνυμη αποστολή μηνυμάτων ενισχύει την μυστικότητα της επικοινωνίας και ενθαρρύνει την ελεύθερη έκφραση, αφού ο κάθε χρήστης μπορεί να εκφράσει και να ανταλλάξει απόψεις χωρίς να αποκαλύψει την ταυτότητά του. Επιπλέον, η δυνατότητα της κρυπτογράφησης του περιεχομένου των ιδιωτικών συνομιλιών ενισχύει την εμπιστευτικότητα και την ακεραιότητα της επικοινωνίας[280].

Οι «Netizens» ή «Digital Natives»[281], όπως ονομάζονται οι ψηφιακοί χρήστες, αναπτύσσουν μια «ηλεκτρονική κοινωνικότητα» επισκεπτόμενοι ιστοσελίδες κοινωνικής δικτύωσης ή κοινωνικών δικτύων (social networking sites ή social network sites), δημιουργώντας προφίλ, αναπτύσσοντας κοινωνικές σχέσεις, συμμετέχοντας σε ομάδες συζητήσεων (newsgroups) και ιστολόγια, αναζητώντας συντροφιά σε ιστοσελίδες γνωριμιών (dating websites), κ.ο.κ. Πρόκειται κατά τον J. Van Dijk, που ασχολήθηκε με την επιστήμη της επικοινωνίας, για την «κοινωνία των δικτύων» (network society)[282], της οποίας οι σχέσεις οργανώνονται μέσω των μιντιακών δικτύων, αντικαθιστώντας ή συμπληρώνοντας τα κοινωνικά δίκτυα της διαπροσωπικής επικοινωνίας. Η διαδραστική φύση του ψηφιακού περιβάλλοντος δημιουργεί χρήστες

[279] Στο ίδιο, σ. 31-33
[280] ό.π. και σ. 37-39
[281] Βλ. Μήτρου, ό.π., σ. 14 (υποσημείωση 18)
[282] Βλ. Πισκοπάνη, ό.π., σ. 22 (υποσημείωση 9)

που συνδιαμορφώνουν το επικοινωνιακό περιβάλλον και καθίστανται όχι μόνο καταναλωτές του περιεχομένου, αλλά και παραγωγοί του[283].

Το σύγχρονο Διαδίκτυο έχει αποκτήσει συμμετοχική μορφή γι' αυτό και χαρακτηρίζεται ως «συμμετοχικό Διαδίκτυο» ή «Web 2.0.»[284], «συμμετοχικός ιστός» (participative web) ή «ανθρωποκεντρικός ιστός» (people-centric web)[285], όροι που υποδηλώνουν την παρούσα φάση εξέλιξής του. Η τωρινή του φάση υποδηλώνει τη συνδιαμόρφωση του περιεχομένου του από τους χρήστες, οι οποίοι μοιράζονται εμπειρίες και κοινοποιούν προσωπικές τους πληροφορίες[286]. Παραδείγματα λειτουργίας του «Web 2.0» είναι οι ιστότοποι και τα μέσα κοινωνικής δικτύωσης, οι ιστότοποι κοινής χρήσης βίντεο («YouTube»), τα διαδικτυακά «fora», η προσθήκη ετικετών και λέξεων κλειδιών σε συνδέσμους και ιστότοπους («folksonomies», «tagging») κ.ά.[287].

Μολονότι οι ΤΠΕ και η σύγχρονη «αρχιτεκτονική» και λειτουργία του Διαδικτύου προσφέρουν πολλά πλεονεκτήματα στην ηλεκτρονική επικοινωνία, εντούτοις η χρήση τους θεωρείται ενίοτε προβληματική. Ο Κυβερνοχώρος δεν είναι ένας απόλυτα ασφαλής χώρος, καθώς παράσχει καινούριες εγκληματικές ευκαιρίες και δημιουργεί κινδύνους για τα έννομα αγαθά και τα δικαιώματα των ατόμων. Γι' αυτό το λόγο καθίσταται αναγκαία η ρύθμιση της χρήσης και λειτουργίας του[288].

9.2. Η μετεξέλιξη του «συμμετοχικού» Διαδικτύου και του ψηφιακού περιβάλλοντος σε «Ηλεκτρονικό Πανοπτικό»

Το «συμμετοχικό» Διαδίκτυο αποτελεί μια «κοινωνία των δικτύων», στην οποία διασυνδέονται όχι μόνο συστήματα Η/Υ, αλλά και χρήστες μέσω της ηλεκτρονικής επικοινωνίας μεταξύ τους. Η συμμετοχή σε ψηφιακά κοινωνικά δίκτυα διευκολύνει την ανάπτυξη διαπροσωπικών σχέσεων, έστω και σε εικονικό περιβάλλον. Η εγγενής κοινωνική φύση του ανθρώπου έχει συμπληρωθεί ή αντικατασταθεί από εικονικές διαπροσωπικές σχέσεις και πλέον γίνεται λόγος για το «ψηφιακό άτομο» (digital

[283] Στο ίδιο, σ. 24-26
[284] Βλ. Μήτρου, ό.π., σ. 10-11
[285] Στο ίδιο, σ. 11 (υποσημείωση 7)
[286] Επόμενη φάση εξέλιξης του σύγχρονου Διαδικτύου είναι το «Web 3.0» ή «Σημασιολογικός Ιστός» (Semantic Web) ή «Ιστός των Δεδομένων» (Web of data), που θα βασίζεται στο ουσιαστικό περιεχόμενο των ιστοσελίδων με την προσθήκη μετα-δεδομένων (metadata) στις δημοσιευμένες πληροφορίες, βλ. στο ίδιο, σ. 10 (υποσημείωση 6)
[287] Βλ. https://el.wikipedia.org/wiki/Web_2.0 (επίσκεψη την 23-12-2022)
[288] Βλ. Καστανάς, ό.π., σ. 33-39 & 45-48

person)[289], του οποίου οι δραστηριότητες διαμεσολαβούνται από τις σύγχρονες τεχνολογίες.

Η κοινωνικοποίηση στο ψηφιακό περιβάλλον υποκαθιστά την κοινωνικοποίηση στο εξωτερικό περιβάλλον και επιφέρει την απουσία φυσικής επαφής παρέχοντας μια ψευδαίσθηση ασφάλειας και «ψεύτικης» εγγύτητας. Η μεταβολή της φύσης της ανθρώπινης επικοινωνίας και των σχέσεων στο πλαίσιο της ψηφιακής δικτύωσης δημιουργεί κινδύνους για την ιδιωτική ζωή, διότι οι ίδιοι οι χρήστες καθιστούν προσωπικές τους πληροφορίες προσβάσιμες σε τρίτους χωρίς να έχουν τον απόλυτο έλεγχο της περαιτέρω διάδοσης και χρήσης τους[290]. Η κουλτούρα αυτή όμως του διαμοιρασμού των πληροφοριών παρέχει τη δυνατότητα σκιαγράφησης του εαυτού του χρήστη και των διαφορετικών πτυχών της ζωής του, με κίνδυνο να προκύψει ένας τύπος ατόμου, σύμφωνα με τη θεωρία του «μωσαϊκού» (mosaic theory)[291], που θα είναι καθαρά πληροφοριακό αντικείμενο, ένας «γυάλινος άνθρωπος» με πλήρη διαφάνεια και διαπερατότητα στη ζωή του[292].

Η παρακολούθηση της ζωής των άλλων ατόμων έχει μετεξελιθεί ποιοτικά και ποσοτικά με την χρήση των νέων τεχνολογιών και του Διαδικτύου λαμβάνοντας τη μορφή της επιτήρησης (surveillance) στον τομέα των διαπροσωπικών σχέσεων. Το ψηφιακό περιβάλλον εξελίσσεται σε «Ηλεκτρονικό Πανοπτικό»[293], δηλαδή σε ολοκληρωτικό έλεγχο της ανθρώπινης επικοινωνίας μέσω του Διαδικτύου. Η «πανοπτικοποίηση» (panopticanization)[294] των σύγχρονων κοινωνιών πραγματοποιείται αφενός μέσω του επίσημου κοινωνικού ελέγχου και της τεχνο-επιτήρησης από πλευράς του κράτους (κρατικός πανοπτισμός), μεταβάλλοντας έτσι τις κοινωνίες της πληροφορίας σε «κοινωνίες της επιτήρησης» (surveillance societies), και αφετέρου διαμέσου του άτυπου κοινωνικού ελέγχου, δηλαδή των ίδιων των πολιτών[295].

Διανύουμε την εποχή του «διαδικτυακού διαπροσωπικού πανοπτισμού», σύμφωνα με την Κατσογιάννου (2016) με την εκτεταμένη συλλογή, επεξεργασία και αποθήκευση πληροφοριών από πλευράς των πολιτών χωρίς την εμπλοκή κρατικών

[289] Βλ. Κατσογιάννου, ό.π., σ. 1443
[290] Στο ίδιο, σ. 1430
[291] Βλ. B-J Koops, B. Newell και I. Skorvanek, Location Tracking by Police: The Regulation of 'Tireless and Absolute Surveillance', *UC Irvine Law Review*, 9, 3, 2019, σ. 693-695, Ανακτήθηκε από: https://www.researchgate.net/publication/323811993_Location_Tracking_by_Police_The_Regulation_of_'Tireless_and_Absolute_Surveillance'
[292] Βλ. Κατσογιάννου, ό.π., σ. 1443
[293] Στο ίδιο, σ. 1442
[294] Στο ίδιο, σ. 1445
[295] Στο ίδιο, σ. 1448

φορέων και ΜΜΕ και για σκοπούς που δεν σχετίζονται με τη δημόσια ασφάλεια, την πρόληψη και την καταστολή της εγκληματικότητας, αλλά με τη συναισθηματική εμπλοκή των δρώντων υποκειμένων που πράττουν έχοντας ως κίνητρο το ερωτικό πάθος, την επιθυμία για εκδίκηση, το θυμό, τη ζήλεια, την απόρριψη. Η παρακολούθηση είναι πιο αθέατη, γίνεται δυσκολότερα αντιληπτή από τον παρακολουθούμενο, είναι παρενοχλητική και προκαλεί δυσφορία, αφού συνεπάγεται παραβιάσεις του ιδιωτικού βίου και των προσωπικών δεδομένων, και ξεκινά ως ιδιωτική πρωτοβουλία κάποιου χρήστη του Διαδικτύου, αφού η συλλογή και χρήση των πληροφοριών προορίζονται αποκλειστικά για προσωπική του χρήση[296].

Ωστόσο, εκτός από τους πολίτες, οι ιδιωτικές εταιρείες διαχείρισης των μέσων κοινωνικής δικτύωσης προβαίνουν σε επεξεργασία και αποθήκευση προσωπικών πληροφοριών των χρηστών τους. Ακόμη και αν ο χρήστης συγκατατίθεται με τους όρους χρήσης και τις πολιτικές ασφαλείας και απορρήτου που εφαρμόζουν οι διαχειρίστριες εταιρείες, προκύπτουν ερωτήματα σχετικά με την ενημέρωση και επίγνωση από πλευράς του χρήστη των συνεπειών της συλλογής και επεξεργασίας των δεδομένων του. Επίσης, οι όροι προστασίας της ιδιωτικότητας και των προσωπικών δεδομένων τροποποιούνται διαρκώς, χωρίς, όμως, ο χρήστης να ενημερώνεται επαρκώς και χωρίς να ανανεώνει τη συγκατάθεσή του. Ακόμη, η αποδοχή των όρων χρήσης και των πολιτικών απορρήτου που θέτουν οι εταιρείες αποτελεί προαπαιτούμενο για τη δημιουργία λογαριασμού. Με αυτόν τον τρόπο επιτυγχάνουν να έχουν τον έλεγχο και να επιτηρούν τις ηλεκτρονικές δραστηριότητες των εγγεγραμμένων χρηστών τους, προβαίνοντας ακόμη και σε απενεργοποίηση του λογαριασμού τους σε περίπτωση που διαπιστωθεί παράνομη δραστηριότητα[297].

9.3. Τα συγκρουόμενα έννομα αγαθά που τυγχάνουν προστασίας στο Διαδίκτυο

9.3.1. Η ελευθερία έκφρασης, επικοινωνίας και πληροφόρησης στο Διαδίκτυο.

Η ***ελευθερία έκφρασης*** αποτελεί συστατικό στοιχείο των δημοκρατικών κοινωνιών και θεμελιώδη βάση της διαδικτυακής επικοινωνίας. Κάνοντας χρήση των υπηρεσιών του Διαδικτύου κάθε άτομο απολαμβάνει το δικαίωμα να εκφράζεται και να διαδίδει σε ένα ευρύ κοινό την γνώμη και τις απόψεις του χωρίς να λογοκρίνεται, συμβάλλοντας κατ' αυτόν τον τρόπο στον δημόσιο διάλογο. Υπάρχουν ιστότοποι στους οποίους μπορεί ο

[296] Στο ίδιο, σ. 1449

[297] Βλ. Φ. Παναγοπούλου-Κουτνατζή, Κοινωνικά Δίκτυα και Προσωπικότητα - Ι, *Δίκαιο Μέσων Ενημέρωσης και Επικοινωνίας (ΔιΜΕΕ)*, Τεύχος 2, Αθήνα, Νομική Βιβλιοθήκη, 2012, σ. 189

καθένας να σχολιάσει ελεύθερα θέματα επικαιρότητας, να σατιρίσει πρόσωπα και καταστάσεις και να μεταδώσει πληροφορίες χωρίς να απαιτείται να γνωστοποιήσει την ταυτότητά του[298] (όπως είναι για παράδειγμα τα ιστολόγια[299], οι διαδικτυακές κοινότητες και τα διαδικτυακά «fora»[300]).

Η ελευθερία γνώμης και έκφρασης αποτελεί το σπουδαιότερο μέσο ανθρώπινης επικοινωνίας που καταδεικνύει την ιδιαιτερότητα και μοναδικότητα κάθε ατόμου, μιας και η κατοχή και έκφραση της προσωπικής γνώμης αποτελεί συστατικό στοιχείο της προσωπικότητας και ο περιορισμός ή κατάργηση της ελευθερίας έκφρασής της συνεπάγεται προσβολή της προσωπικότητας, λόγω του ότι μέσω της γνώμης αποτυπώνεται η διανοητική και συναισθηματική αντίδραση του ατόμου σε εξωτερικά ερεθίσματα[301].

Το δικαίωμα στην ελευθερία της γνώμης είναι ατομικό και πολιτικό δικαίωμα, διότι χωρίς την έκφραση της γνώμης δε θα ήταν δυνατή η διαμόρφωση γνήσιας κοινής γνώμης, άρα και οποιασδήποτε δημοκρατικής διαδικασίας[302]. Το εν λόγω δικαίωμα κατοχυρώνεται σε πλήθος διεθνών συμφώνων και συμβάσεων όπως στο άρ. 19 της Οικουμενικής Διακήρυξης των Δικαιωμάτων του Ανθρώπου και το άρ. 10 της ΕΣΔΑ και σε εθνικό επίπεδο στο 14 παρ. 1 ΕλλΣ. Το περιεχόμενό της αφορά την ελευθερία διαμόρφωσης, σχηματισμού, κατοχής, έκφρασης και εξωτερίκευσης, αλλά και διάδοσης ή αποσιώπησης της γνώμης (αρνητική πλευρά της ελευθερίας έκφρασης), όπως και την ελευθερία λήψης της γνώμης και αντίδρασης σε αυτήν, την ελεύθερη δηλαδή πληροφόρηση[303].

Περιορισμοί στην ελευθερία της έκφρασης επιβάλλονται μόνο όταν κρίνεται απολύτως αναγκαίος ο περιορισμός της, ιδίως στις περιπτώσεις παραβίασης του δικαιώματος της ελεύθερης ανάπτυξης της προσωπικότητας (άρ. 5 παρ. 1 ΕλλΣ), του απαραβίαστου της ιδιωτικής και οικογενειακής ζωής (άρ. 9 παρ. 1 ΕλλΣ) και του δικαιώματος προστασίας των προσωπικών δεδομένων (άρ. 9Α ΕλλΣ), διαφορετικά σε κάθε άλλη περίπτωση το δικαίωμα αυτό υπερτερεί[304].

---

[298] Βλ. Πισκοπάνη, ό.π., σ. 25-26, 33-35 και Τάσσης, ό.π., σ. 94
[299] Βλ. Τάσσης, ό.π., σ. 94
[300] Βλ. Μήτρου, ό.π., σ. 11-12
[301] Βλ. Δαγτόγλου, ό.π., σ. 487
[302] Στο ίδιο, σ. 488
[303] Στο ίδιο, σ. 491-499
[304] Βλ. Ι. Ιγγλεζάκης, *Το δικαίωμα στην ψηφιακή λήθη και οι περιορισμοί του*, Πρόλογος: Λ. Μήτρου, Αθήνα, εκδ. Σάκκουλα, 2014. σ. 158

Ένα ακόμη δικαίωμα που διέπει τη λειτουργία του Διαδικτύου είναι η ***ελευθερία της επικοινωνίας***. Ο Κυβερνοχώρος αποτελεί πρωτίστως τεχνικό και δευτερευόντως κοινωνικό περιβάλλον, στο οποίο ενθαρρύνεται η επικοινωνία και η σύναψη σχέσεων μέσω της ανάπτυξης ψηφιακών κοινωνικών δικτύων. Η διαδικτυακή «δημόσια» σφαίρα εξασφαλίζει όχι μόνο τον δημόσιο διάλογο, αλλά και την ιδιωτική επικοινωνία. Η δυναμική του «συμμετοχικού» Διαδικτύου βασίζεται στην επικοινωνιακή διαδραστικότητα, την ανεμπόδιστη ανταλλαγή μηνυμάτων και πληροφοριών και την έλλειψη λογοκρισίας δημιουργώντας ένα νέο πρότυπο επικοινωνίας, της «επικοινωνίας των δικτύων», που δεν αντικαθιστά, αλλά συμπληρώνει τις παραδοσιακές μορφές επικοινωνίας[305].

Η ελευθερία ανταπόκρισης και επικοινωνίας, ως μορφή της προσωπικής ελευθερίας του ατόμου και πτυχή της ιδιωτικής του ζωής, περιλαμβάνει δύο συνιστώσες: την ελευθερία διεξαγωγής και το απόρρητο κάθε μορφής επικοινωνίας, εφόσον όσοι επικοινωνούν επιθυμούν να διατηρήσουν τη μυστικότητα της επικοινωνίας[306]. Νομοθετικά προβλέπεται στο άρ. 12 της Οικουμενικής Διακήρυξης για τα Δικαιώματα του Ανθρώπου, στο άρ. 8 της ΕΣΔΑ και στο άρ. 19 ΕλλΣ, στο οποίο ρητώς κατοχυρώνεται η ελευθερία του ατόμου να προβαίνει σε ιδιωτική και εμπιστευτική επικοινωνία χωρίς να παρεμποδίζεται από δημόσια Αρχή, όπως και η προστασία του απορρήτου, της εμπιστευτικότητας και της μυστικότητας της επικοινωνίας[307].

Η προστασία του απορρήτου της επικοινωνίας στη χώρα μας προβλέπεται σε πλήθος νομικών διατάξεων, όπως στον Γενικό Κανονισμό για την Προστασία των Δεδομένων/ΓΚΠΔ, τα άρ. 370 και 370^{A} ΕλλΠΚ, στον Ν. 2225/1994 «*Για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας και άλλες διατάξεις*» και Ν. 3471/2006 «*Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του Ν. 2472/1997*», ενώ έχει συσταθεί με τον Ν. 3115/2003 η *Ανεξάρτητη Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών* (ΑΔΑΕ), που είναι επιφορτισμένη με τον έλεγχο της διασφάλισης του απορρήτου, σύμφωνα με τα οριζόμενα στην παρ. 2 άρ. 19 ΕλλΣ. Περιορισμοί στην ελευθερία της ανταπόκρισης και το απόρρητο της επικοινωνίας επιβάλλονται με την επιφύλαξη του νόμου για λόγους εθνικής ασφάλειας ή διακρίβωσης ιδιαίτερα σοβαρών

[305] Βλ. Πισκοπάνη, ό.π., σ. 25
[306] Βλ. Βλαχόπουλος και Χρυσόγονος, ό.π., σ. 296
[307] Βλ. Δαγτόγλου, ό.π., σ. 421-423

εγκλημάτων με την άρση του απορρήτου, στο μέτρο που αυτό κρίνεται αναγκαίο, κατόπιν διάταξης του εισαγγελέα ή απόφασης δικαστηρίου[308].

Το ***δικαίωμα στην πληροφόρηση*** έχει κατοχυρωθεί στα άρ. 19 του ΔΣΑΠΔ, άρ. 10 της ΕΣΔΑ και άρ. 5^{A} ΕλλΣ και είναι στενά συνδεδεμένο με την ελευθερία γνώμης, καθώς στο άρ. 10 παρ. 1 της ΕΣΔΑ ορίζεται πως η ελευθερία λήψης πληροφοριών εμπεριέχει την ελευθερία έκφρασης και αποτελεί προϋπόθεση για την ανάπτυξη της προσωπικότητας του ατόμου. Πρόκειται για ένα κοινωνικό δικαίωμα πρόσβασης στη διαθέσιμη πληροφορία και συστατικό στοιχείο των δημοκρατικών κοινωνιών που δίνουν έμφαση στην ενημέρωση για την άσκηση των δικαιωμάτων των πολιτών και τον έλεγχο της εξουσίας[309]. Στο άρ. 5^{A} παρ. 1 ΕλλΣ κατοχυρώνεται το δικαίωμα στην πληροφόρηση και στην παρ. 2 του ίδιου άρθρου το δικαίωμα συμμετοχής στις λειτουργίες του Κυβερνοχώρου και κατ' επέκταση στην Κοινωνία της Πληροφορίας.

Το δικαίωμα στην πληροφόρηση περιλαμβάνει δύο όψεις, την ενεργητική και την παθητική πληροφόρηση. Η ενεργητική πληροφόρηση είναι η ελευθερία του πληροφορείν, να παράγει δηλαδή ο καθένας και να διαδίδει τη γνώμη του και όχι ψευδείς ειδήσεις. Ωστόσο, η ελευθερία του πληροφορείν περιλαμβάνει και προϋποθέτει την ελευθερία του πληροφορείσθαι, την παθητική δηλαδή πληροφόρηση μέσω της ελεύθερης αναζήτησης, συλλογής και λήψης πληροφοριών και προϋποθέτει την απρόσκοπτη πρόσβαση στις γενικά προσιτές πηγές πληροφοριών[310].

Το δικαίωμα συμμετοχής στην ΚτΠ του άρ. 5^{A} παρ. 2 ΕλλΣ συνεπάγεται το δικαίωμα πρόσβασης στα ηλεκτρονικά δίκτυα και τις ηλεκτρονικά διακινούμενες πληροφορίες με το κράτος να είναι επιφορτισμένο με τη διασφάλιση της λήψης κατάλληλων μέτρων για την πρόσβαση, την παραγωγή, ανταλλαγή και διάδοσή τους. Με αυτόν τον τρόπο ο νομοθέτης συμπεριέλαβε την τεχνολογική εξέλιξη στον τομέα των ατομικών δικαιωμάτων, ώστε να είναι ευχερέστερη η άσκησή τους στο Διαδίκτυο και να διασφαλίζεται η συμμετοχή στη νέα ψηφιακή πραγματικότητα[311].

[308] Στο ίδιο, σ. 425
[309] Βλ. Βιδάλης, Μήτρου, Τάκης, ό.π., σ. 293
[310] Βλ. Δαγτόγλου, ό.π., σ. 523, 525-529
[311] Βλ. Βλαχόπουλος και Χρυσόγονος, ό.π., σ. 249

9.3.2. Η κατοχύρωση του δικαιώματος του πληροφοριακού αυτοκαθορισμού για την προστασία της προσωπικότητας, της ιδιωτικότητας και των προσωπικών δεδομένων στο Διαδίκτυο.

Προσωπικότητα

Η αυτοματοποιημένη επεξεργασία των προσωπικών δεδομένων και η εκούσια αποκάλυψη από τους χρήστες του Διαδικτύου προσωπικών τους πληροφοριών συνεπάγονται κινδύνους προσβολής του δικαιώματος στην ελεύθερη ανάπτυξη της προσωπικότητας του άρ. 5 παρ. 1 ΕλλΣ. Μπορεί το δικαίωμα στην (ψηφιακή) παρουσίαση του εαυτού[312] να αποτελεί έκφανση του γενικού δικαιώματος στην προσωπικότητα και να βοηθά τον χρήστη να συμμετέχει στα διαδικτυακά δρώμενα, η δημοσιοποίηση, όμως, πληροφοριών που άπτονται της ιδιωτικής του σφαίρας, έχει ως αποτέλεσμα την απώλεια του ελέγχου και της περαιτέρω διάδοσής τους, με αποτέλεσμα να μην μπορεί να αποφασίσει ελεύθερα και αυτόνομα για πράξεις και παραλείψεις που τον αφορούν και έτσι να προσβάλλεται η ελεύθερη ανάπτυξη της προσωπικότητάς του[313]. Επίσης, η ψηφιακή μνήμη και η υπόμνηση του ψηφιακού παρελθόντος στο Διαδίκτυο αποστερούν το δικαίωμα από τον χρήστη να διαγραφούν πληροφορίες που τον αφορούν και δεν επιθυμεί να κυκλοφορούν (πλέον), διότι μπορεί να τον συνδέουν με γεγονότα του παρελθόντος που επιθυμεί να ξεχάσει ή επειδή κρίνει πως οι πληροφορίες αυτές δεν ενδιαφέρουν τους υπόλοιπους χρήστες του Διαδικτύου[314]. Επίσης, τα ψηφιακά ίχνη της διαδικτυακής δραστηριότητας των χρηστών συντελούν στο να γίνεται γνωστή η ταυτότητά τους και έτσι να μην απολαμβάνουν την ελευθερία της ανώνυμης πλοήγησης στο Διαδίκτυο[315].

Ιδιωτικότητα

Τα μέσα κοινωνικής δικτύωσης εκλαμβάνονται από τους περισσότερους χρήστες ως ψηφιακή επέκταση της ιδιωτικής τους σφαίρας, μολονότι αποτελούν χώρους της διαδικτυακής «δημόσιας» σφαίρας, αφού έχουν την αντίληψη πως πρόκειται για χώρους που αφενός εξασφαλίζουν την πληροφοριακή ιδιωτικότητα, και αφετέρου επιτρέπουν την έκφραση, πληροφόρηση και την επικοινωνία με ένα κοινό που

[312] Βλ. Φ. Παναγοπούλου-Κουτνατζή, Το νέο πλαίσιο των ανανεωμένων δικαιωμάτων, Στο: Λ. Κοτσαλής και Κ. Μενουδάκος (επιμ.), *Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (GDPR) – Νομική διάσταση και πρακτική εφαρμογή*, Αθήνα, Νομική Βιβλιοθήκη, 2016, σ. 17

[313] Βλ. Παναγοπούλου-Κουτνατζή, ό.π., σ. 17 & 33-34

[314] Στο ίδιο, σ. 15-16

[315] Βλ. Ιγγλεζάκης, *Το δικαίωμα στην ψηφιακή λήθη και οι περιορισμοί του*, ό.π., σ. 60

απαρτίζεται από διαδικτυακούς φίλους (αν και όχι απαραίτητα)[316]. Στο Διαδίκτυο ο χρήστης «ιδιωτεύει δημόσια»[317] και υπάρχει η ψευδαίσθηση της ιδιωτικότητας και ενός «ημι-ιδιωτικού» χώρου στις διαδικτυακές κοινότητες, στις οποίες αναπτύσσονται σχέσεις οικειότητας και εμπιστοσύνης μεταξύ των μελών τους. Ωστόσο, η αποκάλυψη και αποθήκευση προσωπικών πληροφοριών είναι μεγαλύτερη από αυτήν που επιθυμεί τελικά ο χρήστης, ο οποίος καταφεύγει στη συνέχεια σε πρακτικές διασφάλισης της ιδιωτικότητας και των προσωπικών του δεδομένων[318].

Για να γίνει λοιπόν αντιληπτή η έννοια της ιδιωτικότητας, απαραίτητη είναι η εννοιολόγηση του δημόσιου και του ιδιωτικού βίου, σύμφωνα με την H. Arendt, πολιτική επιστήμονα και φιλόσοφο, στο έργο της «Vita Activa»[319]. Ο ιδιωτικός βίος περιορίζεται στο ίδιο το άτομο, την οικογένεια και τον στενό κύκλο των οικείων του, ενώ ο δημόσιος βίος περιλαμβάνει την κοινωνική και επαγγελματική ζωή του ατόμου και τις σχέσεις που αναπτύσσει συμμετέχοντας στα κοινά[320]. Πρόκειται για την ιδιωτική σφαίρα, η οποία σε συνδυασμό με την σφαίρα του απορρήτου διασφαλίζουν την προστασία του ατόμου από τη δημοσιότητα, ενώ μαζί και με την κοινωνική σφαίρα, συγκροτούν την προσωπικότητά του, με βάση τη γερμανική θεωρία των σφαιρών της προσωπικότητας[321]. Σε περίπτωση που η ιδιωτική σφαίρα παραβιάζεται, τότε εμποδίζεται η ελεύθερη ανάπτυξη της προσωπικότητας του ατόμου[322].

Αυτός είναι ο λόγος της νομικής κατοχύρωσης του απαραβίαστου της ιδιωτικής και οικογενειακής ζωής τόσο σε διεθνές όσο και σε εθνικό επίπεδο και συγκεκριμένα στο άρ. 12 της Οικουμενικής Διακήρυξης για τα Δικαιώματα του Ανθρώπου, στο άρ. 8 της ΕΣΔΑ, στα άρ. 7,8,9 του ΧΘΔΕΕ και στο άρ. 9 παρ. 1 ΕλλΣ. Σύμφωνα με το δικαίωμα αυτό, στη ζωή του ατόμου υπάρχει ένας πυρήνας ιδιωτικού βίου, τα όρια και το περιεχόμενο του οποίου καθορίζει το ίδιο το άτομο, χωρίς να επιτρέπει επεμβάσεις του κράτους ή τρίτων[323].

---

[316] Βλ. Καρύδα και Κοκολάκης, ό.π., σ. 120-121
[317] Βλ. Τάσσης, ό.π., σ. 74
[318] Βλ. Καρύδα και Κοκολάκης, ό.π., σ. 121-125
[319] Βλ. Χ. Ακριβοπούλου, *Το δικαίωμα στην ιδιωτική ζωή – Από τη γένεση στη σύγχρονη διαμόρφωση και προστασία του*, Αθήνα, εκδ. Σάκκουλα, 2012, σ. 26
[320] Βλ. Δαγτόγλου, ό.π., σ. 390
[321] Βλ. Ι. Ιγγλεζάκης, *Ευαίσθητα Προσωπικά Δεδομένα - Η Επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων και οι συνέπειές της*, Πρόλογος: Ν. Ιντζεσίλογλου, Ανατύπωση 2004 με προσθήκες των Νόμων 3090/2002, 3144/2003 και 3156/2003, Αθήνα, εκδ. Σάκκουλα, 2004, σ. 167
[322] Βλ. Δαγτόγλου, ό.π., σ. 384
[323] Στο ίδιο, σ. 290

Το απαραβίαστο της ιδιωτικής ζωής έχει στον πυρήνα του το δικαίωμα στην ιδιωτικότητα (right to privacy)[324], που πηγάζει από το αμερικανικό δίκαιο και διατυπώθηκε πρώτη φορά το 1896 από τους Αμερικανούς δικηγόρους S. Warren και L. Brandeis. Υπό το πρίσμα της ***απόλυτης διάκρισης μεταξύ δημόσιου – ιδιωτικού βίου*** η ιδιωτικότητα είναι το δικαίωμα του ατόμου στην απομόνωση, να μην ενοχλείται από τους άλλους και να αφήνεται στην ησυχία του (δικαίωμα εις την εαυτόν συγκέντρωσης του ατόμου – right to be let alone), σύμφωνα με τον Αμερικανό δικαστή T. Cooley[325]. Περιγράφεται ως απόσυρση, ιδιώτευση, κατ' επιλογή απόσταση του ατόμου από τους άλλους και από την παρακολούθηση της κοινωνικής του ζωής[326].

Αντίθετα, υπό το πρίσμα της ***συνθετικής αντίθεσης δημόσιου – ιδιωτικού βίου***, η ιδιωτικότητα εκλαμβάνεται ως οικειότητα[327] που επιτρέπει στο άτομο να παρουσιάζει τον εαυτό του στους άλλους, να επικοινωνεί με ασφάλεια και να απολαμβάνει σχέσεις εμπιστοσύνης με αυτούς χωρίς να απομονώνεται από τον δημόσιο χώρο, αλλά να έρχεται σε επαφή μαζί του συγκροτώντας έτσι την ταυτότητά του τόσο στην ιδιωτική, όσο και στη δημόσια ζωή του[328], αφού κατά τη νομολογία του ΕΔΔΑ η ιδιωτική ζωή έχει κοινωνική διάσταση[329].

Στις διαδικτυακές κοινότητες η ιδιωτικότητα εκφράζεται ως αξίωση των μελών να καθορίζουν τον χρόνο, τον τρόπο και την έκταση της συλλογής και επεξεργασίας των προσωπικών τους δεδομένων[330]. Η προσβολή της αφορά την παρακολούθηση ψηφιακών ιχνών, τη δημοσιοποίηση και έκθεση προσωπικών πληροφοριών στα social media και την παρενόχληση.[331]

<u>Προσωπικά δεδομένα</u>

Η τεράστια δύναμη που έχουν αποκτήσει η πληροφορία και η γνώση στην ΚτΠ θέτουν σε κίνδυνο τον ιδιωτικό βίο των ατόμων και τα προσωπικά τους δεδομένα, ιδίως μέσω της παραγωγής «βιοπορτραίτων»[332], μιας ανάγλυφης δηλαδή εικόνας της

[324] Βλ. Ακριβοπούλου, ό.π., σ. 23
[325] Βλ. Ιγγλεζάκης, ό.π., σ. 49
[326] Βλ. Χ. Ακριβοπούλου, Η ιδιωτικότητα του προσώπου μέσα από τη συνθετική αντίθεση δημόσιου-ιδιωτικού, *Επιστήμη και Κοινωνία – Επιθεώρηση Πολιτικής και Ηθικής Θεωρίας*, Τεύχος 26, Αθήνα, εκδ. Αντ. Ν. Σάκκουλα, 2011, σ. 2
[327] ό.π.
[328] ό.π.
[329] Βλ. Ιγγλεζάκης, ό.π., σ. 124
[330] Βλ. Καρύδα και Κοκολάκης, ό.π., σ. 121
[331] Βλ. Ακριβοπούλου, *Το δικαίωμα στην ιδιωτική ζωή – Από τη γένεση στη σύγχρονη διαμόρφωση και προστασία του*, ό.π., σ. 173-177
[332] Στο ίδιο, σ. 159

προσωπικότητας του ατόμου που προκύπτει από τον συσχετισμό και τη διασύνδεση των διαθέσιμων για εκείνο πληροφοριών. Αυτό έχει ως συνέπεια το άτομο να χάνει την προσωπική του ταυτότητα, και να μετατρέπεται σε καθαρά πληροφοριακό αντικείμενο[333], αφού κατηγοριοποιείται (profiling) σύμφωνα με τις δημοσιευμένες πληροφορίες που το αφορούν. Όμως, η παραγωγή «βιοπορτραίτων» καθιστά το άτομο υποκείμενο ελέγχου και χειραγώγησης από όσους έχουν πρόσβαση σε συστήματα επεξεργασίας πληροφοριών (κρατικοί φορείς και ιδιωτικές επιχειρήσεις)[334].

Οι κίνδυνοι αυτοί εντείνουν ακόμη περισσότερο το «παράδοξο της ιδιωτικότητας» (privacy paradox), σύμφωνα με το οποίο, οι χρήστες των υπηρεσιών του Διαδικτύου, ενώ πρόθυμα δημοσιοποιούν τα προσωπικά τους δεδομένα έχοντας συναινέσει στην επεξεργασία τους και έχοντας αποδεχθεί τους όρους χρήσης, ταυτόχρονα ανησυχούν για την προστασία τους, αφού είναι πιθανή η κατάχρησή τους για σκοπούς άγνωστους, πέραν αυτών που έχουν συναινέσει[335].

Επομένως, το κόστος που προκύπτει από την χρήση του Διαδικτύου είναι τα ψηφιακά ίχνη της «ελεύθερης» πλοήγησης. Το Διαδίκτυο συνιστά έναν χώρο όπου συγκεντρώνεται μεγάλος όγκος δεδομένων (μεγα-δεδομένων/Big Data)[336], στον οποίο υπάρχει υπέρμετρη πληροφοριακή εξουσία και διείσδυση στην σφαίρα απορρήτου του ατόμου, με τα δεδομένα να διατηρούνται ακόμη και όταν εκλείψει ο λόγος της αρχικής τους συλλογής ή σε περίπτωση που διαγραφούν από τον χρήστη, καθώς στο ψηφιακό περιβάλλον δεν υπάρχει λήθη[337]. Όλα τα ανωτέρω έχουν ως αποτέλεσμα ο χρήστης να χάνει τον έλεγχο των προσωπικών του πληροφοριών που διακινούνται στο Διαδίκτυο και να μην γνωρίζει μέχρι ποιο σημείο, από ποιον και για ποιον λόγο γίνεται η επεξεργασία τους[338].

Το δικαίωμα προστασίας των προσωπικών δεδομένων (right to data protection) βασίζεται στο απαραβίαστο της ιδιωτικής ζωής, στον σεβασμό της ανθρώπινης αξιοπρέπειας και στην ελεύθερη ανάπτυξη της προσωπικότητας, ενώ απορρέει από το άρ. 8 της ΕΣΔΑ και βρίσκει συνταγματική θεμελίωση στο άρ. 9^{A} ΕλλΣ. Το δικαίωμα αυτό δεν προβλέπει την απόλυτη απαγόρευση της συλλογής, επεξεργασίας και χρήσης των προσωπικών δεδομένων, αλλά καθιερώνει ένα περιοριστικό ρυθμιστικό πλαίσιο,

[333] Στο ίδιο, σ. 156
[334] Στο ίδιο, σ. 159
[335] Βλ. Ιγγλεζάκης, *Το δικαίωμα στην ψηφιακή λήθη και οι περιορισμοί του*, ό.π., σ. 65
[336] Στο ίδιο, σ. 57
[337] Βλ. Τάσσης, ό.π., σ. 90
[338] Βλ. Ιγγλεζάκης, ό.π., σ. 17

εντός του οποίου οι διαδικασίες αυτές επιτρέπονται. Η θεωρητική του θεμελίωση πηγάζει από τη θεωρία των σφαιρών προστασίας της προσωπικότητας, σύμφωνα με την οποία η ιδιωτική σφαίρα του ατόμου περιλαμβάνει δεδομένα προσωπικού χαρακτήρα που αφορούν ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο, τις «στενά προσωπικές ζώνες» που περιλαμβάνουν τις ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα, τα ευαίσθητα δεδομένα του άρ. 44 περίπτωση ιδ΄ του Ν. 4624/2019, και τις «απόκρυφες ζώνες», που συγκροτούν τον σκληρό πυρήνα του ιδιωτικού βίου και περιλαμβάνουν υπερευαίσθητες πληροφορίες, η αποκάλυψη των οποίων μπορεί να οδηγήσει σε στιγματισμό, διακρίσεις και κοινωνικό αποκλεισμό[339].

<u>Το δικαίωμα του πληροφοριακού αυτοκαθορισμού</u>

Τα δικαιώματα στην ελεύθερη έκφραση, επικοινωνία και πληροφόρηση στο Διαδίκτυο θέτουν σε κίνδυνο τα δικαιώματα στην προσωπικότητα, την ιδιωτικότητα και τα προσωπικά δεδομένα των χρηστών. Οι κίνδυνοι αυτοί επιχειρείται να αντιμετωπιστούν με την ενίσχυση του δικαιώματος του πληροφοριακού αυτοκαθορισμού.

Το δικαίωμα του πληροφοριακού αυτοκαθορισμού ή αυτοδιάθεσης των πληροφοριών καθιερώθηκε με την από 15-12-1983 απόφαση του Γερμανικού Ομοσπονδιακού Συνταγματικού Δικαστηρίου σύμφωνα με την οποία το δικαίωμα της ελεύθερης ανάπτυξης της προσωπικότητας, ο αυτοκαθορισμός και η αυτονομία του ατόμου προϋποθέτουν την ελευθερία του να αποφασίζει για το τι θα πράξει και τι θα παραλείψει σε συνδυασμό με την πραγματική δυνατότητα να ενεργεί σύμφωνα με την απόφασή του αυτή. Όποιος δεν γνωρίζει και δεν είναι σε θέση να υπολογίζει ποιες πληροφορίες που το αφορούν είναι γνωστές στον κοινωνικό του περίγυρο, είναι δυνατόν να περιορίζεται σημαντικά στην ελευθερία του να αποφασίζει αυτόνομα[340].

Για να λειτουργήσει το άτομο αυτόνομα πρέπει η απόφαση για το εάν και σε ποια έκταση θα γίνει επεξεργασία των πληροφοριών που το αφορούν, να είναι αποκλειστικά δική του. Εάν δεν γνωρίζει το αν και το πώς οι πληροφορίες αυτές συλλέγονται, δεν είναι σε θέση να εκτιμήσει τις συνέπειες των πράξεών του και τις αντιδράσεις των συνανθρώπων του. Αυτό έχει ως αποτέλεσμα την παραίτησή του από την άσκηση θεμελιωδών δικαιωμάτων, διότι τελεί σε καθεστώς ανασφάλειας λόγω της ακούσιας καταγραφής δεδομένων που το αφορούν. Άλλωστε, δεν είναι συμβατή με την

[339] Βλ. Ι. Ιγγλεζάκης, *Ευαίσθητα Προσωπικά Δεδομένα, Η Επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων και οι συνέπειές της,* ό.π., σ. 56-58

[340] Βλ. Α. Γέροντας, Το δικαίωμα της αυτοδιάθεσης των πληροφοριών – Υπερβολή ή αναγκαιότητα;, *Το Σύνταγμα,* Τεύχος 4, Αθήνα, εκδ. Αντ. Ν. Σάκκουλα, 1997, σ. 849-850

ανθρώπινη αξιοπρέπεια η συστηματική καταγραφή και αποκάλυψη όλων των πλευρών της προσωπικότητας ενός ατόμου, διότι πρέπει να παραμένει απαραβίαστος ένας χώρος ελευθερίας και έκφρασης[341].

Το δικαίωμα του πληροφοριακού αυτοκαθορισμού, ως ατομικό δικαίωμα, αποτελεί εκδήλωση του δικαιώματος στην ελεύθερη ανάπτυξη της προσωπικότητας και βρίσκει συνταγματική θεμελίωση στις διατάξεις των άρ. 5 παρ. 1, 2 παρ. 1, 9 παρ. 1 και 19 ΕλλΣ[342]. Βρίσκει, επίσης, θεωρητική θεμελίωση στο άρ. 8 της ΕΣΔΑ, καθώς αναπόσπαστο στοιχείο του ιδιωτικού βίου είναι η εξουσία αυτοπροσδιορισμού[343].

Η αναγνώριση του δικαιώματος δεν συνεπάγεται την απόλυτη και απεριόριστη κυριαρχία του ατόμου στα προσωπικά του δεδομένα, διότι το δικαίωμα έχει και κοινωνική διάσταση (status activus), αφού η προσωπικότητα του ατόμου αναπτύσσεται μέσα από τις κοινωνικές του σχέσεις και την αλληλεπίδραση με άλλα άτομα[344]. Ακόμη, δεν συνιστά απόλυτο δικαίωμα, αφού δύναται να περιοριστεί για λόγους δημοσίου συμφέροντος και λειτουργεί ανασχετικά στην τάση μετατροπής του ατόμου σε απλό πληροφοριακό αντικείμενο[345]. Τέλος, έρχεται σε σύγκρουση με την ελευθερία της πληροφόρησης, η οποία περιορίζεται στον βαθμό που απαιτείται για την προστασία της προσωπικότητας και αφορά κυρίως την αποκάλυψη ειδικών κατηγοριών προσωπικών δεδομένων που μπορούν να οδηγήσουν σε στιγματισμό, κοινωνικό αποκλεισμό και κατ' επέκταση να παρεμποδίσουν την ελεύθερη ανάπτυξη της προσωπικότητας του ατόμου[346].

9.4. Τα ατομικά δικαιώματα που παραβιάζονται από τη διάπραξη του αδικήματος του «cyberstalking»

Το «cyberstalking» εξ ορισμού αποτελεί μια συμπεριφορά που δεν είναι ανεκτή από αυτόν που την υφίσταται, διότι συνιστά αυθαίρετη επέμβαση στον ιδιωτικό του βίο και προσβάλλει το συνταγματικά κατοχυρωμένο δικαίωμα του απαραβίαστου της ιδιωτικής και οικογενειακής ζωής του άρ. 9 παρ. 1 ΕλλΣ. Ο «cyberstalker»

[341] Βλ. Κ. Άνθιμου, Το δικαίωμα του πληροφοριακού αυτοκαθορισμού του ατόμου ως έκφανση του δικαιώματος της προσωπικότητας, *Κριτική Επιθεώρηση νομικής θεωρίας και πράξης*, Τεύχος 1, Αθήνα, εκδ. Αντ. Ν. Σάκκουλα, 1998, σ. 165
[342] Βλ. Γέροντας, ό.π., σ. 851
[343] Βλ. Ιγγλεζάκης, ό.π., σ. 40
[344] Βλ. Ιγγλεζάκης, *Ευαίσθητα Προσωπικά Δεδομένα, Η Επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων και οι συνέπειές της,* ό.π., σ. 172
[345] Στο ίδιο, σ. 54
[346] Βλ. Γέροντας, ό.π., σ. 852&860

παρακολουθεί έμμονα, συστηματικά και μεθοδευμένα το θύμα στο Διαδίκτυο, με τρόπο κρυφό και ενοχλητικό με σκοπό να αποσπάσει πληροφορίες για την ιδιωτική του ζωή[347].

Παραβίαση του ιδιωτικού βίου συναντάται και στις τρεις ειδικότερες μορφές τέλεσης του «cyberstalking». Ειδικότερα, στο «email stalking» η αποστολή γραπτών μηνυμάτων, φωτογραφιών κ.λπ. με τρόπο συνεχή, επίμονο και πιεστικό (email bombing), προσβάλλει την ιδιωτικότητα του θύματος και το δικαίωμά του να μην ενοχλείται από τους άλλους. Επίσης, η αποστολή μέσω email κακόβουλου λογισμικού με σκοπό την προσβολή των αρχείων του θύματος από ιό ή τη μετάδοση ιού στη λίστα επαφών του εκλαμβάνεται ως ανεπιθύμητη και ενοχλητική, διότι πρόκειται για επέμβαση στην ιδιωτική του σφαίρα, αφού καταστρέφονται αρχεία με προσωπικές του πληροφορίες εν αγνοία του και χωρίς τη θέλησή του. Ακόμη, η ανεπιθύμητη αλληλογραφία (spam mail) και το ανεπιθύμητο ταχυδρομείο (junk email) αποτελούν επέμβαση στην ιδιωτική ζωή του αποδέκτη, μιας και το θύμα πρέπει να καταναλώσει προσωπικό του χρόνο για να «αδειάσει» το ηλεκτρονικό του ταχυδρομείο από διαρκώς συσσωρευόμενα άχρηστα μηνύματα[348].

Όσον αφορά το «computer stalking» η παραβίαση της ιδιωτικής ζωής συντελείται μέσω της απομακρυσμένης πρόσβασης του «cyberstalker» στον Η/Υ του θύματος και τα αρχεία του προσβάλλοντας την πληροφοριακή του ιδιωτικότητα, ενώ με την εγκατάσταση λογισμικού παρακολούθησης ή κακόβουλου λογισμικού, μπορεί να παρακολουθεί το πληκτρολόγιο ή να χειρίζεται τον κέρσορα, να παρακολουθεί τις δραστηριότητες του θύματος στο Διαδίκτυο ή και να υποκλέπτει προσωπικά του στοιχεία[349]. Επιπρόσθετα, ο δράστης είναι σε θέση να καταγράφει τις κινήσεις και δραστηριότητες του θύματος και να το παρακολουθεί σε πραγματικό χρόνο μέσω της κάμερας του Η/Υ (webcam). Οι δυνατότητες αυτές όμως περιορίζουν σημαντικά την προσωπική ελευθερία των θυμάτων και ιδίως την ελευθερία κίνησης του άρ. 5 παρ. 4 ΕλλΣ. Επίσης, λόγω του ότι η πλοήγηση αφήνει ψηφιακά ίχνη, οι «cyberstalkers» μπορούν να τα συλλέξουν και να τα αξιοποιήσουν για να εντοπίσουν το θύμα τους, το οποίο όμως μπορεί να επιθυμεί να απολαύσει τη δυνατότητα της ανωνυμίας που προσφέρει το Διαδίκτυο[350].

---

[347] Βλ. Κατσογιάννου, ό.π., σ. 1470
[348] Βλ. Κατσογιάννου, ό.π., σ. 1498 και Λάζος, ό.π., σ. 168-169
[349] Βλ. Κατσογιάννου, ό.π., σ. 1499&1501
[350] Βλ. Ιγγλεζάκης, *Το δικαίωμα στην ψηφιακή λήθη και οι περιορισμοί του*, ό.π., σ. V-VI (πρόλογος)

Τέλος, στο «internet stalking» η πληροφοριακή ιδιωτικότητα παραβιάζεται, διότι οι χρήστες αποκαλύπτουν πτυχές του ιδιωτικού τους βίου συμμετέχοντας σε διαδικτυακές ομάδες ή δημοσιεύοντας στο προφίλ τους σε μέσα κοινωνικής δικτύωσης, δίχως να είναι σε θέση να γνωρίζουν απόλυτα ποιες πληροφορίες από αυτές που κοινοποιούν, συλλέγονται από τρίτους και χρησιμοποιούνται με κακόβουλο τρόπο. Επιπλέον, η μέθοδος του «trolling» που περιλαμβάνει τη δημοσίευση στο Διαδίκτυο φωτογραφιών και βίντεο του θύματος και την ανάρτηση αγγελιών με πληροφορίες που προδίδουν την ταυτότητά του, προσβάλλει το δικαίωμα του θύματος να αναπτύσσει σχέσεις εμπιστοσύνης, οικειότητας και επικοινωνίας με άλλα άτομα[351]. Επιπρόσθετα, με την τακτική της διαδικτυακής δυσφήμισης (cyber defamation ή «cybersmearing»), η οποία δύναται να προκαλέσει τέτοια ενόχληση στο θύμα σε σημείο που να το αναγκάσει να τροποποιήσει τη διαδικτυακή του συμπεριφορά, απέχοντας ή περιορίζοντας την χρήση του Διαδικτύου, περιορίζεται το δικαίωμα της ελεύθερης περιήγησης του χρήστη στο Διαδίκτυο χωρίς να γίνεται αντιληπτός, άρα και η προσωπική του ελευθερία του άρ. 5 παρ. 4 ΕλλΣ[352].

Από την στιγμή, λοιπόν, που παραβιάζεται ο ιδιωτικός βίος των θυμάτων προσβάλλονται ταυτόχρονα το δικαίωμα του πληροφοριακού αυτοκαθορισμού, της προστασίας των προσωπικών δεδομένων του άρ. 9^{A} ΕλλΣ και της ελεύθερης ανάπτυξης της προσωπικότητας του άρ. 5 παρ. 1 ΕλλΣ. Η συλλογή προσωπικών πληροφοριών του θύματος από τον «cyberstalker» προσβάλλει το δικαίωμα του θύματος να καθορίζει και να αποφασίζει καταρχήν το ίδιο ελεύθερα ποιες πληροφορίες που το αφορούν θα καταστούν προσιτές και σε ποιο διαδικτυακό κοινό, με αποτέλεσμα να παρεμποδίζεται η αυτονομία και η δυνατότητα αυτοκαθορισμού του, και ως εκ τούτου η ελεύθερη ανάπτυξη της προσωπικότητάς του. Καθίσταται με αυτόν τον τρόπο ένα εν γένει πληροφοριακό αντικείμενο και προσβάλλεται η αξία του ως άνθρωπος (άρ. 2 παρ. 1 ΕλλΣ)[353].

Περαιτέρω, παραβιάζονται και άλλα δικαιώματα του θύματος εξαιτίας των συνεπειών της έμμονης διαδικτυακής παρενοχλητικής παρακολούθησης, όπως είναι, η ελευθερία έκφρασης του άρ. 14 παρ. 1 ΕλλΣ, η ελευθερία ανταπόκρισης και επικοινωνίας του άρ. 19 παρ. 1 εδ. α΄ ΕλλΣ, η ελευθερία του πληροφορείν και του

[351] Βλ. Κατσογιάννου, ό.π., σ. 1504
[352] Βλ. Κατσογιάννου, ό.π., σ. 1484-1485 και Abohassan, Alzeiby, Dhir, Kaur & Tandon, ό.π., σ. 7 και Clarke, Davies & Roden., ό.π., σ. 10-11
[353] Βλ. Κατσογιάννου, ό.π., σ. 1475

πληροφορείσθαι του άρ. 5Α παρ. 1 ΕλλΣ και η ελευθερία του «συνέρχεσθαι» του άρ. 11 ΕλλΣ[354]. Τέλος, ο περιορισμός της συμμετοχής του θύματος στα ηλεκτρονικά κοινωνικά δίκτυα και της ανάπτυξης της «ηλεκτρονικής κοινωνικότητάς» του δια του έμμεσου εξαναγκασμού του από τη συμπεριφορά του «cyberstalker», έχει ως αποτέλεσμα την παραβίαση του δικαιώματος συμμετοχής του στην ΚτΠ του άρ. 5Α παρ. 2 ΕλλΣ, ενώ οι δυσάρεστες για τη σωματική, συναισθηματική και ψυχική υγεία του θύματος επιπτώσεις του «cyberstalking» προσβάλλουν το δικαίωμα στη σωματική και ψυχική ακεραιότητα όπως ορίζει το άρ. 7 παρ. 2 ΕλλΣ[355].

10. Η συμβολή των ψηφιακών δικαιωμάτων (digital rights) στην αποτελεσματική προστασία των ατομικών δικαιωμάτων στο Διαδίκτυο

10.1. Οριοθέτηση των ψηφιακών δικαιωμάτων/δικαιωμάτων στο Διαδίκτυο (Internet rights)

Οι κίνδυνοι που ανακύπτουν για τα ατομικά δικαιώματα από την χρήση του Διαδικτύου έχουν προκαλέσει παγκόσμια ανησυχία και γι' αυτό έχουν ληφθεί πρωτοβουλίες σε υπερεθνικό επίπεδο για συνεργασία όλων των εμπλεκόμενων μερών όσον αφορά τη χάραξη πολιτικών και στρατηγικών με κύριο άξονα την κυβερνοασφάλεια. Η διακυβέρνηση του Διαδικτύου είναι μέγιστης σημασίας τόσο για τις εθνικές κυβερνήσεις, τους ιδιωτικούς φορείς και τις επιχειρήσεις, όσο και για τους υπερεθνικούς οργανισμούς και την ευρύτερη Κοινωνία των Πολιτών.

Για τον λόγο αυτόν δημιουργήθηκε ένα διεθνές δίκτυο συνεργασίας για την ενίσχυση και προάσπιση των ανθρωπίνων δικαιωμάτων στο Διαδίκτυο και την χάραξη ορθών πολιτικών διακυβέρνησής του με την ονομασία «*The Internet Right and Principles Dynamic Coalition/IRP Coalition*». Το διεθνές αυτό δίκτυο βασίζεται στο forum των ΗΕ για τη διακυβέρνηση του Διαδικτύου (The UN Internet Governance Forum/IGF) και έχει ως κύριο έργο τη δόμηση του Κυβερνοχώρου κατά τέτοιο τρόπο, ώστε οι χρήστες του κατά την περιήγησή τους να απολαμβάνουν την προστασία των ατομικών τους δικαιωμάτων[356].

---

[354] Η ελευθερία του «συνέρχεσθαι» δύναται να μεταφερθεί στο ψηφιακό περιβάλλον έχοντας τη μορφή συμμετοχής σε διαδικτυακές κοινότητες, ομάδες ή ιστότοπους που συγκεντρώνονται χρήστες και εκφράζουν απόψεις, επικοινωνούν και συζητούν για διάφορα θέματα, βλ. The Charter of Human Rights and Principles for the Internet, σ. 17 διαθέσιμο στο https://internetrightsandprinciples.org/charter/ (επίσκεψη την 18-10-2022)

[355] Βλ. Κατσογιάννου, ό.π., σ. 1476 & 1480

[356] Βλ. https://internetrightsandprinciples.org/ (επίσκεψη την 18-10-2022)

Στο πλαίσιο λειτουργίας του δικτύου διαμορφώθηκε ο *Χάρτης Ανθρωπίνων Δικαιωμάτων και Αρχών για το Διαδίκτυο* (The Charter of Human Rights and Principles for the Internet)[357], βασιζόμενος στην Οικουμενική Διακήρυξη των Ανθρώπινων Δικαιωμάτων των ΗΕ και τα υπόλοιπα Σύμφωνα και διεθνείς συμβάσεις αναφορικά με την προστασία των ατομικών δικαιωμάτων[358]. Βασικός στόχος του Χάρτη είναι αφενός μεν να αυξηθεί η ευαισθητοποίηση του κοινού σχετικά με την προστασία των ατομικών δικαιωμάτων στο ψηφιακό περιβάλλον προκειμένου αποφευχθεί η πρόκληση ηθικού πανικού (moral panic) για τους κινδύνους στο Διαδίκτυο, και αφετέρου δε να ενθαρρυνθεί η συμμετοχή και να αναβαθμιστεί η σημασία της ύπαρξης ενός συνεκτικού πλαισίου για την χάραξη στρατηγικών διακυβέρνησης στο Διαδίκτυο με γνώμονα την απόλαυση και προστασία των ατομικών (ψηφιακών πλέον) δικαιωμάτων[359].

Συνοπτικά, τα ψηφιακά δικαιώματα που απαριθμούνται στον Χάρτη αφορούν την πρόσβαση και την χρήση του Διαδικτύου, αλλά και την ηλεκτρονική διακυβέρνηση χωρίς διακρίσεις και με γνώμονα τα ανθρώπινα δικαιώματα και τις ελευθερίες έκφρασης, πληροφόρησης, (θρησκευτικής) συνείδησης και του online «συνέρχεσθαι». Ακόμη, κατοχυρώνουν το δικαίωμα στην ασφάλεια και την προστασία της ιδιωτικότητας και του απορρήτου στο Διαδίκτυο με διαφανείς διαδικασίες συλλογής, επεξεργασίας, χρήσης και διατήρησης των δεδομένων. Επίσης, περιλαμβάνουν το δικαίωμα στην ανάπτυξη και την εκπαίδευση στο Διαδίκτυο, στην εργασία και την προστασία του καταναλωτή, ενώ κατοχυρώνουν την αδιάκριτη συμμετοχή παιδιών και ατόμων με αναπηρίες στην χρήση και την προστασία από τους κινδύνους του Διαδικτύου. Τέλος, εξασφαλίζουν δικαίωμα σε έννομη προστασία σε περιπτώσεις παραβίασης των ψηφιακών δικαιωμάτων[360].

---

[357] Βλ. Introduction of The Charter of Human Rights and Principles for the Internet, σ. 1 διαθέσιμο στο https://internetrightsandprinciples.org/charter/ (επίσκεψη την 18-10-2022)

[358] Οι βασικές αρχές στις οποίες στηρίζεται ο Χάρτης είναι οι ακόλουθες: 1) Παγκοσμιότητα και ισότητα, 2) Όλοι έχουν καθήκον να σέβονται τα δικαιώματα των άλλων χρηστών του Διαδικτύου, 3) Προσβασιμότητα και ασφαλής χρήση του Διαδικτύου, 4) Ελευθερία πληροφόρησης χωρίς λογοκρισία, 5) Προστασία προσωπικών δεδομένων, ιδιωτικότητας, απορρήτου και δικαίωμα χρήσης κρυπτογραφικών μεθόδων και ανωνυμίας, 6) Σεβασμός στα δικαιώματα στη ζωή, την προσωπική ελευθερία και την ασφάλεια στο Διαδίκτυο, 7) Διαφορετικότητα – πολλαπλότητα της έκφρασης, 8) Καθολική και ανοιχτή πρόσβαση στο περιεχόμενο που διακινείται στο Διαδίκτυο, 9) Αρχιτεκτονική Διαδικτύου που να εξασφαλίζει διαλειτουργικότητα, ένταξη και ίσες ευκαιρίες για όλους και 10) Διακυβέρνηση με διαφάνεια, συμμετοχή και υπευθυνότητα, βλ. στο ίδιο, σ. 7

[359] Στο ίδιο, σ. 1

[360] Στο ίδιο, σ. 23-27

10.2. Η ενίσχυση της προστασίας των ατομικών δικαιωμάτων και της ασφάλειας των πληροφοριών στο Διαδίκτυο υπό το πρίσμα του Γενικού Κανονισμού για την Προστασία των Δεδομένων (ΓΚΠΔ)

Η αυτοματοποιημένη επεξεργασία των προσωπικών δεδομένων κατέστησε αναγκαία την ενίσχυση και την αποτελεσματική προστασία των ατομικών δικαιωμάτων στο Διαδίκτυο τόσο με την τροποποίηση της υφιστάμενης νομοθεσίας, ώστε να συμβαδίζει το δίκαιο με την τεχνολογική πρόοδο, όσο και με την αξιοποίηση τεχνολογικών μεθόδων και την ευαισθητοποίηση της Κοινωνίας των Πολιτών σχετικά με τη διαμόρφωση ενός ενιαίου ρυθμιστικού πλαισίου σε θέματα προστασίας της ιδιωτικότητας και των προσωπικών δεδομένων. Σε υπερεθνικό επίπεδο η προστασία της ιδιωτικότητας και των προσωπικών δεδομένων πηγάζει από πλήθος διατάξεων διεθνών κειμένων, που αναφέρθηκαν ήδη σε προηγούμενα κεφάλαια, και ενισχύθηκε με τη Σύσταση R (99) 5 της Επιτροπής των Υπουργών του Συμβουλίου της Ευρώπης για την προστασία της ιδιωτικότητας στο Διαδίκτυο. Σε ευρωπαϊκό επίπεδο η Σύμβαση 108 του Συμβουλίου της Ευρώπης της 28-01-1981 αποτελεί το πρώτο διεθνές και νομικά δεσμευτικά κείμενο για την προστασία των προσωπικών δεδομένων, και συνδυαστικά με τον ΧΘΔΕΕ και πλήθος Κανονισμών και Οδηγιών που έχουν εκδοθεί προς την κατεύθυνση αυτή συνδιαμορφώνουν το πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής. Τέλος, η διαμόρφωση του ενιαίου ρυθμιστικού πλαισίου προστασίας των ανωτέρω έννομων αγαθών περιλαμβάνει και την σε εθνικό επίπεδο εναρμόνιση των εσωτερικών νομοθεσιών των εννόμων τάξεων με τις διεθνείς και ευρωπαϊκές επιταγές[361].

Η ανάπτυξη πολιτικών για τον έλεγχο και τη διάδοση της πληροφορίας στο Διαδίκτυο, καθώς και η ενίσχυση των ατομικών δικαιωμάτων των πολιτών αποτελούν τους άξονες, στους οποίους βασίζονται οι στρατηγικές αντιμετώπισης της κατάχρησης των προσωπικών δεδομένων. Η αυξημένη έκταση και ένταση της συλλογής, ανταλλαγής και επεξεργασίας δεδομένων προσωπικού χαρακτήρα, και οι αυξανόμενες παραβιάσεις της ασφάλειας των προσωπικών πληροφοριών οδήγησαν στην έκδοση της Οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24-10-1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και την ελεύθερη κυκλοφορία των δεδομένων αυτών, η οποία

[361] Βλ. Ι. Ιγγλεζάκης, *Ευαίσθητα Προσωπικά Δεδομένα, Η Επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων και οι συνέπειές της,* ό.π., σ. 22

κυρώθηκε στην Ελλάδα με τον Ν. 2472/1997 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Στην συνέχεια, η εν λόγω Οδηγία αντικαταστάθηκε από τις Οδηγίες 2002/58/ΕΚ, 2006/24/ΕΚ και 2009/136/ΕΚ[362].

Ακολούθως, εκδόθηκε ο Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27-04-2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και την ελεύθερη κυκλοφορία των δεδομένων αυτών. Πρόκειται για τον νέο Γενικό Κανονισμό για την Προστασία Δεδομένων (General Data Protection Regulation/GDPR), η εφαρμογή του οποίου στην ελληνική έννομη τάξη περιλαμβάνει τη λήψη μέτρων που ορίζονται στον Ν. 4624/2019. Πιο συγκεκριμένα, στο άρ. 1 ορίζεται η αντικατάσταση του νομοθετικού πλαισίου για τη συγκρότηση και λειτουργία της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), η λήψη μέτρων για την εφαρμογή του ΓΚΠΔ και η ενσωμάτωση της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27-04-2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και την ελεύθερη κυκλοφορία των δεδομένων αυτών[363].

Ο ΓΚΠΔ έχει ως στόχο την ενδυνάμωση και επικαιροποίηση των υφιστάμενων δικαιωμάτων των υποκειμένων των δεδομένων, και ιδίως του δικαιώματος του πληροφοριακού αυτοκαθορισμού, την αναγνώριση νέων δικαιωμάτων και την αυστηροποίηση τόσο των υποχρεώσεων των υπευθύνων επεξεργασίας, όσο και των κυρώσεων σε περιπτώσεις παραβιάσεων[364]. Έτσι, με τον ΓΚΠΔ τίθεται καταρχήν ένα ενιαίο και συνεκτικό πλαίσιο για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα, η οποία είναι σύννομη εφόσον υπάρχει προηγούμενη συγκατάθεση του υποκειμένου των δεδομένων (άρ. 6 ΓΚΠΔ), ως εκδήλωση του δικαιώματος της πληροφοριακής αυτοδιάθεσης, και δεν αντίκειται στις διατάξεις του Κανονισμού. Βασικές εκφάνσεις του ανωτέρω αναφερόμενου δικαιώματος που αναγνωρίζονται και ενισχύονται στον ΓΚΠΔ είναι το δικαίωμα της ενημέρωσης του άρ. 12, της πρόσβασης του άρ. 15, της διόρθωσης του άρ. 16, της διαγραφής (δικαίωμα στη λήθη) του άρ. 17, της εναντίωσης του άρ. 21, του να μην υπόκειται το υποκείμενο σε αποφάσεις που λαμβάνονται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας

[362] Βλ. Άνθιμου, ό.π., σ. 177
[363] ό.π.
[364] Βλ. Παναγοπούλου-Κουτνατζή, ό.π., σ. 6

συμπεριλαμβανομένης και της κατάρτισης προφίλ του άρ. 22, της υποβολής καταγγελίας σε εποπτική αρχή του άρ. 77 κ.ά.[365].

Η καινοτομία του ΓΚΠΔ έγκειται στην κατοχύρωση του δικαιώματος διαγραφής ή άλλως του δικαιώματος στην ψηφιακή λήθη (droit á l' oubli numérique)[366] του άρ. 17. Λόγω του ότι διανύουμε την εποχή της απόλυτης ψηφιακής μνήμης και της εκτεταμένης συλλογής και διατήρησης για μεγάλο χρονικό διάστημα προσωπικών πληροφοριών, έχει ανακύψει η ανάγκη της ψηφιακής λήθης, να μπορεί δηλαδή το υποκείμενο να διαγράφει γεγονότα που αφορούν το παρελθόν του, αλλά και να παραλείπονται πληροφορίες που συντείνουν στην αναγνώριση της ταυτότητας του ατόμου από τρίτους (right to forget and to be forgotten) ανεξάρτητα αν τις δημοσιοποίησε το ίδιο το άτομο ή κάποιος άλλος[367].

Σύμφωνα με το άρ. 17 του ΓΚΠΔ, το υποκείμενο των δεδομένων μπορεί να ζητήσει τη διαγραφή και την μη περαιτέρω διάδοση δεδομένων που το αφορούν και τα οποία είχαν δημοσιευτεί από το ίδιο ή άλλο άτομο ένεκα ανάκλησης της συγκατάθεσής του ή άσκησης του δικαιώματος εναντίωσης, επειδή η επεξεργασία δεν είναι πλέον απαραίτητη σε σχέση με τον αρχικό σκοπό συλλογής των δεδομένων, επειδή η επεξεργασία είναι πλέον παράνομη ή διότι υπάρχει οριστική απόφαση από δικαστική αρχή ή από την ΑΠΔΠΧ περί διαγραφής τους. Μάλιστα, η παρ. 1 του άρθρου ορίζει δύο όψεις του δικαιώματος στην ψηφιακή λήθη: το δικαίωμα διαγραφής (erasure) των δεδομένων που αφορούν το υποκείμενο και τίθενται σε επεξεργασία, στο πλαίσιο του οποίου μπορεί να ζητήσει από τρίτους να διαγράψουν παραπομπές σε δεδομένα του και να μην προβαίνουν σε περαιτέρω αντιγραφή ή αναπαραγωγή τους (π.χ. αφαίρεση συνδέσμων που συνδέουν ένα πρόσωπο με συγκεκριμένα δεδομένα), και το δικαίωμα στη λήθη (right to oblivion), που παρέχει προστασία έναντι βλάβης από τη διατήρηση προσωπικών δεδομένων στο Διαδίκτυο για μεγάλο χρονικό διάστημα από την στιγμή που το υποκείμενο που αφορούν δεν είναι πια στο επίκεντρο της δημοσιότητας[368].

Το δικαίωμα στην ψηφιακή λήθη βρίσκει νομοθετικό έρεισμα[369] στο δικαίωμα στην ιδιωτικότητα και το απαραβίαστο της ιδιωτικής ζωής του άρ. 9 παρ. 1 ΕλλΣ, στο δικαίωμα προστασίας των προσωπικών δεδομένων του άρ. 9^{A} ΕλλΣ, στο άρ. 8 της

[365] Βλ. Ι. Ιγγλεζάκης, *Ευαίσθητα Προσωπικά Δεδομένα, Η Επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων και οι συνέπειές της,* ό.π., σ. 78-79
[366] ό.π.
[367] Βλ. Ιγγλεζάκης, *Το δικαίωμα στην ψηφιακή λήθη κι οι περιορισμοί του*, ό.π., σ. 1
[368] Στο ίδιο, σ. 127-131
[369] Στο ίδιο, σ. 23&93

ΕΣΔΑ, το άρ. 8 του ΧΘΔΕΕ και τα άρ. 16 και 114 της ΣΛΕΕ. Ωστόσο, δεν αποτελεί απόλυτο δικαίωμα και υπόκειται σε περιορισμούς, βάσει του άρ. 17 παρ. 3 ΓΚΠΔ, για λόγους δημοσίου συμφέροντος και για ιστορικούς, επιστημονικούς και στατιστικούς σκοπούς. Επιπλέον, υποχωρεί έναντι της ελευθερίας έκφρασης και πληροφόρησης στο Διαδίκτυο, η οποία κατοχυρώνεται ρητά στα άρ. 85, 86 και 17 παρ. 3 περ. α΄ ΓΚΠΔ, εξασφαλίζοντας έτσι τη διατήρηση της συλλογικής μνήμης και της ιστορικής αλήθειας. Επίσης, το δικαίωμα στην ψηφιακή λήθη μπορεί να περιορίσει το δικαίωμα πρόσβασης και συμμετοχής στην ΚτΠ του άρ. 5^{α} παρ. 2 ΕλλΣ[370]. Τέλος, το εν λόγω δικαίωμα δεν μεταβάλλει το καθεστώς αυτορρύθμισης των φορέων παροχής υπηρεσιών Διαδικτύου, ειδάλλως ο έλεγχός τους θα οδηγούσε σε λογοκρισία[371].

Εκτός λοιπόν από την έμφαση που δίνεται στα δικαιώματα των υποκειμένων στον ΓΚΠΔ, τα οποία δύνανται να ασκηθούν σε οποιαδήποτε περίπτωση πλην εκείνων που η επεξεργασία των δεδομένων προσωπικού χαρακτήρα προορίζεται αποκλειστικά για προσωπική ή οικιακή χρήση κατά το άρ. 2 παρ. 2 περ. γ΄ του Κανονισμού, γίνεται ταυτόχρονα προσπάθεια προώθησης και υλοποίησης μιας ολιστικής προσέγγισης για την ασφάλεια των πληροφοριών που περιλαμβάνει συμπληρωματικά μέτρα[372], όπως είναι το καθεστώς αυτορρύθμισης των ISPs, οι πολιτικές προστασίας της ιδιωτικότητας εκ σχεδιασμού και εξ ορισμού (Privacy by design and by default) και η ανάπτυξη Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας (Privacy Enhancing Technologies/ PETs)[373].

Η ανάπτυξη φιλικών προς τα ανθρώπινα δικαιώματα τεχνολογιών εντάσσεται σε μια προσπάθεια ευρύτερης προσέγγισης που αφορά τον σχεδιασμό, την λειτουργία και διαχείριση των ΤΠΕ και των πληροφοριακών συστημάτων, ώστε να

---

[370] Στο ίδιο, σ. 113

[371] Στο ίδιο, σ. 49

[372] Στο ίδιο, σ. 115

[373] Πρόκειται για ΤΠΕ που προστατεύουν την πληροφοριακή ιδιωτικότητα εξαλείφοντας ή περιορίζοντας τη μη αναγκαία επεξεργασία δεδομένων χωρίς να απομειώνεται, όμως, η λειτουργικότητα των πληροφοριακών συστημάτων, συμβάλλοντας έτσι στον έλεγχο της κοινοποίησης και μετάδοσης προσωπικών πληροφοριών. Μια κατηγοριοποίησή τους είναι σε τεχνολογίες που προσανατολίζονται προς τον χρήστη ενισχύοντας τις παρεχόμενες από το Διαδίκτυο δυνατότητες ανωνυμοποίησης και ψευδωνυμοποίησης (anonymizers)[373]. Παραδείγματα αυτών είναι τα φίλτρα μπλοκαρίσματος ανεπιθύμητης αλληλογραφίας στο ηλεκτρονικό ταχυδρομείο, οι μηχανισμοί κρυπτογράφησης (encryption mechanisms), οι διαμεσολαβητές ιδιωτικότητας (privacy proxies) κ.ά. Αν και μπορούν να συμβάλλουν θετικά στην προσπάθεια για μεγαλύτερη ασφάλεια των πληροφοριών, αντιμετωπίζονται ακόμη με επιφύλαξη λόγω μη επαρκούς ενημέρωσης και ευαισθητοποίησης των χρηστών του Διαδικτύου σχετικά με τη λειτουργία και την αποτελεσματικότητά τους, βλ. Γ. Γιαννόπουλος, Λ. Μήτρου & Γρ. Τσόλιας, Υποχρεώσεις του υπευθύνου επεξεργασίας, Στο: Λ. Κοτσαλής και Κ. Μενουδάκος (επιμ.), *Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (GDPR) – Νομική διάσταση και πρακτική εφαρμογή*, Αθήνα, Νομική Βιβλιοθήκη, 2016, σ. 180-181

ανταποκρίνονται στις απαιτήσεις που έχουν ήδη προδιατυπωθεί για την προστασία της πληροφοριακής ιδιωτικότητας. Ο προληπτικός χαρακτήρας της ολιστικής αυτής προσέγγισης περιλαμβάνει τον σχεδιασμό τεχνολογικών προδιαγραφών και τη συμμόρφωση προς αυτές όλων των εκτελούμενων από πληροφοριακά συστήματα διαδικασιών. Πρόκειται για την προστασία της ιδιωτικότητας εκ σχεδιασμού και εξ ορισμού, που περιλαμβάνει τη λήψη κατάλληλων τεχνικών και οργανωτικών μέτρων στον τομέα των τηλεπικοινωνιών, της ηλεκτρονικής διακυβέρνησης και της χρήσης των πληροφοριακών συστημάτων, ώστε να τίθενται σε επεξεργασία όσο το δυνατόν λιγότερα δεδομένα προσωπικού χαρακτήρα (data minimization) και να εξασφαλίζεται η διαφάνεια στις διαδικασίες επεξεργασίας. Η τεχνολογική αυτή διάσταση της προστασίας της ιδιωτικότητας και των προσωπικών δεδομένων επιχειρεί να εξασφαλίσει ένα επίπεδο ασφάλειας των δεδομένων σε συνάρτηση με τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση τους (π.χ. ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα) και διαπνέει τον ΓΚΠΔ (data protection by design and by default)[374].

Έτσι λοιπόν, τα τεχνικά και οργανωτικά μέτρα που μπορούν να ληφθούν εκ σχεδιασμού και εξ ορισμού δεν απαιτούν κάποια ενέργεια των υποκειμένων των δεδομένων, αφού είναι ήδη ενσωματωμένα στη διαδικασία της επεξεργασίας και συντελούν στο να μη συλλέγονται, τίθενται υπό επεξεργασία και τηρούνται πέραν του ελάχιστου δυνατού και αναγκαίου για την επεξεργασία μέτρου. Για παράδειγμα, στα μέσα κοινωνικής δικτύωσης υπάρχει η δυνατότητα ρύθμισης ώστε το προφίλ των χρηστών να μην είναι εξ ορισμού δημόσια προσβάσιμο, αλλά να γίνεται ορατό σε συγκεκριμένους αποδέκτες που ορίζει ο ίδιος ο χρήστης[375].

[374] Στο ίδιο, σ. 182
[375] Στο ίδιο, σ. 187

Επίλογος – Συμπεράσματα

Από την ανάπτυξη των κεφαλαίων της παρούσας διπλωματικής εργασίας συνάγεται το γενικότερο συμπέρασμα πως η τεχνολογική εξέλιξη που χαρακτηρίζει τον 21ο αιώνα, έχει επιφέρει μεταβολές σε όλες τις πτυχές της ανθρώπινης ζωής και δραστηριότητας όπως, επίσης, και στο έγκλημα. Οι παραδοσιακές μορφές εγκληματικότητας εξελίσσονται, ενώ ταυτόχρονα εμφανίζονται νέες μορφές εγκληματικής συμπεριφοράς, που περιλαμβάνουν την εργαλειακή αξιοποίηση των ΤΠΕ, του Η/Υ και του Διαδικτύου.

Η έμμονη διαδικτυακή παρενοχλητική παρακολούθηση, σύμφωνα με τα όσα παρατέθηκαν στα σχετικά κεφάλαια του παρόντος πονήματος, αποτελεί μια νέα μορφή εγκληματικής συμπεριφοράς, η οποία τελεί ακόμη υπό εγκληματολογική διερεύνηση. Η κατανόησή της ως κοινωνικό φαινόμενο που εμφανίστηκε εξαιτίας της ευρείας χρήσης των ΤΠΕ και του Διαδικτύου, καθώς και η αποκρυστάλλωση των χαρακτηριστικών της γνωρισμάτων αποτελούν αντικείμενα μελέτης και ενδιαφέροντος για τους ερευνητές – εγκληματολόγους, προκειμένου να εμπλουτιστεί η υπάρχουσα βιβλιογραφία για το φαινόμενο. Οι προβληματικές της απουσίας ενός καθολικά αποδεκτού ορισμού της συμπεριφοράς και της μη τυποποίησής της ως αυτοτελές ποινικό αδίκημα από το σύνολο των έννομων τάξεων αποτελούν κατευθύνσεις για μελλοντική έρευνα, ώστε να μην εκλαμβάνεται ως προέκταση της παραδοσιακής έμμονης παρενοχλητικής παρακολούθησης στο Διαδίκτυο, και ως εκ τούτου, να μην τιμωρείται με βάση τις διατάξεις που ισχύουν για το «offline stalking».

Επιπλέον, η δημιουργία ενός καθολικού προφίλ για τους δράστες και τα θύματα του «cyberstalking», όπως και η μελέτη των κινήτρων της συμπεριφοράς και των επιπτώσεων της θυματοποίησης αποτελούν άξονες για το σχεδιασμό περαιτέρω εμπειρικής διερεύνησης του φαινομένου.

Η κατανόηση του «online stalking» ως νέα μορφή εγκληματικής συμπεριφοράς αποτελεί απαραίτητη προϋπόθεση για την αντιμετώπισή του. Η ολιστική προσέγγιση του φαινομένου περιλαμβάνει την ευαισθητοποίηση, ενημέρωση και δραστηριοποίηση όλων των ενδιαφερόμενων μερών. Τα νέα δεδομένα που προκύπτουν από την εγκληματολογική έρευνα βοηθούν την πολιτεία και τις διωκτικές Αρχές να λάβουν μέτρα και να εκπονήσουν στρατηγικές για την πρόληψη και αποτελεσματική αντιμετώπιση της συμπεριφοράς όπως επίσης, και για την αρωγή αλλά και την ουσιαστικότερη προστασία των θυμάτων, δίνοντας περισσότερη έμφαση στις επιπτώσεις της θυματοποίησης.

Ακολούθως, η εκπαίδευση των διωκτικών Αρχών στη διαχείριση υποθέσεων ηλεκτρονικού εγκλήματος θα αυξήσει την εμπιστοσύνη των πολιτών στην αποτελεσματικότητά τους στους τομείς της πρόληψης και της καταστολής των νέων μορφών εγκληματικότητας, και θα ενθαρρύνει τα θύματα να καταγγείλουν τη θυματοποίησή τους στις Αρχές μειώνοντας κατ' αυτόν τον τρόπο τον σκοτεινό αριθμό των ηλεκτρονικών εγκλημάτων, άρα και του «cyberstalking». Ακόμη, αναγκαία καθίσταται στην προσπάθεια αυτή και η υπευθυνοποίηση των ιδιωτικών εταιρειών παροχής υπηρεσιών Διαδικτύου, καθώς και η συνεργασία τους με τις διωκτικές Αρχές παρέχοντας τις αιτούμενες πληροφορίες για πελάτες – συνδρομητές που εκδηλώνουν ύποπτη δραστηριότητα στο Διαδίκτυο.

Τέλος, η ενημέρωση και ευαισθητοποίηση της Κοινωνίας των Πολιτών αναφορικά με τους ελλοχεύοντες κινδύνους στο Διαδίκτυο είναι κρίσιμης σημασίας για την αντιμετώπιση του αδικήματος του «cyberstalking». Η κουλτούρα διαμοιρασμού προσωπικών δεδομένων στο Διαδίκτυο και η έμφαση που δίνεται πλέον στη σύναψη εικονικών σχέσεων ενέχουν κινδύνους για τους χρήστες του, ιδίως όσων χρησιμοποιούν εκτεταμένα τις υπηρεσίες και τα μέσα κοινωνικής δικτύωσης. Η έμμονη διαδικτυακή παρενοχλητική παρακολούθηση συνιστά παρέμβαση στον ιδιωτικό βίο του θύματος μέσω της άντλησης προσωπικών πληροφοριών, που το ίδιο το θύμα έχει δημοσιοποιήσει σε ένα ευρύ ή μη κοινό. Ο έλεγχος και ο περιορισμός της αυτοδιάθεσης προσωπικών δεδομένων στο πλαίσιο της «ηλεκτρονικής κοινωνικότητας», αλλά και η λήψη τεχνικών μέτρων αυτοπροστασίας, ιδίως της προσωπικότητας και της ιδιωτικότητάς τους, αποτελεί ατομική ευθύνη των χρηστών του Διαδικτύου. Η ενίσχυση, τέλος, του δικαιώματος του πληροφοριακού αυτοκαθορισμού μέσω νομοθετικών ρυθμίσεων και η ουσιαστική του άσκηση από τη σύγχρονη γενιά των «Digital Natives» μπορεί να συμβάλλει στη δραστική μείωση της ψηφιακής θυματοποίησης, ώστε το ψηφιακό περιβάλλον να καταστεί ένας ασφαλής χώρος δραστηριοποίησης των χρηστών του Διαδικτύου, στον οποίο θα απολαμβάνουν απόλυτης προστασίας τα ατομικά τους δικαιώματα.

Πηγές - Βιβλιογραφία

Πηγές

Α΄ Νόμοι

Διεθνές νομικό πλαίσιο

- Διεθνές Σύμφωνο για τα Ατομικά και Πολιτικά Δικαιώματα (ΔΣΑΠΔ) : άρ. 17, 19
- Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου : άρ. 12, 19

Ενωσιακό νομικό πλαίσιο

- Γενικός Κανονισμός για την Προστασία των Δεδομένων (ΓΚΠΔ) : άρ. 2, 6, 12, 15, 16, 17, 21, 22, 77, 85, 86
- Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ) : άρ. 8, 10
- Χάρτης Θεμελιωδών Δικαιωμάτων Ευρωπαϊκής Ένωσης (ΧΘΔΕΕ) : άρ. 7, 8, 9

Ημεδαπό νομικό πλαίσιο

- Ελληνικό Σύνταγμα (ΕλλΣ) : άρ. 2 παρ. 1, 5 παρ. 1, 3&4, 5^{A} παρ. 1&2, 9 παρ. 1&2, 9^{A}, 11, 14 παρ. 1, 19, 25 παρ. 1 εδ. γ΄
- Νόμος 4619/2019 ΦΕΚ 95/Α/11-06-2019 «*Κύρωση του Ποινικού Κώδικα*» : άρ. 333 παρ. 1 εδ. β΄, 292Β, 370, 370Α
- Νόμος 4624/2019 Τεύχος Α΄ 137/29-08-2019 «*Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις*» : άρ. 1

Β΄ Ιστοσελίδες

https://cyberalert.gr/cybercrime/ (επίσκεψη την 09-08-2022)

https://cyberalert.gr/spamming/ (επίσκεψη την 12-08-2022)

https://el.wikipedia.org/wiki/Web_2.0 (επίσκεψη την 23-12-2022)

https://en.wikipedia.org/wiki/Hacktivism (επίσκεψη την 26-01-2023)

https://en.wikipedia.org/wiki/Instant_messaging (επίσκεψη την 26-01-2023)

https://www.beds.ac.uk/nccr/ (επίσκεψη την 24-08-2022)

https://www.cyberangels.org/cyber-security/ (επίσκεψη την 11-08-2022)

https://www.haltabuse.org/ (επίσκεψη την 24-08-2022)

https://internetrightsandprinciples.org/ (επίσκεψη την 18-10-2022)

Βιβλιογραφία

Ελληνόγλωσση

Ακριβοπούλου, Χ. (2011). Η ιδιωτικότητα του προσώπου μέσα από τη συνθετική αντίθεση δημόσιου-ιδιωτικού. *Επιστήμη και Κοινωνία – Επιθεώρηση Πολιτικής και Ηθικής Θεωρίας*. Τεύχος 26. (σ. 1-25). Αθήνα: εκδ. Αντ. Ν. Σάκκουλα

Ακριβοπούλου, Χ. (2012). *Το δικαίωμα στην ιδιωτική ζωή – Από τη γένεση στη σύγχρονη διαμόρφωση και προστασία του*. Αθήνα: εκδ. Σάκκουλα

Άνθιμου, Κ. (1998). Το δικαίωμα του πληροφοριακού αυτοκαθορισμού του ατόμου ως έκφανση του δικαιώματος της προσωπικότητας. *Κριτική Επιθεώρηση νομικής θεωρίας και πράξης*. Τεύχος 1. (σ. 155-179). Αθήνα: εκδ. Αντ. Ν. Σάκκουλα

Βιδάλης, Τ., Μήτρου, Λ. και Τάκης, Α. (2006). Συνταγματική πρόσληψη των τεχνολογικών εξελίξεων και «νέα» δικαιώματα. Στο: Ξ. Ι. Κοντιάδης (επιμ.), *Πέντε χρόνια μετά τη συνταγματική αναθεώρηση του 2001*. Πρόλογοι: Άννα Μπενάκη-Ψαρούδα & Δημήτρης Τσάτσος. Επίμετρο: Ευάγγελος Βενιζέλος & Ιωάννης Βαρβιτσιώτης. Τόμος Πρώτος. (σ. 273-312). Αθήνα: εκδ. Αντ. Ν. Σάκκουλα

Βλαχόπουλος, Σ. και Χρυσόγονος, Κ. (2017). *Ατομικά και Κοινωνικά Δικαιώματα,* 4η αναθεωρημένη έκδοση. Αθήνα: Νομική Βιβλιοθήκη

Γερμάνος, Γ. & Παπαθανασίου, Α. (2016). Εξέλιξη και ανάπτυξη νέων μορφών ψηφιακής εγκληματικότητας στον Κυβερνοχώρο σε εποχές κρίσης. Στο Μ. Γασπαρινάτου (επιμ.), *Έγκλημα και Ποινική Καταστολή σε Εποχή Κρίσης*, Τιμ. Τόμος Ν. Κουράκη. (σ. 1305-1319). Αθήνα: εκδ. Σάκκουλα

Γέροντας, Α. (1997). Το δικαίωμα της αυτοδιάθεσης των πληροφοριών – Υπερβολή ή αναγκαιότητα;. *Το Σύνταγμα.* Τεύχος 4. (σ. 849-867). Αθήνα: εκδ. Αντ. Ν. Σάκκουλα

Γέροντας, Α (2006). Η αρχή της αναλογικότητας και η τριτενέργεια των θεμελιωδών δικαιωμάτων μετά την αναθεώρηση του 2001. Στο Ξ. Ι. Κοντιάδης (επιμ.), *Πέντε Χρόνια Μετά τη Συνταγματική Αναθεώρηση του 2001*. Πρόλογοι: Άννα Μπενάκη-Ψαρούδα & Δημήτρης Θ. Τσάτσος. Επίμετρο: Ευάγγελος Βενιζέλος & Ιωάννης Βαρβιτσιώτης. (σ. 313-523). Αθήνα: εκδ. Αντ. Ν. Σάκκουλα

Γιαννόπουλος, Γ., Μήτρου, Λ. & Τσόλιας, Γρ. (2016). Υποχρεώσεις του υπευθύνου επεξεργασίας. Στο: Λ. Κοτσαλής και Κ. Μενουδάκος (επιμ.), *Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (GDPR) – Νομική διάσταση και πρακτική εφαρμογή*. (σ. 167-231). Αθήνα: Νομική Βιβλιοθήκη

Δαγτόγλου, Π. (2005). *Συνταγματικό Δίκαιο - Ατομικά Δικαιώματα*. Τόμος Α΄. Δεύτερη Αναθεωρημένη Έκδοση. Αθήνα: εκδ. Αντ. Ν. Σάκκουλα

Ιγγλεζάκης, Ι. (2004). *Ευαίσθητα Προσωπικά Δεδομένα - Η Επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων και οι συνέπειές της*. Πρόλογος: Ν. Ιντζεσίλογλου. Ανατύπωση 2004 με προσθήκες των Νόμων 3090/2002, 3144/2003 και 3156/2003. Αθήνα: εκδ. Σάκκουλα

Ιγγλεζάκης, Ι. (2014). *Το δικαίωμα στην ψηφιακή λήθη και οι περιορισμοί του*. Πρόλογος: Λ. Μήτρου. Αθήνα: εκδ. Σάκκουλα

Καρύδα, Μ. και Κοκολάκης, Σπ. (2013). Ψηφιακά κοινωνικά δίκτυα: Ζητήματα ιδιωτικότητας και η τεχνολογική αντιμετώπισή τους. Στο: Μ. Καρύδα, Σπ. Κοκολάκης, Λ. Μήτρου, Μ. Πισκοπάνη & Σπ. Τάσσης (επιμ.). *facebook, blogs και δικαιώματα*. (σ.117-140). Αθήνα: εκδ. Σάκκουλα

Καστανάς, Η (2004). Το Internet και η προστασία της ιδιωτικής ζωής και της ελευθερίας έκφρασης: σε αναζήτηση έξυπνων ρυθμίσεων. Στο: Χ. Σαββάκης, Π. Δόνος, Ηλ. Καστανάς, Δ. Χριστόπουλος, Κ. Τσιτσελίκης, Αν. Τάκης, Β. Βουτσάκης, Ευ. Μάλλιος, Φ. Βασιλόγιαννης, Τ. Βιδάλης, Γ. Κτιστάκις (επιμ.). *Νέες τεχνολογίες και συνταγματικά δικαιώματα*. Πρόλογος: Ν. Αλιβιζάτος. Δίκαιο & Κοινωνία στον 21ο αιώνα. (σ. 29-56). Αθήνα: εκδ. Σάκκουλα

Κατσογιάννου, Μ. (2016). Η δυστοπική πραγματικότητα της κρίσης ως θρυαλλίδα έκπτυξης αντικοινωνικής συμπεριφοράς και ανάδυσης αθέατης θυματοποίησης: Η περίπτωση της «έμμονης διαδικτυακής παρενοχλητικής παρακολούθησης» (“Cyberstalking”). Στο Μ. Γασπαρινάτου (επιμ.), *Έγκλημα και Ποινική Καταστολή σε Εποχή Κρίσης*, Τιμ. Τόμος Ν. Κουράκη, (σ. 1422-1521). Αθήνα: εκδ. Σάκκουλα

Κοϊμτζόγλου, Ι. (2005). *Στοιχεία Δημοσίου Δικαίου*. Συνταγματικό και Διοικητικό Δίκαιο σε συνδυασμό με Διεθνές και Κοινοτικό Δίκαιο. Πρόλογος Καθηγητή Α. Ι. Τάχου. Γ΄ Έκδοση. Αθήνα: εκδ. Σάκκουλα

Λάζος, Γρ. (2001). *ΠΛΗΡΟΦΟΡΙΚΗ & ΕΓΚΛΗΜΑ*. Αθήνα: Νομική Βιβλιοθήκη

Μήτρου, Λ. (2013). Μια σύντομη εισαγωγή. Στο: Μ. Καρύδα. Σπ. Κοκολάκης. Λ. Μήτρου. Μ. Πισκοπάνη & Σπ. Τάσσης (επιμ.), *facebook, blogs και δικαιώματα*. (σ. 9-18). Αθήνα: εκδ. Σάκκουλα

Παναγοπούλου-Κουτνατζή, Φ. (2012). Κοινωνικά Δίκτυα και Προσωπικότητα-Ι. *Δίκαιο Μέσων Ενημέρωσης και Επικοινωνίας (ΔιΜΕΕ)*. Τεύχος 2. (σ. 186-195). Αθήνα: Νομική Βιβλιοθήκη

Παναγοπούλου-Κουτνατζή, Φ. (2016). Το νέο πλαίσιο των ανανεωμένων δικαιωμάτων. Στο: Λ. Κοτσαλής και Κ. Μενουδάκος (επιμ.), *Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (GDPR) – Νομική διάσταση και πρακτική εφαρμογή*. (σ. 1-38). Αθήνα: Νομική Βιβλιοθήκη

Πισκοπάνη, Α. Μ. (2013). Η ελευθερία της έκφρασης στο «ιδιωτικοποιημένο» δημόσιο δίκτυο του Facebook. Στο: Μ. Καρύδα, Σπ. Κοκολάκης, Λ. Μήτρου, Μ. Πισκοπάνη & Σπ. Τάσσης (επιμ.). *facebook, blogs και δικαιώματα*, (σ. 19-70). Αθήνα: εκδ. Σάκκουλα

Σπυριδάκης, Ι. Μ. (2011). *Ατομικά και Κοινωνικά Δικαιώματα*. Επιτομή. Μ. Ι. Σπυριδάκης (επιμ.). Αθήνα: εκδ. Αντ. Ν. Σάκκουλα

Τάσσης, Σπ. (2013). Ό,τι πεις θα χρησιμοποιηθεί εναντίον σου; Η χρήση ψηφιακών δικτύων κοινωνικής δικτύωσης και ιστολογίων. Στο: Μ. Καρύδα, Σπ. Κοκολάκης, Λ. Μήτρου, Μ. Πισκοπάνη & Σπ. Τάσσης (επιμ.). *facebook, blogs και δικαιώματα*. (σ. 71-116). Αθήνα: εκδ. Σάκκουλα

Φαρσεδάκης, Ι. (2005). Στοιχεία Εγκληματολογίας. Αθήνα: Νομική Βιβλιοθήκη

Furnell, St. (2006). *ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ: Καταστρέφοντας την κοινωνία της πληροφορίας* (επιμ. Χρ. Ε. Τσουραμάνης μτφρ Φωτ. Α. Μηλιώνη). Αθήνα: εκδ. Παπαζήση

Ξενόγλωσση

Abohassan, A., Alzeiby, E., Dhir, A., Kaur, P. & Tandon, A. (2021). A Systematic literature review on cyberstalking. An analysis of past achievements and future promises. *Technological Forecasting & Social Change. 163.* σ. 1-15. doi: https://doi.org/10.1016/j.techfore.2020.120426

Akdeniz, Y. & Ellison, L. (1998). Cyber-stalking: the Regulation of Harassment on the Internet. *Criminal Law Review. December Special Edition: Crime, Criminal Justice, and the Internet*. σ. 29-48. Ανακτήθηκε από:

https://www.academia.edu/943428/Cyber_stalking_the_Regulation_of_Harassment_on_the_Internet

Al Mutawa, N., Bryce, J., Franqueira, N. L. V. & Marrington, A. (2016). Forensic investigation of cyberstalking cases using Behavioural Evidence Analysis. *Digital Investigation*. 16. σ. 96-103. doi: https://doi.org/10.1016/j.diin.2016.01.012

Bocij, P. (2002). Corporate Cyberstalking: An Invitation to Build Theory. *First Monday* (Peer-Reviewed Journal on the Internet). Vol. 7. No. 11. σ. 1-8. Ανακτήθηκε από: https://firstmonday.org/

Bocij, P. (2003). Victims of Cyberstalking: An Explanatory Study of Harassment Perpetrated via the Internet. *First Monday* (Peer-Reviewed Journal on the Internet). Vol. 8. Number 10. σ. 1-12. Ανακτήθηκε από: https://firstmonday.org/ojs/index.php/fm/article/view/1086/1006

Bocij, P. (2004). Chapter 1: What Is Cyberstalking?. Στο P. Bocij (επιμ.), *Cyberstalking: Harassment in the Internet Age and How to Protect Your Family*. (σ. 1-18). Westport, Connecticut London: Praeger Publishers. Διαθέσιμο στο: https://books.google.gr/books?id=q8NZLBE0sm0C&printsec=frontcover&hl=el#v=onepage&q&f

Bocij, P. (2004). Chapter 2: Stalking or Cyberstalking?. Στο P. Bocij (επιμ.), *Cyberstalking: Harassment in the Internet Age and How to Protect Your Family*. (σ. 19-30). Westport, Connecticut London: Praeger Publishers. Διαθέσιμο στο: https://books.google.gr/books?id=q8NZLBE0sm0C&printsec=frontcover&hl=el#v=onepage&q&f

Bocij, P. (2018). OVIAR: Towards a Model for Cyberstalking Intervention and Reduction. *International Journal of Emerging Trends in Social Sciences*. 4. 2. σ. 58-66. Ανακτήθηκε από: https://www.researchgate.net/publication/329165349_OVIAR_Towards_a_Model_for_Cyberstalking_Intervention_and_Reduction

Bocij, P. & McFarlane, L. (2002). Online harassment: towards a definition of cyberstalking. *Prison Service Journal*. Issue 139. σ. 31-38. Ανακτήθηκε από: https://www.researchgate.net/publication/284807346_Online_harassment_Towards_a_definition_of_cyberstalking

Bocij, P. & McFarlane, L. (2003). An Exploration of Predatory Behaviour in Cyberspace: Towards a Typology of Cyberstalkers. *First Monday (Peer-Reviewed Journal on the Internet*. Vol. 8. Number 9. σ. 1-10. Ανακτήθηκε από: https://www.researchgate.net/publication/220167750_An_exploration_of_predatory_behaviour_in_cyberspace_Towards_a_typology_of_cyberstalkers

Brown, C. (2015). Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice. *International Journal of Cyber Criminology*. 9. 1 σ. 55-119. Ανακτήθηκε από: https://www.researchgate.net/publication/282161204_Investigating_and_Prosecuting_Cyber_Crime_Forensic_Dependencies_and_Barriers_to_Justice

Challa, C., Dhillon, G. και Smith, K. (2016). Defining Objectives for Preventing Cyberstalking. *International Federation for Information Processing*. σ. 76-87. Ανακτήθηκε από: https://link.springer.com/article/10.1007%2Fs10551-017-3697-x

Clarke, J., Davies, E. & Roden, A-L. (2016). Self-Reports of Adverse Health Effects Associated with Cyberstalking and Cyberharassment: A Thematic Analysis of Victims' Lived Experiences. *Faculty Articles & Research.* 1. σ. 1-37. Ανακτήθηκε από: https://dc.swosu.edu/cas_act_articles/

Clarke, R. & Felson, M. (1998). Opportunity Makes The Thief – Practical theory for crime prevention. *Police Research Series.* Paper 98. Policing and Reducing Crime Unit and Research. Development and Statistics Directorate of the Home Office. σ. 1-36. Ανακτήθηκε από: https://popcenter.asu.edu/sites/default/files/opportunity_makes_the_thief.pdf

Dickinson, J. (2006). The phenomenon of cyberstalking on the RIT campus: Definitions, behaviors, and normalization. *Thesis.* Rochester Institute of Technology. σ. 1-67. Ανακτήθηκε από: https://scholarworks.rit.edu/theses/index.49.html

Fisher, B. & Henson, B. (2011). Being Pursued Online: Applying Cyberlifestyle - Routine Activities Theory to Cyberstalking Victimization. *Criminal Justice and Behavior*. Vol. 38. No. 11. σ. 1149-1169. doi: http://dx.doi.org/10.1177/0093854811421448

Fisher, B. S., Fox, K. A., Nobles, M. R. και Reyns, B.W. (2014). Protection Against Pursuit: A Conceptual and Empirical Comparison of Cyberstalking and Stalking

Victimization Among a National Sample. *Justice Quarterly*. Vol. 31. No. 6 σ. 986-1014. doi: http://dx.doi.org/10.1080/07418825.2012.723030

Goodno, N. (2007). Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws. *Federal Laws*. Vol. 72. Issue 1. σ. 125-197. Ανακτήθηκε από: https://scholarship.law.missouri.edu/mlr/vol72/iss1/7/

Higgins, G., Marcum, C., Navarro, J. & Ricketts, M. (2016). Addicted to the Thrill of the Virtual Hunt: Examining the Effects of Internet Addiction on the Cyberstalking Behaviors of Juveniles. *Deviant Behavior*. 37. 8. σ. 1-11. doi: https://psycnet.apa.org/doi/10.1080/01639625.2016.1153366

Koops, B-J, Newell, B. & Skorvanek, I. (2019). Location Tracking by Police: The Regulation of 'Tireless and Absolute Surveillance. *UC Irvine Law Review*, 9, 3, σ. 635-697. Ανακτήθηκε από: https://www.researchgate.net/publication/323811993_Location_Tracking_by_Police_The_Regulation_of_'Tireless_and_Absolute_Surveillance'

Mansourabadi, A. και Salimi, E. (2014). The Criminology of Cyber stalking: Investigating the Crime, Offenders and Victims of Cyber Stalking. *International Journal of Criminology and Sociological Theory*. Vol. 7. No. 2. σ. 1-9. Ανακτήθηκε από: https://ijcst.journals.yorku.ca/index.php/ijcst/issue/view/2266

McEwan, T., Mullen, P. E. και Purcell, R. (2007). Identifying risk factors in stalking: A review of current research. *International Journal of Law and Psychiatry*. 30. 1. σ. 1-9. doi: http://dx.doi.org/10.1016/j.ijlp.2006.03.005

Nuth, S. M. (2008). Crime and technology - Challenges or solutions? Taking advantage of new technologies: For and against crime. *Computer Law & Security Report*. 24. σ. 437-446. doi: https://doi.org/10.1016/j.clsr.2008.07.003

Ogilvie, E. (2000). Cyberstalking. *Trends and Issues in Crime and Criminal Justice*. Australian Institute of Criminology. No. 166. σ. 1-6. Ανακτήθηκε από: https://www.aic.gov.au/publications/tandi/tandi166

Pittaro, M. (2007). Cyber stalking: An Analysis of Online Harassment and Intimidation. *International Journal of Cyber Criminology (IJCC)*. Vol. 1. Issue 2. σ. 180-197 Ανακτήθηκε από: https://www.researchgate.net/publication/241843583_Cyber_stalking_An_Analysis_of_Online_Harassment_and_Intimidation

Roberts, L. (2008). Jurisdictional and definitional concerns with computer-mediated interpersonal crimes: Analysis on Cyber Stalking. *International Journal of Cyber Criminology*. Vol. 2. Issue. σ. 271-285, Ανακτήθηκε από: https://www.researchgate.net/publication/242074185_Jurisdictional_and_Definitional_Concerns_with_Computermediated_Interpersonal_Crimes_An_Analysis_on_Cyber_Stalking

Rosenfeld, B. (2003). Recidivism in stalking and obsessional harassment. *Law and Human Behavior*. Vol. 27. No. 3. σ. 251-265. doi: https://doi.org/10.1023/a:1023479706822

Ross, E. (1995). E-Mail Stalking: Is Adequate Legal Protection Available?. *J. Marshall Journal of Computer & Information Law 405*. Vol. 13. Issue 3 σ. 405-432. Ανακτήθηκε από: "E-Mail Stalking: Is Adequate Legal Protection Available?, 13 J. Marsha" by Eileen S. Ross (uic.edu)

Spence-Diehl, E. (2003). Stalking and Technology: The Double-Edged Sword. *Journal of Technology in Human Services*. Vol. 22. Issue 1. σ. 5-18. Ανακτήθηκε από: https://www.researchgate.net/publication/254377993_Stalking_and_Technology_The_Double-Edged_Sword