ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ
University of the Peloponnese

ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΜΣ ΣΤΗΝ ΕΠΙΣΤΗΜΗ ΥΠΟΛΟΓΙΣΤΩΝ

Διπλωματική Εργασία

Ψηφιακή Εγκληματολογία

Συγγραφέας: ΑΝΔΡΙΚΟΠΟΥΛΟΣ ΒΑΣΙΛΕΙΟΣ

ΑΜ: 2022202202001

Επιβλέπων: Βασιλάκης Κωνσταντίνος

Συνεπιβλέπων: Μάργαρης Διονύσιος

ΦΕΒΡΟΥΑΡΙΟΣ 2026

ΕΥΧΑΡΙΣΤΙΕΣ

Το λιγότερο που μπορώ να εκφράσω είναι τις ειλικρινείς μου ευχαριστίες σε όσους συνέβαλαν στην ολοκλήρωση αυτής της διπλωματικής εργασίας. Αρχικά θέλω να ευχαριστώ θερμά τον επιβλέποντα καθηγητή μου, κ. ΒΑΣΙΛΑΚΗ Κωνσταντίνο για την καθοδήγηση, υποστήριξη και την πολύτιμη βοήθεια του κατά την διάρκεια της εκπόνησης της εργασίας αυτής. Οι επισημάνσεις και η βοήθεια του ήταν καθοριστικοί παράγοντες για την επιτυχία αυτής της προσπάθειας. Επιπρόσθετα θέλω να ευχαριστήσω την οικογένειά μου για την αμέριστη υποστήριξη που μου παρείχαν καθ' όλη την διάρκεια της εκπόνησης της.

«Τα πράγματα είναι απλούστερα από ότι νομίζουμε, αλλά ταυτόχρονα πιο πολύπλοκα από ότι μπορούμε να φανταστούμε»

Johann Wolfgang von Goethe[1]

[1] Γερμανός συγγραφέας, φιλόσοφος, ζωγράφος, παιδαγωγός, αλλά και θετικός επιστήμονας, ποιητής, λόγιος, νομικός και πολιτικός. Γεννήθηκε 28 Αυγούστου 1749 στη Φρανκφούρτη και πέθανε στις 22 Μαρτίου 1832. Σπούδασε Νομική στη Λειψία το 1765, όπου ήλθε σε επαφή με το ελληνικό στοιχείο της πόλης. Ως φίλος τον Ελλήνων και της Ελλάδος αφιέρωσε πολλά έργα του στην Ελληνική Αρχαιότητα. Ο Γιόχαν Βόλφγκανγκ Φον Γκαίτε θεωρείται ο πιο ολοκληρωμένος δημιουργός. Το έργο του περιλαμβάνει πληθώρα τραγουδιών, ποιημάτων, αφηγημάτων, θεατρικών έργων, μυθιστορημάτων, επιστολών αλλά και πραγματειών με επιστημονικό χαρακτήρα. Εξέφρασε με εμβληματικό τρόπο το ευρωπαϊκό πνεύμα και -στο πλαίσιο του ευρωπαϊκού αλλά και του παγκόσμιου πολιτισμού- συνιστά μία οικουμενική φυσιογνωμία. Τα ενδιαφέροντά του εκτείνονται πέραν των διαφόρων μορφών ποίησης (δραματικής, επικής και λυρικής) και καλύπτουν και τον χώρο των φυσικών επιστημών, στον οποίο δραστηριοποιήθηκε και δημοσίευσε και σχετικές εργασίες. Το έργο του Γκαίτε είναι πολυδιάστατο, με υψηλή ποιότητα και αξιοσημείωτο όγκο, και επιχειρηματολογείται ότι είναι ίσως η τελευταία παρουσία στην Ευρωπαϊκή διανόηση με τόσο πληθωρική και πολυσχιδή πνευματική παρουσία και παραγωγή, χαρακτηριστικά που τον τοποθετούν δίπλα στους εμβληματικούς καλλιτέχνες και διανοούμενους της Αναγέννησης.

Περιεχόμενα

Περίληψη

Η παρούσα εργασία επικεντρώνεται στη μελέτη της ψηφιακής εγκληματολογίας, κυρίως σε μια θεωρητική προσέγγιση, παραθέτοντας μία επισκόπηση του τομέα αυτού της εγκληματολογίας, ο οποίος, αν και σχετικά πρόσφατος, εξελίσσεται, διευρύνεται και αναπτύσσεται, ενώ εκτιμάται ότι στο μέλλον θα κυριαρχήσει στην επιστήμη της Εγκληματολογίας τόσο σε θεωρητικό και ακαδημαϊκό επίπεδο, όσο και στα επίπεδα της έρευνας και του πεδίου, όπου ήδη οι ανακριτικοί υπάλληλοι κάθε κλάδου χρησιμοποιούν τις εφαρμογές της ψηφιακής εγκληματολογίας.

Η παρούσα εργασία ξεκινάει με μια ιστορική αναδρομή της Εγκληματολογίας και την εξέλιξη του εγκλήματος παρουσιάζοντας ως ένα "ζωντανό" οργανισμό που διευρύνεται. Στη συνέχεια δίνονται οι ορισμοί του Ψηφιακού Εγκλήματος και της Ψηφιακής Εγκληματολογίας, καθώς επίσης μια θεωρητική ανάλυση των διαδικασιών στην Εγκληματολογική έρευνα. Εν συνεχεία καταγράφονται οι αναμενόμενες εξελίξεις που αφορούν το μέλλον της Ψηφιακής Εγκληματολογίας με την είσοδο της Τεχνητής Νοημοσύνης στις διαδικασίες διερεύνησης των εγκλημάτων. Τέλος επισκοπείται το νομικό πλαίσιο εφαρμογής των διαδικασιών της Ψηφιακής Εγκληματολογίας στο Ελληνικό Ποινικό Σύστημα, καθώς επίσης η θέση της Ελληνικής Αστυνομίας και οι δυνατότητες αυτής.

Abstract

This thesis focuses on the study of digital criminology, following mainly a theoretical approach, surveying the particular field of criminology which -despite being relatively recent- is rapidly evolving, expanding and developing, while it is estimated that in the future it will dominate the science of Criminology, both at a theoretical and academic level, as well as at research level and the field level in which its applications are already used by investigative officers of every branch/specialty.

This thesis begins with a historical review of Criminology and the evolution of crime, presenting it as a "living" organization that is evolving. The definitions of Digital Crime and Digital Criminology are subsequently given, along with a theoretical analysis of the processes in Criminological investigation. Afterwards, the expected developments in the domain of Digital Criminology are listed, especially with a focus on the exploitation of Artificial Intelligence in the investigation processes of crimes. Finally, the legal framework for the implementation of Digital Forensics procedures in the Greek Criminal System is overviewed, as well as the position of the Greek Police and its capabilities.

1 ΕΙΣΑΓΩΓΗ - ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ – ΟΡΙΣΜΟΣ

Αν και σε πραγματολογικό επίπεδο, τόσο το έγκλημα όσο και η συγκροτημένη θεσμική αντιμετώπισή του έχουν ως χρονική αφετηρία τα χρόνια της αρχαιότητας, πολλοί μελετητές θέτουν ως αφετηρία της μελέτης τους την εποχή του Διαφωτισμού. Αυτό εδράζεται στη σκέψη ότι στη συγκεκριμένη περίοδο μεταβλήθηκε ριζικά η θεώρηση και η νοηματοδότηση των βασικών όρων «κοινωνία» και «κράτος», όπως και της αντίληψης για την οικονομία και την οικονομική δραστηριότητα, καθώς και των σχέσεων μεταξύ των ανωτέρω όρων. Τα κύρια χαρακτηριστικά που αποδόθηκαν στα προαναφερθέντα στοιχεία κατά την περίοδο του διαφωτισμού, διατηρούνται σε σημαντικό βαθμό έως και σήμερα.

Μέχρι το σημείο εκείνο, η ποινική πολιτική διεπόταν από τις αρχές του Κλασικισμού, με βάση τις οποίες η εγκληματικότητα συνδεόταν άρρηκτα με την ελεύθερη βούληση του ατόμου. Η θεώρηση αυτή ωστόσο μεταβλήθηκε, και η εγκληματικότητα αντιμετωπίζεται εφεξής ως συνέπεια συγκεκριμένων αιτίων, τα οποία δεν συνδέονται με την ελεύθερη βούληση του ατόμου. Περαιτέρω, από τα μέσα του 19ου αιώνα κέρδιζε έδαφος η αντίληψη ότι η κατάλληλη οργάνωση της λειτουργίας του κράτους είναι δυνατόν να συμβάλλει στην πρόληψη της εγκληματικότητας. Σε ένα ευρύτερο επίπεδο, οι μελετητές διατύπωσαν τη σκέψη ότι όπως οι φυσικοί νόμοι επηρεάζουν την ανάπτυξη των ζώων και των φυτών, έτσι και οι νόμοι ασκούν επίδραση στις ανθρώπινες κοινωνίες και τις ατομικές συμπεριφορές[2].

Σημαντικό ρόλο στην προσέγγιση των μελετητών έχει ο τρόπος λειτουργίας του συστήματος του τυπικού κοινωνικού ελέγχου, όπως αυτό δομείται από τους θεσμούς (α) της αστυνομίας που αντιστοιχεί στην πρόληψη, καταστολή και έρευνα στο πεδίο, (β) της δικαιοσύνης, που αντιστοιχεί στην συστηματική κρίση και αξιολόγηση των πράξεων με βάση το νομικό πλαίσιο και την επιμέτρηση των τυχόν ποινών και (γ) του σωφρονισμού, που αποσκοπεί στη βελτίωση της συμπεριφοράς των ατόμων που έχουν εμπλακεί σε αδικοπραξίες, μέσω κατάλληλων μέτρων. Έτσι, το σύστημα του τυπικού κοινωνικού ελέγχου κρίνεται ότι αποτελεί αντίμετρο στην εξάπλωση του εγκλήματος, και η συστηματική και κατάλληλη ανάπτυξή του θα ενδυναμώσει την εφαρμογή του νόμου και θα οδηγήσει αντίστοιχα στην υποχώρηση του εγκλήματος.

Θα πρέπει να σημειωθεί εδώ ότι ο όρος «εγκληματικότητα» στην πράξη προσεγγίζεται ως ένα στατιστικό μέγεθος και υπολογίζεται βάσει του συνόλου των καταγεγραμμένων εγκλημάτων που λαμβάνουν χώρα σε μία προσδιορισμένη περιοχή και μέσα σε ένα καθορισμένο χρονικό διάστημα. Οι πρώτες μετρήσεις της εγκληματικότητας υπό τη στατιστική αυτή προσέγγιση εντοπίζονται χρονικά στον 19ο αιώνα και έχουν ισχυρή συσχέτιση με την εισαγωγή και διαμόρφωση της έννοιας του μέσου συνετού ανθρώπου[3].

Η Σχολή του Σικάγου, όπως ευρέως είναι γνωστή είναι η πρώτη ομάδα Κοινωνιολόγων του ομώνυμου Πανεπιστημίου που ξεκίνησε έρευνες αναφορικά με την παραβατική συμπεριφορά και το έγκλημα, είναι μια από τις σημαντικότερες συλλογικές διανοητικές εκφράσεις της κοινωνιολογίας με σημαντική συμβολή στην εγκληματολογία. Στο περιβάλλον

[2] Σοφία ΒΙΔΑΛΗ *ΕΓΚΛΗΜΑ ΚΑΙ ΚΟΙΝΩΝΙΑ.* ΑΘΗΝΑ 2019 ΚΕΦ 3

[3] Σοφία ΒΙΔΑΛΗ ΕΓΚΛΗΜΑ ΚΑΙ ΚΟΙΝΩΝΙΑ. ΑΘΗΝΑ, 2019 ΚΕΦ 3

της ομώνυμης πόλης με τα έντονα κοινωνικά προβλήματα έθεσε τις βάσεις για έναν ιδιαίτερα παραγωγικό ερευνητικό πυρήνα, ο οποίος από τα πρώτα χρόνια του εικοστού αιώνα έως και τη σημερινή εποχή, παραμένει πηγή δημιουργίας και στοχασμού. Κύριοι εκφραστές της είναι οι Mead, Park, Veblen, Thomas, Blumer, Hughes και πιο πρόσφατα οι Goffman και Becker. Οι μελέτες που συνέγραψαν με μεθοδολογική αρτιότητα και στοχευμένη κοινωνική ευαισθησία για την παραβατικότητα, έθεσαν τα θεμέλια και τις κατευθύνσεις για τον ανθρωπιστικό προσανατολισμό στον συγκεκριμένο τομέα μελέτης για όλο τον κόσμο.

Ενδεικτικά ο Robert Park ήταν ο βασικός εκφραστής των ερευνών της Σχολής, ο οποίος στο πρακτικό και πρωτοπόρο για την εποχή του τρόπο διδασκαλίας και έρευνας ταυτόχρονα, έλεγε στους μαθητές του να ζουν κοντά στους ανθρώπους που μελετούσαν. Ο Robert Park είχε εργαστεί αρχικά, πριν ενταχθεί στην ακαδημαϊκή κοινότητα, έντεκα χρόνια ως ρεπόρτερ εφημερίδων, γεγονός που του έδωσε την ευκαιρία να γνωρίσει από κοντά και στην πηγή της την ζωή των πόλεων και τις εγκληματικές συμπεριφορές από το «πεζοδρόμιο». Στην ακαδημαϊκή του πορεία σε μια δύσκολη πόλη με μετανάστες και βιομηχανικά κέντρα, όπως το Σικάγο, μπορούσε να του προσφέρει όλα τα απαραίτητα εργαλεία για να μελετήσει στην πράξη προβατικές και εγκληματικές συμπεριφορές. Οι συνθήκες διαβίωσης των κατοίκων στις φτωχογειτονιές και η εγκληματικότητα ήταν τα βασικότερα ζητήματα που εξέτασε.

Κόντρα στην εποχή του, μελέτησε τόσο αυτός όσο και άλλοι συνάδελφοι του τη συμπεριφορά των ανθρώπων, τόσο σε ατομικό αλλά και ομαδικό επίπεδο, τόσο στην έκφανση στης συμμόρφωσής της με τον νόμο αλλά και στην έκφανση της απόκλισης από αυτόν, υπό το πρίσμα της επιρροής του περιβάλλοντος του ατόμου και των ευρύτερων κοινωνικών συνθηκών και καταστάσεων, σε αντιδιαστολή με τη θεώρηση της συμπεριφοράς ως ατομική ιδιομορφία. Με αυτό τον τρόπο προσέγγισης, η ζωή των παραβατικών ανθρώπων παρουσιάστηκε όπως ήταν πραγματικά. Οι έρευνες οδήγησαν στη διατύπωση της θεωρίας για την κοινωνική αποδιοργάνωση[4].

Οι περισσότερες θεωρίες που επικεντρώνονται στους ανθρωπολογικούς παράγοντες που εκτιμάται ότι διευκολύνουν τη δημιουργία και εκδήλωση παραβατικών συμπεριφορών, ενώ άλλες θεωρίες θέτουν στο επίκεντρο της μελέτης τους κοινωνικούς παράγοντες. Αυτό αποτελεί μια χρόνια διαμάχη ανάμεσα στους επιστήμονες, με διατύπωση αποκλινουσών προσεγγίσεων με αντίστοιχες τεκμηριώσεις, χωρίς έως τις μέρες μας να έχει αποσαφηνιστεί ποιος παράγοντας είναι πιο καθαριστικός. Στη σημερινή εποχή, οι κοινωνιολόγοι και λοιποί επιστήμονες επικεντρώνονται στους παράγοντες που γεννούν το έγκλημα και τις αιτίες που οδηγούν κάποιον να «παρανομήσει», πάντα μέσα στα χαρακτηριστικά κάθε κοινωνίας. Στην Ελληνική κοινωνία παρατηρούμε κυρίως φαινόμενα μικρό-εγκληματικότητας και λιγότερο ανάπτυξης σοβαρού οργανωμένου εγκλήματος, έχοντας ωστόσο και η συνθήκη αυτή τα δικά της χαρακτηριστικά. Επιπρόσθετα ένεκα της αλματώδης αύξησης της τεχνολογίας και της αύξησης χρήσης του διαδικτύου παρατηρείται να υπάρχουν στην Ελλάδα νέες μορφές εγκληματικότητας, όπως τα εγκλήματα του διαδικτύου. Μέσα από αυτό το απλό παράδειγμα μπορούμε να αντιληφθούμε πόσο σημαντικό ρόλο διαδραματίζει η κοινωνία και η εξέλιξη αυτής, καθώς και ότι παράλληλα το έγκλημα εξελίσσεται σαν ένας ζωντανός οργανισμός που

[4] Τάτσης – Θωμοπούλου, Η Κοινωνιολογία της Σχολής του Σικάγου. ΑΘΗΝΑ 2009 ΚΕΦ 6

βρίσκει πάντα τρόπους «επιβίωσης». Αυτό όμως δεν παραβλέπει τον άνθρωπο σαν μονάδα και τον τρόπο με τον οποίο αυτός συμμετέχει στη διαμόρφωση και στην εξέλιξη των παραβατικών συμπεριφορών.

Έτσι σύμφωνα με όλα τα παραπάνω μπορούμε να προσεγγίσουμε των όρο έγκλημα μέσα στην κοινωνία αναπτύσσοντας θεωρίες που διατυπώθηκαν τόσο σε σχέση με το γενικό πλαίσιο της εγκληματικότητας, αλλά και σε ειδικότερο επίπεδο σε σχέση με επί μέρους εκφάνσεις της, όπως επί παραδείγματι την παραβατικότητα των νέων, αλλά και την οπαδική εγκληματικότητα, υπό τη θεώρηση ότι καμία εξ αυτών δεν διαθέτει από μόνη της αυτοτέλεια, ερμηνευτική πληρότητα για το σύνολο της εγκληματικότητας και αποτελεσματικότητα[5]. Οι θεωρίες που έχουν διαμορφωθεί σε σχέση με το πεδίο της εγκληματικότητας - παραβατικότητας μπορούν να ενταχθούν σε τρεις κύριες κατευθύνσεις:

1. την ανθρωπολογική κατεύθυνση,
2. την κοινωνιολογική κατεύθυνση,
3. την ψυχολογική κατεύθυνση.

1.1 Πρόληψη Εγκλήματος

Ο όρος *Εγκληματολογία* ξεκινά να διαμορφώνεται στο ιστορικό και κοινωνικό πλαίσιο του δεύτερου ημίσεος του 19ου αιώνα. Κομβικό σημείο στην εξέλιξη του νέου αυτού πεδίου αποτέλεσε το πόνημα του Cesare Lombroso[6] με τίτλο “Ο εγκληματίας άνθρωπος” (L’uomo delinquente). Στο πόνημα αυτό ο Lombroso κατέγραφε την άποψη ότι η ροπή προς το έγκλημα ήταν αποτέλεσμα γενετικής προδιάθεσης. Για την Κλασική Σχολή, η συζήτηση για το θέμα του εγκλήματος εστιαζόταν κυρίως στις προσήκουσες ποινές, ωστόσο με την εμφάνιση της Ιταλικής Θετικής Σχολής, το επίκεντρο της συζήτηση μετατοπίζεται στον παραβάτη των κανόνων, δηλαδή τον εγκληματία, και στη διερεύνηση των αιτίων που είχαν ως αποτέλεσμα την εκδήλωση εγκληματικής συμπεριφοράς και δραστηριότητας. Έτσι, η εστίαση μετακινείται περισσότερο στο άτομο - εγκληματία και όχι στο φαινόμενο - αποτέλεσμα, δηλαδή στο έγκλημα. Η νέα αυτή προσέγγιση για τη μελέτη του εγκλήματος είχε σημαντικό αντίκτυπο. Εντός μίας εικοσαετίας από την έκδοση του του πονήματος “Ο εγκληματίας άνθρωπος”, δημιουργήθηκε μία ισχυρή κατεύθυνση μελέτης και κοινωνικής δράσης, η οποία υποστηρίχθηκε από πολλούς επιστήμονες. Το πιο σημαντικό στοιχείο που πρέπει να αναδειχθεί στο σημείο αυτό, είναι ότι διαμορφώνεται πλέον εστίαση σε ένα θεωρητικό πλαίσιο, στο οποίο διατυπώνονται, είτε με ρητό τρόπο, είτε υπόρρητα μέσω της επιλογής επιχειρημάτων, αρχές για τη μελέτη της εγκληματικής συμπεριφοράς.

Με βάση τη θεωρία της θετικής σχολής, εξετάζεται τυχόν ύπαρξη ατομικής ευθύνης του δράστη, αλλά και οι λόγοι (τα κίνητρα) που τον οδήγησαν στην παράβαση. Οι εγκληματίες διαχωρίστηκαν σε κατηγορίες, και ειδικότερα σε:

I. εγκληματίες ένεκα πάθους
II. περιστασιακούς εγκληματίες,

[5] ΠΑΠΑΖΑΧΑΡΙΟΥ Ι., Παραδόσεις εγκληματολογίας, εκδόσεις Α. Αναστασίου, Τεύχος Β΄, Αθήνα 1968 σελ. 6.

[6] Ιταλός ιατρός.

III. παράφρονες εγκληματίες,
IV. εγκληματίες ένεκα κληρονομικότητας.

Με απαρχή αυτή την κατάταξη, επιτεύχθηκε τελικά εξατομίκευση του εγκλήματος. Για την ανάλυση του φαινομένου της εγκληματικότητας αλλά και την κατανόησή του, θεωρούνταν πλέον οι ακόλουθες παράμετροι:

- η κοινωνική δομή,
- το οικονομικό επίπεδου κάθε κοινωνίας,
- η οικογένεια,
- η ηλικία
- το φύλο,
- το επάγγελμα,
- η προέλευση του ως προς την εθνικότητα του,
- το θρήσκευμα,
- ο κοινωνικός έλεγχος,
- η κοινωνική κριτική.

Το μεγαλύτερο ζήτημα για κάθε ερευνητή αλλά και για την παραγωγή καλύτερων αποτελεσμάτων είναι να αξιολογηθούν σωστά οι παράμετροι αυτοί έτσι ώστε να εξάγονται καλύτερα αποτελέσματα. Βαρύνουσα σημασία διαδραματίζουν τα στοιχεία και οι πληροφορίες, τα οποία πρέπει να είναι αξιόπιστα και ακριβή, καθώς η αξιοπιστία και η ακρίβεια των στοιχείων συνεισφέρει στο να προσεγγίζει η μελέτη της εγκληματικότητας την πραγματικότητα και να την αποτυπώνει με τον καλύτερο δυνατό τρόπο.

Δεν είναι τυχαία η προσέγγιση των τεχνών στον τομέα της εγκληματολογίας, κυρίως της λογοτεχνίας, όπου οι συγγραφείς αποτύπωσαν στα έργα τους προβλήματα των κοινωνιών, καταδεικνύοντας με αυτό τον τρόπο ότι μέσα στην κοινωνία και στον άνθρωπο, οι εγκληματικές πράξεις επηρεάζουν την καθημερινότητα του, την ζωή του. Αυτό δημιούργησε την τάση των ανθρώπων μέσα στην κοινωνία να ελέγχουν μέσω κανόνων - νόμων, τις εγκληματικές αυτές συμπεριφορές, οι οποίες απειλούσαν την εύρυθμη ζωή της κοινωνίας. Ένα κοινό παράδειγμα είναι η ποινικοποίηση της φτώχειας και της αεργίας το 1870 στις Η.Π.Α.[7].

1.2 Αστική Παραβατικότητα στην Ελλάδα

Δυστυχώς στην Ελλάδα δεν υπάρχουν έρευνες - μελέτες που να αποτυπώνουν την εγκληματικότητα από την σύσταση του Νέου Ελληνικού Κράτους, το 1828, έως και την

[7] Πρβλ. Dennis Porter, The Pursuit of Crime, New Haven & London 1981. Στην εργασία του Dennis Porter όπου εξετάζεται η αποτύπωση στη λογοτεχνία της εγκληματικότητας σε σύνδεση με την εξαθλίωση των ανθρώπων. Παραδείγματα απεικόνισης εγκλημάτων σε λογοτεχνικά κείμενα ορισμένων μορφών μπορούμε να αντλήσουμε από το έργο «Το παράπονο του νεκροθάπτου» (1895) του Εμμανουήλ Ροΐδη, στο οποίο η αφήγηση του βιασμού της κόρης του ήρωα από έναν νεαρό αξιωματικό συνδέεται με την προστασία που απολάμβανε ο αξιωματικός από πολιτικό παράγοντα, ενώ επίσης πληθώρα υγειονομικών παραβάσεων από τον σφαγέα της περιοχής, η οποία οδηγούσε σε ασθένειες και θανάτους, παρέμενε ακαταδίωκτη λόγω (φερόμενων) σχέσεων του σφαγέα με το κυβερνών κόμμα.

πρόσφατη Ιστορία. Υπάρχουν κάποιες αποσπασματικές αναφορές που μας δείχνουν μια εικόνα, ωστόσο σε επίπεδο ενδείξεων και περιστατικών μόνο και όχι σε επίπεδο συνολικής καταγραφής της εγκληματικότητας στον Ελλαδικό χώρο.

Ιδιαίτερη σημασία για την κατανόηση της εγκληματικότητας στην Ελλάδα διαδραμάτισαν οι σχετικές εργασίες του Thomas Gallant που εστίασαν στην ανάπτυξη και εξέλιξη του φαινομένου κατά τον 19ο αιώνα στην περιοχή των Επτανήσων. Ο Gallant εστίασε κυρίως στην αλληλεπίδραση μεταξύ του εθιμικού δικαίου που οδηγούσε σε βίαιες πράξεις και στην αντίστοιχη βία που προκαλούνταν από αυτό. Το έργο του αποτέλεσε σημείο αναφοράς για πολλούς ερευνητές. Τόσο το γεωγραφικό κριτήριο που τέθηκε, δηλαδή τα Επτάνησα, όσο και το χρονολογικό, ο 19ος αιώνας, είχαν σημαντικό ρόλο στα δεδομένα που ελήφθησαν υπ' όψιν αλλά και στα συμπεράσματα της έρευνας. Η διατριβή με τίτλο «Η εγκληματικότης εν Κρήτη» το 1968 με συγγραφέα τον κ. Εμμανουήλ Ανδριανάκη, ήταν μία ακόμη σημαντική μελέτη. Η διατριβή αυτή έλαβε κυρίως υπ' όψιν εγκληματολογικές στατιστικές και έγγραφα δικαστικού χαρακτήρα και συμπεριέλαβε στο σύνολο των κατηγοριών του εγκλήματος. Προσέγγισε το φαινόμενο από τη νομική θεώρηση, χρησιμοποίησε στατιστικά στοιχεία και δεδομένα αναφορικά με καταδικαστικές αποφάσεις που εκδόθηκαν στην Κρήτη και τις συνέκρινε με την εγκληματικότητα στο σύνολο της τότε Ελλάδας. Επιπρόσθετα επικεντρώθηκε στην γενεσιουργός αιτία του εγκλήματος, καθώς και στις ιδιάζουσες συνθήκες που επικρατούσαν στην Κρητική κοινωνία.

Οι λόγοι τιμής αποτελούσαν το αίτιο για τα περισσότερα εγκλήματα στην Ελλάδα κατά τον πρώτο αιώνα συστάσεως του κράτους. Αυτό εξηγείται ένεκα του τρόπου ζωής της Ελληνικής κοινωνίας τα χρόνια αυτά, όπου η θρησκεία διαδραμάτιζε και διαδραματίζει σημαντικό ρόλο στην ηθική του ανθρώπου, καθώς και στα ήθη των ανθρώπων αναφορικά με τη θέση του μέσα στην κοινωνία και τυχόν παραβίαση των «άτυπων» αυτών κανόνων.

Πολλές επίσης μελέτες επικεντρώθηκαν στην παραβατικότητα των ανηλίκων. Ως παραβατικότητα ανηλίκων μπορεί να οριστεί η συμμετοχή σε έκνομες συμπεριφορές ατόμων που δεν έχουν ακόμα ενηλικιωθεί σύμφωνα με το δίκαιο της οικείας έννομης τάξης. Σε κάθε περίπτωση, η ενηλικίωση, όπως αναφέρουν οι νόμοι, συνίσταται η ωρίμανση του ανθρώπου έτσι ώστε να είναι ικανός να έχει πλήρη αυτόνομη δικαιοπραξία για κάθε είδους νομική πράξη[8]. Στην Χώρα μας η ενηλικότητα ξεκινάει όταν ένα άτομο συμπληρώσει το 18ο έτος της ηλικίας του. Ποινικά η παραβατικότητα ανηλίκων αντιμετωπίζεται με ήπιες μορφές ποινών που έχουν ως κύριο στόχο να δίνουν στον ανήλικο ευκαιρίες για ομαλή συμμέτοχη στα κοινά μιας κοινωνίας. Πάντα τα κράτη προσέγγιζαν την νεανική παραβατικότητα με πιο ευαίσθητο τρόπο και κινητοποιώντας όλους τους διαθέσιμους φορείς της κοινωνίας για να πρόληψη και καταστολή της νεανικής παραβατικότητας. Στις αρχές του 20ου αιώνα, η εκβιομηχάνιση κυρίως, αλλά και άλλοι παράγοντες, συνέβαλαν στη διάσωση παιδιών από τα φτωχότερα στρώματα, για τα οποία υπήρχε αυξημένη πιθανότητα να εμφανίσουν ροπή προς την παραβατικότητα, καθώς συγκέντρωναν τις σχετικές προϋποθέσεις. Ήταν σχεδόν βέβαιο ότι εάν δεν λαμβανόταν κατάλληλα προληπτικά μέτρα, τα αρσενικά παιδιά νεαρής ηλικίας που

[8]Ρίκα Μπενβενίστε, Η ποινική καταστολή της νεανικής εγκληματικότητας τον 19ο αιώνα (1833-1911), Αθήνα & Κομοτηνή 1994, σελ 20-35.

προερχόταν από τα κατώτερα κοινωνικά στρώματα, θα κατέφευγαν σε αδικοπραγίες που θα αφορούσαν την περιουσία (κλοπές, ληστείες κ.λπ.), ενώ τα θήλεα τέκνα θα εξωθούνταν στην πορνεία. Κοινός παρονομαστής και στις δύο περιπτώσεις θα ήταν η αντιμετώπιση της φτώχιας. Όλες έρευνες σχεδόν διατυπώνουν τα συμπεράσματα τους αναλύοντας τον βαθμό στον οποίο μπορούσε να θεμελιωθεί σύνδεση μεταξύ των ποσοστών εγκληματικότητας ανά συνοικία με το οικονομικοκοινωνικό επίπεδο στο οποίο βρισκόταν οι κάτοικοί της[9].

1.3 Η Κοινωνιολογία των Καταγραφόμενων Εγκλημάτων

Με βάση τη μαθηματική – στατιστική προσέγγιση ο όρος **έγκλημα** αναφέρεται σε μια μοναδιαία εγκληματική πράξη. Η εγκληματική πράξη αποτελεί διακριτή έννοια σε σχέση με το εγκληματικό φαινόμενο. Ο όρος ***εγκληματικό φαινόμενο*** αναφέρεται σε ένα σύνολο εγκληματικών πράξεων, συμπεριλαμβάνει ωστόσο πέραν των ίδιων των πράξεων και τη θεσμική αντίδραση στις πράξεις αυτές, αλλά και τις κοινωνικές συνθήκες οι οποίες πλαισιώνουν αυτές τις πράξεις. Υπό αυτή τη θεώρηση, οι εγκληματικές πράξεις αντιμετωπίζονται ως ένα κοινωνικό φαινόμενο με πιο μόνιμα χαρακτηριστικά, το οποίο εκδηλώνεται στο πλαίσιο των κοινωνικών σχέσεων και μπορεί να εκλαμβάνεται είτε ως φυσιολογικό, είτε ως μη φυσιολογικό. Ο όρος ***εγκληματικότητα*** από την άλλη πλευρά αφορά τη στατιστική διάσταση των εγκληματικών πράξεων και αναφέρεται στο σύνολο των εγκληματικών πράξεων που λαμβάνουν χώρα σε συγκεκριμένη γεωγραφική περιοχή, για παράδειγμα σε ένα Κράτος, σε ένα Δήμο, μέσα σε ένα συγκεκριμένο χρονικό διάστημα. Την εγκληματικότητα, επιστημονικά, την χωρίζουμε σε δύο κατηγορίες, σε ***εμφανή εγκληματικότητα*** όπου περιλαμβάνει τα εγκλήματα που καταγγέλλονται στις αρχές ενός κράτους, και σε ***αφανή εγκληματικότητα***, δηλαδή στον άγνωστο αριθμό των εγκλημάτων τα οποία παραμένουν εκτός επίσημων καταγραφών[10].

Οι διαδικασίες επιλογής δεδομένων για το έγκλημα έχουν αποτελέσει αντικείμενο προβληματισμού επί μακρόν όπου ακόμα και σήμερα οι επιστήμονες πολλές φορές εκφράζουν επιφυλάξεις και διαφορετικές προσεγγίσεις. Το 1957 ο Donald Cressey επισημαίνει αποτελέσματα των ερευνών του σχετικά με προβλήματα αξιοπιστίας των στατιστικών δεδομένων των Αρχών. Οι επισημάνσεις για την αξιοπιστία των εγκληματολογικών στατιστικών σταδιακά εμπλουτίστηκε από τις θεωρίες της κοινωνικής αλληλεπίδρασης, της κριτικής ριζοσπαστικής θεωρίας και αργότερα του αριστερού ρεαλισμού. Σύμφωνα με τις θεωρίες αυτές, προκύπτει ότι η εγκληματικότητα: α) είναι ένα σύνολο ερμηνειών, διαθέσιμων πηγών δεδομένων, ποινικών τυποποιήσεων και εγκληματικών συμπεριφορών, στοιχεία ανεξάρτητα από την επιστήμη της στατιστικής, β) αντιπροσωπεύουν πολιτικές πρόληψης και καταστολής του εγκλήματος[11].

Η στατιστική μέτρηση της εγκληματικότητας πραγματοποιείται ανάλογα με τις ιστορικές συγκυρίες που είναι συνυφασμένες με τη συγκρότηση ενός σύγχρονου κράτους. Η

[9] Έφης Αβδελά, Η ποινική καταστολή της νεανικής εγκληματικότητας τον 19ο αιώνα (1833-1911), Αθήνα & Κομοτηνή 1994, σελ 55-75

[10] Σοφία ΒΙΔΑΛΗ «Εισαγωγή στην Εγκληματολογία» Εκδόσεις «Νομική Βιβλιοθήκη», μέρος Α', κεφ. Α', σελ. 15

[11] Σοφία ΒΙΔΑΛΗ «Εισαγωγή στην Εγκληματολογία» Εκδόσεις «Νομική Βιβλιοθήκη», μέρος Α', κεφ. Α', σελ. 17

εγκληματικότητα, ως η επιστήμη καταγραφής των εγκλημάτων που λαμβάνουν χώρα στο νεοσύστατο Ελληνικό κράτος, έχει την απαρχή της στον 19ο αιώνα και συνδέεται με διακριτές χρονικές περιόδους που κυρίως ορίζονται από την εμφάνιση στην Ευρωπαϊκή Ήπειρο βιομηχανικών και αστικών κέντρων, καθώς και από την επιστημονική πρόοδο στο ανωτέρω χρονικό πλαίσιο. Μετά το Β΄ Παγκόσμιο Πόλεμο, η αλλαγή του τρόπου αστυνόμευσης στις Η.Π.Α., η ροπή προς τη μέτρηση του έργου της αστυνομίας με ποσοτικούς δείκτες, σε συνδυασμό με τα αυξανόμενα κοινωνικά προβλήματα και ρατσιστικά ζητήματα, αύξησε υπέρμετρα την αστυνομική βία αλλά και τις συγκρούσεις με ρατσιστικά αίτια. Αυτό οδήγησε αργότερα και στην μετεξέλιξη των στατιστικών της εγκληματικότητας σε δείκτη απόδοσης έργου της αστυνομίας, τροπή που επηρέασε τις κοινωνίες όλης της Ευρώπης[12].

1.4 Η Πολιτική Λειτουργία του Εγκλήματος

Στην καθημερινότητά μας, συναντάμε συχνά φράσεις όπως «αποκλίνουσα συμπεριφορά», «παραβατικότητα» και «εγκληματικότητα» ως σχεδόν ταυτόσημες έννοιες.

Ωστόσο στην εγκληματολογία έχουν δοθεί ορισμοί για κάθε φράση και έννοια, προκειμένου να αποσαφηνιστούν οι όροι και το ακριβές περιεχόμενό τους.

Ο Ιταλός Cesare Beccaria ήταν από τους πρωτοπόρους και προσπάθησε να εστιάσει στις συνέπειες στην κοινωνία όταν διαπράττεται ένα έγκλημα και όχι τόσο στους «πρωταγωνιστές» αυτού, δηλαδή στον θύτη και στο θύμα. Μέσα από τις απόψεις του και την επιστημονική προσέγγιση του, η ανάλυση του όρου «έγκλημα» επικεντρωνόταν στις συνέπειες μετά από μία εγκληματική πράξη μέσα στην κοινωνία, στα μέλη και τις δομές αυτής. Χαρακτηριστικά ανέφερε: «Το μέτρο των εγκλημάτων είναι η ζημιά που προκαλούν στο έθνος, και όχι η πρόθεση του δράστη, η αξιοπρέπεια του προσβληθέντος ή η βαρύτητα του αμαρτήματος, χαρακτηριστικά που είναι εξαρτημένα με πρόσκαιρες εντυπώσεις, ψυχικές προδιαθέσεις, μη δυνάμενες να προσμετρηθούν διαστάσεις ή με ανεξιχνίαστη ψυχική κακία που υπερβαίνει τα όρια και τις δυνατότητες της ανθρώπινης δικαιοσύνης. Τα αληθινό μέτρο των εγκλημάτων είναι η βλάβη της κοινωνίας αφού όλα τα εγκλήματα –ακόμα και εκείνα που προσβάλλουν έναν ιδιώτη-πλήττουν την κοινωνία»[13].

Υπήρχαν και εγκληματολόγοι που εστιάζουν όχι τόσο στις συνέπειες ενός εγκλήματος, αλλά πιο πολύ στο γιατί κάποιος να κάνει έγκλημα, τι δηλαδή ωθεί τον δράστη στην πράξη αυτή ή αλλιώς ποια είναι τα κίνητρα του. Χαρακτηριστικό παράδειγμα της «κουλτούρας» αυτής είναι ο Βρετανός Jeremy Bentham που επικεντρωνόταν κυρίως στον εγκληματία, τον λόγο που τον ωθεί στο έγκλημα και τον αντίκτυπο του κινήτρου του μέσα στις δομές της κοινωνίας. Διαχρονική φράση του Bentham είναι η «κανένα έγκλημα, καμία ποινή χωρίς υφιστάμενο νόμο», η οποία διατυπώθηκε και από τον σύγχρονό του Paul Anselm Johann von Ritter Feuerbach με τη λατινική μορφή «Nullum crimen nulla poena sine lege».

Η δεκαετία 1950-1980 ήταν μια περίοδο ανατροπών των κοινωνικών σχέσεων, λόγω κυρίως της λήξης του Β΄ Παγκοσμίου Πολέμου, δημιουργώντας προϋποθέσεις για τη δημοκρατική

[12] Σοφία ΒΙΔΑΛΗ «Εισαγωγή στην Εγκληματολογία» Εκδόσεις «Νομική Βιβλιοθήκη», μέρος Α', κεφ. Α', σελ. 19

[13] Σοφία ΒΙΔΑΛΗ «Εισαγωγή στην Εγκληματολογία» Εκδόσεις «Νομική Βιβλιοθήκη», μέρος Α', κεφ. Α', σελ. 32

άνοιξη σε πολλές χώρες της Δύσης. Σε αυτό το πλαίσιο πολιτικοποιούνται και τα ζητήματα που εξετάζει η Εγκληματολογία και ταυτόχρονα αναδεικνύεται με συστηματικό τρόπο ο τομέας των εγκλημάτων εξουσίας. Η αρχή αυτής της περιόδου εγκαινιάζεται με τις λεγόμενες *υποπολιτισμικές θεωρίες* και με την έρευνα στη νεολαία. Οι υποπολιτισμικές θεωρίες περιλαμβάνουν ένα ευρύ φάσμα θεωριών που διατυπώθηκαν μετά το 1950 και έχουν ως κεντρικό άξονα την σύνδεση και συσχέτιση κοινωνικών πρακτικών, επιμέρους προτύπων συμπεριφοράς διαφόρων ομάδων πληθυσμού και πεποιθήσεων με την παραβίαση των κανόνων και ως εκ τούτου με το έγκλημα[14]

1.5 Γκέτο

Πολλές φορές οι εγκληματολόγοι προσπαθούν να εντοπίσουν τα αίτια που οδηγούν τον δράστη στο έγκλημα ομαδοποιώντας, κυρίως σε αστικές περιοχές, τα μέλη αυτής. Η ομαδοποίηση αυτή πολλές φορές γίνεται κυρίως με όρους θρησκευτικούς και πολιτισμικούς. Η λέξη που χρησιμοποιείται συχνά για να ορίσουμε μια ομαδοποίηση ατόμων μέσα στην κοινωνία είναι η λέξη γκέτο («ghetto»). Η Ιταλική αυτή λέξη *ghetto* αναφέρεται σε μια περιοχή τα μέλη της οποίας ανήκουν σε συγκεκριμένη εθνικότητα ή θρησκεία, ή διαθέτουν κάποιο άλλο κοινό γνώρισμα και ζουν ομαδικά, σε ήπια ή έντονη απομόνωση[15].

Οι ιστορικές καταβολές της λέξης προέρχονται από αναφορές σε περιορισμένες οικιστικές ζώνες στις οποίες οι Γερμανοί Ναζί υποχρέωναν τους Εβραίους να ζουν, σήμερα ωστόσο η έννοια του όρου έχει διευρυνθεί και συμπεριλαμβάνει κάθε αστική περιοχή με έντονα τα στοιχεία της φτώχειας και της παραβατικότητας.

Τα πρώτα «γκέτο», οι πρώτες ομάδες εμφανίζονται, στην Ιταλία και ειδικότερα στην πόλη της Βενετίας, περιοχή όπου προέρχεται και η λέξη αυτή όπου εξαναγκάζονταν, ένεκα νομικών αποφάσεων, να διαμένουν οι Εβραίοι από τις αρχές του 16^{ου} αιώνα. Στη διάρκεια του Β' παγκοσμίου πολέμου διαμορφώθηκαν εβραϊκά γκέτο σε πολλές πόλεις στην Ευρώπη. Οι συνθήκες ζωής στα γκέτο αυτά ήταν ιδιαίτερα δύσκολες και οι κάτοικοί τους ερχόταν αντιμέτωποι με πληθώρα προβλημάτων που είχαν ως πρωταρχική αιτία τη φτώχεια και την πείνα, ενώ αρκετές φορές υποβάλλονταν σε βασανισμούς και εξευτελισμούς ή ακόμη και εκτελούνταν από τις ναζιστικές δυνάμεις.

Στην Ευρώπη λοιπόν το γκέτο εμφανίζεται ως ομάδα πληθυσμού που αποτελούνταν από Εβραίους. Οι πρώτες ομαδοποιήσεις που μπορούν να χαρακτηριστούν «γκέτο» εμφανίζονται τον 13^{ο} αιώνα σε Ισπανία, Γερμανία και Πορτογαλία[16]**.**

Ο κοινωνιολόγος Kenneth Clark διατυπώνει τη θεωρία για τον κοινωνικό αποκλεισμό σε συγκεκριμένη περιοχή, αναδεικνύοντας ως κοινό στοιχείο των μελών αυτής το χρώμα, και παρατηρώντας ότι αποτέλεσμα της συμβίωσης αυτής είναι η αύξηση της νοσηρότητας και

[14] Σοφία ΒΙΔΑΛΗ«Εισαγωγή στην Εγκληματολογία» Εκδόσεις «Νομική Βιβλιοθήκη», μέρος Α', κεφ. Α', σελ. 97

[15] https://el.wikipedia.org/wiki/%CE%93%CE%BA%CE%AD%CF%84%CE%BF

[16] Σοφία ΒΙΔΑΛΗ «Εισαγωγή στην Εγκληματολογία» Εκδόσεις «Νομική Βιβλιοθήκη», μέρος Α', κεφ. Α', σελ. 103

της εκδήλωσης ασθενειών, η διόγκωση της εγκληματικότητας και η αυξημένη παιδική θνησιμότητα.

Ο κοινωνιολόγος Marcuse Peter, στη θεωρία του ως προς το τι σημαίνει γκέτο, διατυπώνει τον ορισμό ότι πρόκειται για περιοχές όπου διαμένουν άνθρωποι με συγκεκριμένα φυλετικά ή θρησκευτικά χαρακτηριστικά, τα οποία διαφέρουν από την υπόλοιπη κοινωνία. Σε συνολικότερο πλαίσιο, εντός της κοινωνίας υφίσταται μία κυρίαρχη ομάδα, η οποία οριοθετεί με επαρκή ακρίβεια έναν χώρο με σκοπό εντός αυτού του χώρου να περιοριστεί μία δεύτερη κοινωνική ομάδα η οποία θεωρείται κατώτερη και με τον τρόπο αυτό η δεύτερη αυτή ομάδα να διαχωριστεί από την υπόλοιπη κοινωνία. Είναι δυνατόν η κυρίαρχη ομάδα να αποτελεί το σύνολο της υπόλοιπης κοινωνίας (πλην της δεύτερης δηλαδή ομάδας).

Ο Γάλλος κοινωνιολόγος Loic Wacquant θεωρεί ότι τα ανωτέρω αποτελούν ένα τμήμα, ένα κομμάτι ενός μεγαλύτερου γκέτου, εισάγοντας τον όρο «hyperghetto» θέλοντας να τονίσει τον βασικό ρόλο του κράτους, ως βασικό θεσμό στην διαμόρφωση δομών ικανών να αποτρέψουν την δημιουργία τέτοιων μικρών ομάδων, εστιών εγκληματικότητας[17].

1.5.1 Προαπαιτούμενα του Ορισμού μιας Περιοχής ως «γκέτο»

Η διεθνής επιστημονική έρευνα και βιβλιογραφία υποδεικνύει οι το σύνολο των κάτωθι συνθηκών είναι αναγκαίο για τη διαπίστωση της ύπαρξης γκέτο. Σημειώνεται ότι πρέπει να υπάρχει σωρευτική συνδρομή όλων των συνθηκών.

1. Ύπαρξη μειονοτικών ομάδων σε αστικές περιοχές με στατιστική υπεροχή έναντι του συνόλου του πληθυσμού.
2. Διαχωρισμός.
3. Κοινωνική προβλήματα (φτώχεια, ανεργία, εγκληματικότητα).
4. Η μειονοτική ομάδα αντιμετωπίζεται ως ξένη, από τον υπόλοιπο πληθυσμό.
5. Ανεκτικότητα του κράτους.[18]

1.6 Πρόληψη Εγκλήματος - Φυλακές

Η αντεγκληματική πολιτική που ακολουθεί μια κοινωνία αποτελεί ένα σημαντικό στοιχείο για την λειτουργία όλων δημοκρατικών θεσμών. Δεν είναι τυχαίο ότι οι κυβερνήσεις των κρατών ανά τον κόσμο αποδίδουν μεγάλη σημασία στην πολιτική που θα ακολουθήσουν κατά του εγκλήματος, αφού το έγκλημα αποτελεί τον λόγω διακινδυνεύσεις της ειρηνικής συνύπαρξης των πολιτών, η οποία αποτελεί το κεφαλαιώδες τμήμα του κοινωνικού συμβολαίου. Η πρόληψη της εγκληματικότητας επικεντρώνεται στην υιοθέτηση πολιτικών που αποσκοπούν στην μείωση της συμμετοχή ατόμων σε εγκληματικές πράξεις με καταπολέμηση των αιτιών που οδηγούν σε αυτές καθώς και στην μείωση της θυματοποίησης των πολιτών. Τέτοιες πολιτικές έχουν να κάνουν κυρίως με προληπτικές ενέργειες όπως με την ενημέρωση, ακόμα και σε μικρές ηλικίες, στον ρόλο του σχολείου και των εκπαιδευτικών μονάδων γενικότερα,

[17] Χριστίνα ΖΑΡΑΦΩΝΙΤΟΥ, Καθηγήτρια Εγκληματολογίας, Τμήμα Κοινωνιολογίας Παντείου Πανεπιστημίου, Άρθρο Ιούνιος 2012 https://theartofcrime.gr/

[18] Χριστίνα ΖΑΡΑΦΩΝΙΤΟΥ, Καθηγήτρια Εγκληματολογίας, Τμήμα Κοινωνιολογίας Παντείου Πανεπιστημίου, ΥΠΑΡΧΟΥΝ GHETTOS ΣΤΟ ΚΕΝΤΡΟ ΤΗΣ ΑΘΗΝΑΣ; Εγκληματολογία 2/2012 www.nbonline.gr

όπως για παράδειγμα από την πρώτες ηλικίες τα παιδιά να μαθαίνουν το ρόλο των ορίων στην ζωή τους. Η αντεγκληματική πολιτική απαιτεί επεξεργασμένη στρατηγική, σωστή οργάνωσή, σχεδιασμό τουλάχιστον με ορίζοντα 10ετίας και πρόνοια για δυναμική ενσωμάτωση αλλαγών, καθόσον το έγκλημα είναι ζωντανός οργανισμός, εξελίσσεται και μεταμορφώνεται ταχέως και οι αλλαγές αυτές πρέπει να οδηγούν σε αντίστοιχη προσαρμογή και των αντεγκληματικών πολιτικών. Ένα χαρακτηριστικό παράδειγμα είναι το ψηφιακό έγκλημα, το οποίο εξελίσσεται με γρήγορους ρυθμούς λόγω και της τεχνολογικής προόδου όπου και αντίστοιχα οι αντεγκληματικές πολιτικές πρέπει να προσαρμόζονται με την ίδια ταχύτητα που εξελίσσεται και το ψηφιακό έγκλημα[19].

Ένα κεφάλαιο στη διαμόρφωση της πρόληψης έχει να κάνει με τους υπότροπους, δηλαδή με άτομα που έχουν διαπράξει ένα ή περισσότερα εγκλήματα και οι οποίοι μετά την έκτιση της όποιας ποινής τους πρέπει να ενταχθούν ομαλά στην κοινωνία. Στατιστικές αναφέρουν ότι οι υπότροποι ευθύνονται για την αύξηση της εγκληματικότητας σε πολλές κοινωνίες. Επιπρόσθετα μελέτες αναφέρουν ότι αν μειωθεί η υποτροπή σε ένα σημαντικό ποσοστό, τότε θα έχουμε μια πολύ σημαντική μείωση της εγκληματικότητας. Η επανένταξη των υπότροπων, όπως παράλληλα και η σωφρονιστική πολιτική, αποτελούν κύρια χαρακτηριστικά της έννοιας του σωφρονισμού δηλαδή της ουσιαστικής προσπάθεια της πολιτείας να επανεντάξει στην κοινωνία τον υπότροπο μετά την καταδίκη του. Το όφελος του σωφρονισμού είναι διττό, και αφορά τόσο τον ίδιο τον σωφρονιζόμενο όσο και την κοινωνία. Όσο πιο ομαλά γίνει αυτή η επανένταξη, τόσο η απόσταση του υπότροπου από το να διαπράξει νέο έγκλημα θα αυξάνεται, με θετικές συνέπειες για τη μείωση της εγκληματικότητας μέσα στην κοινωνία. Για την επίτευξη αυτού του στόχου, απαιτούνται επεξεργασμένες πολιτικές με ορίζοντα 10ετίας τουλάχιστον και με έμφαση στον σωφρονισμό και ειδικότερα στην αλλαγή κουλτούρας στην έκτιση της ποινής, με κατάλληλα εργαλεία ψυχολογικής και κοινωνικής υποστήριξης, με σοβαρό επαγγελματικό προσανατολισμό για άμεση εύρεση εργασίας μετά την έκτιση της ποινής, όπως επίσης πολύ αυστηρό πλαίσιο του μέτρου της αναστολής, λειτουργώντας αποτρεπτικά στην διάπραξη νέων εγκλημάτων[20].

Ο θεσμός των κέντρων ημιελεύθερης διαβίωσης, σε συνδυασμό με τη θεσμοθέτηση κανόνων και θεσμών ικανών να προετοιμάσουν τον κρατούμενο για το διάστημα μετά την απόλυσή του, έχει θετικά αποτελέσματα. Στο πλαίσιο αυτό, οι φυλακές διαμορφώνονται ως πιο ανοιχτές δομές, μη αποτελώντας πλέον κλειστά συστήματα, και αποφεύγοντας, στο μέτρο του δυνατού, την εξοικείωση του κρατούμενου με τη φυλακή (με την τρέχουσα μορφή της) και ό,τι απορρέει από την κλειστή κοινωνία αυτή και πως επηρεάζει την μετέπειτα ζωή του.

[19] Κωνσταντίνος ΚΟΣΜΑΤΟΣ. «Κρίση, φόβος και ποινική καταστολή», στον τιμητικό τόμο για τον ομότιμο καθηγητή Γιάννη Πανούση, «ΕΓΚΛΗΜΑΤΟΛΟΓΙΑ: ΠΕΡΙΒΛΕΠΤΟΝ ΑΛΕΞΙΦΩΤΟΝ», εκδόσεις Ι. ΣΙΔΕΡΗΣ, Αθήνα, 2020, σελ. 215

[20] ΚΟΥΡΑΚΗΣ Νεστορ – ΜΗΛΙΩΝΗ Φωτεινή «Αναπλαισιώνοντας και εκτιμώντας ερευνητικά δεδομένα για την παραβατικότητα των νέων για το πρόβλημα της υποτροπής νεαρών αποφυλακισμένων στην Ελλάδα με βάση τα πορίσματα επαναληπτικής (follow – up) έρευνας του Εργαστηρίου Ποινικών και Εγκληματολογικών Ερευνών» (Πανεπιστήμιο Αθηνών), παρουσιάστηκε στο EPANODOS WORKSHOP ON RECIDIVISM στις 5-7-2019

Σε φυλακές υψίστης ασφαλείας όπου εφαρμόζεται το καθεστώς αυτό, κυρίως σε χώρες της Βόρειας Ευρώπης, το ποσοστό υποτροπής έχει μειωθεί τα τελευταία χρόνια κατακόρυφα[21].

Επιπρόσθετα, σημαντικό ρόλο διαδραματίζουν και οι εκπαιδευτικές πολιτικές που υπάρχουν μέσα στις φυλακές και ειδικότερα αυτές που προσανατολίζονται στην τεχνική εκπαίδευση. Τα εκπαιδευτικά προγράμματα αυτά, αν εφαρμοστούν με σωστό τρόπο, μπορούν να προετοιμάσουν τον υπότροπο και να του δώσουν ευκαιρίες για μια ομαλή μετάβαση από την κοινωνία των φυλακών στην πραγματική κοινωνία. Πολλές έρευνες σε χώρες της Ευρώπης που εφαρμόζονται ανάλογες δράσεις - παρεμβάσεις, αποδεικνύουν ότι η εκμάθηση εργασίας και επιμόρφωση στα σωφρονιστικά καταστήματα έχουν ως αποτέλεσμα τη σημαντική μείωση των ποσοστών εμφάνισης υποτροπών. Η υποστήριξη του δικαιώματος στην εργασία και της ομαλής κοινωνικής (επαν)ένταξης των ατόμων στην κοινωνία έχει αποδειχθεί συνεισφέρουν σημαντικά στη μείωση των υποτροπών, η οποία συγκαταλέγεται στους κύριους στόχους κάθε σωφρονιστικού συστήματος[22].

1.7 Διάκριση Εγκλημάτων

Κάθε μία από τις ποιοτικές κατηγοριοποιήσεις των εγκλημάτων αποτελεί στην εποχή μας έναν ξεχωριστό κλάδο έρευνας της επιστήμης της Εγκληματολογίας. Σε αντίθεση με τον Ποινικό Κώδικα, όπου οι διακρίσεις των εγκλημάτων γίνεται με βάση το έννομο αγαθό που προσβάλλεται με μια πράξη (ζωή, περιουσία κ.λπ.) και επιπλέον με βάση τη βαρύτητα του εγκλήματος όπου προκύπτουν τα είδη του εγκλήματος κατά της ζωής, κατά του πολιτεύματος κ.λπ., στην επιστήμη της Εγκληματολογίας οι ποιοτικές κατηγοριοποιήσεις αναπτύσσονται με βάση γενικότερα χαρακτηριστικά της πράξης του δράστη, τον τρόπο διάπραξης αλλά και το έννομο αγαθό που προσβάλλεται. Ειδικότερα, η σημερινή κοινωνία έρχεται αντιμέτωπη με τις κάτωθι κατηγορίες εγκλημάτων οι οποίες αποτελούν και τις βασικές στοχεύσεις της αντεγκληματικής πολιτικής[23]:

- **Εγκλήματα με δράστες ιδιαίτερες ομάδες πληθυσμού**, όπου οι ομάδες διαμορφώνονται με βάση την ικανότητα τους να έχουν ποινική ευθύνη. Στην κατηγορία αυτή για παράδειγμα μπορούμε να εντάξουμε την νεανική εγκληματικότητα, επειδή οι δράστες τους έχουν και διαφορετική ποινική μεταχείριση σε όλα τα στάδια εμπλοκής τους με το ποινικό σύστημα.

- **Τα κοινά εγκλήματα.** Πρόκειται για εγκλήματα που προσβάλλουν περιουσιακά αγαθά, όπως ληστείες, κλοπές κ.λπ., αλλά και την σωματικής ακεραιότητα (σωματικές βλάβες κ.ο.κ.).

---

[21] Τσιλίκης Χ. – Γάκου Ε.Μ. «Κοινωνική επιχειρηματικότητα και σωφρονιστική. Προτεινόμενο μοντέλο εργασιακής επανένταξης έγκλειστων και αποφυλακισμένων στην Ελλάδα», Κοινωνική Πολιτική, 9, σελ.88 επ.

[22] BATIUK M. «The State of Post Secondary Correctional Education in Ohio», Journal of Correctional Education, 1997, 48, 70-72 και ALLEN J.P. «Administering Quality Education in an Adult Correctional Facility», Community Service Catalyst, 1988, 18, 28-29.

[23] Σοφία ΒΙΔΑΛΗ, «Εισαγωγή στην Εγκληματολογία», Εκδόσεις Νομική Βιβλιοθήκη, Αθήνα, Μέρος Δ, Κεφ. Α, σελ. 277-286

- **Τα εγκλήματα των ισχυρών**. Οι δράστες των εγκλημάτων αυτών κατέχουν σημαντική κοινωνική, οικονομική ή πολιτική εξουσία. Μπορεί να διαπράττονται από εταιρείες, κρατικούς φορείς ή κρατικούς αξιωματούχους.

- **Εγκλήματα μίσους.** Ως έγκλημα μίσους ορίζεται η εγκληματική πράξη της οποίας τα θεμελιώδη κίνητρα είναι η εχθρότητα ή η προκατάληψη απέναντι σε μεμονωμένα άτομα ή την περιουσία αυτών, και η οποία βασίζεται σε θέματα που αφορούν τη φυλή, την εθνότητα τη θρησκεία, την αναπηρία ή τον σεξουαλικό προσανατολισμό του θύματος. Τα χαρακτηριστικά του θύματος μπορεί να είναι πραγματικά ή εικαζόμενα από τον δράστη.

- **Το «έγκλημα του λευκού κολάρου» (white – collar crimes)** που πρώτος ανέδειξε ο Edwin Sutherland, στο ομώνυμο έργο του 1940, σήμερα εντάσσεται στο πλαίσιο περισσότερο προσεγγίσεων που συνεκτιμούν γενικότερα τα εγκλήματα των ισχυρών. Τα εγκλήματα του λευκού κολάρου είναι παραβάσεις του νόμου, που διαπράττονται από στελέχη επιχειρήσεων και γενικότερα άτομα με υψηλή κοινωνική - οικονομική θέση και μορφωτικό επίπεδο προς όφελος κυρίως της επιχείρησης - εταιρείας, χωρίς ωστόσο να αποκλείεται και η ύπαρξη ιδίου οφέλους.

- **Οργανωμένο έγκλημα.** Το οργανωμένο έγκλημα αποτελεί ένα διακριτικό κοινωνικό φαινόμενο, βασισμένο κατά κανόνα σε κοινωνικές πρακτικές και ανάγκες που η ποινική τυποποίηση του συνοψίζεται στην ιδέα της εγκληματικής οργάνωσης, δηλαδή τυποποιείται με βάση τον τρόπο, τον στόχο και την ιεραρχία της οργάνωσης συγκεκριμένων ατόμων με κύριο σκοπό το προσωπικό όφελος. Το οργανωμένο έγκλημα, στο πλαίσιο της παραδοσιακής εγκληματολογίας, ταυτίζεται με τον εγκληματικό υπόκοσμο, δηλαδή με την ύπαρξη ομάδων πληθυσμού που έχουν δικές τους διακριτές αξίες και επιδιώξεις από αυτές της υπόλοιπης κοινωνίας.

- **Πολιτικά εγκλήματα – Τρομοκρατία.** Μια ειδική κατηγορία εγκλημάτων είναι τα πολιτικά εγκλήματα, δηλαδή εκείνα που διαπράττονται με στόχο την υπονόμευση ή την ανατροπή ενός πολιτικού συστήματος και όχι για προσωπικό όφελος των δραστών. Επίσης και η τρομοκρατία η οποία επιδιώκει με την χρήση βίας και φόβου και την διάπραξη στυγερών εγκλημάτων να πολιτικοποιήσει συμπεριφορές εις όφελος μια ομάδας ατόμων στο όνομα ιδεολογικών, θρησκευτικών και πολιτικών κινήτρων.

- **Εγκλήματα διαπροσωπικής βίας.** Πρόκειται για ένα ευρύ φάσμα εγκλημάτων που περιλαμβάνουν την κακοποίηση, συμπλοκές και σωματικές βλάβες, ανθρωποκτονίες σε ακραίες μορφές βίας όπως βιασμούς, κακοποίηση ανηλίκων ακόμα και βασανιστήρια και γενικά εγκλήματα βίας μεταξύ ιδιωτών.

1.8 Αστικός Σχεδιασμός και Πρόληψη Εγκληματικότητας

Το κοινωνικό περιβάλλον μέσα στο οποίο ζούμε είναι άρρηκτα συνδεδεμένο με την εγκληματικότητα, από την εμφάνιση της μέσα στα χρόνια έως σήμερα. Εξάλλου η εγκληματικότητα, εντός της κοινωνίας, είναι άμεσα συνδεδεμένη με την ανθρώπινη συμπεριφορά. Η Σχολή του Σικάγο, από το 1930, επιχείρησε να αναδείξει τον συσχετισμό

αυτό διευρύνοντας τον και σε μια άλλη μορφή του προσεγγίζοντας την σχέση που υπάρχει στο είδος των ανθρώπων μιας περιοχής, των κατοίκων της και την εγκληματογόνα συμπεριφορά τους. Κατά τη δεκαετία του 1970, κάποιοι εγκληματολόγοι προβληματίστηκαν αναφορικά με το πως ο τρόπος ζωής μας, η συμπεριφορά μας μέσα στην κοινωνία μπορεί να επηρεάσει και την συμπεριφορά μας απέναντι στο έγκλημα. Ο προβληματισμός αυτός ανέδειξε την σκέψη ότι το έγκλημα αποτελεί μια συμπεριφορά συνηθισμένη μεν αλλά κλιμακωτή ανάμεσα στα όρια που έχει ο κάθε άνθρωπος, όρια τα οποία ο καθένας τοποθετεί ανάλογα με το περιβάλλον του, την εκπαίδευση του, την κοινωνία που ζει, τα ερεθίσματα που δέχεται κατά την διάρκεια της ζωής του.

Χαρακτηριστικό παράδειγμα αποτελεί η θεωρία που εκπονήθηκε από τους κοινωνιολόγους James Q. Wilson και George L. Kelling το 1982, και υποστηρίζει ότι αν ***«ένα παράθυρο σπάσει, τυχαία ή σκόπιμα, σε ένα εγκαταλελειμμένο κτίριο και δεν αποκατασταθεί η ζημιά, σύντομα θα σπάσουν κι άλλα και αμέσως μετά θα γίνει στέκι – σημείο κάθε μορφής παραβατικότητας»***[24]***.***

Οι Wilson και Kelling, βασίστηκαν στις παρατηρήσεις και τα συμπεράσματα ενός πειράματος που διεξήχθη με επικεφαλής τον καθηγητή Philip Zimbardo το 1969. Στο πείραμα αυτό, τοποθετήθηκαν δύο αυτοκίνητα δίχως πινακίδες, το καθένα σε μία διαφορετική περιοχή. Οι δύο περιοχές επιλέχθηκαν ώστε να έχουν σημαντικές αντιθέσεις, τόσο στο γεωγραφικό όσο και στο οικονομικό/κοινωνικό επίπεδο. Συγκεκριμένα, η πρώτη περιοχή ήταν η συνοικία του Μπρονξ, η οποία ήταν υποβαθμισμένη, ενώ η δεύτερη περιοχή ήταν μία εύπορη συνοικία του Palo Alto στην Καλιφόρνια. Στη συνοικία του Μπρονξ, εντός δέκα λεπτών ξεκίνησαν να διενεργούνται πράξεις βανδαλισμού, ενώ μέσα σε ένα 24ωρο είχε αποσπαστεί το σύνολο των εξαρτημάτων του αυτοκινήτου. Σε αντιδιαστολή, στο Palo Alto δεν υπήρξε καμία ανάλογη πράξη και το αυτοκίνητο παρέμεινε άθικτο. Στη συνέχεια τα μέλη της ομάδας διεξαγωγής του πειράματος έσπασαν τα τζάμια του αυτοκινήτου που είχε τοποθετηθεί στο Palo Alto και παρατήρησαν τις εξελίξεις. Τότε διαπίστωσαν ότι μέσα σε ένα 24ωρο, είχαν προκληθεί ανάλογες συμπεριφορές με αυτές που είχαν παρατηρηθεί στο Μπρονξ. Με βάση αυτά τα στοιχεία, η ομάδα πειραματισμού αποφάνθηκε ότι πράξεις βανδαλισμού είναι δυνατόν να λάβουν χώρα σε κάθε περιοχή, και ορατές ενδείξεις αταξίας και παραμέλησης ενθαρρύνουν την αποκλίνουσα συμπεριφορά και τις εγκληματικές πράξεις[25].

Η αντιεγκληματική πολιτική αποτελεί κορυφαία επιλογή και κατεύθυνση μιας κοινωνίας στην προσπάθεια της να αποτραπούν εγκληματικές συμπεριφορές. Αποτελεί μία σύνθετη διαδικασία συμμετοχής πολλών επιστημών (στατιστική, κοινωνιολογία, εγκληματολογία, πολιτικές επιστήμες κ.λπ.) στην προσπάθεια σχεδιασμού προληπτικών και κατασταλτικών μέτρων καταπολέμησης του εγκλήματος. Στο τομέα της πρόληψης, οι μελέτες των Newman και Jeffery αποτέλεσαν τις κεντρικές κατευθυντήριες γραμμές. Στις μελέτες τους, οι Newman και Jeffery υποστήριξαν ότι οι κατάλληλα στοχευμένες παρεμβάσεις στο αστικό και οικιστικό περιβάλλον, οι οποίες διαθέτουν μεταξύ τους συνοχή στο πλαίσιο συγκροτημένου ανασχεδιασμού, μπορούν να συνεισφέρουν στη μείωση συμπεριφορών με εγκληματικά

[24] Joël J. Van der Weele, Broken Window Effect, University of Amsterdam January 2017

[25] Joël J. Van der Weele, Broken Window Effect University of Amsterdam January 2017

ή/και παραβατικά χαρακτηριστικά. Ο Jeffery εξέλιξε και ολοκλήρωσε αυτή τη θεωρία, και σε αυτόν αποδίδεται η πρώτη χρήση του όρου *Crime Prevention Through Environmental Design (C.P.T.E.D.)*. Στόχος της θεωρίας αυτής είναι η σταχυολόγηση όλων των στοιχειών και χαρακτηριστικών με σκοπό να παρθούν οι σωστές αποφάσεις αναφορικά με μέτρα ικανά να αποτρέψουν το έγκλημα.[26].

1.8.1 Οι θεμελιώδεις αρχές του C.P.T.E.D.

Το C.P.T.E.D. όπως αναφέραμε έχει στόχο να παρουσιάσει πολιτικές και κατευθύνσεις με κύριο στόχο την πρόληψη του εγκλήματος. Ενδεικτικά τέτοιες πολιτικές είναι:

- Δημιουργία περιοχών ελέγχου – αποτροπής.
- Παρότρυνση στην δημιουργία πολιτικών υπέρ υγιών δραστηριοτήτων (αθλητισμός – πολιτισμός).
- Ενίσχυση πολιτικών και παρεμβάσεων αποτρεπτικού χαρακτήρα όπως κάμερες, εμπόδια, φωτισμός.
- Ελεγχόμενη πρόσβαση ελέγχου.
- Καθαριότητα περιοχών – γειτονιών.
- Ολιστική προσέγγιση του πολεοδομικού σχεδιασμού με αντεγκληματικό χαρακτήρα.

[26] Αγγελική Ρούσσου Δικηγόρος, Υποψήφια Διδάκτωρ Ποινικού Δικαίου ΕΚΠΑ ΝΟΕΜΒΡΙΟΣ 2018, Ο περιβαλλοντικός σχεδιασμός ως μέθοδος πρόληψης του εγκλήματος στις σύγχρονες πόλεις (CPTED), https://theartofcrime.gr/

2 ΨΗΦΙΑΚΟ ΕΓΚΛΗΜΑ

2.1 Ορισμός

Το έγκλημα είναι μέρος της ανθρώπινης συμπεριφοράς και κατ' επέκταση σημαντικό κομμάτι του παζλ που συνθέτουν την κοινωνία, το οποίο εξελίσσεται και μεταβάλλεται κατά τον τρόπο με τον οποίο εξελίσσεται και διαμορφώνεται και η ίδια η κοινωνία σε όλα τα χαρακτηριστικά της. Για να εντοπίσουμε τις ρίζες του ηλεκτρονικού εγκλήματος, θα πρέπει να εξετάσουμε τον χώρο της κοινωνίας και να δούμε πότε εμφανίστηκαν οι ηλεκτρονικοί υπολογιστές σε αυτή και πότε έγινε ευρεία η χρήση τους. Ως αποτέλεσμα αυτών των εξελίξεων είναι η νέα μορφή του, το ψηφιακό έγκλημα και οι ψηφιακοί εγκληματίες που έκαναν σε συνάφεια τότε την εμφάνισή τους. Παράλληλα η νέα μορφή αυτή του εγκλήματος έφερε και νέα δεδομένα αλλά και δυσκολίες στις αρχές επιβολής του Νόμου. Οι Barn και Barn υποστηρίζουν ότι ένας πιθανός παράγοντας που οδηγεί σε δυσκολίες στην μελέτη και εξιχνίαση του εγκλήματος στον κυβερνοχώρο είναι η έλλειψη δομών και εργαλείων ικανών να οδηγήσουν στην εξάλειψη και έλεγχο της νέας αυτής μορφής της εγκληματικότητας. Για παράδειγμα στην παγκόσμια νομοθετική αναθεώρηση, που αφορά ανήλικους, του I.C.M.E.C. (International Centre for Missing and Exploited Children) για το «Grooming» προβληματίστηκαν πώς αυτό θα το οριστεί και μεταφερθεί σε νομικό κείμενο προκειμένου να αντιμετωπιστεί. Τα προβλήματα ξεκινούν με την ίδια την ορολογία. Υπάρχει ένα σύνολο όρων που χρησιμοποιούνται, τις περισσότερες φορές με τα προθέματα «cyber», «computer», και «e-», ή στα Ελληνικά «κυβερνο», «υπολογιστών» ή «ηλεκτρονικών». Οι όροι αυτοί εφαρμόζονται χωρίς διάκριση μεταξύ τους και αλληλεπικαλύπτονται ως προς το περιεχόμενο, παρουσιάζοντας σημαντικά κενά στο νόημα που προσπαθούν να αποδώσουν. Για παράδειγμα το ηλεκτρονικό έγκλημα διατυπώνεται ως «έγκλημα στον κυβερνοχώρο», «έγκλημα ηλεκτρονικών υπολογιστών», «έγκλημα που σχετίζεται με υπολογιστές», «ηλεκτρονικό έγκλημα», «έγκλημα που βασίζεται στην τεχνολογία», «έγκλημα υψηλής τεχνολογίας»[27]. Η πρακτική αυτή υπογραμμίζει την έλλειψη ενός κοινού λεξικού, ενός συνόλου κοινά αποδεκτών ορισμών που πρέπει να αποτυπωθούν με ακρίβεια σε νομικά κείμενα. Αυτό αποτελεί προϋπόθεση ώστε να είναι δυνατό οριστεί τι είναι το ψηφιακό έγκλημα και κατά συνέπεια πώς θα αποδοθεί η δικαιοσύνη στα εγκλήματα αυτά. Χαρακτηριστικά στην Αγγλική γλώσσα έχουν χρησιμοποιηθεί αντίστοιχα οι ακόλουθοι όροι[28]:

1. Cybercrime
2. Cyber crime
3. Computer crime
4. E-crime
5. Internet crime
6. Digital crime

[27] Kirsty Phillips, Julia C. Davidson, Ruby R. Farr, Christine Burkhardt, Stefano Caneppele and Mary P. Aiken, Review about Cybercrime and specially about definition, typologies and taxonomies, 19 April 2022

[28] Rutger Leukfeldt and Thomas J. Hollt , The Human Factor of Cybercrime, 2020 publised by Routledge, page 10-25

7. Online crime
8. Virtual crime
9. Techno-crime
10. Netcrime

Σαν έναν κοινό αποδεκτό ορισμό σύμφωνα με τους Forester και Morrison (1994) μπορούμε να αποδώσουμε ότι το ηλεκτρονικό έγκλημα ορίζεται ως «***μια εγκληματική πράξη στην οποία ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως το κυριότερο μέσο τέλεσης της***». Οι Ελληνικοί όροι που χρησιμοποιούνται για αναφορά στο φαινόμενο αυτό είναι ***ηλεκτρονικό έγκλημα, ψηφιακό έγκλημα, διαδικτυακό έγκλημα και έγκλημα του κυβερνοχώρου***[29]***.***

Βασικό στοιχείο αυτής της μορφής του εγκλήματος είναι η ένταξη στο πλαίσιο της εγκληματικής πράξης μιας ηλεκτρονικής συσκευής που έχει τη δυνατότητα να επεξεργάζεται ή/και να μεταδίδει δεδομένα όπως π.χ. ένας Η/Υ, ένα κινητό τηλέφωνο, ένας υπολογιστής-ταμπλέτα (tablet) κ.ο.κ. Ο ρόλος της ηλεκτρονικής συσκευής στο πλαίσιο της πράξης μπορεί να διαφοροποιείται ως εξής[30]:

- Να είναι το «θύμα».
- Να είναι το μέσο που χρησιμοποιεί ο δράστης για να διαπράξει το έγκλημα.

Το ψηφιακό ή διαδικτυακό έγκλημα λοιπόν αποτελεί λοιπόν ένα σύγχρονο κεφάλαιο στον τομέα της εγκληματολογίας και οι κοινωνίες προσπαθούν να προσαρμόσουν τις ανάγκες για την πρόληψη και την καταστολή του στα νέα δεδομένα, έχοντας την δυσκολία να «παντρέψει» νομικούς και κοινωνιολογικούς όρους με ορισμούς και εξειδικευμένη θεματολογία της πληροφορικής.

Ως το πρώτο ηλεκτρονικό έγκλημα τοποθετείται χρονολογικά στην Γαλλία 1820 ο Sir Joseph-Marie Jacquard, δημιούργησε έναν αυτοματοποιημένο αργαλειό. Αυτή η συσκευή συνδυάστηκε με αναλογική τεχνολογία στην ύφανση. Τότε δημιουργήθηκε φόβος στους εργαζόμενους του Jacquard ότι απειλούνταν η παραδοσιακή απασχόληση και η διαβίωση τους. Για αυτό τον λόγο οι εργαζόμενοι διέπραξαν δολιοφθορές για να αποτρέψουν τον Jacquard από το να διευρύνει τη χρήση της νέας τεχνολογίας[31].

2.1.1 Βασικές Κατηγορίες Ηλεκτρονικού Εγκλήματος

Οι βασικές κατηγορίες Ηλεκτρονικού Εγκλήματος είναι οι κάτωθι:

- Εγκλήματα που διαπράττονται σε υπολογιστικό περιβάλλον.
- Εγκλήματα που διαπράττονται χωρίς εμπλοκή/χρήση του διαδικτύου (π.χ. υπεξαγωγή δεδομένων από φυσικό μέσο αποθήκευσης).

[29] Monica Horten, Cautionary Tales and Ethical Dilemmas in Computing, Published in 18 December 2007, Article

[30] Scene of the Cybercrime, Computer Forensics Handbook Book 2002, Debra Littlejohn Shinder and Ed Tittel, Technical Editor

[31] www.chaintech.network/blog/1820-textile-industry-weaving-the-threads-of-the-first-cybercrime

- Εγκλήματα που διαπράττονται με την αξιοποίηση ή κατάχρηση της διασυνδεσιμότητας μέσω διαδικτύου.

Οι διαφορές των ψηφιακών εγκληματών σε σχέση με τα κοινά εγκλήματα επικεντρώνονται στα κάτωθι:

- Ανωνυμία – απόσταση δράστη - θύματος.
- Ο εντοπισμός του δράστη είναι περίπλοκος και απαιτεί περαιτέρω γνώσεις πληροφορικής.
- Μεγάλος αριθμός θυμάτων.
- Μεγαλύτερες οικονομικές απώλειες.

Μια ενδεικτική λίστα για να καταδείξει το εύρος των εγκλημάτων στον κυβερνοχώρο και των πράξεων που παρεκκλίνουν στον κυβερνοχώρο είναι ή κάτωθι[32]:

- Botnets
- Coercion
- Computer - related forgery
- Computer - related fraud
- Copyright infringements
- Criminal communications
- CSAM/CSE
- Cyber troops
- Cyberbullying
- Cyberfraud
- Cyberwarfare
- Data interference
- Deep fakes
- Digital piracy
- Drug trade
- Espionage
- Extorsion (e.g., Romance Fraud)
- Grooming
- Harassment
- Hate speech
- Heist Religious offenses
- Identity theft
- Illegal access (hacking/cracking)
- Illegal data acquisition
- Illegal gambling
- Illegal gaming
- Illegal interception
- Image based abuse
- Inciting violence
- Laundering Terrorism
- Misuse of devices
- Money muling
- Phishing
- Political interference
- Pornographic material
- Radicalisation
- Ransomware
- Sex tourism
- Sex trade
- Sex trafficking
- Sexting
- Sextortion
- Spam
- Stalking
- System interference
- Trademark related offenses
- Trolling
- Xenophobia

2.2 Κυβερνο-έγκλημα

Η έννοια του κυβερνο-εγκλήματος έχει εισαχθεί στην καθημερινότητα μας κατά τα πρόσφατα έτη. Σύμφωνα με τον Antony Reyes, ως κυβερνο-έγκλημα θα ήταν δυνατόν να ορισθεί «το

[32] Rutger Leukfeldt and Thomas J. Hollt , The Human Factor of Cybercrime, 2020 publised by Routledge, page 5-15

έγκλημα για το όποιο ο δράστης χρησιμοποιεί ειδικές γνώσεις γύρω από τον κυβερνοχώρο»[33]. Ο ίδιος ο συγγραφέας διαχωρίζει το κυβερνο-έγκλημα από το ηλεκτρονικό έγκλημα αποδίδοντας στο δεύτερο τον ορισμό ότι πρόκειται για «*το έγκλημα στο όποιο ο δράστης χρησιμοποιεί ειδικές γνώσεις γύρω από την τεχνολογία των υπολογιστών*». Η διαφορά έγκειται στο ότι ο κυβερνοχώρος αποτελεί ευρύτερη έννοια από την τεχνολογία των υπολογιστών.

Είναι χαρακτηριστικό να τονισθεί ότι το κυβερνο-έγκλημα απασχόλησε έντονα τις αρμόδιες αρχές της Μεγάλης Βρετανίας και ειδικότερα την δεκαετία του 80΄s όπου ανεξάρτητες επιτροπές διενήργησαν έρευνες προκειμένου να εκτιμηθεί η έκταση των εγκλημάτων που συμπεριλαμβάνουν ηλεκτρονικούς υπολογιστές σε όλες τις εκφάνσεις του δημόσιου ή ιδιωτικού βίου της τότε κοινωνίας. Στα αποτελέσματα των ερευνών το 1981, τα μοναδικά είδη εγκλημάτων που εμφανιζόταν ήταν η απάτη και η κλοπή, ενώ μετά από 17 έτη, το 1998, το μερίδιο αυτό είχε αυξηθεί σημαντικά, δεδομένου ότι είχαν κάνει την εμφάνισή τους και πρόσθετα είδη εγκλημάτων.

2.3 Χαρακτηριστικά του εγκλήματος στον Κυβερνοχώρο.

Το ηλεκτρονικό έγκλημα αποτελεί την πιο διαδεδομένη μορφή εγκλήματος στον ολόκληρο τον κόσμο. Μπορεί να οριστεί με πολλαπλούς τρόπους, όπως η σκόπιμη εκμετάλλευση δικτύων υπολογιστών, συστημάτων και επιχειρήσεων που εξαρτώνται από την τεχνολογία για παράνομους σκοπούς. Υπάρχουν διάφοροι τύποι εγκλήματος στον κυβερνοχώρο όπως ενδεικτικά η χρήση κακόβουλου κώδικα για την τροποποίηση δεδομένων, η απόκτηση μη εξουσιοδοτημένης πρόσβασης κ.λπ..

Τα εγκλήματα που διαπράττονται εντός του κυβερνοχώρου μπορούν να διακριθούν σε τρεις μεγάλες κατηγορίες[34]:

- **Εγκλήματα κατά ατόμων (against individuals)**: Είναι τα εγκλήματα όπου ο στόχος είναι μεμονωμένα άτομα. Τα εγκλήματα αυτά συμπεριλαμβάνουν τη διάδοση κακόβουλων ή παράνομων πληροφοριών μέσω Διαδικτύου και ψηφιακών εφαρμογών, τις απάτες, τους εκβιασμούς κ.λπ. Παραδείγματα μπορούμε να αναφέρουμε την διαδικτυακή εκμετάλλευση παιδιών, την παράνομη διανομή πορνογραφίας, το phishing.
- **Εγκλήματα κατά της περιουσίας**: Πρόκειται για τα εγκλήματα στον κυβερνοχώρο κατά κάθε μορφής ιδιοκτησίας. Αυτή η κατηγορία σχετίζεται συνήθως με χρηματοπιστωτικά ιδρύματα και εταιρείες ή έχει ως σκοπό τη διάπραξη οικονομικών εγκλημάτων. Αυτά τα εγκλήματα περιλαμβάνουν βανδαλισμό (διατάραξη της λειτουργίας) ηλεκτρονικών υπολογιστών, εγκλήματα πνευματικής ιδιοκτησίας, απειλές, παραβίαση δεδομένων, κ.ο.κ.

[33] Antony Reyes, Cyber Crime Investigations Bridging the Gaps Between Security Professionals, Law Enforcement and Prosecutors, 1st Edn, Rockland, Syngress. 2007 page 2-25

[34] Crimes in cyberspace: A threat to human rights & national security, Article, 28/04/2023, Columbia University Libraries

- **Κρατικά**: Πρόκειται για τα εγκλήματα στον κυβερνοχώρο κατά κρατικών οργανισμών και κρατών. Η κυβερνοτρομοκρατία (cyber-terrorism) είναι ένα παράδειγμα εγκλήματος αυτού του είδους. Άτομα και ομάδες χρησιμοποιούν τον κυβερνοχώρο για να πιέσουν κυβερνήσεις και διεθνείς οργανισμούς, καθώς και να τρομοκρατήσουν τους πολίτες μιας χώρας.

Υπάρχουν και πρόσθετοι τύποι κυβερνο-εγκλημάτων, όπως το έγκλημα στο MetaVerse (π.χ. η περίπτωση του ομαδικού βιασμού στο MetaVerse[35] ή της εικονικής δημοπρασίας μουσουλμάνων γυναικών[36]). Μολονότι και οι δύο αυτές περιπτώσεις προσβάλλουν δικαιώματα ατόμων, έχουν ιδιαίτερα χαρακτηριστικά όπως π.χ. το θρήσκευμα των θυμάτων, και έτσι χρήζουν ιδιαίτερης προσέγγισης και μέριμνας.

Στον χώρο του κυβερνοεγκλήματος μπορούμε να εντοπίσουμε ένα πλήθος χαρακτηριστικών τα οποία αυξάνουν τη δυσχέρεια της ποινικής του δίωξης σε σύγκριση με τα «συμβατικά» εγκλήματα :

- **Ταχύτητα**: Οι εγκληματικές πράξεις διαπράττονται σε πολύ σύντομο χρόνο και σε πολλές περιπτώσεις δεν γίνονται άμεσα αντιληπτές από τα θύματα.
- **Ευκολία**: Οι εγκληματικές πράξεις διαπράττονται συγκριτικά με μεγαλύτερη ευκολία και πραγματοποιούνται από τον Η/Υ του δράστη, σε οικείο προς αυτόν χώρο (π.χ. από το σπίτι του).
- **Ανωνυμία**: Οι εγκληματικές πράξεις διαπράττονται υπό τη σκέπη της σχετικής ανωνυμία, που προσφέρεται από τεχνολογίες αλλά και κανονιστικά πλαίσια του διαδικτύου.
- **Διασυνοριακός χαρακτήρας**: Διαφορετικές ενέργειες της ίδιας εγκληματικής πράξης μπορούν να εκτελούνται σε διαφορετικές χώρες, με αποτέλεσμα να μην υπάρχει συγκεκριμένη δωσιδικία για το σύνολο της πράξης και η διερεύνηση να απαιτεί τη χρονοβόρα και διαδικαστικά επίπονη συνεργασία αρχών διαφορετικών κρατών.
- **Δυσχέρεια στη διερεύνηση**: Η διασυνοριακή διάσταση αλλά και η δυνατότητα παραποίησης ή καταστροφής των ψηφιακών ιχνών του εγκλήματος στον κυβερνοχώρο εισάγουν δυσχέρειες στη διερεύνηση και εξιχνίαση του. Η διερεύνηση από τις αστυνομικές αρχές παρουσιάζει αυξημένα επίπεδα δυσκολίας, προϋποθέτει δε εξαιρετικά επίπεδα εκπαίδευσης και γνώσεις υψηλής εξειδίκευσης. Η ύπαρξη γνώσεων υψηλής εξειδίκευσης απαιτείται επίσης και από έτερους συντελεστές της διερεύνησης και δίωξης της συγκεκριμένης μορφής εγκλήματος (εισαγγελείς, δικαστές, δικηγόρους).
- **Συχνή ανάγκη διακρατικής συνεργασίας**: Λόγω της διασυνοριακής φύσης του κυβερνοεγκλήματος, απαιτείται η συνεργασία διωκτικών αρχών από πολλαπλά κράτη.
- **Έλλειψη επαρκούς καταγραφής**: Αποτελεί κοινή πεποίθηση ότι το πλήθος και η βαρύτητα των κυβερνοεγκλημάτων που τελούνται είναι σημαντικά μεγαλύτερο των

[35]Can virtual gang rape occur in the Metaverse? UK police launch investigation, Article in THE ECONOMIC TIMES NEWS, 03/01/2024

[36] en.wikipedia.org/wiki/Bulli_Bai_case

περιστατικών που αναφέρονται και καταγράφονται. Σε αυτή την κατεύθυνση συντελεί το γεγονός ότι μερικά κυβερνοεγκλήματα θα μείνουν απαρατήρητα για μεγάλο χρονικό διάστημα, καθώς και το γεγονός ότι είναι πιθανό οι απώλειες να μην συσχετιστούν με τεχνολογικές ενέργειες, κάτι που ιδίως ισχύει σε περιπτώσεις θυμάτων με χαμηλή εξειδίκευση σε τεχνολογικό επίπεδο.

- **Η διάπραξή του δεν απαιτεί να μετακινηθεί φυσικά ο δράστης**, ο οποίος εκτελεί τις έκνομες ενέργειες από τον χώρο (ενδεικτικά) του γραφείου ή του σπιτιού του, διά μέσω του υπολογιστή του και -ενδεχομένως- χρησιμοποιώντας αυτοματοποιημένα εργαλεία.
- **Δυσκολία στην καταγγελία.** Ελάχιστες περιπτώσεις εγκλημάτων του κυβερνοχώρου καταγγέλλονται. Ένας από τους λόγους που συμβάλλουν στα περιορισμένα ποσοστά καταγγελιών, είναι η διατήρηση του επιπέδου φήμης και αξιοπιστίας των θυμάτων, τα οποία συνήθως είναι εταιρείες. Ως αποτέλεσμα, για την εγκληματικότητα στον χώρο του διαδικτύου τυγχάνει εφαρμογής η «θεωρία του παγόβουνου», σύμφωνα με την οποία μέρος του προβλήματος είναι ορατό ενώ ένα το υπόλοιπο και μεγαλύτερο σε ποσοστό δεν το «βλέπουμε».

2.4 Τυπολογία εγκλημάτων στον Κυβερνοχώρο

Τα εγκλήματα στη Νομική Επιστήμη διακρίνονται σε μείζονες κατηγορίες, ανάλογα με κάποια κοινά χαρακτηριστικά. Η διάκριση αυτή γίνεται στη χώρα μας στον Ποινικό Κώδικα, στον οποίο κατηγοριοποιούνται τα εγκλήματα που διαπράττονται στο διαδίκτυο ή μέσω αυτού. Μια βασική κατηγοριοποίηση είναι να τα διακρίνουμε αυτά **σε γνήσια και μη γνήσια εγκλήματα.**

- **Ως γνήσια εγκλήματα** αναφέρονται τα εγκλήματα, τα οποία προσβάλουν τα συστήματα υπολογιστών και δεδομένα αυτών. Στην κατηγορία των εγκλημάτων μπορούμε να εντάξουμε ενδεικτικά τα εγκλήματα που προβλέπονται στον Ποινικό Κώδικα και είναι αυτά της παρακώλυσης λειτουργίας πληροφοριακών συστημάτων (Άρθρο 292Β Ποινικού Κώδικα), της παράνομης πρόσβασης σε πληροφοριακό σύστημα (Άρθρο 370Γ Ποινικού Κώδικα), των απατών σε υπολογιστή (Άρθρο 386Α Ποινικού Κώδικα).
- **Ως μη γνήσια εγκλήματα** είναι τα εγκλήματα που διαπράττονται στο διαδίκτυο και ειδικότερα σε αυτά που τελούνται οι κλασικές μορφές εγκλημάτων που περιγράφονται στον Ποινικό Κώδικα, όπως η απειλή, η εξύβριση, η δυσφήμιση, κ.ά. Στα μη γνήσια εγκλήματα η αντικειμενική υπόσταση του δεν σχετίζεται άμεσα με την ηλεκτρονική διάσταση[37].

Τα μη γνήσια εγκλήματα στο κλάδο της πληροφορικής χωρίζονται σε τρεις κατηγορίες, σύμφωνα με την Σύμβαση της Βουδαπέστης το 2001:

[37] ΓΕΡΜΑΝΟΣ ΓΕΩΡΓΙΟΣ, ΓΕΩΡΓΙΟΥ ΝΙΚΟΛΑΟΣ, Κυβερνοέγκλημα- Πρόληψη, Διερεύνηση, Αντιμετώπιση, 01/2021 σελ. 71-72 επ.

Α) Στα εγκλήματα που τελούνται μέσω υπολογιστή και προσβάλλουν έννομα αγαθά τα οποία προστατεύονται από τον Ποινικό Κώδικα, όπως για παράδειγμα το έγκλημα της απάτης με υπολογιστή.

Β) Στα εγκλήματα που διαπράττονται μέσω των πληροφοριακών συστημάτων, όμως η προσβολή αυτή λαμβάνει χώρα μέσω του παράνομου περιεχομένου των πληροφοριών, όπως για παράδειγμα η παιδική πορνογραφία.

Γ) Στα εγκλήματα τα οποία γίνονται μέσω των υπολογιστών και προσβάλλονται ψηφιακά δεδομένα, τα οποία ενίοτε ενσωματώνονται σε ένα ιδιαίτερο έννομο αγαθό όπως για παράδειγμα το υπόμνημα[38].

Όπως είναι γνωστό και επαναλαμβάνεται στην παρούσα, τα εγκλήματα στο διαδίκτυο «είναι ζωντανοί οργανισμοί» οι οποίοι έχουν δυναμικό χαρακτήρα και εξελίσσονται διαρκώς. Στην Εθνική Στρατηγική Κυβερνοασφάλειας 2020 - 2025 της Εθνικής Αρχής Κυβερνοασφάλειας του Υπουργείου Ψηφιακής Διακυβέρνησης[39] αναφέρονται οι τεχνολογικές εξελίξεις σε συνδυασμό με την άνοδο του βιοτικού επιπέδου των λαών της Ευρωπαϊκής Ένωσης οι οποίες έχουν ευνοήσει την αύξηση των ανωτέρω εγκλημάτων. Το συγκεκριμένο περιβάλλον είναι δυναμικό και εξελισσόμενο καθιστώντας την αποτελεσματική αντιμετώπιση του μία δύσκολη εξίσωση[40].

2.4.1 Hacking – cracking

Με τον όρο **Hacking** εννοούμε κάθε προσπάθεια, με οποιονδήποτε τρόπο κάποιος με κακόβουλα κίνητρα εισχωρεί σε υπολογιστή ή σε οποιοδήποτε πληροφοριακό σύστημα, ενώ **cracking** είναι η ίδια πρακτική με εγκληματική πρόθεση, έχοντας όμως λιγότερες συνέπειες για τον κάτοχο του υπολογιστή ή του πληροφοριακού συστήματος που γίνεται η εισβολή.

Με τον όρο **Hacker** εννοούμε τους χρήστες υπολογιστών οι οποίοι ασχολούνται με τον χώρο του διαδικτύου επαγγελματικά ή ερασιτεχνικά και οι οποίοι έχουν την δυνατότητα να παραβιάζουν συστήματα ασφάλειά τους (craker). Συνήθως πρόκειται για άτομα με εξειδικευμένη γνώση ηλεκτρονικών υπολογιστών και τους διακρίνουμε σε τρεις κατηγορίες*:* τους **black hat hackers**, τους **white hat hackers** και τους **grey hat hackers**.

- **Ως black hat hackers** νοούνται αυτοί που έχοντας ειδικές γνώσεις στους υπολογιστές ενεργούν κακόβουλα οργανώνοντας επιθέσεις DoS/DDoS και υποκλέπτοντας προσωπικά δεδομένα χρηστών.
- **Ως white hat – ethical hackers** νοούνται αυτοί που έχοντας εξειδικευμένες γνώσεις και αγαθές προθέσεις, δουλεύουν κυρίως στον ιδιωτικό τομέα σε εταιρείες σχετικές με την προστασία των δικτύων υπολογιστών.
- **Ως grey hat hackers** νοούνται οι ερασιτέχνες χρήστες υπολογιστών, με απλές γνώσεις, όπου η παραβατικότητα τους επικεντρώνεται σε χρήση παράνομου

[38] ΔΑΛΑΚΟΥΡΑ Θ,Ηλεκτρονικό έγκλημα, Νομική Βιβλιοθήκη, Θεσσαλονίκη 2019, σελ. 37

[39] Εθνική Στρατηγική Κυβερνοασφάλειας 2020 – 2025 σελ 5-8

[40] Εθνική Στρατηγική Κυβερνοασφάλειας 2020 -2025, σελ. 10

λογισμικού, κοινή χρήση ταινιών, χρήση συνδρομητικής τηλεόρασης χωρίς πληρωμή κ.ά.

2.4.2 Malware

Με τον όρο malware ή πιο αναλυτικά Malicious software αναφερόμαστε σε προγράμματα που χρησιμοποιείται για να βλάψουν συστήματα υπολογιστών, να αποκτήσουν πρόσβαση σε ευαίσθητες πληροφορίες και να τις υποκλέψουν ή να εμπλακούν σε διάφορες μορφές εγκλήματος στον κυβερνοχώρο. Τέτοια προγράμματα χαρακτηριστικά και ευρέως γνωστά είναι οι ιοί (viruses), τα σκουλήκια (worms), οι δούρειοι ίπποι (trojan horses)[41].

2.4.3 Spamming

Με τον γνωστό όρο **«Spam»** εννοούμε την μαζική αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου (email), τα οποία ως αποστολέας φαίνεται ψευδώς, με απατηλά μέσα, να είναι τραπεζικό ίδρυμα, υπηρεσία του κράτους ή εταιρείες ταχυμεταφορών και σκοπό έχουν να εξαπατήσουν τον παραλήπτη υποκλέπτοντας του στοιχεία ικανά να του προκαλέσουν οικονομική απώλεια.

2.4.4 Phishing

Με τον όρο «phishing» αναφερόμαστε στα μηνύματα ηλεκτρονικού ταχυδρομείου απατηλού χαρακτήρα, των οποίων στόχος είναι η εξαπάτηση των παραληπτών τους με τρόπο που θα οδηγήσει να αποκαλυφθούν στους δράστες / απατεώνες πληροφορίες προσωπικού ή οικονομικού χαρακτήρα των θυμάτων ή/και συνθηματικά / διαπιστευτήρια σύνδεσης (passwords/login credentials). Συνήθως οι δράστες δημιουργούν μηνύματα ηλεκτρονικού ταχυδρομείου που προσιδιάζουν με εκείνα που αποστέλλονται από νομότυπους οργανισμούς (όπως για παράδειγμα τράπεζες, πάροχοι υπηρεσιών ηλεκτρονικού ταχυδρομείου κ.λπ.) στους πελάτες τους. Στα απατηλά μηνύματα υπάρχει πεδίο εισαγωγής κωδικών πρόσβασης στις νομότυπες υπηρεσίες, ωστόσο εάν τα υποψήφια θύματα εισάγουν τους κωδικούς πρόσβασης στα πεδία αυτά, οι κωδικοί θα κοινοποιηθούν αυτόματα στους δράστες. Συνήθως χρησιμοποιείται ορολογία που δίνει την αίσθηση του έκτακτου ή του κατεπείγοντος για να προκληθεί η άμεση αντίδραση / ενέργεια του θύματος, σε μία προσπάθεια μείωσης του περιθωρίου ψύχραιμης σκέψης που θα οδηγούσε στην αποκάλυψη της απάτης.

2.4.5 Διαδικτυακός εκφοβισμός

Με τον όρο εκφοβισμός, ως ελεύθερη μετάφραση του όρου «bullying», χαρακτηρίζεται γενικά η συμπεριφορά ενός ή περισσοτέρων ατόμων που σκοπό έχουν να προσβάλλουν ένα άτομο, το θύμα, με επαναλαμβανόμενο, εκφοβιστικό, ρατσιστικό ή προσβλητικό τρόπο, έτσι ώστε να προκαλέσουν κυρίως συναισθηματική και ψυχολογική βλάβη, αλλά και σωματική. Όταν ο εκφοβισμός αυτός γίνεται μέσω ηλεκτρονικών και ψηφιακών μέσων τότε τον

[41] Thomas Holt, Adam Bossler, Kathryn Seigfried-Spellar, 2022, 3rd edition, publish Routledge

ονομάζουμε **διαδικτυακό εκφοβισμό «cyberbullying»**. Πλέον κάθε μορφή τέτοιων φαινομένων στην Ελλάδα διώκεται ποινικά, σύμφωνα με όσα ορίζει ο Ποινικός Κώδικας[42].

Ο διαδικτυακός εκφοβισμός μπορεί ενδεικτικά να πραγματοποιηθεί με τους κάτωθι τρόπους:

- Μηνυμάτων υβριστικού περιεχομένου (Flaming),
- Παρενόχληση,
- Διαδικτυακή Καταδιώξη (Cyberstalking),
- Δυσφήμηση (Denigration - Put-downs),
- Μεταμφίεση (Masquerade)
- Οικειοποίηση (Impersonation),
- Διασυρμός (Outing),
- Λήψη Οπτικού υλικού (Happy slapping),
- Φυλετικές Διακρίσεις,
- Email
- Social Media
- Online παιχνίδι.

Στον διαδικτυακό εκφοβισμό ο δράστης νομίζει φαινομενικά ότι λειτουργεί ανώνυμα χρησιμοποιώντας ψεύτικα στοιχεία. Με αυτόν τον τρόπο ο δράστης έχει υψηλότερα επίπεδα άρσης αναστολών, έχοντας την ψευδή αίσθηση ότι είναι άτρωτος, προκαλώντας έτσι μεγαλύτερη έντασης συνεπειών στο θύμα ή στα ΄θύματα του. Καλό είναι να ααναφερθεί ότι ο εκφοβισμός γενικότερα εμπλέκει τους παρατηρητές ως θύτες. Είναι σημαντικό να συνειδητοποιηθεί ότι οι θεατές δεν πρέπει να είναι αμέτοχοι στις προσπάθεια καταπολέμησης του φαινομένου αυτού, που τον τελευταίο καιρό έχει πάρει διαστάσεις ειδικότερα σε μικρές ηλικίες.

2.4.6 Παιδική πορνογραφία

Το ζήτημα της παιδικής εκμετάλλευσης υφίσταται από την αρχαιότητα, ενώ αντίστοιχα δίκτυα παραβατών είχαν διαμορφωθεί και είχαν εγκαθιδρύσει διαύλους επικοινωνίας πριν την εισαγωγή των υπολογιστών και του Διαδικτύου. Με τον όρο παιδική πορνογραφία νοείται η κάθε είδους και με οιοδήποτε μέσο αντιπροσώπευση ενός παιδιού σε οπτικοακουστικά μέσα όπου το παρουσιάζουν να λαμβάνει μέρος σεξουαλικές δραστηριότητες που τελούνται πραγματικά ή προσομοιώνονται. Επίσης στην παιδική πορνογραφία εμπίπτει η οποιαδήποτε αντιπροσώπευση των σεξουαλικών τμημάτων του σώματος ενός παιδιού, η οποία πραγματοποιείται με κύριο στόχο τη σεξουαλική αναφορά[43].

Ως υλικό παιδικής πορνογραφίας ορίζεται κάθε είδους αναπαράσταση ή περιγραφή, τόσο πραγματική όσο και εικονική, ανεξαρτήτως υλικού φορέα στον οποίο έχει αποτυπωθεί μέρος

[42] Ποινικός Κώδικας Άρθρο 312

[43] Ορισμός παιδικής πορνογραφίας, Όμιλος Νομικών ΠΡΟΒΑΤΑ Σωκράτη, Επίσημη Ιστοσελίδα, Ανάρτηση Μάϊος 2019

ή όλο το σώμα του ανηλίκου και έχει ως στόχο τη γενετήσια διέγερση. Στον ορισμό του υλικού παιδικής πορνογραφίας περιλαμβάνεται επίσης η καταγραφή ή αποτύπωση, ανεξαρτήτως υλικού φορέα, μίας ασελγούς πράξης, που είτε τελείται στην πραγματικότητα, είτε προσποιητά και η οποία ενεργείται με στόχο τη γενετήσια διέγερση και στην οποία λαμβάνει μέρος ανήλικος. Σύμφωνα με το άρθρο 348Α του Ποινικού Κώδικα και εστιάζοντας στην πρώτη παράγραφο αυτού, το έγκλημα της πορνογραφίας ανηλίκων διαπράττεται από αυτόν «*που εκ προθέσεως συμμετέχει στις παρακάτω πράξεις, δηλαδή στην παραγωγή, διανομή, δημοσίευση, επίδειξη, εισαγωγή στην Επικράτεια ή εξαγωγή από αυτήν, μεταφορά, προσφορά, πώληση ή με οιονδήποτε τρόπο διάθεση, αγορά, προμήθεια, απόκτηση ή κατοχή υλικού παιδικής πορνογραφίας ή συμμετέχει με οιονδήποτε τρόπο στη διάδοση ή μετάδοση πληροφοριών σχετικά με την τέλεση των παραπάνω πράξεων»*[44]. Θα εστιάσουμε εδώ ενδεικτικά στην λέξη "κατέχει" ερμηνεύοντας ότι και μόνο για παράδειγμα η ύπαρξη τέτοιου υλικού στην μνήμη ενός υπολογιστή ή κινητού είναι ποινικό αδίκημα. Με βάση τις διατάξεις του άρθρου 121 Π.Κ., ως ανήλικος νοείται κάθε πρόσωπο ηλικίας μικρότερο των 18 ετών.
Σύμφωνα με τη Σύμβαση του Συμβουλίου της Ευρώπης για τα Διαδικτυακά Εγκλήματα, καταγράφονται οι εξής μορφές παιδικής πορνογραφίας[45, 46]:

- Η συμμετοχή ανηλίκου σε δραστηριότητες σεξουαλικής φύσεως / περιεχομένου.
- Η συμμετοχή ατόμου, το οποίο παρουσιάζεται ως ανήλικο, ανεξαρτήτως της πραγματικής του ηλικίας, σε δραστηριότητες σεξουαλικής φύσεως / περιεχομένου.
- Οι εικόνες, που αναπαριστούν ένα ανήλικο άτομο να λαμβάνει μέρος σε δραστηριότητες σεξουαλικού περιεχομένου.

2.4.7 Οικονομικό έγκλημα

Κατά την τελευταία περίοδο, η εξέλιξη της τεχνολογίας και της πληροφορικής, έχει μετακινήσει ένα σημαντικό μέρος της ζωής μας και των δραστηριοτήτων μας από τον φυσικό κόσμο στις οθόνες των κινητών, tablet, και ηλεκτρονικών υπολογιστών, μετασχηματίζοντας μεταξύ άλλων τις οικονομικές συναλλαγές πάσης φύσεως, αλλά παράλληλα προσαρμόστηκε και το έγκλημα στην εξέλιξη αυτή. **Ως οικονομικό έγκλημα δύναται να οριστεί ως η αξιόποινη πράξη που, διά μέσω της εκμετάλλευσης δυνατοτήτων και χαρακτηριστικών του οικονομικού συστήματος, αποβλέπει στο οικονομικό κέρδος των δραστών, προσβάλλοντας τους κανόνες που διέπουν την οικονομία** .

Το οικονομικό έγκλημα διαφοροποιείται από το έγκλημα με οικονομικό μόνον περιεχόμενο ή με κάποια οικονομική σημασία, όπως συμβαίνει με την κατηγορία των εγκλημάτων που στρέφονται κατά της ιδιοκτησίας ή κατά περιουσιακών δικαιωμάτων, όπως επίσης διαφοροποιείται και από τα εγκλήματα τα οποία μολονότι δεν έχουν οικονομική διάσταση, συνήθως μέσω αυτών βλάπτεται άλλο έννομο αγαθό το οποίο έχει τέτοιο περιεχόμενο. Σε επίπεδο Ευρωπαϊκής Ένωσης, ήδη από το 1981 η Επιτροπή Υπουργών της τότε Ε.Ο.Κ.

[44] Ποινικός Κώδικας Άρθρο 348Α

[45] Παιδική Σεξουαλική Κακοποίηση μέσω Διαδικτύου, Ανάρτηση της Υποδιεύθυνση Ηλεκτρονικού Εγκλήματος – Τμήμα Καταπολέμησης Εγκλήματος Αστυνομίας Κύπρου, Επίσημη Ιστοσελίδα

[46] ΔΑΛΑΚΟΥΡΑ Θ, Ηλεκτρονικό έγκλημα, Νομική Βιβλιοθήκη, Θεσσαλονίκη 2023

υιοθέτησε σύσταση για την οικονομική εγκληματικότητα, στην οποία, αναγνωριζόταν η δυσκολία να διατυπωθεί ένας ορισμός που θα περιέγραφε με πλήρη ακρίβεια το οικονομικό έγκλημα. Η δυσκολία αυτή οφείλεται στην αδυναμία να καλυφθεί η επινοητικότητα των δραστών του οικονομικού εγκλήματος, η οποίοι αξιοποιώντας τις δυνατότητες της διαρκώς εξελισσόμενης τεχνολογίας διαμορφώνουν διαρκώς καινοφανείς μεθόδους και τεχνάσματα για τη διάπραξη εγκλημάτων.

Η φαινομενική ανωνυμία, η αμεσότητα και ταχύτητα των επικοινωνιών που προσφέρει το διαδίκτυο, αξιοποιούνται από τους παραβατικούς προκειμένου να αναπτύξουν νέες μορφές εγκληματικότητας (π.χ. phishing), να διευρύνουν ήδη υπάρχουσες μορφές (όπως τις ηλεκτρονικές απάτες / κλοπές) και να διοχετεύσουν με μεγαλύτερη ευκολία τα έσοδα τους από τις παράνομες δραστηριότητες αυτές.

Επιπρόσθετα μια μορφή οικονομικού εγκλήματος, η οποία ανθεί στο διαδίκτυο είναι το ξέπλυμα χρήματος, δηλαδή όπως αποκαλούμε με νομικούς όρους, η νομιμοποίηση εσόδων από παράνομες οικονομικές δραστηριότητες. Τόσο όλες οι μορφές του οργανωμένου εγκλήματος αλλά και η τρομοκρατία χρησιμοποιούν κοινές μεθόδους για τις οικονομικές δράσεις και την αποφυγή εντοπισμού από τις αρχές. Για αυτόν τον λόγο, χρησιμοποιώντας πολύπλοκες και σύνθετες διαδικασίες μεταφοράς κεφαλαίων μεταξύ προσώπων σε διαφορετικά κράτη, ξεπερνώντας ελέγχους και νομικές δυσκολίες λόγω της διασυνοριακού χαρακτήρα αυτού του εγκλήματος, εξασφαλίζουν και ασφαλίζουν τα έσοδα τους από τις παράνομες δραστηριότητες, οι οποίες είναι ζωτικής σημασίας για την επιβίωσή τους και τη συνέχιση της παράνομης δράσης τους. Σε αυτό βοηθάει κατά πολύ ο τομέας της πληροφορικής και του διαδικτύου, τον οποίο εκμεταλλεύεται το οργανωμένο έγκλημα και οι τρομοκράτες για να νομιμοποιήσουν τα έσοδα τους[47]. Το ξέπλυμα χρήματος πραγματοποιείται σε τρεις φάσεις, οι οποίες είναι[48]:

1. Τοποθέτηση (placement)
2. Διαστρωμάτωση (layering)
3. Ενσωμάτωση (integration)
   3.1 Δικαιολόγηση (justification)
   3.2 Επένδυση (investment)

[47] Convention on Cybercrime Wikipedia

[48] United States Joint Forces Command, The Join Operating Enviromnet, Report, 18/02/2010

3 ΨΗΦΙΑΚΗ ΕΓΚΛΗΜΑΤΟΛΟΓΙΑ

3.1 Ιστορική αναδρομή

Μέχρι την δεκαετία του 1970, η ποινική αντιμετώπιση των εγκλημάτων που διαπράχθηκαν μέσω υπολογιστών ή εις βάρος αυτών έγινε με βάση τους νόμους που ίσχυαν για τα κοινά εγκλήματα επειδή η ανάπτυξη της πληροφορικής ήταν σαφώς μικρή και περιορισμένη και το πλήθος των εγκλημάτων δεν σχετιζόταν με τον τομέα αυτόν και ευρύτερα με τη χρήση ηλεκτρονικών υπολογιστών. Η πρώτη ποινική καταγραφή με τον όρο εγκλήματα πληροφορικής[49] πραγματοποιήθηκε με νόμο το 1978 για τα αδικήματα συστημάτων ηλεκτρονικών υπολογιστών, στην πολιτεία της Φλόριντα των Η.Π.Α. (Florida Computer Crimes Act)[50]. Ειδικότερα έγινε αναφορά σε νομικό κείμενο που παρήγαγε έννομα αποτελέσματα εις βάρος της άνευ εξουσιοδότησης τροποποίησης ή διαγραφής δεδομένων από ηλεκτρονικούς υπολογιστές. Τα επόμενα χρόνια διευρύνθηκε το εύρος των εγκλημάτων που εντάσσονταν στο τομέα της πληροφορικής και των ηλεκτρονικών υπολογιστών ένεκα της αύξησης χρήσης αυτών σε όλο το φάσμα της δημόσιας και ιδιωτικής ζωής. Άρχισαν ένεκα αυτών, να εντάσσονται νομικές έννοιες σχετικές με την πληροφορική όπως ενδεικτικά την αντιμετώπιση θεμάτων πνευματικής ιδιοκτησίας, την προστασίας της ιδιωτικής ζωής, την προστασίας των δεδομένων των υπολογιστών, έννοιες του απορρήτου.

Ο Καναδάς ήταν η πρώτη χώρα που ψήφισε σχετική νομοθεσία το 1983 σχετικά με νομικές έννοιες για την χρήση ηλεκτρονικών υπολογιστών, εν συνεχεία οι Η.Π.Α. το 1986 ενέταξε στην Ομοσπονδιακή Νομοθεσία την έννοια της απάτης μέσω υπολογιστών, το 1989 η Αυστραλία όρισε την έννοια των εγκλημάτων μέσω υπολογιστών και το 1990 η Βρετανία όρισε νομικά την έννοια της κατάχρησης των ηλεκτρονικών υπολογιστών[51].

Παράλληλα με τις νομοθετικές πρωτοβουλίες στο χώρο της Δικαιοσύνης, οι Αστυνομικές αρχές άρχισαν να αντιμετωπίζουν και αυτές την νέα μορφή εγκλήματος που εντάχθηκε στις κοινωνίες και με σκοπό την πρόληψη, κατανόηση και καταστολή του ιδρύοντας εξειδικευμένες ομάδες Αστυνομικών και εντάσσοντας στις εκπαιδεύσεις εγκλήματα αναφορικά με τους ηλεκτρονικούς υπολογιστές. Το 1984 η Η.Π.Α. με την πιο διακεκριμένη υπηρεσία σε ομοσπονδιακό επίπεδο, το F.B.I., ίδρυσε ειδική ομάδα σχετική με τα εγκλήματα των υπολογιστών με την επωνυμία Computer Analysis and Response Team, ενώ το 1985 στην Βρετανία οι Αστυνομικές Αρχές και ειδικότερα η Μητροπολιτική Αστυνομία δημιουργήσαν ειδικό τμήμα Ηλεκτρονικού Εγκλήματος εξειδικευμένο στις απάτες.

Τον Ιούνιο του 1992 χρησιμοποιήθηκε στην ακαδημαϊκή βιβλιογραφία ο όρος **Εγκληματολογία Υπολογιστών** (Computer Forensics) από τους από τους P.A. Collier και B.J. Spaul αναφορικά με τα εγκλήματα που διαπράττονται με τους ηλεκτρονικούς υπολογιστές στο Ηνωμένο Βασίλειο δίνοντας μια πιο επιστημονική προσέγγισή στο νέο κλάδο αυτό της

[49] Ηλεκτρονικό έγκλημα, Wikipedia

[50] Patrick L. Imhof Edwin A. Levine, Impact of the Information Age on Access and Dissemination of Government Information in Florida, Article, Florida State University Law Review, 1986

[51] Computer Misuse Act, UK Public General Act, 1990

εγκληματολογίας πλέον και εισάγοντας έννοιες όπως ανασύνθεση αποδεικτικών στοιχείων και τεχνικές διατήρησης αυτών[52]. Το 1995 ο K. S .Rosenblatt στο βιβλίο του με τίτλο High – Technology Crime: Investigating Cases Involving Computers[53] που εκδόθηκε στις Η.Π.Α. αναφέρει σχετικά:

> *«Η λήψη, η διατήρηση και η ανάλυση πειστηρίων, τα οποία βρίσκονται αποθηκευμένα σε ένα σύστημα ηλεκτρονικού υπολογιστή είναι η μεγαλύτερη εγκληματολογική πρόκληση που αντιμετωπίζει η επιβολή του νόμου κατά τη δεκαετία του 1990. Αν και οι περισσότερες εγκληματολογικές εξετάσεις, όπως η αποτύπωση δακτυλικών αποτυπωμάτων και το τεστ DNA, εκτελούνται από ειδικευμένο και κατάλληλα εξουσιοδοτημένο προσωπικό, το καθήκον της συλλογής και ανάλυσης στοιχείων από συστήματα ηλεκτρονικών υπολογιστών ανατίθεται συχνά σε αξιωματικούς περιπολιών και ερευνητές της αστυνομίας»*[54]

Επιπλέον το 2004 το Συμβούλιο της Ευρώπης σε ψήφισμα του με την ονομασία η Σύμβαση για την εγκληματικότητα στον Κυβερνοχώρο[55], κατάφερε, ως μια πρώτη προσπάθεια, την ενοποίηση της νομοθεσίας των κρατών για την πρόληψη και αντιμετώπιση της νέας μορφής αυτής εγκληματικότητας και την συνεργασία μεταξύ αυτών, απαραίτητη προϋπόθεση για την καταπολέμηση του. Η συνθήκη υπογράφηκε από 43 κράτη, εκτός των κρατών της Ευρωπαϊκής Ένωσης, υπέγραψαν και οι Η.Π.Α., ο Καναδάς, η Ιαπωνία, η Νότια Αφρική, το Ηνωμένου Βασίλειο.

Με την ανάπτυξη της Ψηφιακής Εγκληματολογίας, αναπτύχθηκαν από τα κράτη και τις υπηρεσίες ασφάλειας αυτών, σχετικές δομές για την καταπολέμηση του κυβερνοεγκλήματος. Επιπρόσθετα, και ο ιδιωτικός τομέας και οι τομείς του εμπορίου και των υπηρεσιών έδωσαν ιδιαίτερη προσοχή στον τομέα της κατάρτισης. Εμπορικές εταιρείες άρχισαν να προσφέρουν σειρές μαθημάτων και πιστοποιήσεις πάνω στο αντικείμενο της Ψηφιακής Εγκληματολογίας.

Επιπλέον για λόγους Εθνικής Ασφάλειας τα κράτη ανέπτυξαν στους τομείς της άμυνας τμήματα με σκοπό την πρόληψη και καταστολή των ψηφιακών εγκλημάτων, επικεντρωμένα κυρίως στο κλάδο της κατασκοπείας και υποκλοπής δεδομένων - πληροφοριών εθνικής σημασίας. Χαρακτηριστικά μια έκθεση του Φεβρουαρίου 2010 από την Κοινή Διοίκηση Δυνάμεων του στρατού των Ηνωμένων Πολιτειών (United States Joint Forces Command)[56] κατέληξε:

> *«Μέσω του κυβερνοχώρου, οι εχθροί θα στοχεύσουν τη βιομηχανία, τον ακαδημαϊκό κόσμο, την κυβέρνηση, καθώς και τον στρατό στον αέρα, τη γη, τη ναυτιλία και το διάστημα. Με τον ίδιο τρόπο που η δύναμη της αεροπορίας*

[52] P.A. Collier, B.J. Spau, A Forensic methodology for countering computer crime,Article 1992

[53] Kenneth S. Rosenblatt, High-Technology Crime - Investigating Cases Involving Computers, 1995

[54] Kenneth S. Rosenblatt, High-Technology Crime - Investigating Cases Involving Computers, 1995

[55] Convention on Cybercrime, Wikipedia

[56] United States Joint Forces Command, The Join Operating Enviromnet, Report, 18/02/2010, pages 34–36

μετασχημάτισε το πεδίο της μάχης του Β 'Παγκοσμίου Πολέμου, ο κυβερνοχώρος έχει σπάσει τα φυσικά εμπόδια, τα οποία προστατεύουν ένα έθνος από τις επιθέσεις στο εμπόριο και την επικοινωνία του.»

3.2 Ψηφιακή Εγκληματολογία: Έννοιες - Ορισμός

Η αλματώδης αύξηση της τεχνολογίας με όρους γεωμετρικής προόδου και η ευρεία χρήση του Διαδικτύου, που έχει συντελεστεί τις τελευταίες δεκαετίες, έχει καταστήσει δυνατή την διάπραξη νέων μορφών εγκληματικών πράξεων με τη χρήση ηλεκτρονικών υπολογιστών, κινητών τηλεφώνων και του διαδικτύου γενικότερα. Ως εκ τούτου οι Αρχές Επιβολής του Νόμου, ήτοι οι Αστυνομικές και Δικαστικές Αρχές, καλούνται να προσαρμοστούν στα νέα δεδομένα που δημιουργήθηκαν και οφείλουν να αναπτύξουν κατάλληλες στρατηγικές με σκοπό την ενημέρωση, πρόληψη και καταστολή των νέων μορφών εγκληματικότητας σε ψηφιακό περιβάλλον. Μια επισήμανση σε αυτά είναι ο κατάλληλος χειρισμός των ψηφιακών τεκμηρίων και πειστηρίων κατά τη διερεύνηση τέτοιων υποθέσεων. Με τις κατάλληλες διαδικασίες και τον σωστό χειρισμό, θα καθίσταται ευχερέστερο και αξιόπιστο να αποδειχθούν τα πραγματικά περιστατικά υποθέσεων όπου εμπλέκεται η χρήση των ηλεκτρονικών υπολογιστών και της ψηφιακής τεχνολογίας και συνακόλουθα να διευκολύνεται η αναζήτηση και εύρεση της αλήθειας.

Όπως και για τα συνήθη τεκμήρια, έτσι και για τα ψηφιακά, είναι αναγκαία η εφαρμογή μιας κοινά αποδεκτής μεθοδολογίας με απώτερο σκοπό να εξασφαλιστεί η αξιοπιστία τους μέχρι τη στιγμή που αυτά θα κατατεθούν και θα αξιοποιηθούν σε μια ποινική διαδικασία, προκειμένου να έχουν πλήρη αποδεικτική αξία. Η συγκεκριμένη μεθοδολογία θα πρέπει να δομείται με τέτοιο τρόπο έτσι ώστε να αποτελείται από συγκεκριμένες διαδικασίες εξασφαλίζοντας την αξιόπιστη και σωστή συλλογή των πιεστηρίων. Ο ιδιαίτερος επιστημονικός κλάδος που μελετά το συγκεκριμένο αντικείμενο, ορίζεται ως ακολούθως[57]:

"Η επιστήμη που προσπαθεί να ανιχνεύσει αποδεικτικά στοιχεία για εγκληματικές πράξεις εξετάζοντας ψηφιακά πειστήρια και τεκμήρια όπως ηλεκτρονικούς υπολογιστές, σκληρούς δίσκους, έξυπνα κινητά τηλέφωνα και εν γένει οποιοδήποτε υπολογιστικό σύστημα ονομάζεται Ψηφιακή Εγκληματολογία (Digital Forensics)".

Ένας εναλλακτικός ορισμός που θα μπορούσε να δοθεί, είναι ότι ως Ψηφιακή Εγκληματολογία νοείται η δομημένη χαρτογράφηση διαδικασιών, με δυναμικό χαρακτήρα που στόχο έχουν τον εντοπισμό, συλλογή, ανάλυση, εξέταση και τεκμηρίωση και παρουσίαση των στοιχείων που προέρχονται από ψηφιακή πηγή, με νομική βάση, προκειμένου να συμβάλουν στη διερεύνηση ενός εγκλήματος.

[57] Ψηφιακή εγκληματολογία, Wikipedia

4 ΣΤΑΔΙΟΠΟΙΗΣΗ ΤΩΝ ΔΙΑΔΙΚΑΣΙΩΝ ΣΤΗΝ ΨΗΦΙΑΚΗ ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΗ ΕΡΕΥΝΑ

Στην παραδοσιακή εγκληματολογία, τα αποδεικτικά στοιχεία είναι αυτά που θα μπορούσαν να ταυτοποιήσουν τον εγκληματία, όπως είναι ενδεικτικά τα ίχνη από D.N.A. ή τα δακτυλικά αποτυπώματα. Αντίθετα, η ψηφιακή εγκληματολογία ασχολείται με αρχεία και δεδομένα σε ψηφιακή μορφή, που εξάγονται από ψηφιακές συσκευές. Η ψηφιακή εγκληματολογία είναι ένας ευρέως χρησιμοποιούμενος όρος, που αναφέρεται στην αναγνώριση, απόκτηση και ανάλυση ψηφιακών στοιχείων που προέρχονται τόσο από υπολογιστές, όσο και από πληθώρα άλλων μέσων όπως π.χ. έξυπνα τηλέφωνα, φορητοί υπολογιστές, συσκευές IoT και δεδομένα που είναι αποθηκευμένα στο υπολογιστικό νέφος. Στο σχετικά πρόσφατο παρελθόν, οι περισσότερες υποθέσεις στις οποίες διενεργούνταν ψηφιακή εγκληματολογική έρευνα αφορούσαν εγκληματίες που χρησιμοποιούσαν υπολογιστές, δίκτυα ή άλλη υποδομή πληροφορικής ως εργαλείο για τη διεξαγωγή διάπραξη των εγκλημάτων τους. Εκείνη την εποχή, το σύνολο των συσκευών που απαιτούσαν ανάλυση αποτελούνταν συνήθως από έναν μόνο υπολογιστή και οι περιπτώσεις που αφορούσαν ψηφιακή έρευνα ήταν σπάνιες. Ωστόσο, με την πάροδο του χρόνου οι συσκευές πλήθυναν και απέκτησαν μεγαλύτερη ποικιλομορφία (έξυπνα ρολόγια, αυτοκίνητα, έξυπνο σπίτι κ.λπ.). Πλέον υπάρχει μεγάλη πληθώρα και μεγάλη ποικιλία ψηφιακών συσκευών, με διάφορες μορφές αποθήκευσης, διαφορετικά συστήματα αρχείων, π.χ. συσκευές Διαδικτύου των πραγμάτων (Internet of Things - IoT), φορητές συσκευές (wearables), αποθήκευση στο υπολογιστικό νέφος (cloud), κ.λπ. έχοντας ως αποτέλεσμα να εισάγεται πρόσθετη πολυπλοκότητα στην ψηφιακή εγκληματολογική διαδικασία.

Η ψηφιακή εγκληματολογία είναι η επιστήμη που οφείλει εκ φύσεως για να μπορεί να είναι τα αποτελέσματα της νομικά βάσιμα, να ακολουθεί και να εφαρμόζει μεθόδους, διαδικασίες και εργαλεία με αξιόπιστο τρόπο. Η ψηφιακή εγκληματολογία επεμβαίνει σε ένα έγκλημα από την αρχική ειδοποίηση για την ύπαρξη του και ολοκληρώνεται με την καταγραφή - επεξεργασία των ευρημάτων και τη σύνταξη των σχετικών αναφορών. Η διαδικασία που ακολουθείται είναι δυναμική και με την πάροδο του χρόνου βελτιώνεται, αλλάζει και προστίθενται νέα στοιχεία ένεκα της παράλληλης εξέλιξης της νέας αυτής μορφής του εγκλήματος. Οι διαδικασίες αποτελούνται από φάσεις, οι οποίες έχουν συγκεκριμένα αντικείμενα και στόχους, διατάσσονται σε λογικές ακολουθίες και επικοινωνούν μεταξύ τους. Όσο πιο τυποποιημένη είναι η διαδικασία που θα πρέπει να ακολουθείται κατά την συλλογή των στοιχείων ενός εγκλήματος, τόσο περισσότερη αποδεικτή αξία έχουν.

Για τον σκοπό αυτό προκειμένου να ορισθούν συγκεκριμένες διαδικασίες ορίστηκαν τα βήματα αυτών προκειμένου η διερεύνηση των ψηφιακών εγκλημάτων να γίνεται με τρόπο αξιόπιστο και μεθοδικό για τα υπάρχουν τα βέλτιστα αποτελέσματα. Η διαδικασία αυτή έχει δυναμικό χαρακτήρα καθώς με τις πάροδο του χρόνου και την εξέλιξη της τεχνολογίας αυτή προσαρμόζεται στις εκάστοτε απαιτήσεις. Στις επόμενες παραγράφους συνοψίζονται αρχικά οι διάφορες φάσεις, ενώ στη συνέχεια παρουσιάζονται τα μοντέλα διαδικασιών.

4.1 Συλλογή - Κατάσχεση

Τα ψηφιακά μέσα, πριν υποβληθούν σε εξέταση από τους εμπειρογνώμονες, οφείλουν να κατασχεθούν με συγκεκριμένες διαδικασίες οι οποίες είναι απόλυτα σαφείς και εγκεκριμένες. Η κατάσχεση σε ποινικές υποθέσεις πραγματοποιείται από τους ανακριτικούς υπαλλήλους (αστυνομία κ.λπ.), οι οποίοι είναι διαθέτουν επαρκή κατάρτιση και εκπαίδευση σε τεχνικά ζητήματα, ώστε υπάρξει διασφάλιση της προστασία των αποδεικτικών στοιχείων. Οι ανακριτικοί υπάλληλοι στο πλαίσιο αυτό ακολουθούν το κείμενο πλαίσιο νομοθετικών και κανονιστικών διατάξεων καθώς και τις σχετικές υπηρεσιακές διαταγές. Όταν ολοκληρωθεί η κατάσχεση των πηγών και των επιμέρους στοιχείων, αντιγράφονται σε κατάλληλο ψηφιακό δίσκο και η αρχική μονάδα ασφαλίζεται σε κατάλληλο αποθηκευτικό χώρο, για την αποφυγή ενδεχομένων παραβιάσεων ή αλλοιώσεων.

4.2 Ανάκτηση - Ανάλυση

Η πιο σημαντική διαδικασία κατά την εξέταση των αποδεικτικών στοιχείων και ειδικότερα των ψηφιακών τεκμηρίων σε ένα έγκλημα, είναι ο τρόπος με τον οποίον αυτά θα αναζητηθούν και θα ανακτηθούν. Ειδικότερα στον ψηφιακό κόσμο, αυτή η εργασία απαιτεί εκτός από γνώσεις και συγκεκριμένες μεθοδολογίες και τεχνικές που θα πρέπει να τηρούνται απαρέγκλιτα, λόγω της ευαισθησίας των στοιχείων. Στην ανάκτηση των στοιχείων χρησιμοποιούνται διάφορες μέθοδοι, που τυπικά περιλαμβάνουν αναζήτηση λέξεων-κλειδιών ή σχετικών φράσεων στα κατασχεθέντα μέσα, προκειμένου να εντοπισθούν αντιστοιχίες. Κατόπιν αναλύεται το περιεχόμενο του ψηφιακού μέσου (σκληρού δίσκου), τόσο σε επίπεδο μαγνητικού μέσου αποθήκευσης όσο και λαμβάνοντας υπ' όψιν τη δομή του συστήματος αρχείων, προκειμένου να εντοπιστούν και να ανακτηθούν στοιχεία που τεκμηριώνουν ή αντικρούουν συγκεκριμένες υποθέσεις, καθώς και να αναδειχθούν τυχόν ίχνη προσπαθειών αλλοίωσης ή απόκρυψης δεδομένων. Σε κρίσιμα σημεία της διαδικασίας ανάκτησης-ανάλυσης πραγματοποιείται εκ νέου επαλήθευση των μέσων προκειμένου να διαπιστωθεί ότι δεν έχει υπάρξει οποιαδήποτε υποβάθμιση της κατάστασης των αποδεικτικών στοιχείων.

Στο πλαίσιο της διαδικασίας ανάκτησης-ανάλυσης, ένας ειδικός ανακριτικός υπάλληλος τυπικά διενεργεί την ανάκτηση του αποδεικτικού υλικού εφαρμόζοντας πολλαπλές μεθοδολογίες και χρησιμοποιώντας διαφορετικά εργαλεία, και επιχειρεί να ανακτήσει τυχόν διαγεγραμμένο υλικό. Ανάλογα με την έρευνα, ο στόχος της ανάκτησης μπορεί να διαφοροποιείται ως προς το είδος και τον τύπο των δεδομένων-στόχων. Τυπικά, τα δεδομένα-στόχοι περιλαμβάνουν μηνύματα ηλεκτρονικού ταχυδρομείου, αρχεία καταγραφής συνομιλιών, φωτογραφίες/εικόνες, video, ιστορικό/καταγραφές ενεργειών (συμπεριλαμβάνοντας την πλοήγηση στο διαδίκτυο), καθώς και έγγραφα διαφόρων τύπων.

4.3 Διασφάλιση Ευρημάτων

Οι ειδικοί ανακριτικοί υπάλληλοι, ιδίως σε ποινικές υποθέσεις, πρέπει να διασφαλίσουν ότι τα συμπεράσματα βασίζονται σε δεδομένα τα οποία είναι ορθά και συναφή με την υπόθεση, καθώς και στις δικές τους ειδικές γνώσεις. Επιπρόσθετα, όταν ολοκληρωθεί μια έρευνα, οι πληροφορίες αποτυπώνονται συχνά σε κατάλληλη μορφή ώστε να μπορούν να γίνουν κατανοητές και σε άτομα χωρίς ισχυρό τεχνικό υπόβαθρο. Οι αναφορές μπορεί επίσης να

περιλαμβάνουν πληροφορίες ελέγχου, πρωτόκολλα που τηρήθηκαν, τη μεθοδολογία που εφαρμόστηκε, τα εργαλεία που χρησιμοποιήθηκαν κ.λπ. Όταν ολοκληρωθούν, οι αναφορές διαβιβάζονται συνήθως στους αναθέσαντες την έρευνα, ώστε να αξιολογηθούν και να αποφασιστεί εάν θα χρησιμοποιηθούν τα αποδεικτικά στοιχεία στη συνέχεια της διαδικασίας.

4.4 Μεθοδολογία

Η πορεία μέσα στο χρόνο της ψηφιακής εγκληματολογίας και της ψηφιακής εγκληματολογικής έρευνας είναι συνυφασμένη με την εξέλιξη και πορεία των ψηφιακών εξελίξεων καθώς και με την πρόοδο του εγκλήματος και τις μορφές που θα παρουσιάσει κάθε φορά. Ως εκ τούτου η έρευνα αυτών των εγκληματών πρέπει να είναι πέρα από δυναμική και τυποποιημένη δηλαδή να ακολουθεί τα σωστά εργαλεία και να ακολουθεί συγκεκριμένες διαδικασίες. Με αυτό τον τρόπο μια τυπική μεθοδολογική προσέγγιση στον τρόπο που πρέπει να γίνεται η έρευνα στο ψηφιακό έγκλημα αποτελεί μια σειρά απαραίτητων ενεργειών, που συγκροτούν ένα μοντέλο διαδικασιών.

Τα μοντέλα διαδικασιών μπορεί να διαφέρουν σε πολυπλοκότητα, πλήθος σταδίων και βαθμό λεπτομέρειας. Για παράδειγμα εάν ένα μοντέλο είναι πολύπλοκο, δύσκολο και μη κατανοητό κάνοντας την χρήση του δύσκολη είναι σφόδρα πιθανό ότι τα αποτελέσματα που θα έχουμε δεν θα ανταποκρίνονται στην πραγματικότητα και η έρευνα που θα κάνουμε δεν θα έχει τα σωστά αποτελέσματα παρόλο τις δυνατότητες των μοντέλων που θα χρησιμοποιήσουμε, ενώ εάν είναι το μοντέλο πιο απλό θα είναι κατανοητό θα έχει λίγες δυνατότητες. Για αυτούς λόγους ένα σωστό αξιόπιστο μοντέλο διαδικασιών θα πρέπει να είναι εύχρηστο, λειτουργικό και να παρέχει δυνατότητες που θα βοηθήσουν στην έρευνα με τρόπο αποτελεσματικό. Επιπρόσθετα θα πρέπει να είναι δυναμικό και να προσαρμόζεται με την εξέλιξη των τεχνολογιών και του εγκλήματος με τέτοιο τρόπο που να βοηθά να αναβαθμίζει την έρευνα με την πάροδο του χρόνου.

Τρία χαρακτηριστικά, ενδεικτικά, που επικεντρώνονται οι ειδικοί στην ψηφιακή εγκληματολογία και έρευνα είναι:

1. Η αναβάθμιση του μοντέλου των διαδικασιών.
2. Η επιμέρους εξειδίκευση των ενεργειών με γνώμονα την συσκευή που πρέπει να εξερευνηθεί.
3. Η ανάπτυξη συγκεκριμένων μοντέλων διαδικασιών για εγκλήματα ευαίσθητά ως προς τον τρόπο δράσης, την διαχείριση των θυμάτων, στο χρόνο, όπως ενδεικτικά οι απαγωγές παιδιών.

Στο σημείο αυτό είναι χρήσιμο να αναφέρουμε ότι τα τελευταία χρόνια, η υπολογιστική νέφους (cloud computing) έχει αναδειχθεί ως μια κυρίαρχη τάση και πολλές κορυφαίες επιχειρήσεις στο χώρο της πληροφορικής και του διαδικτύου έχουν δημιουργήσει τις δικές τους υπηρεσίες που βασίζονται σε υπολογιστική νέφους. Στον τομέα της ψηφιακής εγκληματολογικής έρευνας, η μετάβαση σε ένα μοντέλο επεξεργασίας αποδεικτικών στοιχείων που βασίζεται σε υπολογιστική νέφους θα ήταν εξαιρετικά επωφελής και ήδη έχουν γίνει προκαταρκτικές προσπάθειες προς αυτή την κατεύθυνση.

4.5 Μοντέλα διαδικασιών

Παρόλο που η ψηφιακή εγκληματολογία είναι ένας σχετικά νέος ερευνητικός τομέας, έχει ήδη σημειώσει σημαντική πρόοδο. Η πρόοδος δεν εντοπίζεται μόνο στην τεχνολογική πλευρά, όπως εργαλεία συλλογής και ανάλυσης ψηφιακών στοιχείων, αλλά άπτεται επίσης και της βελτίωσης της μεθοδολογίας και των διαδικασιών. Στην ψηφιακή εγκληματολογία ένα μοντέλο διαδικασιών είναι η μεθοδολογία που χρησιμοποιείται για τη διεξαγωγή έρευνας μέσα σε ένα πλαίσιο με μια σειρά από φάσεις που καθοδηγούν μια έρευνα. Γενικά, για την ακολουθητέα διαδικασία έχουν προταθεί μοντέλα βάσει της εμπειρίας προηγούμενων εργασιών και ερευνών. Λόγω της ποικιλίας των περιπτώσεων, π.χ. κυβερνοεπιθέσεων που διεξάγονται από ειδικούς πληροφορικής, υποθέσεις με αντικείμενο αστικές διαφορές ή υποθέσεις με ποινικό περιεχόμενο, οι ειδικοί τείνουν να ακολουθούν διαφορετικές μεθόδους στην ερευνητική τους διαδικασία, ανάλογα με τα χαρακτηριστικά της υπόθεσης, το αντικείμενό της, αλλά και τις προσωπικές τους γνώσεις και εμπειρία. Μια τυπική μεθοδολογία στην ψηφιακή εγκληματολογική έρευνα αποτελείται από έναν ορισμό των σταδίων που είναι απαραίτητες για την ασφαλής διεξαγωγή της έρευνας. Όπως προαναφέρθηκε, είναι ένα πλαίσιο είναι πολύ απλοϊκό ή έχει λιγότερες φάσεις, μπορεί να μην παρέχει καθοδήγηση στη διαδικασία έρευνας, ενώ ένα πλαίσιο με περισσότερες φάσεις όπου η κάθε φάση αντιμετωπίζει με σαφή τρόπο συγκεκριμένα προβλήματα μπορεί να αποδειχθεί πιο χρήσιμο.

Μέχρι σήμερα, έχουν προταθεί πολλά μοντέλα διαδικασιών στη βιβλιογραφία. Γενικά, κάθε μοντέλο επιχειρεί να ορίσει ή να βελτιώσει την τυπική μεθοδολογία για μια συγκεκριμένη περίπτωση χρήσης και εν γένει τα μοντέλα διαδικασιών ακολουθούν, σε ευρύ πλαίσιο, μία παρόμοια προσέγγιση. Κατά τα πρώτα έτη της ψηφιακής εγκληματολογίας, η έρευνα επικεντρώθηκε στον καθορισμό της διαδικασίας της ψηφιακής εγκληματολογικής έρευνας. Πιο πρόσφατα, η έρευνα μοντέλων διαδικασιών επικεντρώνεται στην επίλυση πιο συγκεκριμένων θεμάτων και σε πιο συγκεκριμένες περιπτώσεις χρήσης ή εστίαση σε συγκεκριμένα βήματα (συλλογή αποδεικτικών στοιχείων, διατήρηση ή εξέταση, ανάλυση). Ορισμένα μοντέλα εστιάζουν σε περιπτώσεις που είναι ευαίσθητες στον χρόνο. Στις επόμενες παραγράφους περιγράφονται τα μοντέλα διαδικασιών και η εξέλιξή τους.

4.5.1 Η Εξέλιξη της Έρευνας στα Ψηφιακά Εγκληματολογικά Μοντέλα Διαδικασιών

Μέχρι σήμερα οι θεματικοί επιστήμονες της ψηφιακής εγκληματολογίας έχουν δημοσιεύσει πολυάριθμα ερευνητικά αποτελέσματα για τα Ψηφιακά Εγκληματολογικά Μοντέλα Διαδικασιών. Η έρευνα αυτή μπορεί να κατηγοριοποιηθεί σε τρεις τύπους[58]:

1. **Ο πρώτος τύπος** αποτελείται από γενικά μοντέλα και κατηγοριοποιούν από την αρχή έως το τέλος όλη την διαδικασία της ψηφιακής εγκληματολογικής έρευνας και χρονικά τοποθετούνται γύρω το 2000.
2. **Ο δεύτερος τύπος** επικεντρώνεται σε ένα συγκεκριμένο στάδιο της διαδικασίας έρευνας μιας υπόθεσης.

[58] Xiaoyu Du, Nhien - An, Le - Khac, Mark Scanlon, Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service, Paper in University College Dublin, Ireland, June 2017

3. **Ο τρίτος τύπος** καθόρισε νέα προβλήματα και διερεύνησε νέες μεθόδους ή εργαλεία για την αντιμετώπιση συγκεκριμένων προβλημάτων.

Στις επόμενες ενότητες αναπτύσσονται ζητήματα σχετικά με τους τρεις αυτούς τύπους έρευνας.

4.5.2 Πρώιμα Μοντέλα Ψηφιακής Εγκληματολογικής Διαδικασίας

Στις αρχές του 21ου αιώνα, οι επιστήμονες και οι ανακριτικοί υπάλληλοι προσπαθούσαν να ορίσουν τις πρώτες διαδικασίες αναφορικά με την ψηφιακή εγκληματολογία, την ψηφιακή εγκληματολογική διαδικασία, μέσω της δημιουργίας κάποιων αρχικών μοντέλων. Αρχικά, το φλέγον ζήτημα στην ψηφιακή εγκληματολογία ήταν ο ορισμός ενός μοντέλου διαδικασιών που θα χαρακτηριζόταν από συνέπεια και τυποποίηση. Έτσι ορίσθηκε ένα πλαίσιο που ορίζει μια ομάδα απαραίτητων βημάτων σε ένα σύνολο διαδικασιών έρευνας. Με την πάροδο του χρόνου τα μεταγενέστερα μοντέλα βελτιώνονται από τα προηγούμενα συμπεριλαμβάνοντας πρόσθετα βήματα ή/και καθορίζοντας επακριβέστερα τα βήματα.

Έτσι διαμορφώθηκαν μοντέλα όπου ενδεικτικά τα πιο σημαντικά από αυτά είναι τα ακόλουθα:

- Αφηρημένο Ψηφιακό Εγκληματολογικό Μοντέλο (Abstract Digital Forensic Model - A.D.F.M.)[59].
- Ολοκληρωμένοο Μοντέλο Ψηφιακής Έρευνας (Integrated Digital Investigation Process Model - I.D.I.P.)[60].
- Βελτιωμένο Μοντέλο Διαδικασίας Ψηφιακής Έρευνας (Enhanced Digital Investigation Process Model -E.D.I.P.)[61].
- Το μοντέλο Διαδικασιών Διαλογής στην Ψηφιακή Εγκληματολογία (Computer Forensics Field Triage Process Model - C.F.F.T.P.M.)[62].

4.5.3 Βελτίωση Μοντέλων Ψηφιακής Εγκληματολογικής Διαδικασίας

Τυπικά η ύπαρξη ενός μοναδικού μοντέλου δεν αρκεί για να ανταποκριθεί στο χειρισμό ενός ευρύ φάσματος υποθέσεων που συνήθως αντιμετωπίζουν οι αρχές επιβολής του νόμου. Ο εγκληματίας στον κυβερνοχώρο θα μπορούσε να έχει εξειδικευμένες γνώσεις ελαχιστοποιώντας τα ίχνη του ή και καταστρέφοντας τα, ώστε να μην είναι εύκολο να εντοπιστούν. Για παράδειγμα, ο εισβολέας μπορεί να διαγράψει τα αρχεία καταγραφής του συστήματος ή να τα αλλοιώσει, ή και να χρησιμοποιήσει ενδιάμεσους σταθμούς για την επίθεσή του ώστε να μην είναι ευχερής η συσχέτιση του υπολογιστή του ή της διεύθυνσης IP

[59] Reith Mark, Clint Carr, Gunsh Gregg, An Examination of Digital Forensics Models, Air Force Institute of Technology, Article 2002

[60] Carrier Brian, Spafford Eugene, Getting Physical with the Digital Investigation Process, Article in International Journal of Digital Evidence, 2003

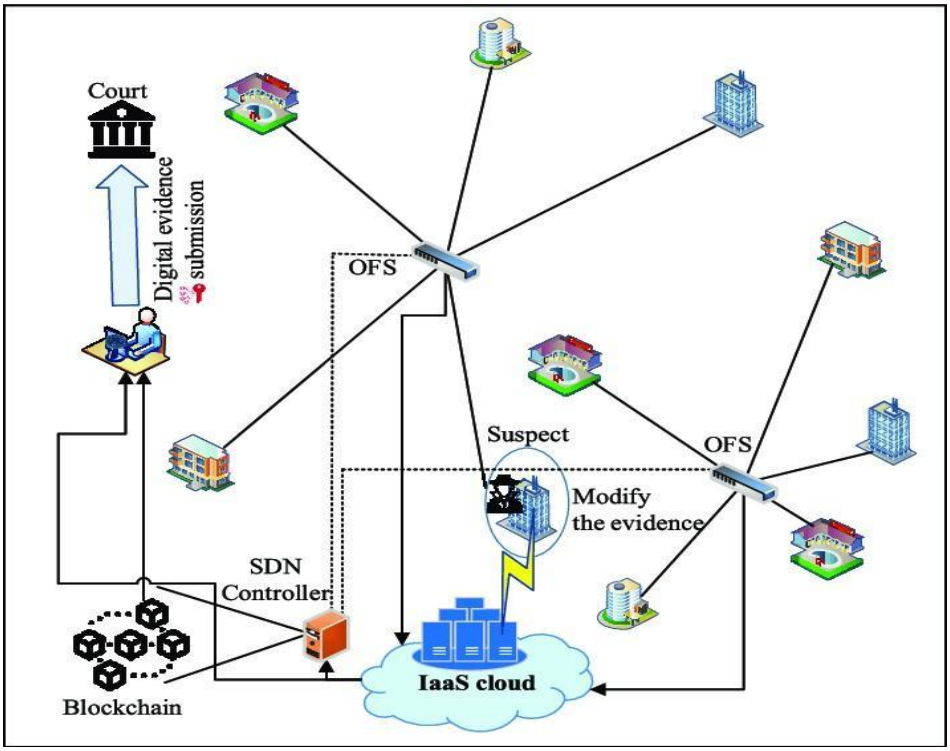
[61] Baryamereeba Venansius, Tushabe Florence, The Enhanced Digital Investigation Process Model, Paper in Institute of computer science, Makerere University, 2004

[62] Rogers Markus, James Goldman, Rick Mislan, Wedge Timothy, Debrota, Steve, Computer Forensic Field Triage Process Model, Digital Forensics, Security and Law, Article, 2006

από την οποία έγινε η επίθεση με την ταυτότητα του επιτιθέμενου. Λαμβάνοντας υπόψη τα ανωτέρω, οι ερευνητές άρχισαν να εργάζονται σε συγκεκριμένες πιο εξειδικευμένες πτυχές, όπως:

1. Στην τελειοποίηση ενός μοντέλου διαδικασιών, μέσω διαδοχικών βελτιώσεων σε ένα συγκεκριμένο βήμα στην έρευνα.
2. Στην εξειδίκευση ενός μοντέλου σε συγκεκριμένες κατηγορίες υποθέσεων, όπως π.χ. ψηφιακή εγκληματολογία για το δίκτυο ή για κινητές συσκευές.
3. Στη σκιαγράφηση συγκεκριμένων διαδικασιών για ευαίσθητες υποθέσεις, όπως π.χ. πορνογραφία ανηλίκων κ.λπ.

Στην Εικόνα 1 παρουσιάζεται μία αρχιτεκτονική για συλλογή τεκμηρίων και διασφάλιση της συσχέτισης με την πηγή (provenance preservation) σε περιβάλλοντα υπολογιστικής νέφους που ακολουθούν το υπόδειγμα «Infrastructure as a Service» (IaaS), με χρήση τεχνικών Blockchain[63].



Εικόνα 1. Εκτεταμένο Μοντέλο Διερεύνησης Ηλεκτρονικού Εγκλήματος

Ένα εκτεταμένο μοντέλο διερεύνησης του εγκλήματος στον κυβερνοχώρο προτάθηκε από τον Seamus O Clardhuain. Αυτό το μοντέλο διαρθρώνει τις απαραίτητες δραστηριότητες σε διαδοχικά στάδια, επιτρέπει ωστόσο την επανάληψη σε κάποιο μέρος της έρευνας, για

[63] Mehran Pourvahab, Gholamhossein Ekbatanifard, Digital Forensics Architecture for Evidence Collection and Provenance Preservation in IaaS Cloud Environment Using SDN and Blockchain Technology, Article in IEEE Access, October 2019

παράδειγμα, η επαναληπτική διαδικασία ήτοι την εξέταση - υπόθεση - παρουσίαση - απόδειξη [64].

Σε ορισμένες ειδικές περιπτώσεις, όπως απαγωγές, η άμεση απόκτηση ενδείξεων από ψηφιακές συσκευές είναι ζωτικής σημασίας ή σε κάποιες άλλες περιπτώσεις όπως η ληστεία, απαιτούνται κρίσιμες πληροφορίες το συντομότερο δυνατό για να αυξηθεί η πιθανότητα σύλληψης του εγκληματία, προτού διαφύγει ακόμα και σε άλλη χώρα. Συχνά τα παραδοσιακά μοντέλα είναι ανεπαρκή για αυτή τη χρήση και ενδέχεται να χρειαστεί υπολογίσιμο χρονικό διάστημα για να ληφθούν τα αποτελέσματα. Τα κλιμακωτά μοντέλα έχουν σχεδιαστεί για να επιταχύνουν καταστάσεις όπως αυτή. Λαμβάνοντας υπόψη ότι τα παραδοσιακά μοντέλα έχουν σχεδιαστεί για να παρέχουν καθοδήγηση σε όλη την έκταση της έρευνας, το μοντέλο της διαδικασίας διαλογής με την επωνυμία Triage, προτάθηκε για την αντιμετώπιση περιπτώσεων ευαίσθητων στο χρόνο. Αυτό το μοντέλο επικεντρώνεται στις κρίσιμες πρώτες ώρες μιας έρευνας[65].

4.5.4 Νεότερα Μοντέλα Ψηφιακής Εγκληματολογικής Διαδικασίας

Οι εξελίξεις της τεχνολογίας οδηγούν σε νέα προβλήματα που δημιουργούν προκλήσεις για τις έρευνες ψηφιακής εγκληματολογίας. Για παράδειγμα η εισαγωγή και χρήση της υπολογιστική νέφους (cloud computing), κάνει τη συλλογή αποδεικτικών στοιχείων πιο δύσκολη, καθώς τα στοιχεία μπορεί να είναι αποθηκευμένα σε άγνωστες τοποθεσίες ή σε χώρες εκτός δικαιοδοσίας έρευνας. Επιπρόσθετα το IoT (Internet of Things) προσθέτει μια ποικιλία νέων συσκευών και μορφών αποθήκευσης, περισσότερες ψηφιακές συσκευές που συνδέονται στο διαδίκτυο και συνακόλουθα έναν συνεχώς αυξανόμενο όγκο δεδομένων. Τα τελευταία χρόνια, η έρευνα σε μοντέλα διαδικασιών επικεντρώνεται περισσότερο στην ενσωμάτωση νέων τεχνολογιών, όπως η εξόρυξη δεδομένων, για παροχή αυξημένης υποστήριξης στα αρχικά μοντέλα, ή να προτείνει νέα μοντέλα διεργασιών για την επίλυση των προβλημάτων που προκαλούνται αυτές τις νέες τεχνολογίες[66].

Στην Εικόνα 2 απεικονίζονται τρία πιο εξελιγμένα μοντέλα, τα οποία είναι:

- Ένα ολοκληρωμένο εννοιολογικό ψηφιακό εγκληματολογικό πλαίσιο για περιβάλλον υπολογιστικής νέφους[67].
- Ένα πλαίσιο μείωσης και εξόρυξης δεδομένων[68].

---

[64] Seamus O Clardhuain, An Extended Model of Cybercrime Investigations, Article in International Journal of Digital Evidence, 2004

[65] Marcus K. Rogers, Kathryn Seigfried, Kirti Tidke, Self-reported computer criminal behavior - A psychological analysis, Article in Digital Investigation Volume 3, Supplement, September 2006, Pages 116-120

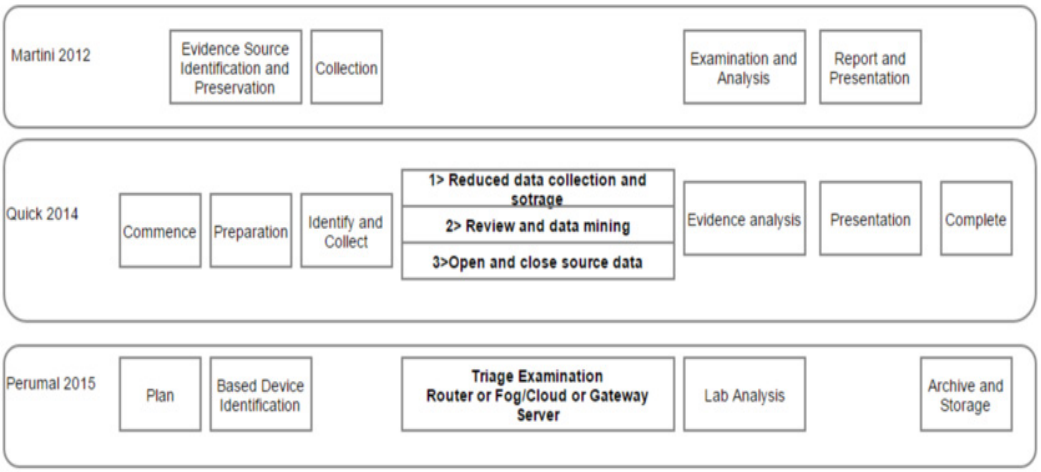
[66] Xiaoyu Du, Nhien – An Le- Khac, Mark Scanlon, Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service, article of the 16th European Conference on Cyber Warfare and Security (ECCWS 2017) on August 2017.

[67] Ben Martini, Kim Kwang Raymont Choo, K.-K.R., An Integrated Conceptual Digital Forensic Framework for Cloud Computing. Article in Digital Investigation, November 2012, pages 71–80.

[68] Quick Darren, Kim Kwang Raymont Choo, Data Reduction and Data Mining Framework for Digital Forensic Evidence: Storage, Intelligence, Review and Archive, Article in Australian Criminal Institute, 17/09/2014,

- Ένα ψηφιακό Εγκληματολογικό Μοντέλο Βασισμένο στο Διαδίκτυο των Πραγμάτων (IoT)[69].

Τα μοντέλα αυτά περιγράφονται συνοπτικά στις ακόλουθες παραγράφους.



Εικόνα 2. Μοντέλα ψηφιακής εγκληματολογίας

4.5.4.1 Ολοκληρωμένο εννοιολογικό ψηφιακό εγκληματολογικό πλαίσιο για περιβάλλον υπολογιστικής νέφους.

Οι υπηρεσίες υπολογιστικού νέφους (cloud) αυξάνονται, καθιστώντας μεταξύ άλλων απαραίτητη τη συλλογή ψηφιακών στοιχείων από απομακρυσμένους διακομιστές. Στις μέρες μας, οι ειδικοί στην ψηφιακή εγκληματολογία προσπαθούν να βρουν τρόπους ώστε να εντάξουν στην έρευνα τους στοιχεία που περιέχονται σε συσκευές σε περιβάλλον υπολογιστικού νέφους.

Το ψηφιακό εγκληματολογικό πλαίσιο προτάθηκε από τους Ben Martini και Kim Kwang Raymond Choo το 2012 με βάση δύο ευρέως χρησιμοποιούμενα βασικά μοντέλα των McKemmish το 1999[70] και Kent το 2006[71]. Οι προκλήσεις που συναντώνται κατά τη διεξαγωγή μιας εγκληματολογικής έρευνας που περιλαμβάνει υπηρεσίες νέφους μπορούν να εντοπιστούν σε κάθε στάδιο μιας τυπικής διαδικασίας.

Πρώτον**,** ο προσδιορισμός ότι είναι απαραίτητη η εφαρμογή εξειδικευμένων προσεγγίσεων και τεχνικών για υποθέσεις cloud είναι δυνατός μόνο μετά την απόκτηση κάποιων αρχικών πληροφοριών ή αποθηκευμένων διαπιστευτηρίων σύνδεσης από μια φυσική ψηφιακή συσκευή, όπως π.χ. έναν φορητό υπολογιστή ή ένα smartphone, έτσι ώστε να διαπιστωθεί η

[69] Perumal Sundresan, Norwawi, Norita Md, and Raman Valliappan, Internet of Things (IoT) Digital Forensic Investigation Model: TopDown Forensic Approach Methodology, Paper in Fifth International Conference on Digital Information Processing and Communications (ICDIPC), IEEE, October 2015, pp. 19–23,

[70] Rodney McKemmish, What is Forensic Computing?, paper in Australian Institute of Criminology, June 1999

[71] Kent Karen, Chevalier Suzanne, Tim Grance, Dang Hunag, Guide to Integrating Forensic Techniques into Incident Response, National Institute of Standards and Technology, August 2006, publication 800–886.

χρήση υπηρεσιών cloud και να προσδιοριστούν οι συγκεκριμένες υπηρεσίες που χρησιμοποιούνται.

Δεύτερον**,** στη συλλογή των τεκμηρίων από περιβάλλον cloud, εντοπίζονται ζητήματα που συχνά περιλαμβάνουν τα ακόλουθα[72]:

- Δεν υπάρχει δυνατότητα φυσικής κατάσχεσης όλων των διακομιστών και των αντίστοιχων φυσικών συσκευών σε περιβάλλον υπολογιστικού νέφους.
- Η φυσική θέση του διακομιστή θα μπορούσε να βρίσκεται εκτός της δικαιοδοσίας των αρχών (π.χ. σε άλλη χώρα) και έτσι να απαιτούνται σχετικά αιτήματα δικαστικής συνδρομής.
- Δυσχέρειες στη συλλογή μεταδεδομένων ή αδυναμία ανάκτησής τους.

4.5.4.2 Ψηφιακό Εγκληματολογικό Μοντέλο Βασισμένο στο Διαδίκτυο των Πραγμάτων - Internet of Things

Η επέκταση της χρήσης του IoT (Internet of Things) δημιουργεί νέες προκλήσεις για την ψηφιακή εγκληματολογία. Σημαντική πρόκληση σε αυτόν τον τομέα είναι το πλήθος των ψηφιακών συσκευών που πρέπει να συλλεχθούν, να αναλυθούν, να εξεταστούν και να διατηρηθούν καθώς και ο συναφώς μεγαλύτερος όγκος δεδομένων, αλλά και η ποικιλία των μορφών αποθήκευσης. Ένα πιο εξελιγμένο ερευνητικό μοντέλο, που στοχεύει στην αντιμετώπιση του συγκεκριμένου ζητήματος που σχετίζονται με τη διερεύνηση που βασίζεται στο IoT, είναι αυτό που προτείνεται από τον Perumal το 2015[73]. Αυτό το μοντέλο ορίζει μια τυποποιημένη διαδικασία διεξαγωγής έρευνας για τη διερεύνηση συσκευών IoT. Επιπρόσθετα, η έρευνα και η συλλογή εγκληματολογικών πληροφοριών από συσκευές σε περιβάλλον IoT (στην οποία διαδικασία θα αναφερόμαστε εν συντομία ως IoT Forensics) είναι σε πρώιμο στάδιο, εντούτοις η χρήση κάποιων μοντέλων έχει ήδη αρχίσει να γίνεται από ειδικούς ανακριτικούς υπαλλήλους στο πεδίο. Μερικά από τα μοντέλα στο IoT Forensics είναι τα ακόλουθα:

α) Ψηφιακό Μοντέλο Εγκληματολογικής Έρευνας

Κύριος στόχος του μοντέλου αυτού είναι η βελτίωση της διαδικασίας ψηφιακής εγκληματολογικής έρευνας, έχοντας ως στόχο την εύρεση κρυμμένων στοιχείων που θα βοηθήσουν την εκάστοτε έρευνα.

β) Το Υβριδικό Μοντέλο

Το μοντέλο αναπτύχθηκε ώστε να αναλύει και να επεξεργάζεται είτε φυσικά στοιχεία είτε ψηφιακά στοιχεία, χωρίς ωστόσο οι δύο κατηγορίες να ανάλυσης να συνδυάζονται, γεγονός που αποτελεί μειονέκτημα για το περιβάλλον IoT.

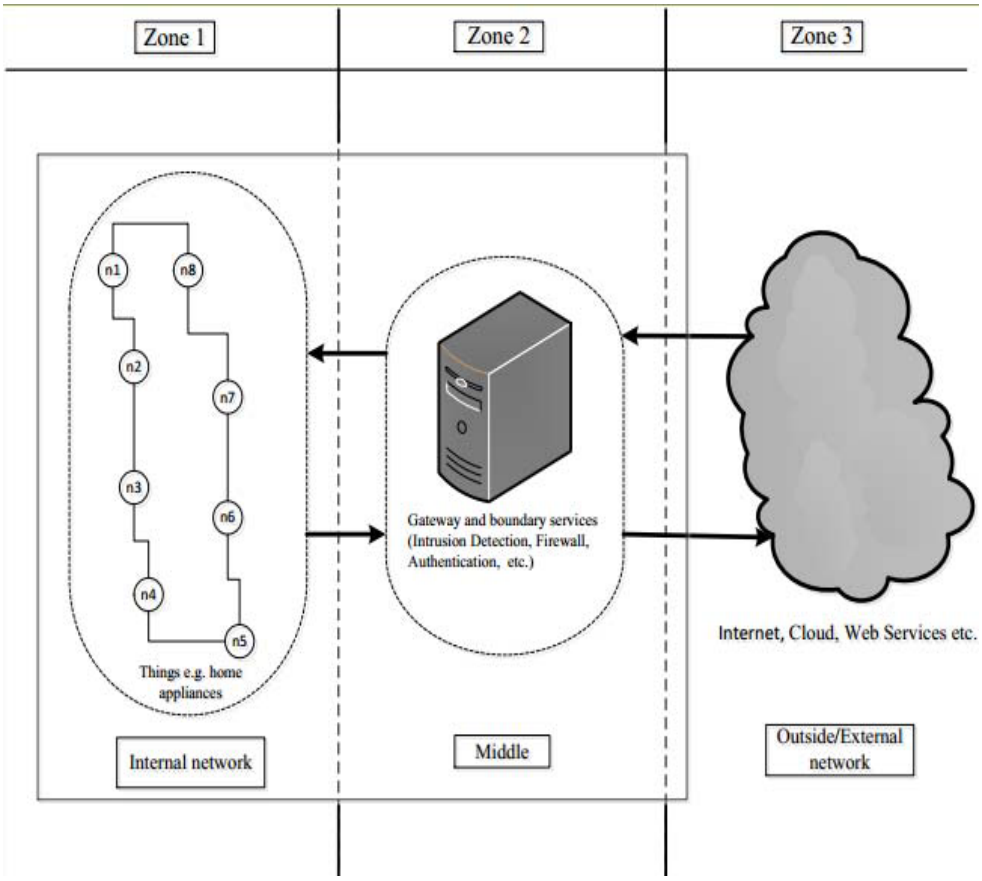
---

[72] Ben Martini, Kim Kwang Raymont Choo, An integrated conceptual digital forensic framework for cloud computing, paper in Digital Investigation, July 2012, Pages 71-80

[73] Sundresan Perumal, Norita Md Norwawi, Valliappan Ramman, Internet Of Things(IoT) Digital Forensic Investigation Model: Top-Down Forensic Approach Methodology, paper in IEEE on 2015

γ) 1-2-3 Ζώνες Ψηφιακής Εγκληματολογικής Έρευνας

Αυτό το μοντέλο θεωρείται ως ένα από τα σταθερά ψηφιακά εγκληματολογικά μοντέλα όταν αναφερόμαστε σε περιβάλλον IoT. Το παρακάτω σχήμα απεικονίζει το μοντέλο αυτό:



Εικόνα 3. 1-2-3 Ζώνες Ψηφιακής Εγκληματολογικής Έρευνας

Το μοντέλο λειτουργεί με προσεγγιστική μέθοδο. Χωρίζει την περιοχή του τόπου του εγκλήματος σε ζώνες. Η ζώνη 1 λειτουργεί ως εσωτερική, η ζώνη 2 είναι αυτή στην οποία βρίσκονται οι διασυνδέσεις με το διαδίκτυο καθώς και αμυντικοί μηχανισμοί όπως λ.χ. firewalls και IDS, και η ζώνη 3 αφορά το διαδίκτυο, το νέφος και κάθε εξωτερικό σύστημα[74].

4.5.4.3 Μοντέλο Επεξεργασίας Πεδίου - Μεθοδικής Εγκληματολογικής Μεθοδολογίας

Ένα από τα πιο πρόσφατα προτεινόμενα μοντέλα περιβάλλει ένα ερευνητικό μοντέλο επεξεργασίας ψηφιακού πεδίου με την ονομασία «*Μοντέλο Κλιμακωτής Εγκληματολογικής Μεθοδολογίας για Ψηφιακή Διαλογή Πεδίου από Ειδικούς σε Μη Ψηφιακά Αποδεικτικά*

[74] Sundresan Perumal, Norita Md Norwawi, Valliappan Ramman, Internet Of Things(IoT) Digital Forensic Investigation Model: Top-Down Forensic Approach Methodology, paper in IEEE on 2015

Στοιχεία» που δημοσίευσαν οι Hitchcock, Le-Khac και Scanlon το 2016[75]. Αυτό το μοντέλο επικεντρώνεται στην εκπαίδευση ειδικών σε μη - ψηφιακές έρευνες πεδίου να διεξάγουν αναγνώριση και διαλογή ψηφιακών τεκμηρίων στο πεδίο. Αυτό επιτυγχάνεται μέσω της ανάπτυξης ενός νέου μοντέλου διαδικασιών, για την παροχή κατευθύνσεων και συμβουλών στα στελέχη που μεταβαίνουν στο χώρο του εγκλήματος πρώτοι (πρώτοι ανταποκριτές Αστυνομικοί). Αφού επιλεγούν τα ψηφιακά τεκμήρια, στη συνέχεια πραγματοποιούνται πιο λεπτομερείς εξετάσεις και αναλύσεις στο εργαστήριο. Με τον τρόπο αυτό αντιμετωπίζεται το πρόβλημα της έλλειψης εξειδικευμένων ανακριτικών υπαλλήλων στο χώρο του εγκλήματος χωρίς την κατάλληλη εξειδίκευση στην ψηφιακή εγκληματολογία και από την άλλη πλευρά επιτυγχάνεται αυξημένη ταχύτητα και μείωση του όγκου του προς εξέταση υλικού[76].

4.6 Ψηφιακά Πειστήρια, Ψηφιακά Τεκμήρια και Χειρισμός Αυτών

4.6.1 Ψηφιακά Πειστήρια

Ως ψηφιακά πειστήρια ορίζονται τα αποδεικτικά μέσα τα οποία έχουν αποθηκευμένες πληροφορίες σε ψηφιακή μορφή. Παραδείγματα ψηφιακών πειστηρίων είναι τα ακόλουθα[77]:

- κεντρική μονάδα ηλεκτρονικού υπολογιστή,
- φορητός ηλεκτρονικός υπολογιστής,
- σκληροί δίσκοι,
- δρομολογητές (routers),
- μεταγωγείς (switches),
- modem,
- κινητά τηλέφωνα,
- κάρτες SIM,
- κάρτες μνήμης,
- έξυπνες κάρτες,
- ψηφιακές φωτογραφικές μηχανές και ψηφιακές κάμερες,
- cd, dvd, usb dongles/sticks, usb, ταινίες, μονάδες ψηφιακής αποθήκευσης,
- ψηφιακές συσκευές αναπαραγωγής / λήψης ήχου / εικόνας / βίντεο,
- αυτοσχέδιες ή προσαρμοσμένες διατάξεις και συσκευές αναγνώρισης καρτών.

4.6.2 Ψηφιακά Τεκμήρια

Δεν υπάρχει ένας κοινά αποδεκτός ορισμός σχετικά με το τι συνιστά ψηφιακό αποδεικτικό στοιχείο. Η διατύπωση ενός ακριβούς αλλά και πλήρως συμπεριληπτικού ορισμού είναι δυσχερής, καθώς π.χ. ένα μήνυμα ηλεκτρονικού ταχυδρομείου ή ένα μήνυμα σε εφαρμογή

[75] Hitchcock Ben, Le-Khac Nhien An, Scanlon, Mark, Tiered forensic methodology model for Digital Field Triage by non-digital evidence specialists, paper in Digital Investigation on 2016, s75- s85

[76] Hitchcock Ben, Le-Khac Nhien An, Scanlon, Mark, Tiered forensic methodology model for Digital Field Triage by non-digital evidence specialists, paper in Digital Investigation on 2016, s75- s85

[77] Εγχειρίδιο Συλλογής και Εξέτασης Ψηφιακών Πειστηρίων – Δ.Ε.Ε., εκδ 2023, Ελληνική Αστυνομία

κοινωνικής δικτύωσης που έχουν εκτυπωθεί, αμφότερα θα μπορούσαν να θεωρηθούν ως τέτοια αφού υπάρχουν και σε ψηφιακή μορφή. Υπάρχουν ωστόσο κάποιες προσπάθειες καθορισμού του τι μπορεί να χαρακτηριστεί ως ψηφιακό τεκμήριο, και ένας τέτοιος ορισμός είναι αυτός που παρέχεται από μια επιστημονική ομάδα εργασίας για τα ψηφιακά αποδεικτικά στοιχεία (Scientific Working Group on Digital Evidence το 1999)[78]. Αυτή η επιστημονική ομάδα απαρτίζεται από Αστυνομικές και Δικαστικές Αρχές, ακαδημαϊκούς και εμπορικούς οργανισμούς που συμμετέχουν ενεργά στον τομέα της ψηφιακής εγκληματολογίας, και έχει ως στόχο την ανάπτυξη διεπιστημονικών κατευθυντήριων γραμμών και προτύπων για την ανάκτηση, τη διατήρηση και την εξέταση των ψηφιακών αποδεικτικών στοιχείων[79]. Με βάση τον ορισμό αυτό ***ψηφιακά τεκμήρια είναι οι πληροφορίες με αποδεικτική αξία, οι οποίες είναι αποθηκευμένες ή μεταδίδονται σε ψηφιακή μορφή.***

Σύμφωνα με τον Ποινικό Κώδικα που ισχύει, στα πλαίσια εφαρμογής της Σύμβασης της Βουδαπέστης για το Κυβερνοέγκλημα, που εισήχθησαν σε αυτόν με τις διατάξεις του Νόμου 4411 / 2016, ενσωματώνονται ορισμοί για τα ψηφιακά δεδομένα και τα ψηφιακά τεκμήρια. Ειδικότερα, στο άρθρο 13 περ. θ΄ ο Νόμος 4411 / 2016 ορίζει ότι τα «Ψηφιακά δεδομένα είναι η παρουσίαση γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη προς επεξεργασία από πληροφοριακό σύστημα, συμπεριλαμβανομένου προγράμματος που παρέχει τη δυνατότητα στο πληροφοριακό σύστημα να εκτελέσει λειτουργία»[80].

Ως ψηφιακά τεκμήρια, ορίζονται **«τα πειστήρια τα οποία υπάρχουν σε ψηφιακή μορφή και εντοπίζονται και εξάγονται κατά την διαδικασία της ψηφιακής εγκληματολογικής έρευνας (digital forensics) με επιστημονικά αποδεκτές μεθόδους, προκειμένου να αξιοποιηθούν στην ποινική διαδικασία»** [81]**.**

Τα ψηφιακά τεκμήρια μπορούν να διαδραματίσουν σημαντικό ρόλο στη διερεύνηση σοβαρών ποινικών υποθέσεων, όπως ανθρωποκτονιών, βιασμών, σεξουαλικής κακοποίησης παιδιών, διακεκριμένων κλοπών, απατών, ξέπλυμα χρήματος και εκβιασμών, αλλά και σε αστικές υποθέσεις. Με την αναζήτηση ψηφιακών τεκμηρίων μπορούν να εξασφαλιστούν πληροφορίες σχετικές με το έγκλημα πριν την τέλεση του, κατά τη διάρκεια της τέλεσης του και μετά την τέλεση του. Οι ηλεκτρονικοί υπολογιστές και οι συναφείς συσκευές αποθήκευσης, όπως σκληροί δίσκοι, οπτικοί δίσκοι και μνήμες είναι οι πιο διαδεδομένοι φορείς ψηφιακών τεκμηρίων, ωστόσο δεν είναι οι μόνοι, αφού ψηφιακά τεκμήρια μπορούν να εντοπιστούν σε ένα ευρύ φάσμα συσκευών όπως τα PDAs, MP3 players, φωτογραφικές μηχανές, ρολόγια, συσκευές εντοπισμού θέσεις GPS, κινητά τηλέφωνα κ.ά.

Χαρακτηριστικά αναφέρεται ότι σε ανθρωποκτονία που διαπράχθηκε στην Ελλάδα και ειδικότερα στα Γλυκά Νερά Αττικής το 2021, με θύμα μία γυναίκα, οι ειδικοί πραγματογνώμονες της Ελληνικής Αστυνομίας ανέκτησαν στοιχεία κρίσιμα για την έρευνα

[78] Scientific Working Group on Digital Evidence, SWGDE, Glossary, official web site

[79] Scientific Working Group on Digital Evidence, SWGDE, Glossary, official web site

[80] Ποινικός Κώδικας, Άρθρο 13, ενσωμάτωση Νόμου 4619/2019

[81] ΔΑΛΑΚΟΥΡΑ Θεοχάρης, Ηλεκτρονικό έγκλημα, Νομική Βιβλιοθήκη, Θεσσαλονίκη 2019

από τα ψηφιακά πειστήρια και ειδικότερα ανέλυσαν το κινητό τηλέφωνο και το ψηφιακό ρολόι του δράστη, από τα οποία απεδείχθη ότι οι καταθέσεις του περιείχαν ανακρίβειες και ψεύδη. Ειδικότερα, στο ρολόι του δράστη είχαν καταγραφεί βήματα, αποστάσεις αλλά και άνοδος ορόφων από τον δράστη στην οικία – χώρο διάπραξης του εγκλήματος. Από την έκθεση της Υποδιεύθυνσης Εξέτασης Ψηφιακών Πειστηρίων της Διεύθυνσης Εγκληματολογικών Ερευνών είχε αποτυπωθεί πλήρως η δραστηριότητά του δράστη το χρονικό διάστημα κατά το οποίο έλαβε χώρα το έγκλημα[82].

4.6.3 Αρχές Χειρισμού Ψηφιακών Τεκμηρίων

Για να υπάρχει μεταξύ των Αστυνομικών Αρχών και των Αρχών επιβολής του νόμου σε κάθε χώρα μια κοινή συνισταμένη για τον τρόπο που θα συλλέγονται και θα διατηρούνται τα ψηφιακά πειστήρια θα πρέπει να ορισθεί ένας κοινός κανόνας - πρότυπο. Τέτοιο αποτελεί σαν ένα πρώτο βήμα το διεθνές πρότυπο ISO/IEC 27037:2012 «Αναγνώριση, Διαλογή, Συλλογή και Διατήρηση Ψηφιακών Τεκμηρίων»[83] και μετέπειτα ο οδηγός ορθής πρακτικής για τις ψηφιακές αποδείξεις που δημοσιεύτηκε στο Ηνωμένο Βασίλειο τον Μάρτιο του 2012 από το Association of Chief Police Officers[84].

Σύμφωνα με το ανωτέρω διεθνές πρότυπο ISO/IEC 27037:2012, ο χειρισμός των ψηφιακών τεκμηρίων πρέπει να διέπεται από τις ακόλουθες βασικές αρχές[85]:

1. Συνάφεια των πειστηρίων με την ερευνώμενη υπόθεση.
2. Αξιοπιστία των πειστηρίων χωρίς να υπάρχει ίχνος αμφισβήτησής.
3. Επάρκεια δηλαδή συγκέντρωση ικανού αριθμού πειστηρίων.

4.6.4 Σύντομη Αναδρομή στην Ανάπτυξη Εγκληματολογικών Εργαλείων

Την δεκαετία του ‘80 η ανάλυση των πειστηρίων γινόταν εν λειτουργία στους ηλεκτρονικούς υπολογιστές καθόσον δεν υπήρχαν τότε προγράμματα για την εξαγωγή των ψηφιακών πειστηρίων. Η μεθοδολογία αυτή δεν ήταν αξιόπιστη ενέχοντας τον κίνδυνο μεταβολής των ψηφιακών δεδομένων του σκληρού δίσκου, κυρίως λόγω εσφαλμένων χειρισμών ή χειρισμών των οποίων οι επιπτώσεις δεν είχαν αξιολογηθεί δεόντως, γεγονός που οδηγούσε στην υποβάθμιση της αξιοπιστίας των πειστηρίων.

Προκειμένου η μεθοδολογία των ερευνών να γίνει πιο αξιόπιστη και με καλύτερα αποτελέσματα το 1989 και 1990 αντίστοιχα το Ομοσπονδιακό Κέντρο Εκπαίδευσης για την Επιβολή του Νόμου των Η.Π.Α., δημιούργησε δύο εξειδικευμένα προγράμματα το IMDUMP

[82] Άρθρο εφημερίδα Καθημερινή στην επίσημη ιστοσελίδα την 20/06/2021

[83] ΕΛΛΗΝΙΚΟΣ ΟΡΓΑΝΙΣΜΟΣ ΤΥΠΟΠΟΙΗΣΗΣ ΕΛΟΤ ΕΚΟΔΟΣΗ 27037, Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Κατευθυντήριες οδηγίες για την αναγνώριση, συλλογή, απόκτηση και διατήρηση ψηφιακών ενδείξεων

[84] Association of Chief Police Officer, Good Practice Guide for Digital Evidence, Metrpolitan Police Services, march 2012

[85] ΔΑΛΑΚΟΥΡΑ Θεοχάρης, Ηλεκτρονικό έγκλημα, Νομική Βιβλιοθήκη, Θεσσαλονίκη 2019, σελ. 272.

και το Safeback[86]. Επιπρόσθετα σε άλλες χώρες, όπως το Ηνωμένο Βασίλειο, κυκλοφόρησε ο σταθμός εργασίας για έλεγχο ψηφιακών πειστηρίων DIBS το 1991, ενώ στην Αυστραλία το λογισμικό Fixed Disk Image, το οποίο διατίθετο δωρεάν στις αρχές επιβολής του νόμου[87].

Η καινοτομία των προγραμμάτων αυτών ως εργαλεία στα χέρια των ερευνητών εστιάζεται στο γεγονός ότι αυτά δημιουργούν ακριβές αξιόπιστο αντίγραφο του ψηφιακού μέσου που γίνεται η έρευνα. Με αυτό τον τρόπο οι ερευνητές έχουν την δυνατότητα που τους προσφέρει πολλές επιλογές να κάνουν την έρευνα τους έχοντας την αρχική μνήμη, τον αρχικό σκληρό δίσκο άθικτο. Στα τέλη της δεκαετίας του 90΄, καθώς αυξήθηκε η ζήτηση για ψηφιακά εγκληματολογικά πειστήρια, λόγω και της αυξανόμενης χρήσης των ηλεκτρονικών υπολογιστών, αναπτύχθηκαν προγράμματα τα οποία είχαν την δυνατότητα έρευνας και ανάλυσης ψηφιακών πειστηρίων χωρίς να είναι σε λειτουργία ο ηλεκτρονικός υπολογιστής ή η προς εξέταση ψηφιακή συσκευή. Αργότερα την δεκαετία του 2000 αναπτύχθηκαν προγράμματα όπως ενδεικτικά το Windows SCOPE με το οποίο οι ερευνητές μπορούν να διευρύνουν την ανάλυση εις βάθος της μνήμης ενός υπολογιστή ή μιας ψηφιακής συσκευής όπως των κινητών συσκευών που πλέον την δεκαετία αυτή έχουν κάνει ευρέως την εμφάνιση τους. Ειδικότερα για τις κινητές συσκευές εμφανίστηκαν προγράμματα πιο εξειδικευμένα όπως ενδεικτικά το XRY και το Radio Tactics Aceso.

4.6.5 Στάδια Χειρισμού Ψηφιακών Τεκμηρίων

Στις ακόλουθες παραγράφους περιγράφονται τα στάδια χειρισμού των ψηφιακών πειστηρίων, σε όλη τη ροή εργασιών για τον χειρισμό τους.

4.6.5.1 Αναγνώριση

Η αξιοπιστία των των ψηφιακών τεκμηρίων και η έρευνα και ανάλυση αυτών με τρόπο μη αμφισβητήσιμο αποτελούν τον ακρογωνιαίο λίθο της αποδεικτικής διαδικασίας στην ποινική δίκη. Η έρευνα αρχικά θα πρέπει να διενεργείται σύμφωνα με όσα ορίζουν οι νόμοι και ειδικότερα ο Κώδικας Ποινικής Δικονομίας. Επιπρόσθετα ο υπό έρευνα χώρος επιβάλλεται να διατηρηθεί αναλλοίωτος για να διερευνηθεί κατάλληλα από τους πρώτους προστρέξαντες υπαλλήλους (Αστυνομία, Ε.Κ.Α.Β.)[88]. Εν συνεχεία θα ξεκινήσει η διαδικασία της αναζήτησης για αναγνώριση πιθανών ψηφιακών τεκμηρίων, τα οποία να είναι σχετικά με τη διεξαγόμενη έρευνα και τα οποία πιθανό να είναι αποθηκευμένα σε συσκευές ψηφιακών μέσων αποθήκευσης και επεξεργασίας. Πρωταρχικό είναι όλες οι ενέργειες να έχουν επίκεντρο ώστε τα ψηφιακά τεκμήρια να μην αλλοιωθούν και μεταβληθούν. Επίσης πριν την αναγνώριση και πιθανή κατάσχεση κάποιου αντικειμένου θα πρέπει να λαμβάνονται υπόψη το κατά πόσο αυτό θα έχει αποδεικτική αξία, όπως για παράδειγμα η κατοχή ενός υπολογιστή, ενός κινητού αλλά και οι χρήστες αυτού.

[86] George M. Mohay, Computer and Intrusion Forensics, Artech House,2003

[87] George M. Mohay, Computer and Intrusion Forensics, Artech House,2003

[88] Νόμος 4620/2019, Κώδικας Ποινικής Δικονομίας (ΦΕΚ Τεύχος Α’ 96/11.06.2019)

4.6.5.2 Συλλογή

Κατά τη διεξαγωγή μιας έρευνας, πρώτη και βασική ενέργεια των ανακριτικών υπαλλήλων που ερευνούν την προς εξέταση υπόθεση είναι, εκτός του να διατηρηθεί η σκηνή του εγκλήματος ανέπαφη είναι και η φωτογράφιση, η βιντεοσκόπηση καθώς και η δημιουργία σχεδιαγράμματος της σκηνής για να περιγραφούν μέσα στο χώρο της σκηνής. Από τη στιγμή που οι ψηφιακές συσκευές είναι πιθανό να περιέχουν ψηφιακά τεκμήρια, τότε γίνεται περισυλλογή τους, προκειμένου να ανακτηθούν τα ψηφιακά αυτά τεκμήρια από την κάθε συσκευή ξεχωριστά. Οι ακριβείς διαδικασίες ανάκτησης εξαρτώνται από τις ιδιαιτερότητες των συσκευών και τις περιστάσεις της κάθε περίπτωσης ξεχωριστά.

Η συλλογή είναι η διαδικασία χειρισμού των ψηφιακών τεκμηρίων όπου συσκευές που πιθανόν να περιέχουν ψηφιακά τεκμήρια μετακινούνται από την αρχική τους θέση σε εργαστήριο ή άλλο κατάλληλο περιβάλλον, με σκοπό την ανάκτηση των δεδομένων από τις συσκευές αυτές και την ανάλυσή των δεδομένων αυτών. Για τον σκοπό αυτό οι ανακριτικοί υπάλληλοι θα αναζητήσουν στο χώρο της σκηνής του εγκλήματος τυχόν κωδικούς πρόσβασης, επιπρόσθετα περιφερειακά εξαρτήματα όπως φορτιστές, καλώδια. Επιπρόσθετα USB μνήμες, κινητά τηλέφωνα, σκληροί δίσκοι, ψηφιακά ρολόγια, κάθε φύσεως ψηφιακές συσκευές και άλλα παρόμοια αντικείμενα εξετάζονται με χρήση κατάλληλων εργαλείων και τεχνικών στα εξειδικευμένα εργαστήρια. Τα ψηφιακά τεκμήρια πρέπει να αντιμετωπίζονται με προσοχή για διατηρηθεί η ακεραιότητα τόσο της συσκευής όσο και του περιεχομένου της, λαμβάνοντας υπόψη ότι κάποια ψηφιακά τεκμήρια απαιτούν ειδική μεταχείριση σε σχέση με τη συλλογή, συσκευασία και μεταφορά τους[89]. Χαρακτηριστικά, το άρθρο 265 του Κώδικα Ποινικής Δικονομίας αναφέρει ότι η κατάσχεση ψηφιακών δεδομένων μπορεί να επιβληθεί[90] (i) στο σύνολο ενός υπολογιστικού συστήματος ή σε τμήμα αυτού και στα δεδομένα που υπάρχουν στο αντικείμενο της κατάσχεσης καθώς και (ii) σε ένα αποθηκευτικό μέσο και στα δεδομένα που αυτό φέρει. Και στις δύο εκδοχές, ο ανακριτικός υπάλληλος είτε έχει φυσική πρόσβαση στο υπό κατάσχεση στοιχείο, στην οποία περίπτωση προβαίνει στην κατάσχεση του φυσικού αντικειμένου, είτε ο ανακριτικός υπάλληλος έχει πρόσβαση σε υπολογιστικό σύστημα με το οποίο είναι διασυνδεδεμένο το σύστημα που φέρει τα προς κατάσχεση στοιχεία. Για την τελευταία περίπτωση, υπάρχει ειδική πρόνοια για τις υπηρεσίες νέφους, οι οποίες δεν είναι εφικτό να κατασχεθούν, και όταν αντιμετωπίζεται τέτοια περίσταση η εστίαση μετατοπίζεται στα στοιχεία και τα δεδομένα και όχι στην υποδομή.

4.6.5.3 Απόκτηση

Μετά τη συλλογή ακολουθεί η διαδικασία της απόκτησης των ψηφιακών τεκμηρίων που πρέπει να γίνει η έρευνα από την συσκευή στην οποία εντοπίστηκαν έτσι ώστε να εξαχθούν και απομονωθούν. Η απόκτηση πραγματοποιείται είτε σε εξειδικευμένο εργαστήριο, είτε στο τόπο του εγκλήματος. Η διαδικασία αυτή περιλαμβάνει τη δημιουργία ενός ψηφιακού αντιγράφου (π.χ. ένα πλήρες αντίγραφο σκληρού δίσκου). Οι συσκευές οι οποίες

[89] Παπαθανασίου Χρ. Αναστάσιος, Κυβερνοέγκλημα, Ψηφιακή Εγκληματολογία και Κατάσχεση Ψηφιακών Δεδομένων, Ηλεκτρονικό Έγκλημα, 2023

[90] Άρθρο 265 του Κώδικα Ποινικής Δικονομίας

κατασχέθηκαν ως μέρος της έρευνας θα μεταφερθούν σε εξειδικευμένο εργαστήριο, σύμφωνα τις ακολουθούμενες διαδικασίες για να υποβληθούν σε εργαστηριακή εξέταση. Η επίτευξη των στόχων δυσχεραίνεται στην παρούσα περίοδο λόγω του όγκου και της πολυπλοκότητας των δεδομένων τα οποία είναι αποθηκευμένα στις ψηφιακές συσκευές, καθώς δεν δυνατό ή επιθυμητό να ανακτηθούν όλα τα δεδομένα για έλεγχο, και ως εκ τούτου η ανακριτική αυτή εξέταση πρέπει να περιορίζεται στα απολύτως απαραίτητα. Αυτό θα το ορίσει και η εκάστοτε Δικαστική Αρχή, η οποία ανάλογα με την έρευνα θα διαμορφώσει τη σχετική παραγγελία για τη διενέργεια των εξετάσεων. Ένα σημαντικό στοιχείο του σταδίου αυτού είναι να μην υπάρξει η παραμικρή αλλοίωση των τεκμηρίων και ειδικότερα εκτός των άλλων να αποφευχθείί οποιεσδήποτε παρέμβαση σε αυτά. Για τον σκοπό αυτό κρίνεται σκόπιμο και επιβάλλεται η δημιουργία αντιγράφου των δεδομένων, πριν γίνει η ανάλυση τους, με σκοπό ο ερευνητής να εργαστεί πάνω στο αντίγραφο και όχι στο πρωτότυπο.

4.6.5.4 Διατήρηση

Η ορθή διατήρηση των ψηφιακών τεκμηρίων από τον τόπο του εγκλήματος θα συμβάλει στη διεξαγόμενη έρευνα και επίσης θα συνεισφέρει στο να παραμείνουν τα τεκμήρια σε καλή, λειτουργική και αξιοποιήσιμη κατάσταση[91].

Χαρακτηριστικά, το άρθρο 265 του Κώδικα Ποινικής Δικονομίας στις παραγράφους 4, 5 και 6 αναφέρει ότι τα ψηφιακά δεδομένα που κατάσχονται διατηρούνται αποθηκευμένα καθ' όλη τη διάρκεια της προανακριτικής και ανακριτικής διαδικασίας σε ειδικά μέσα αποθήκευσης για λόγους ασφάλειας και με πρόσβαση μόνο όσων έχουν το δικαίωμα από τον νόμο αυτό προστατεύοντάς, με αυτό τον τρόπο το υλικό αυτό να χρησιμοποιηθεί για άλλους σκοπούς.[92]

4.6.5.5 Αναφορά - Παρουσίαση

Το τελευταίο βήμα αποτελεί και τον τελικό στόχο για τον οποίο διεξάγεται η εξέταση και έρευνα των ψηφιακών πειστηρίων, και είναι η σύνταξη αναφοράς των αποτελεσμάτων των ερευνών για παρουσίαση ενώπιον των αρμοδίων προανακριτικών και δικαστικών αρχών. Η εγκυρότητα και σαφήνεια των αποτελεσμάτων των εξετάσεων αποτελούν κρίσιμα σημεία προκειμένου να βασιστεί το δικαστήριο πάνω σε αυτά για τη λήψη της απόφασης.

[91] Ana Nieto, Ruben Rios, Javier Lopez, Javier Wei Ren, Javier Lizhe Wang, Kim-Kwang Raymond Choo, and Fatos Raymond Xhafa, Privacy - aware digital forensics, 2019

[92] Άρθρο 265 του Κώδικα Ποινικής Δικονομίας

5 Η ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΣΤΗΝ ΨΗΦΙΑΚΗ ΕΓΚΛΗΜΑΤΟΛΟΓΙΑ

Η Τεχνητή Νοημοσύνη γεννήθηκε, ως όρος, στο Κολέγιο του Dartmouth των Η.Π.Α., το 1956 όταν σε συνάντηση επιστημόνων χρησιμοποιήθηκε για να αναφερθεί κάθε υπολογιστικό μηχάνημα ή σύστημα το οποίο "σκέφτεται"[93]. Η Τεχνητή Νοημοσύνη (στην Αγγλική γλώσσα ονομάζετε Artificial Intelligence - ή με τα αρχικά και ευρέως γνωστή ως AI) γνωρίζει στις μέρες μας μεγάλη ανάπτυξη και διαδραματίζει ήδη ενεργό ρόλο στον χώρο της ψηφιακής εγκληματολογίας. Ειδικότερα η Τεχνητή Νοημοσύνη στην Εγκληματολογία και ειδικότερα στην Ψηφιακή Εγκληματολογία μπορεί να βελτιώσει τις διαδικασίες σε όλα τα στάδια της έρευνας ήτοι στην συλλογή, την επεξεργασία και την ερμηνεία αποδεικτικών στοιχείων. Οι δυνατότητες της τεχνητής νοημοσύνης αξιοποιούνται για τη βελτίωση της αποτελεσματικότητας και της αποδοτικότητας των ερευνών των ειδικών ανακριτικών υπαλλήλων και των δικαστικών αρχών. Ενδεικτικά μπορούμε να αναφέρουμε μερικές διαδικασίες που η Τεχνητή Νοημοσύνη τυγχάνει εφαρμογής στην ψηφιακή εγκληματολογία[94]:

- **Αυτοματοποιημένη συλλογή αποδεικτικών στοιχείων**: Η Τεχνητή Νοημοσύνη μπορεί να συνεισφέρει στην αυτοματοποίηση της συλλογής ψηφιακών στοιχείων και δεδομένων για ένα υπό έρευνα έγκλημα από πολλές πηγές, όπως κινητές συσκευές, υπολογιστές και υπηρεσίες νέφους, διευκολύνοντας τους ανακριτικούς υπαλλήλους.
- **Αναζήτηση λέξεων-κλειδιών**: Ειδικά προγράμματα είναι ικανά με την βοήθεια της Τεχνητής Νοημοσύνης να κατανοήσουν το πλαίσιο των λέξεων αναζήτησης μέσω της χρήσης της επεξεργασίας φυσικής γλώσσας (NLP). Αυτό επιτρέπει την ακριβέστερη και αποτελεσματικότερη αναζήτηση σχετικών αποδεικτικών στοιχείων για παράδειγμα στη μνήμη ενός υπολογιστή με πολυάριθμα αρχεία και δεδομένα.
- **Αναζήτηση κακόβουλου λογισμικού:** Η Τεχνητή Νοημοσύνη έχει τη δυνατότητα να συμβάλει στον εντοπισμό κακόβουλου λογισμικού και παράλληλα να συνεισφέρει στην αξιολόγηση πιθανών απειλών εξετάζοντας με αυτοματοποιημένο τρόπο ύποπτα αρχεία και κώδικα.
- **Ανάλυση εικόνας και βίντεο:** Η Τεχνητή Νοημοσύνη έχει τη δυνατότητα να συμβάλει στην ανάλυση εικόνων και βίντεο από χώρους εγκλημάτων (π.χ. ληστείες), με σκοπό τόσο την αναγνώριση προσώπων όσο και την ανίχνευση αντικειμένων, στοιχεία που είναι πολύ σημαντικά για την ανακάλυψη δραστών και τη διασφάλιση για λογαριασμό των αρχών ισχυρών αποδεικτικών στοιχείων και στοιχείων ταυτοποίησης στο δικαστήριο.
- **Προληπτική Ανάλυση:** Η Τεχνητή Νοημοσύνη με κατάλληλα προγράμματα και αλγόριθμους έχει την δυνατότητα να προβλέψει πιθανούς κινδύνους, ενδεχόμενα πεδία διάπραξης εγκλημάτων και κενά ασφαλείας, επιτρέποντας τη λήψη προληπτικών μέτρων. Η τεχνητή νοημοσύνη μπορεί να εντοπίζει ίχνη ύποπτης

[93] Τεχνητή Νοημοσύνη για όλους, Μανώλης Ανδριωτάκης, εκδ Ψυχογιός 2022, σελ 186-187

[94] Amit Kumar Tyagi, Shrikant Tiwari, Senthil Kumar Arumugam, Avinash Kumar Sharma, Artificial Intelligence-Enabled Digital Twin for Smart Manufacturing, 2024, page 392

δραστηριότητας, παρακολουθώντας τη συμπεριφορά των χρηστών. Ένα παράδειγμα η διακίνηση παιδικής πορνογραφίας[95].

5.1 Απειλές - Προκλήσεις στην Ψηφιακή Εγκληματολογία

Οι απειλές μέσα στον κόσμο του διαδικτύου είναι πολυάριθμες και πολύπλοκες, απαιτώντας για την αντιμετώπιση τους εξειδικευμένες γνώσεις, ειδικές διαδικασίες και τα κατάλληλα εργαλεία. Οι απειλές έχουν δυναμικό χαρακτήρα, αυξάνονται με γεωμετρική πρόοδο και πλέον αποτελούν σημαντικό τομέα της δραστηριότητας των κρατών και των αρχών επιβολής του νόμου, απορροφώντας πολλούς πόρους. Σε πρακτικό επίπεδο, το σύνολο σχεδόν των εγκλημάτων που προβλέπονται από τον Ποινικό Κώδικα έχουν μεταφερθεί στο διαδίκτυο. Ενδεικτικά τέτοιες απειλές είναι:

- Οι επιθέσεις Ransomware, που αποτελούν τις πιο διαδεδομένες στο κόσμο απειλές που πλήττουν την οικονομία και τις επιχειρήσεις και είναι το κακόβουλό λογισμικό οι δράστες εισχωρούν σε κάποιο υπολογιστικά συστήματα εταιρειών ή φυσικών προσώπων και έχουν σαν στόχο να κλειδώσει αρχεία και οι δράστες ζητούν χρήματα για να τα ξανακάνουν προσβάσιμα στους χρήστες τους.
- Οι επιθέσεις στην εφοδιαστική αλυσίδα, όπου με διείσδυση μέσα στις εταιρείες οι δράστες αποκτούν πρόσβαση σε πλήθος από δεδομένα.
- Ευπάθειες συσκευών IoT
- Εξελιγμένες Μόνιμες Απειλές (Advanced Persistent Threats - APTs): Οργανωμένες ομάδες που συνήθως συνδέονται με κράτη, δημιουργούν στοχευμένες επιθέσεις με χαρακτήρα κατασκοπείας, υποκλοπής δεδομένων, παραβίαση κρίσιμων υποδομών κ.λπ.

Η πρόκληση που αντιμετωπίζουν οι κοινωνίες είναι πώς αυτές οι απειλές στον τομέα του Ψηφιακού Εγκλήματος θα εξουδετερωθούν και θα καταστούν διαθέσιμα λογισμικά που θα συμβάλλουν στην πρόληψη των απειλών και τον μετριασμό των επιπτώσεων. Οι δυνατότητες της Τεχνητής Νοημοσύνης αναμένεται να διαδραματίσουν καταλυτικό ρόλο, επιτρέποντας μεταξύ άλλων την αυτοματοποίηση των συνήθων εργασιών ασφαλείας. Οι ειδικοί ανακριτικοί υπάλληλοι έτσι θα μπορούν να επικεντρωθούν σε πιο σύνθετες και ευαίσθητες εργασίες, κάτι που θα προσφέρει την ευκαιρία για την αύξηση της αποτελεσματικότητας στη διερεύνηση των εγκλημάτων.

5.2 Ψηφιακή Εγκληματολογία και Τεχνητή Νοημοσύνη

Η Ψηφιακή Εγκληματολογική έρευνα είναι ίσως η μεγαλύτερη πρόκληση που αντιμετωπίζουν οι διωκτικές αρχές. Όσο το έγκλημα, σαν ένας ζωντανός οργανισμός, εξελίσσεται, μεταβάλλεται για να επιβιώσει να εξελιχθεί, αντίστοιχα θα πρέπει να εξελιχθεί και να αλλάξει ο τρόπος ερευνών των διωκτικών αρχών. Στη νέα εποχή, όπου οι εξελίξεις στην Τεχνητή Νοημοσύνη αναπτύσσει αλματωδώς τις δυνατότητές της είναι αναπόφευκτο

[95] Amit Kumar Tyagi, Shrikant Tiwari, Senthil Kumar Arumugam, Avinash Kumar Sharma, Artificial Intelligence-Enabled Digital Twin for Smart Manufacturing, 2024, page 393-395

αυτές να ενταχθούν στον χώρο του εγκλήματος και από τις πλευρά των δραστών όσο και από τις διωκτικές αρχές. Στο πλαίσιο της ψηφιακής εγκληματολογίας, η Τεχνητή Νοημοσύνη μπορεί να συμβάλλει στην αποτελεσματικότερη διαδικασία ερευνών στην εξιχνίαση ενός εγκλήματος αυτοματοποιώντας διαδικασίες, μειώνοντας την αναγκαιότητα συμβολής του ανθρώπινου παράγοντα στη σταχυολόγηση των στοιχείων που προέρχονται από τον τόπο ενός εγκλήματος. Ενδεικτικά, η Τεχνητή Νοημοσύνη δύναται να συμβάλει στις ακόλουθες δραστηριότητες της ψηφιακής εγκληματολογίας[96]:

- **Ανάλυση και εξαγωγή δεδομένων:** Εφαρμογή αυτοματοποιημένης ανάλυσης και εξαγωγής δεδομένων από διαφορετικές μορφές αρχείων, όπως έγγραφα, email, αρχεία καταγραφής συνομιλιών και βάσεις δεδομένων.
- **Ανάλυση χρονολογίου:** Δημιουργία και τήρηση ημερολογίου / χρονολογίου κατά τη διαδικασία ερευνών.
- **Αναζήτηση λέξεων-κλειδιών και προτύπων:** Χρήση αλγορίθμων μηχανικής μάθησης για τη βελτίωση των δυνατοτήτων αναζήτησης.
- **Ανάλυση αρχείων καταγραφής:** Αυτοματοποίηση της ανάλυσης των αρχείων καταγραφής σε διάφορες συσκευές και πιο αποτελεσματική ανίχνευση ύποπτων δραστηριοτήτων.
- **Ενοποίηση συστημάτων διαχείρισης υποθέσεων:** Ενσωμάτωση και ενοποίηση όλων των ψηφιακών εγκληματολογικών διαδικασιών που εκτελούνται από υπηρεσίες που είναι αρμόδιες για την έρευνα.
- **Ανίχνευση ανωμαλιών και προγνωστική ανάλυση:** Χρήση της μηχανικής μάθησης και της τεχνητής νοημοσύνης για ανίχνευση ανωμαλιών και προγνωστική ανάλυση.
- **Διασφάλιση Ποιότητας:** Ποιοτική εξασφάλιση των ερευνών και ενίσχυση της αξιοπιστίας των διαδικασιών.
- **Συνεχής βελτίωση - Διαρκής Εκπαίδευση**: Ενημέρωση και βελτίωση πάνω σε δημιουργία σεναρίων που αφορούν μελλοντικές απειλές αλλά και ήδη τετελεσμένα εγκλήματα.

5.3 Οφέλη, Μειονεκτήματα και Προκλήσεις της Τεχνητής Νοημοσύνης στην Ψηφιακή Εγκληματολογία

Όπως αναφέρθηκε ανωτέρω, η τεχνητή νοημοσύνη δύναται να συνεισφέρει σε πολλούς τομείς της Ψηφιακής Εγκληματολογίας και να διαμορφώσει ένα νέο περιβάλλον στον τρόπο διεύρυνσης του εγκλήματος. Επιπρόσθετα προς την κατεύθυνση της αυτοματοποίησης ή ενίσχυσης της ποιότητας εργασιών, ένα πρόσθετο σημαντικό όφελος είναι η μείωση του απαιτούμενου χρόνος για την εκτέλεση των ενεργειών, ακόμη και σε επίπεδα απόκρισης σε πραγματικό χρόνο. Σημαντική ωφέλεια είναι επίσης η παροχή δυνατότητας να διεκπεραιωθεί συνδυαστικός ο χειρισμός μεγάλου όγκου δεδομένων από πολλαπλές πηγές σε σύντομο χρονικό διάστημα. Επιπρόσθετα, με την Τεχνητή Νοημοσύνη υπάρχει η δυνατότητα να μπορούν οι ειδικοί ανακριτικοί υπάλληλοι, ειδικά στα εγκλήματα που διαπράττονται στο διαδίκτυο, να παρακολουθούν τη συμπεριφορά των χρηστών και του

[96] Artificial Intelligence-Enabled Digital Twin for Smart Manufacturing, Amit Kumar Tyagi, Shrikant Tiwari, Senthil Kumar Arumugam, Avinash Kumar Sharma, 2024 Scrivener Publishing, page 400-403

συστήματος ταυτόχρονα και να εντοπίζουν πιθανές ανωμαλίες, τρωτά σημεία και πιθανές απειλές. Επιπλέον με την Τεχνητή Νοημοσύνη είναι δυνατόν να βελτιωθεί ο βαθμός αξιοποίησης των πόρων που είναι διαθέσιμοι για την έρευνα ενός εγκλήματος, τόσο ανθρώπινων όσο και οικονομικών. Με τον τρόπο αυτό μπορούν να εξοικονομηθούν οικονομικοί πόροι για να διατεθούν σε άλλους σκοπούς, όπως π.χ. υλικοτεχνικές προμήθειες, αλλά και να εξοικονομηθούν εργατοώρες και ανθρώπινο δυναμικό για να επικεντρωθούν σε πιο σύνθετες εργασίες[97].

Παρόλα αυτά, με την είσοδο της Τεχνητής Νοημοσύνης δημιουργήθηκαν ή μπορούν να δημιουργηθούν καταστάσεις αρνητικές για την έρευνα στο πλαίσιο ενός εγκλήματος. Μία αρχική αρνητική διάσταση είναι η δυνατότητα χρήσης της Τεχνητής Νοημοσύνης από τους δράστες για τη διάπραξη του εγκλήματος ή για την αποφυγή του εντοπισμού τους. Μία ακόμη αρνητική πτυχή θα μπορούσε να είναι η αδυναμία της Τεχνητής Νοημοσύνης να κατανοήσει επαρκώς το πλαίσιο λειτουργιών μια υπηρεσίας ή το νομικού συστήματος από το οποίο διέπονται οι έρευνες και η προανάκριση. Μία σημαντική διάσταση είναι το κατά πόσο η χρήση της Τεχνητής Νοημοσύνης στις έρευνες και στην ψηφιακή εγκληματολογία θα παρέχει την αξιοπιστία της προστασίας των διαδικασιών και κυρίως της προστασίας του απορρήτου των προσωπικών δεδομένων των θυμάτων και των θυτών καθώς και της αρχής της μυστικότητας από την οποία οφείλει να διέπεται η προανάκριση και οι δικαστικές διαδικασίες.

Οι προκλήσεις για τη χρήση της Τεχνητής Νοημοσύνης στη διερεύνηση εγκλημάτων και γενικότερα στην εισδοχή της στον τομέα της Εγκληματολογίας, είναι πολλές. Πριν από χρόνια διαγραφόταν ως μία εξέλιξη που αφορά το μακρινό μέλλον, πλην όμως οι εξελίξεις ήταν ραγδαίες και πλέον Τεχνητή Νοημοσύνη εφαρμόζεται στην Ψηφιακή Εγκληματολογία, όπως και σε άλλους τομείς της ανθρώπινης δραστηριότητες. Οι προκλήσεις που παρουσιάζονται, και θα πρέπει να αντιμετωπιστούν από τους ειδικούς και τα κέντρα λήψης αποφάσεων ενδεικτικά μπορεί να είναι[98]:

- **Έλλειψη δεξιοτήτων:** Υπάρχει έλλειψη ατόμων οι οποίοι είναι εκπαιδευμένοι στον τομέα Τεχνητής Νοημοσύνης γενικότερα, αλλά και στον τομέα της ψηφιακής εγκληματολογίας. Είναι κατανοητό ότι ελάχιστο προσωπικό κατέχει δεξιότητες τόσο στην τεχνητή νοημοσύνη όσο και στην ψηφιακή εγκληματολογία.
- **Ποιότητα στοιχείων:** Η αποτελεσματικότητα των μοντέλων τεχνητής νοημοσύνης εξαρτάται από την ποιότητα και ποσότητα στοιχείων πάνω στα οποία εκπαιδεύονται οι σχετικοί αλγόριθμοι.
- **Δικαιοσύνη:** Η αυστηρή εφαρμογή του γράμματος του νόμου δεν οδηγεί απαραίτητα σε καλύτερης ποιότητας αποφάσεις που να εναρμονίζονται με το δίκαιο. Η διαρκής αλλαγή των νόμων και των κανόνων είναι επίσης ένα ζήτημα που θα πρέπει να εξετασθεί.

[97] Artificial Intelligence-Enabled Digital Twin for Smart Manufacturing, Amit Kumar Tyagi, Shrikant Tiwari, Senthil Kumar Arumugam, Avinash Kumar Sharma, 2024 Scrivener Publishing, page 405-407

[98] Artificial Intelligence-Enabled Digital Twin for Smart Manufacturing, Amit Kumar Tyagi, Shrikant Tiwari, Senthil Kumar Arumugam, Avinash Kumar Sharma, 2024 Scrivener Publishing, page 407-408

- **Ταχεία εξέλιξη:** Οι απειλές και το έγκλημα εξελίσσονται συνεχώς και τα συστήματα που βασίζονται σε Τεχνητή Νοημοσύνη πρέπει να προσαρμόζονται τάχιστα για να παραμείνουν αποτελεσματικά.

5.4 Τεχνητή Νοημοσύνη στην Πρόληψη και Ανίχνευση Απειλών

Οι απειλές στο διαδίκτυο αλλά και στις διαδικασίες συλλογής στοιχείων κατά τη διερεύνηση εγκλημάτων αποτελούν ένα παράγοντα που η Τεχνητή Νοημοσύνη μπορεί να συμβάλλει αποτελεσματικά. Αυτό μπορεί να επιτευχθεί με τη δημιουργία σχετικών αλγορίθμων, οι οποίοι θα συλλέγουν στοιχεία και θα τα αναλύουν προκειμένου να εντοπίζουν πιθανές απειλές, λειτουργώντας με τη διαδικασία της προσομοίωσης. Τέτοιοι αλγόριθμοι και συναφείς προσομοιώσεις μπορεί να είναι[99]:

- **Πλατφόρμες Πληροφοριών Απειλών**: Πρόκειται για λογισμικό που συλλέγει, αναλύει και διαχειρίζεται δεδομένα απειλών από διάφορες πηγές, παρέχοντας στους οργανισμούς αξιοποιήσιμες πληροφορίες για τη αναβάθμιση της ασφάλειάς τους και την αντιμετώπιση απειλών.
- **Honeypots - Honeynets**: Πρόκειται για δίκτυα που έχουν σχεδιαστεί για να προσελκύουν παράνομες συμπεριφορές, δίνοντας πολύτιμες πληροφορίες στις διωκτικές αρχές και λειτουργώντας αποτρεπτικά. Επιπρόσθετα μέσα από την συλλογή και αξιοποίηση των στοιχείων συμβάλουν στην καταστολή και συνεπώς στην εξιχνίαση των εγκλημάτων.
- **Malware Sandboxing**: Τα sandboxes κακόβουλου λογισμικού βοηθούν στον εντοπισμό και μελέτη των κακόβουλων συμπεριφορών.
- **Ανάλυση Απειλών:** Η Ανάλυση Απειλών αποτελεί προληπτική μέθοδο κυβερνοασφάλειας που χρησιμοποιείται για την ανίχνευση κακόβουλου λογισμικού (malware) και άλλων απειλών, αναλύοντας τη συμπεριφορά και τα χαρακτηριστικά τους αντί να βασίζεται αποκλειστικά σε γνωστές υπογραφές ή μοτίβα.
- **Machine Learning – AI**: Οι αλγόριθμοι μηχανικής μάθησης, έχουν δυνατότητα να αναλύουν ταυτόχρονα πολλά δεδομένα αναγνωρίζοντας γνωστές αλλά και νέες απειλές σε ελάχιστο χρόνο.
- **Αλγόριθμοι Ανίχνευσης Απειλών**: Αυτοί αλγόριθμοι έχουν την ικανότητα να προσδιορίζουν τις αποκλίσεις από την κανονική συμπεριφορά χρηστών, η οποία μπορεί να υποκρύπτει παραβατικές συμπεριφορές.
- **Αλγόριθμοι Παρακολούθησης Dark Web**.: Οι αλγόριθμοι αυτοί παρακολουθούν ένα κομμάτι του διαδικτύου όπου κατά κύριο λόγο εξελίσσονται εγκλήματα και διακινούνται στοιχεία και δεδομένα που αφορούν παραβατικές συμπεριφορές (παιδική πορνογραφία, εμπόριο ναρκωτικών και όπλων, ξέπλυμα χρήματος μέσω ψηφιακών νομισμάτων κ.ά.).
- **Κανόνες YARA**[100]: Οι κανόνες YARA είναι ουσιαστικά ένα σύνολο οδηγιών που καθορίζουν τα χαρακτηριστικά ενός συγκεκριμένου τύπου κακόβουλου λογισμικού

[99] Artificial Intelligence-Enabled Digital Twin for Smart Manufacturing, Amit Kumar Tyagi, Shrikant Tiwari, Senthil Kumar Arumugam, Avinash Kumar Sharma, 2024 Scrivener Publishing, page 409-411

[100] YARA's documentation, Ιστοσελίδα https://yara.readthedocs.io/en/latest/

ή απειλής. Λειτουργούν σαρώνοντας αρχεία ή ροές δεδομένων για συγκεκριμένα μοτίβα ή συμβολοσειρές που σχετίζονται με κακόβουλη δραστηριότητα.

- **Τεχνικές επεξεργασίας φυσικής γλώσσας -NLP:** Οι τεχνικές NLP χρησιμοποιούνται για να αντλούν οι ερευνητές στοιχεία για απειλές από πηγές του διαδικτύου ευρέως γνωστές όπως ειδήσεις, άρθρα, αναφορές και από τα μέσα κοινωνικής δικτύωσης.
- **Ανάλυση GeoIP**: Οι αλγόριθμοι αυτοί χρησιμοποιούνται στην ανάλυση και εντοπισμό απειλών με γεωγραφικό προσδιορισμό. Μπορούν να έχουν χρήση στην ψηφιακή εγκληματολογία για υβριδικού τύπου απειλές όπως πολλαπλοί εμπρησμοί σε διάφορα μέρη μιας περιοχής.

Θα πρέπει να προστεθεί εδώ ότι όλες οι ωφέλειες και οι προκλήσεις που σχετίζονται με την Τεχνητή Νοημοσύνη, θα πρέπει να εξετάζονται σε συνδυασμό με τα τυχόν ηθικά ζητήματα που ανακύπτουν. Η χρήση της Τεχνητής Νοημοσύνης θα πρέπει να γίνεται πάντα στο πλαίσιο της τήρησης δεοντολογικών κανόνων και βέλτιστων πρακτικών, προάγοντας τη διαφάνεια, τη δικαιοσύνη, τον σεβασμό στα δικαιώματα των εμπλεκομένων και λοιπές αρχές που σχετίζονται με την ηθική και τη δεοντολογία.

5.5 Μελλοντικές τάσεις της Τεχνητής Νοημοσύνης στην Ψηφιακή Εγκληματολογία

Ήδη διαγράφονται τάσεις για εισαγωγή και αξιοποίηση της τεχνητής νοημοσύνης στον τομέα της Ψηφιακής Εγκληματολογίας, οι οποίες συζητούνται και αναπτύσσονται. Αρχικά, δημιουργούνται ειδικές πλατφόρμες Τεχνητής Νοημοσύνης για την έγκαιρη και έγκυρη αναζήτηση απειλών όπως η AI – Enhanced Security Information and Event Management - SIEM. Σχεδιάζονται αλγόριθμοι Τεχνητής Νοημοσύνης που θα αναλύουν και θα επεξεργάζονται την συμπεριφορά χρηστών στο διαδίκτυο με την βοήθεια της Μηχανικής Μάθησης. Αναπτύσσονται προγράμματα που θα βοηθήσουν στον εντοπισμό παραβατικών συμπεριφορών μέσα σε ένα δίκτυο, ερευνώντας την συσκευή και όχι ολόκληρο δίκτυο. Επιπρόσθετα, στο μέλλον η Τεχνητή Νοημοσύνη θα μπορεί να χρησιμοποιεί πληροφορίες για την εκπαίδευση στελεχών στο έγκλημα χωρίς να διακινδυνεύονται απόρρητες πληροφορίες και διαδικασίες, βελτιώνοντας σημαντικά τον τρόπο εκπαίδευσης. Επιπλέον η Τεχνητή Νοημοσύνη αναμένεται να βοηθήσει στο μέλλον τις υπηρεσίες ασφαλείας να ανταποκριθούν πιο γρήγορα σε περιστατικά με αυτοματοποιημένες διαδικασίες. Η Τεχνητή Νοημοσύνη εκτιμάται ότι θα συμβάλει στην αντιμετώπιση της απάτης μέσω διαδικτύου, όπως π.χ. το phishing, με δημιουργία και εφαρμογή κατάλληλων μοντέλων μηχανικής μάθησης που να αναλύουν τα δεδομένα και θα εντοπίζουν με αποτελεσματικό τρόπο παραβατικές και επικίνδυνες συμπεριφορές. Μελετάται επίσης η δημιουργία μεθόδων που βασίζονται στην Τεχνητή Νοημοσύνη για την ανάπτυξη ασφαλών τρόπων κρυπτογράφησης, αλλά και ανίχνευσης μη εξουσιοδοτημένης πρόσβασης σε περιβάλλοντα cloud.

Όσο εξελίσσεται η τεχνολογία τόσο εξελίσσονται και οι διαδικασίες στην Ψηφιακή Εγκληματολογία σημειώνοντας βελτίωση στο τρόπο αντιμετώπισης νέων μορφών εγκληματικότητας αλλά και διευρύνοντας την αντιμετώπιση των παραδοσιακών μορφών. Η εξέλιξη όμως αυτή έχει να κάνει παράλληλα και με την εξέλιξη της τεχνητής νοημοσύνης ως όπλο στα χέρια των εγκληματιών. Υπάρχουν ακόμα τομείς που η Τεχνητή Νοημοσύνη μπορεί

να βοηθήσει και να αναπτύξει για την αποτελεσματική αντιμετώπιση του εγκλήματος. Τέτοιοι τομείς ενδεικτικά μπορεί να είναι[101]:

- Αντιμετώπιση επιθέσεων που χρησιμοποιούν κβαντική υπολογιστική.
- Χρήση Τεχνητής Νοημοσύνης για επαύξηση της ασφάλειας σε περιβάλλον IoT.
- Χρήση Τεχνητής Νοημοσύνης για επαύξηση της ασφάλειας Δικτύων 5G και 6G.
- Χρήση Τεχνητής Νοημοσύνης για επαύξηση της ασφάλειας σε περιβάλλον Cloud.
- Χρήση Τεχνητής Νοημοσύνης για επαύξηση της ασφάλειας Συστημάτων Βιομηχανικού Ελέγχου (ICS).
- Χρήση Τεχνητής Νοημοσύνης για επαύξηση της ασφάλειας σε περιβάλλοντα Edge Computing.
- Χρήση Τεχνητής Νοημοσύνης για επαύξηση της ασφάλειας σε συστήματα Cyber - Physical Systems (αυτόνομα οχήματα).
- Χρήση Τεχνητής Νοημοσύνης για επαύξηση της ασφάλειας σε συστήματα ταυτοποίησης και ελέγχου πρόσβασης – Enhanced Identity and Access Management.
- Χρήση Τεχνητής Νοημοσύνης για την ασφαλή ανάπτυξη λογισμικού.
- Χρήση Τεχνητής Νοημοσύνης για επαύξηση της ασφάλειας του απορρήτου.

[101] Amit Kumar Tyagi, Shrikant Tiwari, Senthil Kumar Arumugam, Avinash Kumar Sharma, Artificial Intelligence-Enabled Digital Twin for Smart Manufacturing, 2024, page 411-417

6 ΨΗΦΙΑΚΗ ΑΝΑΚΡΙΤΙΚΗ ΠΡΑΞΗ

6.1 Έννοια

Η ανακριτική πράξη αποτελεί τη βασική ενέργεια κάθε ανακριτικού υπαλλήλου καθώς επίσης και την βασική ενέργεια όπως ορίζει ο Κώδικας Ποινικής Δικονομίας με σκοπό την ανακάλυψη της αλήθειας όταν διαπράττεται ένα έγκλημα, την ταυτοποίηση των κατηγορουμένων και την διαδικασία να οδηγηθούν αυτοί ενώπιων των δικαστηρίων. Στα ηλεκτρονικά εγκλήματα συμβαίνει ακριβώς το ίδιο δηλαδή η ανακριτική πράξη, που εδώ την ονομάζουμε ψηφιακή ανακριτική πράξη. Χαρακτηριστικό γνώρισμα των εγκλημάτων αυτών και βασικό πλεονέκτημα των αρχών είναι το γεγονός ότι ο δράστης αφήνει ίχνη σε επεξεργάσιμη μορφή.

Ιδανικά μια έρευνα ενός εγκλήματος γενικά για να θεωρηθεί ολοκληρωμένη θα πρέπει να απαντά στα κάτωθι ερωτήματα:

- Ποιος έκανε το έγκλημα; Σε βάρος ποιου; Ποιοι εμπλέκονται; (ερώτημα Who)
- Που έγινε το έγκλημα; (ερώτημα Where)
- Πότε έγινε το έγκλημα; (ερώτημα When)
- Τι ακριβώς συνέβη; (ερώτημα What)
- Γιατί έγινε το έγκλημα; (ερώτημα Why)
- Πώς έγινε το έγκλημα; (ερώτημα How)

Η συγκεκριμένη αποτελεί την αρχή Five W & One H, κλασική διαχρονική προσέγγιση αστυνομικής έρευνας αλλά και δημοσιογραφικής. Στην έρευνα ψηφιακών εγκλημάτων ο τρόπος προσέγγισης της έρευνας ακολουθεί επίσης τα ανωτέρω ερωτήματα, ωστόσο μεταβάλλονται ως προς τον χαρακτήρα και τις ιδιότητες κάποια στοιχεία, όπως όπως ο χώρος, καθόσον ο τόπος στο διαδίκτυο δεν είναι κάτι ξεκάθαρο και τα πληροφοριακά συστήματα που χρησιμοποιούνται για τη διάπραξη εγκλημάτων μπορεί να βρίσκονται οπουδήποτε και δεν υπάρχει ανάγκη να ταυτίζονται με τον φυσικό χώρο που βρίσκεται ο δράστης, το θύμα ή ο μάρτυρας.

Με αυτό τον τρόπο, το μέσο τέλεσης του εγκλήματος, το σώμα του εγκλήματος, τα προϊόντα του εγκλήματος (π.χ. η κίνηση χρημάτων που αποκτήθηκαν με την χρήση ψηφιακών δεδομένων ταυτότητας, που έχουν υποκλαπεί με phishing) και τα ψηφιακά ίχνη (δεδομένα κίνησης και θέσης) που δημιουργήθηκαν κατά την τέλεση του ηλεκτρονικού εγκλήματος και αφορούν στον αποστολέα, τον αποδέκτη, τον τόπο, τον χρόνο, τον τρόπο και τυχόν άλλες περιστάσεις που χρησιμοποιήθηκαν για την τέλεση του, μπορούν να απαντήσουν στα ανωτέρω ερωτήματα προσαρμοζόμενα στην νέα ορολογία και στοιχεία που έχουμε σε μια σκηνή εγκλήματος, στα ψηφιακά εγκλήματα.

6.2 Ψηφιακή Πραγματογνωμοσύνη

Η πιο σημαντική ανακριτική πράξη και ταυτόχρονα το ισχυρότερο αποδεικτικό μέσο στα ψηφιακά εγκλήματα είναι η πραγματογνωμοσύνη. Αυτό ισχύει διότι είναι η μόνη που μπορεί να προσφέρει σε όλη τη διάρκεια μιας ανάκρισης, αστυνομικής – δικαστικής, αλλά και σε μια ποινική δίκη ειδικές και εξειδικευμένες γνώσεις. Στο πλαίσιο αυτό, η πραγματογνωμοσύνη

διενεργείται από έμπειρα και με γνώσεις στελέχη της αστυνομίας, καθώς επίσης και σε εξειδικευμένα εργαστήρια με κατάλληλα υπολογιστικά συστήματα και πιστοποιημένο λογισμικό για την διενέργειά εξειδικευμένων εξετάσεων.

6.3 Ειδικές Ανακριτικές Πράξεις

Οι ανακριτικές πράξεις που ορίζονται με το άρθρο 6 του Νόμου 2928/2001 είναι οι αυτές που διενεργούνται κατ' απόλυτη μυστικότητα για συγκεκριμένα εγκλήματα με σκοπό την σύλληψη των δραστών. Τέτοιες ανακριτικές πράξεις ενδεικτικά και πιο συχνές είναι η ανακριτική διείσδυση, οι ελεγχόμενες μεταφορές, η παρακολούθηση της αλληλογραφίας και των τηλεφωνικών συνδιαλέξεων, η ηχητική και οπτική παρακολούθηση. Η διεξαγωγή των ανακριτικών πράξεων αυτών γίνεται πάντα και υποχρεωτικά με την άδεια των Δικαστικών και Εισαγγελικών Αρχών για τον λόγο ότι μπαίνει στην σφαίρα ευαίσθητων δεδομένων ενός ανθρώπου της προσωπικής ζωής του.

Σύμφωνα με το άρθρο 254 του Κώδικα Ποινικής Δικονομίας οι Αστυνομικές και Δικαστικές Αρχές μπορούν να προβούν και έχουν την δυνατότητα να διενεργούν άρσης απορρήτου των επικοινωνιών, καταγραφής της δραστηριότητας εκτός κατοικίας με συσκευές ήχου ή εικόνας, πράξεις δηλαδή που λειτουργούν καθαρά κατασταλτικά για την εξιχνίαση σοβαρών αδικημάτων και την σύλληψη των δραστών**.**[102]

Οι ανακριτικές αυτές πράξεις διεξάγονται, με την τήρηση κάποιων προϋποθέσεων. Αυτές είναι:

α) Να υπάρχουν σοβαρές ενδείξεις ότι έχει τελεστεί αξιόποινη πράξη.

β) Η εξιχνίασή της εγκληματικής οργάνωσης να είναι αδύνατη ή ιδιαιτέρως δυσχερής, χωρίς την εφαρμογή αυτών των πράξεων.

Για να εφαρμοστούν οι ανακριτικές αυτές πράξεις απαραίτητη προϋπόθεση είναι να έχει εκδοθεί σχετικό βούλευμά του δικαστικού συμβούλιου και η οποία έχει ισχύ έως -2- μήνες αρχικά και έως -1- χρόνο συνολικά. Σε επείγουσες περιπτώσεις την έρευνα μπορεί να διατάξει ο εισαγγελέας ή ο ανακριτής.

Οι ειδικές ανακριτικές πράξεις που χρησιμοποιούνται στην Ψηφιακή Εγκληματολογία είναι οι εξής[103] «:

α) Η συγκαλυμμένη έρευνα, κατά την οποία ο ανακριτικός υπάλληλος ή ένας ιδιώτης που ενεργεί κατ' εντολής του, διαπράττει κάποιό συγκεκριμένο έγκλημα.

β) Η ανακριτική διείσδυση, κατά την οποία ανακριτικός υπάλληλος με συγκαλυμμένα στοιχεία ταυτότητας αναλαμβάνει εξωτερικά καθήκοντα σε μια εγκληματική οργάνωση με σκοπό την εξιχνίαση της.

[102] Άρθρο 254 του Κώδικα Ποινικής Δικονομίας

[103] Άρθρο 20 - Νόμος 4947/2022 - Ειδικές ανακριτικές πράξεις επί ορισμένων εγκλημάτων - Τροποποίηση παρ. 1 άρθρου 254 ΚΠΔ, παρ. 1 άρθρου 13 της Οδηγίας 2019/713

γ) Η άρση του απορρήτου του περιεχομένου των επικοινωνιών.

δ) Η καταγραφή της δραστηριότητας ή άλλων γεγονότων εκτός κατοικίας με συσκευές ήχου ή εικόνας.

ε) Η συσχέτιση των δεδομένων προσωπικού χαρακτήρα.»

6.4 Εγκληματολογική εξέταση των υπολογιστικών συστημάτων και ψηφιακών πειστηρίων

Η εγκληματολογική εξέταση υπολογιστικών συστημάτων και ψηφιακών πειστηρίων περιλαμβάνει τη συλλογή, τεκμηρίωση, εξέταση, ανάλυση και διαφύλαξη των ψηφιακών πειστηρίων, που φέρονται να σχετίζονται με συγκεκριμένους Η/Υ, περιφερειακές αυτών συσκευές ή υπολογιστικά συστήματα. Κάθε τέτοια εξέταση διατάσσεται - στα πλαίσια νόμιμης έρευνας- και διέπεται από τις νομικές προϋποθέσεις των εγκληματολογικών εξετάσεων.

Η εγκληματολογική εξέταση των υπολογιστικών συστημάτων και ψηφιακών πειστηρίων διέπεται από συγκεκριμένες αρχές, η τήρηση των οποίων πρέπει να γίνεται με απόλυτη προσήλωση στο γράμμα και το πνεύμα των προβλέψεων, έτσι ώστε να υπάρχει πλήρης τεκμηρίωση και θεμελίωση των εργαστηριακών εξετάσεων και ευρημάτων, καθώς και αυξημένη αξιοπιστία και πλήρης αποδεικτική ισχύς των συμπερασμάτων.

Οι εν λόγω αρχές αναφέρονται:

- στον τρόπο συλλογής και τεκμηρίωσης των υπολογιστικών συστημάτων και ψηφιακών πειστηρίων,
- στον τρόπο εξέτασης και ανάλυσης,
- στον χρησιμοποιούμενο εξοπλισμό και εργαστηριακές τεχνικές.

6.4.1 Κύρια Διαδικασία Εξέτασης

Η κύρια διαδικασία εξέτασης περιλαμβάνει:

α. Την αναγνώριση των πειστηρίων υπολογιστικών συστημάτων

- Αναγνώριση του μηχανικού μέρους του υπολογιστικού συστήματος – hardware (ηλεκτρονικοί υπολογιστές, κινητά, καλώδια δικτύου, ηλεκτρονικές πλακέτες κ.λπ.), που περιέχουν ψηφιακές πληροφορίες.
- Διάκριση των χρήσιμων πληροφοριών, συσκευών και δεδομένων.

β. Την προστασία, συλλογή και τεκμηρίωση των πειστηρίων υπολογιστικών συστημάτων

- Συλλογή των πειστηρίων υπολογιστικών συστημάτων, με παράλληλη καταγραφή της ακριβής θέσης ανευρέσεώς τους.
- Προσεκτική συσκευασία, φύλαξη και μεταφορά των πειστηρίων.
- Προστασία των πειστηρίων από τη δόλια ή τυχαία αλλοίωσή (εγγραφή / διαγραφή) τους. Για τον σκοπό αυτό ακολουθούνται συγκεκριμένες -διεθνώς παραδεκτές- διαδικασίες και τεχνικές που είναι αποδεκτές από τις Δικαστικές ή άλλες αρμόδιες

Αρχές. Το πειστήριο ως υπολογιστικό σύστημα πρέπει να διατηρείται στην αρχική του κατάσταση, με σκοπό να επιδειχθεί αναλλοίωτο σε κάθε αρμόδιο και να τύχει σχετικής εργαστηριακής αξιοποίησής του από τυχόν τεχνικούς συμβούλους.
- Δημιουργία ακριβούς αντιγράφου.
- Καταγραφή των ημερομηνιών που προκύπτουν και αποδεικνύουν το χρόνο δημιουργίας του ψηφιακού πειστηρίου και το χρόνο τελευταίας τροποποίησης του.
- Παραγωγή μοναδικής αλφαριθμητικής ταυτότητας του πειστηρίου μέσω αλγορίθμου (Hash Value).

γ. Την ταξινόμηση, εξέταση, σύγκριση και εξατομίκευση των ψηφιακών πειστηρίων

- Ταξινόμηση μέσω αναζήτησης «γενικών» χαρακτηριστικών.
- Σύγκριση αρχείων, πληροφοριών. Αποτελεί το «κλειδί» της εξέτασης των ψηφιακών πειστηρίων, διαμέσου της οποίας εντοπίζονται εξατομικευμένα χαρακτηριστικά.

δ. Την ανασυγκρότηση και διατήρηση των υπολογιστικών συστημάτων και ψηφιακών πειστηρίων

- Ανασυγκρότηση πειστηρίων υπολογιστικών συστημάτων που έχουν καταστραφεί. Η ανασυγκρότηση εξαρτάται από τον τύπο του υπολογιστικού συστήματος και των ψηφιακών πειστηρίων, όπως π.χ. τον τύπο του Η/Υ, το λειτουργικό σύστημα, τη διαμόρφωση του μηχανικού μέρους του Η/Υ- hardware και τις εφαρμογές.

ε. Ανασυγκρότηση πειστηρίου.

- Ταξινόμηση των ψηφιακών πειστηρίων, με τρόπο ώστε να ανασυγκροτηθεί η σειρά των γεγονότων που συντέλεσαν στο έγκλημα. Η ανασυγκρότηση είναι πολύ σημαντική για να μπορέσει να διαπιστωθεί η πρόθεση τέλεσης ή όχι του εγκλήματος.

Για την εργαστηριακή εξέταση των ψηφιακών πειστηρίων από τις Ελληνικές αρμόδιες Αρχές χρησιμοποιείται ειδικός εγκληματολογικός εξοπλισμός και λογισμικό, ανάλογα με εκείνα που χρησιμοποιούν τα πιο προηγμένα αντίστοιχα εγκληματολογικά Εργαστήρια της Ευρώπης και των Η.Π.Α. και σύμφωνα με τις διεθνώς αποδεκτές πρακτικές.

6.5 Διατήρηση Ψηφιακών Δεδομένων

Σύμφωνα με την Οδηγία 2006/24/ΕΚ, η οποία εφαρμόζεται στην Ελλάδα με τον Νόμο 3917/2011, ρυθμίστηκε η διατήρηση των δεδομένων κίνησης και θέσης που παράγονται κατά τη διαβίβαση ηλεκτρονικών επικοινωνιών για τη διερεύνηση και τη δίωξη εγκλημάτων. Οι πάροχοι ηλεκτρονικών επικοινωνιών υποχρεούνται να διατηρούν για συγκεκριμένο χρονικό διάστημα ήτοι από -6- μήνες έως -2- έτη, τα δεδομένα κίνησης που παράγονται από την ηλεκτρονική επικοινωνία.[104]

[104] Οδηγία 2006/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Μαρτίου 2006 , για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών και για την τροποποίηση της οδηγίας 2002/58/ΕΚ

Ο πλήρης κατάλογος των δεδομένων που θα πρέπει να διατηρούνται από τους παρόχους των εταιρειών επικοινωνίας περιλαμβάνει μεταξύ άλλων, τον τηλεφωνικό αριθμό, τα προσωπικά στοιχεία του καλούντος, την ημερομηνία και ώρα της επικοινωνίας και την διάρκεια αυτής, τους κωδικούς IMSI[105] και IMEI[106], τη γεωγραφική θέση του καλούντος και του καλουμένου, τη χρονοσήμανση της σύνδεσης με την υπηρεσία ηλεκτρονικού ταχυδρομείου, τα στοιχεία του κατόχου του πρωτοκόλλου IP. Είναι σημαντικό να τονίσουμε ότι στην οδηγία προβλέπεται ρητά η απαγόρευση διατήρησης του περιεχομένου της επικοινωνίας.

[105] Η διεθνής ταυτότητα συνδρομητή κινητής τηλεφωνίας (International Mobile Subscriber Identity - IMSI) είναι ένας μοναδικός αριθμός 64-bit που αποθηκεύεται στην κάρτα SIM και προσδιορίζει μοναδικά τον συνδρομητή στα δίκτυα κινητής τηλεφωνίας.

[106] Ο αριθμός Διεθνούς Ταυτότητας Κινητού Εξοπλισμού (International Mobile Equipment Identity, IMEI) είναι ένας αριθμός, συνήθως μοναδικός, για την αναγνώριση κινητών τηλεφώνων. Ο αριθμός IMEI χρησιμοποιείται τόσο για την αναγνώριση των νομότυπων συσκευών, όσο και για τον αποκλεισμό συσκευών που έχουν δηλωθεί ως κλαπείσες.

7 Η ΕΛΛΗΝΙΚΗ ΑΣΤΥΝΟΜΙΚΗ ΠΡΑΓΜΑΤΙΚΟΤΗΤΑ

Τα τελευταία χρόνια για τα ελληνικά δεδομένα διαπιστώθηκε μία ραγδαία αύξηση υποθέσεων οι οποίες αφορούν εγκλήματα που διαπράττονται με την χρήση της ψηφιακής τεχνολογίας αλλά και υποθέσεων εγκληματικής δραστηριότητας μέσω του διαδικτύου.

Η Ελληνική Αστυνομία κατελήφθη απροετοίμαστη στις αρχές του 2000 και ο προβληματισμός που επικράτησε ήταν μεγάλος, καθώς εκτιμήθηκε ότι οι διαστάσεις του προβλήματος είναι πολύ μεγαλύτερες από αυτές που απεικονίζουν οι υποθέσεις που καταγγέλλονται. Είναι εύλογο να φθάνει στις αστυνομικές αρχές μόνο ένα μέρος των υποθέσεων που αφορούν το ηλεκτρονικό έγκλημα.

Με το Προεδρικό Διάταγμα 178 του 2014 ιδρύθηκε στην Ελληνική Αστυνομία η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος με έδρα την Αθήνα η Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος με έδρα τη Θεσσαλονίκη. Με σκοπό την πρόληψη, την έρευνα και την καταστολή εγκλημάτων ή αντικοινωνικών συμπεριφορών, που διαπράττονται μέσω του διαδικτύου ή άλλων μέσων ηλεκτρονικής επικοινωνίας. Η ίδρυση των Υπηρεσιών αυτών έγινε ως αναγκαία προσαρμογή των διωκτικών Αρχών και της Ελληνικής Αστυνομίας στην αυξανόμενη τάση διάπραξης εγκλημάτων μέσω διαδικτύου και στην ανάγκη συνεργασίας με λοιπές υπηρεσίες τόσο μέσα στην Ελλάδα όσο και εφάμιλλες σε άλλες χώρες. Η νέα αυτή υπηρεσία αποτελείται από τα κάτωθι Τμήματα[107] :

α. Τμήμα Διοικητικής Υποστήριξης και Διαχείρισης Πληροφοριών,

β. Τμήμα Καινοτόμων Δράσεων και Στρατηγικής,

γ. Τμήμα Ασφάλειας Ηλεκτρονικών και Τηλεφωνικών Επικοινωνιών και Προστασίας Λογισμικού και Πνευματικών Δικαιωμάτων,

δ. Τμήμα Διαδικτυακής Προστασίας Ανηλίκων και Ψηφιακής Διερεύνησης και

ε. Τμήμα Ειδικών Υποθέσεων και Δίωξης Διαδικτυακών Οικονομικών Εγκλημάτων.»

Επιπρόσθετα στην Διεύθυνση Εγκληματολογικών Ερευνών της Ελληνικής Αστυνομίας ιδρύθηκε και λειτουργεί η Υποδιεύθυνση Ψηφιακής Εγκληματολογικής Έρευνας και Ανάλυσης η οποία σκοπό έχει την εξέταση των ψηφιακών πειστηρίων που συλλέγονται από τον τόπο του εγκλήματος. Η Υπηρεσία λειτουργεί με την πιστοποιημένα πρότυπα και διεθνώς αναγνωρισμένες μεθόδους, και εξετάζει ύστερα από αίτημα των Δικαστικών και Αστυνομικών Αρχών ψηφιακά πειστήρια.

Η ανωτέρω υπηρεσία διαρθρώνεται στα ακόλουθα Τμήματα ήτοι:

α) Τμήμα Διαχείρισης Ψηφιακών Δεδομένων και Ελέγχου Ποιότητας.

β) Τμήμα Εξέτασης Ψηφιακών Πειστηρίων.

[107] Ιστοσελίδα της Ελληνικής Αστυνομίας

γ) Τμήμα Διαχείρισης Εθνικής Βάσης Ψηφιακής Ταυτοποίησης Αρχείων Σεξουαλικής Εκμετάλλευσης Ανηλίκων.

δ) Τμήμα Εξέτασης Οπτικοακουστικού υλικού.

Χαρακτηριστικά θα αναφέρουμε τη διάρθρωση του Τμήματος Εξέτασης Ψηφιακών Πειστηρίων το οποίο έχει τα ακόλουθα τα ακόλουθα εργαστήρια:

- Εργαστήριο Διερεύνησης και Ανάλυσης Ψηφιακών Πειστηρίων, το οποίο είναι αρμόδιο για τη διενέργεια εξετάσεων:
  1. δεδομένων που βρίσκονται σε αποθηκευτικά μέσα ηλεκτρονικών υπολογιστών, τοπικών δικτύων, περιφερειακών ή άλλων ειδικών σταθερών και φορητών μέσων,
  2. δεδομένων που βρίσκονται σε περιβάλλον cloud
  3. σε ηλεκτρονικές συσκευές οι οποίες έχουν την δυνατότητα να αποθηκεύουν ψηφιακά δεδομένα,
  4. σε αποθηκευτικά μέσα σε φορητές ηλεκτρονικές υπολογιστικές συσκευές όπως έξυπνες κινητές συσκευές, drone, συσκευές εντοπισμού θέσης,
  5. σε συσκευές IoT
  6. σε οχήματα και συγκεκριμένα στα ψηφιακά μέρη αυτού.
- Το Εργαστήριο Ανάκτησης και Ανάλυσης Δεδομένων Μη λειτουργικών μέσων, το οποίο ανακτά δεδομένα από κατεστραμμένα αποθηκευτικά μέσα.[108]

[108] Νόμος 5187/2025 - ΦΕΚ Α 48 / 21.03.2025

8 ΣΥΝΟΨΗ ΚΑΙ ΜΕΛΛΟΝΤΙΚΕΣ ΚΑΤΕΥΘΥΝΣΕΙΣ

«Ζούμε σ' έναν κόσμο όπου ανοίγονται λαμπρότερες προοπτικές αλλά και μεγαλύτεροι κίνδυνοι παρά ποτέ. Το μέλλον θα εξαρτηθεί εν μέρει και από τις δικές μας ενέργειες. Πρέπει ταυτόχρονα να σκεφτόμαστε παγκόσμια και να ενεργούμε τοπικά».[109]

Η παραδοχή αυτή καταγράφεται στην Ευρωπαϊκή Στρατηγική Ασφάλειας του Συμβουλίου της Ευρωπαϊκής Ένωσης στις Βρυξέλλες την 12 Δεκεμβρίου 2003.

Η δυναμική των κοινωνικών μεταβολών (πολιτικών, οικονομικών, πολιτισμικών κ.λπ.), που συντελέσθη περί τα τέλη κυρίως του 20ου αιώνα, σηματοδότησε τη σταδιακή αλλά ταχεία μετάλλαξη παραδοσιακών δομών και συμπεριφορών, σε σύγχρονες, με νέα χαρακτηριστικά, που ενέχουν την έννοια της αβεβαιότητας. Η έννοια του κινδύνου και της διακινδύνευσης[110] επηρέασε - ως φυσικό επακόλουθο των κοινωνικών μεταβολών - και το εγκληματικό πεδίο που έχει πλέον να επιδείξει νέα πρότυπα και τάσεις, που η αντιμετώπισή τους, σε προληπτικό και κατασταλτικό επίπεδο, απαιτεί άλλες μορφές προσέγγισης, πέραν των έως σχεδόν πρόσφατα γνωστών παραδοσιακών αντεγκληματικών προτύπων και συστημάτων αστυνόμευσης.

Στα πλαίσια αυτά, η τεχνολογία και η νέα ψηφιακή εποχή οδήγησε σε μεταβολή του τρόπου που διαπράττεται το έγκλημα καθώς και των μέσων που χρησιμοποιεί. Νέες ψηφιακές δυνατότητες, διαδίκτυο, νέες συσκευές και Τεχνητή Νοημοσύνη, εκτός του ότι διευκολύνουν την ζωή μας και την καθημερινότητα μας, έγιναν πεδίο ελεύθερο για να καταλάβει "το ζωτικό χώρο" που του αναλογεί, με όρους γεωπολιτικής, το έγκλημα, ως "αναπόσπαστο" κομμάτι της κοινωνίας και της ανθρώπινης συμπεριφοράς. Η Ψηφιακή εγκληματολογία αποτελεί την απάντηση της συγκροτημένης κοινωνίας για την αντιμετώπιση της σύγχρονης αυτής μορφής εγκληματικότητας, δείχνοντας πως η σωστή πλευρά της τεχνολογίας, της πληροφορικής, του ψηφιακού κόσμου μπορούν να αποτελέσουν πρωταγωνιστή των ψηφιακών εξελίξεων προσπερνώντας την εξέλιξη του εγκλήματος, αυτού του διαρκούς μαραθωνίου που δίνουν οι κοινωνίες για την επιβίωση τους.

Για αυτό τον λόγο τα κράτη θα πρέπει να ενισχύσουν τους θεσμούς αρμόδιους για το έγκλημα με ανθρώπινους και οικονομικούς πόρους πάνω στο κομμάτι της Ψηφιακής Εγκληματολογίας, μια επένδυση που θα επιστρέψει στην κοινωνία με πολλαπλά οφέλη. Επιπλέον θα πρέπει να κατευθυνθούν και πόροι για την εκπαίδευση τόσο των αρμόδιων δικαστικών και προανακριτικών υπαλλήλων για την καλύτερη κατανόηση των θεμάτων που άπτονται γύρω από την Ψηφιακή Εγκληματολογία αλλά και την εισαγωγή σχετικών μαθημάτων τόσο στις σχολές, αντίστοιχες της Πληροφορικής όσο και στις Αστυνομικές και Στρατιωτικές Σχολές, αφού δεν θα είναι μακριά που το Ψηφιακό Έγκλημα θα αποτελέσει

[109] Υπ' αριθμ 15895/03 Απόφαση του Ευρωπαϊκού Συμβουλίου που θέσπισε την Ευρωπαϊκή Στρατηγική Ασφάλειας (ΕΣΑ), Δεκέμβριος 2003

[110] Ο όρος έχει κατοχυρωθεί θεωρητικά από τον Γερμανό κοινωνιολόγο Ulrich Beck., ο οποίος τον εισήγαγε στο έργο του «Κοινωνία της διακινδύνευσης. Καθοδόν προς μία διαφορετική Νεωτερικότητα», το οποίο εξεδόθη το 1986.

προστάδιο της εσωτερικής Ασφάλειας μια Χώρας από εξωτερικό κίνδυνο ένεκα ασύμμετρων απειλών.

Η παράθεση, μέσα από την παρούσα εργασία, επιστημονικών απόψεων και εμπειρικών αποτελεσμάτων, που αφορούν στο έγκλημα και στην σύγχρονη διαμόρφωσή του και επίδρασή του στις κοινωνίες, δίνει το έναυσμα έντονου προβληματισμού για την προοπτική του και τον ρόλο των Αρχών επιβολής του νόμου στην σύγχρονη αυτή προβληματική, αλλά ταυτόχρονα παρέχει πρόσφορο έδαφος για την ανάπτυξη και πρόταση πρακτικοποίησης και εφαρμογής νέων ιδεών στο αντικείμενο της δημόσιας ασφάλειας, υπό την έννοια της προστασίας της κοινωνίας.

Η παρούσα εργασία, πέραν της Ιστορικής Αναδρομής του Εγκλήματος και της Ψηφιακής Εγκληματολογίας, παρουσιάζει και την αλληλεξάρτηση της κοινωνίας, των κοινωνικών μεταβολών και του εγκλήματος. Η Ψηφιακή εποχή είναι εδώ και έχει μεταβάλλει και το έγκλημα σε ψηφιακό, αλλά και την αντιμετώπιση αυτού μέσα από την ανάπτυξη της Ψηφιακής Εγκληματολογίας η οποία αναπτύσσεται σε δύο μεγάλους κλάδους, ήτοι τον κλάδο ανάπτυξης εφαρμογών - μοντέλων για την αντιμετώπιση του ψηφιακού – ηλεκτρονικού εγκλήματος αλλά και η ανάπτυξη εφαρμογών για την πιο αξιόπιστη, αποδοτική και καλύτερη συλλογή, επεξεργασία και ανάλυση των εγκληματολογικών πληροφοριών - πειστηρίων - δεδομένων.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Βιβλία – Άρθρα – Μελέτες - Νομοθεσία

1. A Reyes et al, Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement and Prosecutors, 1st Edn, Rockland, Syngress. 2007
2. Artificial Intelligence-Enabled Digital Twin for Smart Manufacturing, Edited by Amit Kumar Tyagi, Shrikant Tiwari, Senthil Kumar Arumugam, Avinash Kumar Sharma, 2024 Scrivener Publishing
3. The Enhanced Digital Investigation Process Model, In Proceeding of Digital Forensic Research Workshop, Baryamereeba, V., and Tushabe, F.,Baltimore, 2004
4. Batiuk M. «The State of Post Secondary Correctional Education in Ohio», Journal of Correctional Education, 1997, και Allen J.P. «Administering Quality Education in an Adult Correctional Facility», Community Service Catalyst, 1988
5. Getting Physical with the Digital Investigation Process. International Journal of Digital Evidence, Carrier, B., and Spafford, E.H., 2003
6. Computer and Intrusion Forensics, George M. Mohay, Artech House,2003
7. Why we still don't understand cybercrime - In The Human Factor of Cybercrime Leukfeldt, R., Holt, T.J., McGuire, M. , Routledge: New York, NY, USA, 2020
8. Cybercrime and Digital Forensics An Introduction, By Thomas Holt, Adam Bossler, Kathryn Seigfried-Spellar, 2022, 3d edition, publish Routledge
9. Dennis Porter, The Pursuit of Crime, New Haven & London 1981
10. Digital Investigation -An integrated conceptual digital forensic framework for cloud computing, Ben Martini, Kim-Kwang Raymond Choo, Volume 9, Issue 2, November 2012
11. Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service, Xiaoyu Du, Nhien-An, Le-Khac, Mark Scanlon School of Computer Science, University College Dublin, Belfield, Dublin 4, Ireland May 2017
12. Forester, Tom and Morrison, Perry 1994, Computer Ethics,Published: 18 December 2007, Monica Horten
13. An Examination of Digital Forensics Models. International Journal of Digital Evidence, Reith, M., Carr, C., and Gunsh, G., 2002
14. Computer Forensic Field Triage Process Model, In Conference on Digital Forensics, Security and Law, Rogers, M. K., Goldman, J., Mislan ,R, Wedge, T., and Debrota, S., 2006,
15. Scene of the Cybercrime,Debra Littlejohn Shinder and Ed Tittel, Technical Editor, Computer Forensics Handbook Book 2002
16. Self-reported computer criminal behavior: A psychological analysis Marcus K. Rogers a, Kathryn Seigfried b, Kirti Tidke a, Digital Investigation Volume 3, Supplement, September 2006
17. Tiered forensic methodology model for Digital Field Triage by non-digital evidence specialists Ben Hitchcock, Nhien-An Le-Khac, Mark Scanlon b, 2016
18. Ulrich Beck., «Κοινωνία της διακινδύνευσης- Καθ Οδόν προς μία διαφορετική Νεωτερικότητα», 1986

19. ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΕΓΚΛΗΜΑΤΟΛΟΓΙΑ ΑΘΗΝΑ, ΒΙΔΑΛΗ Σοφία 2022 ΕΚΔ ΝΟΜΙΚΗ ΒΙΒΛΙΟΘΗΚΗ
20. ΕΓΚΛΗΜΑ ΚΑΙ ΚΟΙΝΩΝΙΑ, ΒΙΔΑΛΗ Σοφία, ΑΘΗΝΑ 2019
21. Έφηβοι παραβάτες και κοινωνία, Θεμελιώδεις αξίες, θεσμοί και νεανική παραβατικότητα στην Ελλάδα, Δ/νση Δαγτόγλου Π-Κουράκης Ν- Σταθόπουλος Μ. Σειρά : μελέτες Ευρωπαϊκής Νομικής Επιστήμης, Εκδόσεις Αντ. Ν.Σάκκουλα, Αθήνα-Κομοτηνή 1999
22. Κυβερνοέγκλημα, Γερμανός, Γ. και Γεωργίου, Ν. 2021
23. Ηλεκτρονικό έγκλημα ,Δαλακούρα, Νομική Βιβλιοθήκη, Θεσσαλονίκη 2019,
24. Κρίση, φόβος και ποινική καταστολή, Κοσμάτος Κ. στον τιμητικό τόμο για τον ομότιμο καθηγητή Γιάννη Πανούση, «ΕΓΚΛΗΜΑΤΟΛΟΓΙΑ: ΠΕΡΙΒΛΕΠΤΟΝ ΑΛΕΞΙΦΩΤΟΝ», εκδόσεις Ι. ΣΙΔΕΡΗΣ, Αθήνα, 2020
25. Παραδόσεις εγκληματολογίας, Παπαζαχαρίου Ι., εκδόσεις Α. Αναστασίου, τεύχος β', Αθήνα 1968
26. Ξέπλυμα βρώμικου χρήματος, Σ. Κάτσιο,1998
27. Η Κοινωνιολογία της Σχολής του Σικάγου, Τάτσης – Θωμοπούλου, ΑΘΗΝΑ, 2009
28. Τεχνητή Νοημοσύνη για όλους, Μανώλης Ανδριωτάκης, εκδ Ψυχογιός 2022
29. «Κοινωνική επιχειρηματικότητα και σωφρονιστική. Προτεινόμενο μοντέλο εργασιακής επανένταξης έγκλειστων και αποφυλακισμένων στην Ελλάδα»,Τσιλίκης Χ. – Γάκου Ε.Μ. Κοινωνική Πολιτική, 2018
30. "The Joint Operating Environment" Αρχειοθετήθηκε 2013-08-10 στο Wayback Machine., Report released, 18 February 2010
31. Broken Window Effect Joël J. Van der Weele University of Amsterdam January 2017
32. Internet Of Things(IoT) Digital Forensic Investigation Model: Top-Down Forensic Approach Methodology, Sundresan Perumal- Norita Md Norwawi- Valliappan Raman, 7-9/1
33. M. Pourvahab and G. Ekbatanifard, "Digital Forensics Architecture for Evidence Collection and Provenance Preservation in IaaS Cloud Environment Using SDN and Blockchain Technology," in IEEE Access, vol. 7, pp. 153349-153364, 2019
34. Nieto, A., Rios, R., Lopez, J., Ren, W., Wang, L., Choo, K. K. R., & Xhafa, F. (2019). Privacy-aware digital forensics
35. Review Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies Kirsty Phillips, Julia C. Davidson, Ruby R. Farr, Christine Burkhardt, Stefano Caneppele and Mary P. Aiken, 19 April 2022
36. Xiaoyu Du, Nhien-An Le-Khac, and Mark Scanlon, Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service, proceedings of the 16th European Conference on Cyber Warfare and Security (ECCWS 2017), 2017
37. Αιτιολογική Έκθεση ΚΠΔ 2019, V5Ββ. 18 ΕΔΔΑ, Roman Zakharov κατά Ρωσίας, No. 47143/06, σκ. 227-231· ΕΔΔΑ, S. and Marper κατά Ηνωμένου Βασιλείου, No 30562/04, σκ. 95· ΕΔΔΑ, Ivashchenko κατά Ρωσίας, No. 61064/10· ΕΔΔΑ, Benedik κατά Σλοβενίας, No. 62357/14. 19 Βλ. και Γ. Μπουρμά, Η νομιμότητα των ερευνών σε ηλεκτρονικά δίκτυα και δεδομένα στις περιπτώσεις εγκλημάτων στον Κυβερνοχώρο, ΠοινΔικ, 2019 Γ. Ναζίρη, Η κατάσχεση ψηφιακών Δεδομένων", Ποινική Δικαιοσύνη, Τεύχος Φεβρουάριος 2020

38. Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών, Το ευρωπαϊκό θεματολόγιο για την ασφάλεια, COM(2015)
39. Άρθρο 20 - Νόμος 4947/2022 - Ειδικές ανακριτικές πράξεις επί ορισμένων εγκλημάτων - Τροποποίηση παρ. 1 άρθρου 254 ΚΠΔ (παρ. 1 άρθρου 13 της Οδηγίας (ΕΕ) 2019/713)
40. Γιάννη Δ. Ληξουριώτη, Κοινωνικές και νομικές αντιλήψεις για το παιδί τον πρώτο αιώνα του νεοελληνικού κράτους, Αθήνα & Γιάννενα, 1986
41. Εγχειρίδιο Συλλογής και Εξέτασης Ψηφιακών Πειστηρίων – Δ.Ε.Ε. (2023)
42. Εθνική Στρατηγική Κυβερνοασφάλειας 2020 -2025
43. Κουράκης Ν. – Μηλιώνη Φ. «Αναπλαισιώνοντας και εκτιμώντας ερευνητικά δεδομένα για την παραβατικότητα των νέων για το πρόβλημα της υποτροπής νεαρών αποφυλακισμένων στην Ελλάδα με βάση τα πορίσματα επαναληπτικής (follow – up) έρευνας του Εργαστηρίου Ποινικών και Εγκληματολογικών Ερευνών
44. ΚΩΔΙΚΑΣ ΠΟΙΝΙΚΗΣ ΔΙΚΟΝΟΜΙΑΣ
45. ΝΟΜΟΣ 4411/2016 (ΦΕΚ Α΄ 142/3.8.2016)
46. ΝΟΜΟΣ 5187/2025 ΦΕΚ Α 48/21.03.2025
47. Οδηγία 2006/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Μαρτίου 2006 , για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών και για την τροποποίηση της οδηγίας 2002/58/ΕΚ
48. Οδηγία 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 3ης Απριλίου 2014, περί της ευρωπαϊκής εντολής έρευνας σε ποινικές υποθέσεις, ΕΕ L 130 της 1.5.2014, η οποία ενσωματώθηκε στο ελληνικό δίκαιο με τον ν. 4489/2017 (ΦΕΚ 140/Α/21-9-2017)
49. ΠΟΙΝΙΚΟΣ ΚΩΔΙΚΑΣ
50. Ρίκα Μπενβενίστε, Η ποινική καταστολή της νεανικής εγκληματικότητας τον 19ο αιώνα (1833-1911), Αθήνα & Κομοτηνή 1994
51. Έφη Αβδελά, Νέοι εν κινδύνω. Επιτήρηση, αναμόρφωση και δικαιοσύνη ανηλίκων μετά τον πόλεμο, Αθήνα 2013
52. Γιάννης Δ. Ληξουριώτης, Κοινωνικές και νομικές αντιλήψεις για το παιδί τον πρώτο αιώνα του νεοελληνικού κράτους, Αθήνα & Γιάννενα, 1986
53. Κουράκης Ν., Έφηβοι παραβάτες και κοινωνία, Θεμελιώδεις αξίες, θεσμοί και νεανική παραβατικότητα στην Ελλάδα, Δ/νση Δαγτόγλου Π-Κουράκης Ν-Σταθόπουλος Μ. Σειρά: μελέτες Ευρωπαϊκής Νομικής Επιστήμης, Εκδόσεις Αντ. Ν.Σάκκουλα, Αθήνα-Κομοτηνή 1999, σελ. 35-39
54. Σ. Κάτσιος, «Ξέπλυμα βρώμικου χρήματος: Η γεωπολιτική του διεθνούς χρηματοπιστωτικού συστήματος: Το φαινόμενο της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες», Εκδόσεις Σάκκουλα, 1997, σελ. 81
55. Ελένη Καμπέρου-Ντάλτα, Ο Ν.3691/2008 ΓΙΑ ΤΟ ΞΕΠΛΥΜΑ ΒΡΩΜΙΚΟΥ ΧΡΗΜΑΤΟΣ-Ερμηνευτική προσέγγιση του νόμου και διεθνές ποινικό πλαίσιο, εκδ Π.Ν. ΣΑΚΚΟΥΛΑΣ

Ιστότοποι –Online Άρθρα

1. https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.h
2. https://economictimes.indiatimes.com/news/international/uk/can-virtual-gang-rape-occur-in-the-metaverse-uk-police-launchinvestigation/articleshow/106520687.cms?from=mdr
3. https://el.wikipedia.org/wiki/%CE%93%CE%BA%CE%AD%CF%84%CE%BF
4. https://el.wikipedia.org/wiki/%CE%97%CE%BB%CE%B5%CE%BA%CF%84%CF%81%CE%BF%CE%BD%CE%B9%CE%BA%CF%8C_%CE%AD%CE%B3%CE%BA%CE%BB%CE%B7%CE%BC%CE%B1
5. https://en.wikipedia.org/wiki/Bulli_Bai_case
6. https://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act
7. https://eshop.elot.gr/product/96542
8. https://mindigital.gr/wp-content/uploads/2022/11/EL-NATIONAL-CYBER-SECURITY-STRATEGY-2020_2025.pdf
9. https://nhrc.nic.in/sites/default/files/Group%201%20April.pdf
10. https://www.chaintech.network/blog/1820-textile-industry-weaving-the-threads-of-the-first-cybercrime
11. https:/www.astynomia.gr
12. www.kathimerini.gr/society/561405952/egklima-sta-glyka-nera-kinito-kai-roloi-symplirosan-to-pazl-tis-stygeris-dolofonias/
13. Ο περιβαλλοντικός σχεδιασμός ως μέθοδος πρόληψης του εγκλήματος στις σύγχρονες πόλεις (CPTED) Αγγελική Ρούσσου Δικηγόρος, Υποψήφια Διδάκτωρ Ποινικού Δικαίου ΕΚΠΑ ΝΟΕΜΒΡΙΟΣ 2018 https://theartofcrime.gr/
14. Χριστίνα ΖΑΡΑΦΩΝΙΤΟΥ Καθ. Καθηγήτρια Εγκληματολογίας, Τμήμα Κοινωνιολογίας Παντείου Πανεπιστημίου Άρθρο Ιούνιος 2012 https://theartofcrime.gr/
15. Χριστίνα ΖΑΡΑΦΩΝΙΤΟΥ Καθ. Καθηγήτρια Εγκληματολογίας, Τμήμα Κοινωνιολογίας Παντείου Πανεπιστημίου ΥΠΑΡΧΟΥΝ GHETTOS ΣΤΟ ΚΕΝΤΡΟ ΤΗΣ ΑΘΗΝΑΣ; Εγκληματολογία 2/2012 www.nbonline.gr