ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Π.Μ.Σ. «Τεχνοοικονομική Διοίκηση και Ασφάλεια Ψηφιακών Συστημάτων»

Διπλωματική εργασία

Αθανασία Κούρμπαση 14011

«Νομικό πλαίσιο εργαστηρίου ψηφιακής εγκληματολογίας σε στρατιωτικό περιβάλλον»

Ευχαριστίες

Σε αυτό το σημείο θα ήθελα να ευχαριστήσω όλους όσους συνέβαλαν καθοριστικά, ο καθένας με το δικό του τρόπο, στη διαμόρφωση και ολοκλήρωση της παρούσας εργασίας.

Με το πέρας των μεταπτυχιακών σπουδών μου, θα ήθελα να εκφράσω την ευγνωμοσύνη μου στην επιβλέπουσα καθηγήτριά μου κ. Λίλιαν Μήτρου για τη συνεχή υποστήριξη, για την πίστη και εμπιστοσύνη στις δυνατότητες μου, για την άμεση ανταπόκριση σε κάθε ζήτημα που πρόκυπτε κατά την εκπόνηση της διπλωματικής μου εργασίας και για την ενθάρρυνση που μου έδινε στη διάρκεια της φοίτησής μου στο μεταπτυχιακό πρόγραμμα.

Επιπρόσθετα, θα ήθελα να ευχαριστήσω ιδιαιτέρως τους καθηγητές κ. Κώστα Λαμπρινουδάκη και κ. Χρήστο Ξενάκη για την καθοδήγηση και την πολύτιμη συμμετοχή τους στη διεκπεραίωση της διπλωματικής εργασίας.

Επίσης, τον κ. Χριστόφορο Νταντογιάν για τη στήριξη που μου προσέφερε, την προθυμία που επέδειξε να λύσει κάθε πρόβλημα ή απορία που μου παρουσιάζονταν, γεγονότα που τον καθιστούν βασικό αρωγό για την εκπόνηση της παρούσας εργασίας.

Αξιοσημείωτη είναι η συμβολή των συμφοιτητών μου, Γεώργιου Τριανταφύλλου, Ιωάννη Πετρόπουλου και Μιχάλη Ηλιόπουλου, με τους οποίους συνεργάστηκα καθ' όλη τη διάρκεια του μεταπτυχιακού προγράμματος. Επιδεικνύοντας αμέριστη υποστήριξη στην προσπάθειά μου και υπομονή στην εκπόνηση των εργασιών έπαιξαν καθοριστικό ρόλο στην ολοκλήρωση των σπουδών μου και αποτέλεσαν κίνητρο για την συνέχιση της πορείας μου στον τομέα της ασφάλειας ψηφιακών συστημάτων.

Τέλος, θα ήθελα να ευχαριστήσω την οικογένειά μου, για την υποστήριξή τους, την αγάπη και την εμπιστοσύνη που μου δείχνουν.

Abstract

In this paper, we examine the science of digital forensic, which is the science that deals with the recognition, preservation, analysis and presentation of digital evidence in a legally acceptable manner, which aims to discover the culprit of an accomplished offense. The research was based on bibliographic references. The first chapter will define the concept of digital forensics. Nowadays, the evidence of an offense is in a digital environment and it becomes quite difficult not only to identify the evidence but also to present it in a legally acceptable manner in court. As a result this science has been developed and is even shared in computer forensics, network forensic, mobile forensics and now in cloud forensics. Subsequently, the second chapter presents the methodologies applied in the digital forensic and the third chapter presents the legal framework that covers these methodologies in general and especially in the military environment.

Περίληψη

Στην υπό κρίση εργασία, εξετάζουμε την επιστήμη της ψηφιακής δικανικής, πρόκειται για την επιστήμη που ασχολείται με την αναγνώριση, διατήρηση, ανάλυση και παρουσίαση ψηφιακών αποδείξεων κατά τρόπο νομικά αποδεκτό, η οποία στόχο έχει να ανακαλυφθεί ο υπαίτιος κάποιας τελεσθείσας αξιόποινης πράξης. Η έρευνα βασίστηκε σε βιβλιογραφικές αναφορές ηλεκτρονικής και έντυπης φύσεως. Στο πρώτο κεφάλαιο θα καθοριστεί η έννοια της ψηφιακής δικανικής (digital forensics) και συνακόλουθα θα οριστούν τα χαρακτηριστικά της γνωρίσματα. Δοθέντος ότι όλο και πιο συχνά, οι αποδείξεις μιας αξιόποινης πράξης βρίσκονται σε ψηφιακό περιβάλλον και καθίσταται αρκετά δύσκολο, όχι μόνο να εντοπίσουμε τις αποδείξεις, αλλά και να παρουσιαστούν κατά τρόπο νομικά αποδεκτό σε μία ακροαματική διαδικασία, έχει αναπτυχθεί η ως άνω επιστήμη και μάλιστα επιμερίζεται στο computer forensics, network forensic, mobile forensics και πλέον στο cloud forensics. Εν συνεχεία, στο δεύτερο κεφάλαιο παρουσιάζονται οι μεθοδολογίες που εφαρμόζονται στην ψηφιακή δικανική και στο τρίτο κεφάλαιο παρουσιάζεται το νομικό πλαίσιο που καλύπτει τις μεθοδολογίες αυτές γενικότερα και ειδικότερα σε στρατιωτικό περιβάλλον.

Περιεχόμενα

Εισαγωγή

Η ψηφιακή εγκληματολογία συνιστά μία υποκατηγορία της επιστήμης των forensics, πρόκειται για μια καινοτόμα εξέλιξη της εγκληματολογίας που προέκυψε ως συνέπεια των τεχνολογικών εξελίξεων που επέφεραν μια σκοτεινή πλευρά στην εγκληματική δράση και προσέθεσαν νέες μορφές εγκλήματος, που εντάσσονται στην ευρύτερη κατηγορία «e-crime» , ήτοι των εγκλημάτων που τελούνται μέσω ηλεκτρονικού υπολογιστή ή διαδικτύου. Η ψηφιακή δικανική ως κλάδος της επιστήμης των forensics ασχολείται με την ανάκτηση και διερεύνηση υλικού σε ψηφιακές συσκευές και συχνά σχετίζεται με το ηλεκτρονικό έγκλημα.

Οι πρακτικές που εφαρμόζονται στην ψηφιακή εγκληματολογία αριθμούνται σε εκατοντάδες, ανά τον κόσμο έχουν αναπτυχθεί διαφορετικές διαδικασίες έρευνας ψηφιακής εγκληματολογίας και κάθε οργανισμός παρουσιάζει την τάση να αναπτύσσει τις δικές του διαδικασίες. Μάλιστα, άλλοι επικεντρώνονται στην τεχνολογία και στον τρόπο απόκτησης των δεδομένων, άλλοι δίνουν έμφαση στην ανάλυση των δεδομένων σε μεγάλο τμήμα της έρευνας. Οι θεμελιώδεις αρχές της Δικανικής Επιστήμης δε φαίνεται να παρουσιάζουν μεγάλες διαφορές από τις παραδοσιακές αρχές της εγκληματολογικής επιστήμης. Ο ρόλος του πραγματογνώμονα, μάλιστα είναι ουσιαστικός και πρωταγωνιστικός τόσο στην παραδοσιακή εγκληματολογία όσο και στην ψηφιακή.1

Τα πειστήρια που συλλέγονται με στόχο να αποτελέσουν αποδείξεις σε μια επ'ακροατηρίω διαδικασία, χρειάζεται να πληρούν κάποιες βασικές προϋποθέσεις, αυθεντικότητα, αξιοπιστία, πληρότητα και ακεραιότητα. Στην ελληνική έννομη τάξη, ο νόμος 1805/1988 αφορά εγκλήματα που διαπράττονται γενικά με ηλεκτρονικούς υπολογιστές, ενώ ο νόμος 4411/2016, ο οποίος δημοσιεύθηκε την 3η Αυγούστου του 2016, επέβαλε σημαντικές αλλαγές ως προς την ποινική αντιμετώπιση του ηλεκτρονικού εγκλήματος. Εξετάζοντας το ελληνικό νομικό πλαίσιο, εστιάζουμε στην εφαρμογή του σε στρατιωτικό περιβάλλον, προκειμένου να οριοθετηθεί το νόμιμο πλαίσιο λειτουργίας ενός τέτοιου εργαστηρίου, στο οποίο τίθενται ζητήματα διασφάλισης του απορρήτου των πληροφοριών. Δεδομένου ότι σε ένα τέτοιο περιβάλλον διακινείται διαβαθμισμένη πληροφορία, με αποτέλεσμα οι απαιτήσεις ασφαλείας να είναι υψηλές, σε συνδυασμό με την αύξηση της εγκληματικότητας στον κυβερνοχώρο, είναι αναγκαία η άμεση αντιμετώπιση περιστατικών ασφαλείας και αποσόβηση πιθανών κινδύνων με εσωτερικές διαδικασίες, ήτοι σε ένα εργαστήριο ψηφιακής εγκληματολογίας σε στρατιωτικό περιβάλλον.

Τέλος, γίνεται μια προσπάθεια να προταθούν κάποια έγγραφα, τα οποία δύνανται να συνοδεύουν τη διεξαγωγή της έρευνας προκειμένου να αποδεικνύεται εγγράφως η χρονική ακολουθία των μεθόδων που υιοθετήθηκαν, τα στοιχεία που συλλέχθηκαν-κατασχέθηκαν καθώς επίσης και τα τμήματα που εξετάσθηκαν.

[1] http://www.elesme.gr

Κεφάλαιο 1ο: «Forensics»

Η ψηφιακή εποχή χαρακτηρίζεται από την εφαρμογή της τεχνολογίας των υπολογιστών ως εργαλείο που ενισχύει τις παραδοσιακές μεθοδολογίες σε διάφορους τομείς της καθημερινότητας. Η ενσωμάτωση των συστημάτων πληροφορικής στον ιδιωτικό, εμπορικό, εκπαιδευτικό, κυβερνητικό τομέα καθώς και σε άλλες πτυχές της σύγχρονης ζωής έχει βελτιώσει την παραγωγικότητα και την αποτελεσματικότητά τους. Παράλληλα, όμως, λειτούργησε ως ενισχυτικό στοιχείο στην εγκληματικότητα και δημιούργησε νέες μορφές εγκλημάτων ή τροποποίησε κάποιες κλασικές μορφές τελειοποιώντας τον τρόπο τέλεσής του. Η αλόγιστη διαθεσιμότητα πληροφοριών στο διαδίκτυο, η ανωνυμία των χρηστών και τελικά η δυσκολία να βρεθεί ο τελικός χρήστης-εγκληματίας, τελικά έχει δυσχεράνει σε μεγάλο βαθμό την εκδίωξη, σύλληψη και επιβολής της ανάλογης ποινής στους δράστες.2

1.1 Εννοιολογική προσέγγιση της έννοιας «forensics»

Η εγκληματολογική επιστήμη γενικότερα σχετίζεται με την «εξέταση του τόπου του εγκλήματος, τη συγκέντρωση των υλικών αποδεικτικών στοιχείων, τις εργαστηριακές εξετάσεις, την ερμηνεία των πορισμάτων και την υποβολή των συμπερασμάτων για τους σκοπούς της συλλογής πληροφοριών και της διεξαγωγής ερευνών ή υπό τη μορφή των αποδεικτικών στοιχείων στο Δικαστήριο».3

Ο όρος forensics συνιστά την επιστημονική μέθοδο για τη συλλογή, διατήρηση και εξέταση πληροφοριών που σχετίζονται με μία τελεσθείσα αξιόποινη πράξη, οι οποίες στη συνέχεια χρησιμοποιούνται ως πειστήρια κατά την ακροαματική διαδικασία. Σύμφωνα με το λεξικό της Οξφόρδης, η λέξη forensics ορίζεται ως «η επιστήμη που εφαρμόζει επιστημονικές μεθόδους για τη διερεύνηση του εγκλήματος» και «ή είναι επιστήμη σχετική με την ακροαματική διαδικασία». 4 Πρόκειται για ένα γενικό ορισμό, το σημαντικό είναι αφενός ότι τονίζει τη σύνδεση των επιστημονικών μεθόδων με την έρευνα ενός εγκλήματος και αφετέρου το δεύτερο σκέλος του ορισμού υπογραμμίζει τη συχνή κατάληξη των ερευνών στις αίθουσες των δικαστηρίων, ήτοι ακροαματική διαδικασία. Στο σημείο αυτό, αξίζει να αναφερθεί ότι υπάρχουν και περιπτώσεις που δεν καταλήγουν στα δικαστήρια και ακολουθούνται εσωτερικές διαδικασίες, εσωτερικές έρευνες, με πιθανές πειθαρχικές κυρώσεις, όπως συμβαίνει συχνά σε ένα στρατιωτικό περιβάλλον, το οποίο τα εξετάσουμε στο δεύτερο κεφάλαιο. Σε κάθε περίπτωση, είναι σύννομη η διαδικασία της έρευνας και σύμφωνη με τα γενικά πρότυπα του νόμου, ωστόσο, η κρισιμότητα των υποθέσεων και η γενικότερη ασφάλεια επιτάσσει συχνά αμεσότερες λύσεις για την επίλυση των όποιων συμβάντων.5

---

[2]Mark Reith, Clint Carr, Gregg Gunsch Department of Electrical and Computer Engineering Graduate School of Engineering and Management Air Force Institute of Technology Wright-Patterson AFB An Examination of Digital Forensic Models, International Journal of Digital Evidence Fall 2002, Volume 1, Issue 3, σελ. 2,3

[3] http://www.e-crime.gr/computerforensics.com

[4] Michael Kohn1, JHP Eloff2 and MS Olivier, Framework for a Digital Forensic Investigation

[5]Van Solms, SH. and Lourens, CP.: A Control Framework for Digital Forensics, IFIP 11.9, 2006.

Κάνοντας μια ευσύνοπτη ιστορική αναδρομή, ανατρέχουμε στο λατινικό forēnsis, που σημαίνει «of or before the forum», χρονολογείται ήδη από τη Ρωμαϊκή εποχή, κατά την οποία ένα αδίκημα, ειδικότερα ποινικό, παρουσιαζόταν ενώπιον μιας ομάδας δημόσιων προσώπων στο δικαστήριο της εποχής. Κατά την ως άνω παρουσίαση, τόσο ο κατηγορούμενος όσο και ο κατήγορος παρουσίαζαν τις αντικρουόμενες πτυχές της ιστορίας, η γνωστή πλέον σήμερα ακροαματική διαδικασία. Η υπόθεση κρινόταν υπέρ του ατόμου με το καλύτερο επιχείρημα. Ο ως άνω όρος, λοιπόν, είχε διττή σημασία, αποτελούσε μια μορφή νομικών στοιχείων, τα οποία θα παρουσιάζονταν στην επ'ακροατηρίω διαδικασία, επομένως ήταν σημαντικό να έχουν την ανάλογη αποδεικτική δύναμη. Στη σύγχρονη χρήση, η έννοια αυτή στο χώρο της εγκληματολογικής επιστήμης είναι πλέον στενά συνδεδεμένη με το επιστημονικό πεδίο και μάλιστα πολλά λεξικά εξισώνουν τη λέξη forensics με την εγκληματολογική επιστήμη.

Η υπό εξέταση ψηφιακή εγκληματολογία συνιστά μία υποκατηγορία της επιστήμης των forensics, πρόκειται για μια καινοτόμα εξέλιξη της εγκληματολογίας που προέκυψε ως συνέπεια των τεχνολογικών εξελίξεων που επέφεραν μια σκοτεινή πλευρά στην εγκληματική δράση και προσέθεσαν νέες μορφές εγκλήματος, που εντάσσονται στην ευρύτερη κατηγορία «e-crime» , ήτοι των εγκλημάτων που τελούνται μέσω ηλεκτρονικού υπολογιστή ή διαδικτύου. Αρχικά αποδόθηκε ως δικανική υπολογιστών, ωστόσο, πλέον ο όρος συμπεριλαμβάνει την εγκληματολογία που ασχολείται με όλη την ψηφιακή τεχνολογία. Δοθέντος ότι η δικανική υπολογιστών ορίζεται ως «η συλλογή τεχνικών και εργαλείων που χρησιμοποιούνται προκειμένου να βρουν αποδεικτικά στοιχεία σε έναν υπολογιστή», η ψηφιακή εγκληματολογία στο σύνολό της έχει οριστεί ως «η χρήση των επιστημονικά δοκιμασμένων μεθοδολογιών με στόχο τη διατήρηση, τη συλλογή, την αναγνώριση, την ανάλυση, την ερμηνεία, την τεκμηρίωση και την παρουσίαση των ψηφιακών αποδεικτικών στοιχείων που προέρχονται από ψηφιακές πηγές, σκοπεύοντας τελικά να διευκολύνουν την ανασυγκρότηση του συμβάντος και τελικά αυτό να παρουσιαστεί με όλα τα σχετικά ευρήματά του, νομότυπα, στην ακροαματική διαδικασία».6

Ζώντας στην κοινωνία της πληροφορίας και της ευρύτατης χρήσης του διαδικτύου και των ηλεκτρονικών μέσων, διαπιστώνει κανείς ότι αναπτύσσονται νέες ευκαιρίες στην ανάπτυξη εγκληματικών δραστηριοτήτων, είτε εξελίσσοντας τα παραδοσιακά εγκλήματα είτε προσθέτοντας και νέα τα οποία μάλιστα εξιχνιάζονται εξαιρετικά δύσκολα. Επιπλέον, σε υπηρεσίες που διακινούνται διαβαθμισμένες πληροφορίες όπως είναι σε ένα στρατιωτικό περιβάλλον, υπάρχει απαίτηση για μείζονα ασφάλεια. Η ανάπτυξη της ψηφιακής εγκληματολογίας τελικά αποτέλεσε απαίτηση της εποχής και η δημιουργία εργαστηρίων ψηφιακής εγκληματολογίας θεωρείται μονόδρομος.

Σε μια προσπάθεια να ορίσουμε τη δικανική υπολογιστών, θα λέγαμε ότι πρόκειται για τη διαδικασία της εφαρμογής επιστημονικών και αναλυτικών τεχνικών στα λειτουργικά συστήματα των υπολογιστών και των δομών των αρχείων με αποτέλεσμα τη δημιουργία νομικά έγκυρων αποδεικτικών στοιχείων. Αξιοσημείωτο είναι δε , ότι ο όρος δικανική υπολογιστών υιοθετήθηκε αρχικά από την κοινότητα της ασφάλειας πληροφοριών προκειμένου να περιγράψει ένα μεγάλο εύρος εργασιών που ασχολούνται με την προστασία των υπολογιστικών συστημάτων και τον εντοπισμό αδυναμιών σε αυτά παρά με τη συλλογή αποδεικτικών στοιχείων (Casey et al,2004), ο όρος αυτός, επομένως, σταδιακά απέκτησε εξέχοντα ρόλο στην ψηφιακή εγκληματολογία.

Η δικανική υπολογιστών ασχολείται με τις τεχνικές ανάλυσης των υποσυστημάτων και των περιεχομένων ενός υπολογιστή, όπως σκληροί δίσκοι, ψηφιακοί δίσκοι και εκτυπωτές. Ο στόχος της δικανικής υπολογιστών είναι η εξέταση των ψηφιακών μέσων με σύννομες μεθόδους

[6] Mark Reith, Clint Carr, Gregg Gunsch Department of Electrical and Computer Engineering Graduate School of Engineering and Management Air Force Institute of Technology Wright-Patterson AFB, OH 45433-7765, An Examination of Digital Forensic Models

με σκοπό την αναγνώριση, διατήρηση, ανάκτηση, ανάλυση και παρουσίαση των γεγονότων και απόψεων σχετικά με την πληροφορία που αποκτήθηκε, η οποία δύναται να αποτελέσει αποδεικτικό στοιχείο σε μία ακροαματική διαδικασία.

Ενώ η εγκληματολογία που αφορά τους υπολογιστές τείνει να επικεντρωθεί σε συγκεκριμένες μεθόδους για την εξαγωγή στοιχείων από μια συγκεκριμένη πλατφόρμα, η ψηφιακή εγκληματολογία στο σύνολό της χρειάζεται να διαμορφωθεί έτσι ώστε να περιλαμβάνει όλους τους τύπους των ψηφιακών συσκευών και να δύναται να προσαρμοστεί στις εξελίξεις των ψηφιακών τεχνολογιών. Ωστόσο, όπως έχουμε προαναφέρει, δεν υφίσταται ένα μοναδικό πρότυπο ή μια ενιαία ψηφιακή μεθοδολογία έρευνας, αλλά αντιθέτως ένα σύνολο διαδικασιών και εργαλείων που προτάθηκε από διάφορες ομάδες σε κάθε περίπτωση , όμως, με στόχο την επιβολή του νόμου.7

Οι προτεινόμενες ψηφιακές αποδείξεις για την εισαγωγή στο δικαστήριο πρέπει να πληρούν αυστηρά τις δύο κάτωθι προϋποθέσεις :

1]αρχικά πρέπει να είναι σχετικές με το υπό κρίση ζήτημα, ήτοι να τελούν σε αιτιώδη συνάφεια με το υπό εξέταση αδίκημα

2]είναι πολύ σημαντικό να προέρχονται από νομικά αναγνωρισμένη επιστημονική μέθοδο, η οποία να υποδεικνύεται και να υποστηρίζεται από κατάλληλη επικύρωση, ένταλμα ή εξουσιοδότηση.

1.2. Δικανική Υπολογιστών-computer forensics

Σε μια προσπάθεια να ορίσουμε τη δικανική υπολογιστών, θα λέγαμε ότι πρόκειται για τη διαδικασία της εφαρμογής επιστημονικών και αναλυτικών τεχνικών στα λειτουργικά συστήματα των υπολογιστών και των δομών των αρχείων με αποτέλεσμα τη δημιουργία νομικά έγκυρων αποδεικτικών στοιχείων. Αξιοσημείωτο είναι δε , ότι ο όρος δικανική υπολογιστών υιοθετήθηκε αρχικά από την κοινότητα της ασφάλειας πληροφοριών προκειμένου να περιγράψει ένα μεγάλο εύρος εργασιών που ασχολούνται με την προστασία των υπολογιστικών συστημάτων και τον εντοπισμό αδυναμιών σε αυτά παρά με τη συλλογή αποδεικτικών στοιχείων (Casey et al,2004), ο όρος αυτός, επομένως, σταδιακά απέκτησε εξέχοντα ρόλο στην ψηφιακή εγκληματολογία.

Η δικανική υπολογιστών ασχολείται με τις τεχνικές ανάλυσης των υποσυστημάτων και των περιεχομένων ενός υπολογιστή, όπως σκληροί δίσκοι, ψηφιακοί δίσκοι και εκτυπωτές. Ο στόχος της δικανικής υπολογιστών είναι η εξέταση των ψηφιακών μέσων με σύννομες μεθόδους με σκοπό την αναγνώριση, διατήρηση, ανάκτηση, ανάλυση και παρουσίαση των γεγονότων και απόψεων σχετικά με την πληροφορία που αποκτήθηκε, η οποία δύναται να αποτελέσει αποδεικτικό στοιχείο σε μία ακροαματική διαδικασία.

Ενώ η εγκληματολογία που αφορά τους υπολογιστές τείνει να επικεντρωθεί σε συγκεκριμένες μεθόδους για την εξαγωγή στοιχείων από μια συγκεκριμένη πλατφόρμα, η ψηφιακή εγκληματολογία στο σύνολό της χρειάζεται να διαμορφωθεί έτσι ώστε να περιλαμβάνει όλους τους τύπους των ψηφιακών συσκευών και να δύναται να προσαρμοστεί στις εξελίξεις των ψηφιακών τεχνολογιών. Ωστόσο, όπως έχουμε προαναφέρει, δεν υφίσταται ένα μοναδικό πρότυπο ή μια ενιαία ψηφιακή μεθοδολογία έρευνας, αλλά αντιθέτως ένα σύνολο διαδικασιών και εργαλείων που προτάθηκε από διάφορες ομάδες σε κάθε περίπτωση , όμως, με στόχο την επιβολή του νόμου.8

[7]Mark Reith, Clint Carr, Gregg Gunsch Department of Electrical and Computer Engineering Graduate School of Engineering and Management Air Force Institute of Technology Wright-Patterson AFB, OH 45433-7765, An Examination of Digital Forensic Models

[8] Mark Reith, Clint Carr, Gregg Gunsch Department of Electrical and Computer Engineering Graduate School of Engineering and Management Air Force Institute of Technology Wright-Patterson AFB, An Examination of Digital Forensic Models, OH 45433-7765

1.3. Ψηφιακή Δικανική

Η ψηφιακή δικανική αποτελεί ένα κλάδο της επιστήμης των forensics η οποία ασχολείται με την ανάκτηση και διερεύνηση υλικού σε ψηφιακές συσκευές και συχνά σχετίζεται με το ηλεκτρονικό έγκλημα. Ο όρος της ψηφιακής δικανικής (digital forensics) αρχικά χρησιμοποιήθηκε ως συνώνυμο του όρου της δικανικής υπολογιστών (computer forensics) , στη συνέχεια, όμως, επεκτάθηκε ο ορισμός του καλύπτοντας όλες τις συσκευές οι οποίες είναι ικανές να αποθηκεύσουν ψηφιακά δεδομένα, περιλαμβάνοντας τις κινητές συσκευές, τις βάσεις δεδομένων και τα δίκτυα, και αυτή τη στιγμή ο όρος μπορεί να χρησιμοποιηθεί ώστε να περιγράψει το σύνολο του κλάδου της ψηφιακής εγκληματολογίας.

Με τον όρο digital forensics εννοούμε το γνωστικό αντικείμενο που προσπαθεί να ανιχνεύσει αποδεικτικά στοιχεία για εγκληματικές πράξεις ερευνώντας ψηφιακά τεκμήρια. Τα εγκλήματα μπορεί να είναι είτε ψηφιακά (κλοπή κωδικών, hacking σε τραπεζικούς λογαριασμούς, παιδική πορνογραφία κτλ) είτε τα κλασικά εγκλήματα που συνήθως εξετάζουμε (κλοπές, ληστείες, δολοφονίες, απαγωγές) τα οποία χρησιμοποιούν τους ηλεκτρονικούς υπολογιστές ως μέσο τέλεσης. Ως κλάδος της εγκληματολογίας εμφανίστηκε τη δεκαετία του 1980 και έκτοτε αναπτύσσεται συνεχώς περνώντας από τους προσωπικούς υπολογιστές στα δίκτυα και πλέον στα κινητά τηλέφωνα. Το 2001 πραγματοποιήθηκε το πρώτο Digital Forensic Research Workshop, στο οποίο αναγνωρίστηκε η ανάγκη να αναθεωρηθεί ο όρος και προτάθηκε ο όρος digital forensic science για να περιγράψει το πεδίο της επιστήμης αυτής. Σημαντικό είναι να αναφερθεί ότι συχνά χρησιμοποιούνται οι όροι forensic computer analysis και forensic computing (Casey et al, 2004) προκειμένου να αποδώσουν την έννοια της ψηφιακής δικανικής-digital forensics.

Οι Biros και Weiser (2006) ορίζουν την ψηφιακή εγκληματολογίας ως «επιστημονικές γνώσεις και μεθόδους που εφαρμόστηκαν για τον εντοπισμό, τη συλλογή, διατήρηση, εξέταση και ανάλυση των πληροφοριών που αποθηκεύονται ή μεταδίδονται σε δυαδική μορφή κατά τρόπο νομικά αποδεκτό, με στόχο τη χρήση του σε δικαστηριακή διαδικασία». Η ψηφιακή εγκληματολογική έρευνα απαιτεί καθορισμένες διαδικασίες που συμμορφώνονται με τη βιομηχανική πρακτική, οργανωτική πρακτική και κατάλληλη νομοθεσία, είτε ως μέρος της ποινικής έρευνας ή ως μέρος μιας γενικότερης αντιμετώπισης περιστατικών ασφαλείας. Η τεχνική και τα εργαλεία που χρησιμοποιούνται από τους ερευνητές της ψηφιακής δικανικής μπορεί να ποικίλλουν, ωστόσο, η διαδικασία κατά κύριο λόγο περιλαμβάνει το σχεδιασμό, την απόκτηση των δεδομένων-στοιχείων, τη διατήρησή τους, την ανάλυσή τους και την υποβολή εκθέσεων, όπως φαίνεται στον Πίνακα 1. Η παρουσίαση των ψηφιακών αποδεικτικών στοιχείων είναι μια μοναδική νομική πρόκληση που αντιμετωπίζουν τεχνικοί της ψηφιακής δικανικής (Kenneally,2002). [9]

Η ψηφιακή δικανική, τελικά, αποτελεί το μεγαλύτερο και πιο πολύπλοκο κομμάτι της δικανικής επιστήμης και αποτελεί επιταγή της συχνά χαρακτηριζόμενης ως «ψηφιακή» εποχής μας. Οι κλάδοι που περιλαμβάνονται στην ψηφιακή δικανική είναι η δικανική υπολογιστών-computer forensics, η δικανική κινητών συσκευών-mobile forensics και η δικανική δικτύων-network forensics. Η ψηφιακή εγκληματολογία είναι απαραίτητη για την επιτυχή δίωξη των ψηφιακών εγκληματιών, οι οποίοι χρησιμοποιούν διαφορετικές ψηφιακές συσκευές, όπως συσκευές υπολογιστών, δικτύου, κινητές συσκευές και συσκευές αποθήκευσης. Η ψηφιακή εγκληματολογική έρευνα, προκειμένου να αποκτήσει τις αποδείξεις που θα είναι αποδεκτές στο δικαστήριο πρέπει να ακολουθήσει μια συγκεκριμένη χαρτογραφημένη διαδικασία.

[9] James Tetteh Ami-Narh, Edith Cowan University, Patricia A.H. Williams, Edith Cowan University, 2008, Digital forensics and the legal system: A dilemma of our times

Οι έρευνες που πραγματοποιούνται στο πλαίσιο της ψηφιακής δικανικής παρουσιάζουν μεγάλη ποικιλομορφία. Τυπικά περιλαμβάνουν αποδεικτικά στοιχεία που ανακτήθηκαν από υπολογιστικά συστήματα, από το διαδίκτυο, ή από διερευνήσεις εισβολών σε δίκτυα. Η ψηφιακή εγκληματολογία επικεντρώνεται στην ανάπτυξη αποδείξεων που σχετίζεται με τον ψηφιακό κόσμο για χρήση αυτών σε ποινικές ή και αστικές δικαστικές διαδικασίες και με σκοπό τη διευκόλυνση ή τη βελτίωση της ανασυγκρότησης των γεγονότων που αφορούν την υπόθεση. 10 Επίσης, μπορεί να χρησιμοποιηθεί για να αναγνωρισθεί ένα έγκλημα, να ταυτοποιηθούν ύποπτοι, να επαληθευτούν ή μη οι ισχυρισμοί διαδίκων και μαρτύρων αλλά ακόμη και να αποδειχθεί η αυθεντικότητα των προσκομισθέντων ως «σχετικών» εγγράφων. Ερευνώντας σκληρούς δίσκους και email, οι ερευνητές συχνά καταφέρνουν να εξιχνιάσουν εγκληματικές ενέργειες. Η έρευνα μπορεί να περιλαμβάνει σκληρούς δίσκους, έλεγχο του υπολογιστή ενώ βρίσκεται σε λειτουργία (για να καταγραφεί π.χ. ο κωδικός πρόσβασης), ακόμη και διαγραμμένα αρχεία.

Πολυάριθμες μέθοδοι έχουν προταθεί για την ψηφιακή εγκληματολογία, ωστόσο, όλες διαφέρουν μεταξύ τους, με μοναδικό κοινό τη διατήρηση της ακεραιότητας του πρωτοτύπου των αποδεικτικών στοιχείων και την εξαγωγή πληροφοριών που έχουν αξία για την εκάστοτε υπόθεση. Αξιοσημείωτο είναι δε, ότι σε κάθε μεθοδολογία επικρατεί η αντίληψη ότι το αρχικό αποδεικτικό υλικό είναι τεράστιο σε μέγεθος, αλλά η «σημαντική» πληροφορία είναι ένα υποσύνολο, συχνά ένα πολύ μικρό υποσύνολο των αρχικών αποδείξεων.11

Από τεχνικής απόψεως, έχουν αναπτυχθεί αρκετά εργαλεία προκειμένου να υποστηρίξουν τις έρευνες ψηφιακής εγκληματολογίας, μερικά από τα οποία είναι τα εξής : EnCase, Forensic Toolkit, ProDiscover και το Sleuth Kit. Τα περισσότερα εργαλεία χρησιμοποιούν τη δομή file system, file type και string searches, και hash value συγκρίσεις, ενώ επίσης έχουν προταθεί και κάποιες καινοτόμες προσεγγίσεις, όπως η εξόρυξη δεδομένων (data mining) και η ανάλυση των κοινωνικών δικτύων. Σε όλες τις μεθοδολογίες, τα ψηφιακά κομμάτια εντάσσονται στο πλαίσιο της υπόθεσης, σε κάθε περίπτωση, όμως, η συλλογή τους χρειάζεται να είναι σύννομη. Αξιοσημείωτο είναι ότι στις Ηνωμένες Πολιτείες, η αποδοχή των επιστημονικών αποδείξεων στην ακροαματική διαδικασία συνδέεται με έναν μάρτυρα πραγματογνώμονα, ο οποίος παρουσιάζει τα αποδεικτικά στοιχεία στο δικαστήριο, το στοιχείο αυτό το παρατηρούμε και στην ελληνική έννομη τάξη. Ένα εκτεταμένο σώμα της αμερικάνικης νομοθεσίας ασχολείται με τη σχέση μεταξύ των αποδεικτικών στοιχείων, του εξεταστή και τη μαρτυρία. Δύο σημαντικά στοιχεία είναι η εμπειρική φύση της διαδικασίας της εξέτασης από τη μία πλευρά και η ικανότητα του εξεταστή να εξηγήσει τη μέθοδο που εφάρμοσε για να συλλέξει τα αποδεικτικά στοιχεία. Στο παραδοσιακό αυτό μοντέλο, είναι σημαντικό η διαδικασία της εξέτασης να διεξάγεται σε ένα "forensically sound" τρόπο, δηλαδή, όλες οι διεργασίες που έλαβαν χώρα θα πρέπει να μπορούν να αποδειχθούν.12

Το πεδίο της ψηφιακής εγκληματολογίας, σε γενικές γραμμές δεν έχει αλλάξει, οι έρευνες, δηλαδή, κατά κύριο λόγο εκτελούνται από το προσωπικό επιβολής του νόμου με κάποιο τυπικό τεχνολογικό υπόβαθρο. Εν ολίγοις, η ψηφιακή δικανική είναι η διαδικασία αναγνώρισης, διατήρησης, ανάλυσης, και παρουσίασης των αποδείξεων κατά τρόπο νομικά αποδεκτό.13

---

[10] Philippe Jougleux, Lilian Mitrou, Tatiana-Eleni Synodinou, The Legal Regulation of Cyber Attacks, Edited by Ioannis Iglezakis

[11] Mark Pollitt , digital forensics as a surreal narrative

[12] Mark Pollitt , digital forensics as a surreal narrative

[13] JCSNS International Journal of Computer Science and Network Security, VOL.8 No.10, October 2008 Mapping Process of Digital Forensic Investigation Framework
Siti Rahayu Selamat1, Robiah Yusof2, Shahrin Sahib3, Faculty of Information Technology and Communication, Universiti Teknikal Malaysia Melaka, Ayer Keroh, Melaka, Malaysia

Το ζήτημα που γεννάται σε αυτή τη μορφή έρευνας είναι η παραβίαση της αρχής της ιδιωτικότητας του φερόμενου ως δράστη, η οποία συνιστά μια βασική ασφαλιστική δικλείδα στη διεξαγωγή της έρευνας, Η έρευνα προϋποθέτει πρόσβαση στην ψηφιακή δραστηριότητα του υπόπτου, ωστόσο, δε δύναται να εκτείνεται καθ'ολοκληρία σε αυτή. Πιο συγκεκριμένα, όπως στις κλασικές εγκληματολογικές έρευνες απαιτείται η χρήση εντάλματος, το οποίο οριοθετεί τον έλεγχο και την έρευνα που θα πραγματοποιηθεί από την αρμόδια αρχή. Επιπλέον, καθ'όλη τη διάρκεια διεξαγωγής της έρευνας γίνεται καταγραφή κάθε ενέργειας των πραγματογνωμόνων και ελέγχεται με ιδιαίτερη επιμέλεια οποιαδήποτε αλλοίωση στοιχείων που μπορεί να ακυρώσει την αξιοπιστία των πειστηρίων, στα πλαίσια της γενικότερης αξιοπιστίας της έρευνας, της εγκυρότητας και ακεραιότητας των στοιχείων, όπως θα δούμε αναλυτικότερα παρακάτω.

1.4. Δικανική Δικτύων

Τα network forensics αναφέρονται στα αποδεικτικά στοιχεία όπως αρχεία καταγραφής που διατηρούνται από παρόχους υπηρεσιών διαδικτύου, και από άλλους απομακρυσμένους δικτυωμένους υπολογιστές. Τα network forensics κατά κύριο λόγο σχετίζονται με την έρευνα των απομακρυσμένων επιθέσεων, όπως απομακρυσμένες επιθέσεις άρνησης εξυπηρέτησης. Αυτή η μορφή δικανικής αφορά στη διαδικασία ανάκτησης και ανάλυσης πληροφοριών από ένα ή περισσότερα δίκτυα υπολογιστών, τα οποία υποψιαζόμαστε ότι εκτέθηκαν ή προσπελάστηκαν από μη εξουσιοδοτημένους χρήστες. Οι πληροφορίες που θα μας δώσει η ως άνω εξέταση περιλαμβάνουν την κίνηση του δικτύου και τα φορτία δεδομένων. Τα network forensics δίνουν τη δυνατότητα στους πραγματογνώμονες να επεξεργαστούν τις συνθήκες τέλεσης μιας αξιόποινης πράξης, τα υποκείμενα τέλεσής της και τα αίτια της ενέργειας που ερευνούν, ενώ τέλος δύνανται κατά περίπτωση να παρέχουν αποδεικτικά στοιχεία που θα υποστηρίξουν είτε ποινική είτε αστική ευθύνη. Ο ορισμός που δόθηκε για τα network forensics στο πρώτο Digital Forensic Research Workshop, το 2001 είναι ο κάτωθι: «Η χρήση επιστημονικά αποδεδειγμένων τεχνικών για την συλλογή, αναγνώριση, εξέταση, συσχέτιση, ανάλυση και καταγραφή των ψηφιακών αποδεικτικών στοιχείων από πολλαπλές, ενεργές ψηφιακές πηγές, επεξεργασίας και μετάδοσης, για τον σκοπό της αποκάλυψης γεγονότων σχετικών με την προσχεδιασμένη πρόθεση, ή τη μετρήσιμη επιτυχία των μη εξουσιοδοτημένων ενεργειών που έχουν ως σκοπό τη διατάραξη, φθορά, ή και τον κίνδυνο των συστατικών του συστήματος, καθώς και την παροχή πληροφοριών ώστε να βοηθήσει στην απάντηση ή την επαναφορά από αυτές τις ενέργειες».

Όπως αναφέρθηκε και παραπάνω, η ραγδαία ανάπτυξη του διαδικτύου οδήγησε σε αυξημένες επιθέσεις μέσω διαδικτύου και σε απρόβλεπτες παραβιάσεις της ασφάλειας. Οι υπάρχουσες μέθοδοι όπως η εξέταση των αρχείων ιστορικού που διατηρούνται στους διακομιστές, οι εγγραφές των firewall, τα γεγονότα ανίχνευσης παρείσφρησης, τα απολεσθέντα πακέτα, και ούτω καθεξής, δεν επαρκούν για να αναγνωρίσουν τον εξελιγμένο επιτιθέμενο ο οποίος χρησιμοποιεί εργαλεία όπως για παράδειγμα κρυπτογραφία. Επομένως, τα εργαλεία των network forensics χρησιμοποιούν εξειδικευμένες τεχνικές με δυνατότητες καταγραφής και συσχέτισης δεδομένων από πολλαπλές οντότητες του δικτύου.

Τα network forensics αποτελούν την αρχή της αναδημιουργίας των ενεργειών που οδήγησαν σε ένα συμβάν που επιδέχεται περαιτέρω διερεύνησης. Ανάλογα με τον τύπο της διερεύνησης μπορεί να ενδιαφερόμαστε για διαφορετικά γεγονότα και να χρησιμοποιήσουμε διαφορετικές πηγές αποδεικτικών στοιχείων. Ωστόσο, ενδιαφερόμαστε συνήθως για πληροφορίες υψηλού επιπέδου σχετικά με διαφορετικές οντότητες και την αλληλεπίδραση μεταξύ τους. Για παράδειγμα, μπορεί να μας ενδιαφέρουν μηνύματα ηλεκτρονικού ταχυδρομείου που εστάλησαν από ένα συγκεκριμένο χρήστη, οι ιστοσελίδες που προσπελάστηκαν ή τα μηνύματα chat που δέχθηκαν .Η δικτυακή κίνηση αποτελεί μία εξαιρετική πηγή αποδεικτικών στοιχείων για την διερεύνηση δικτύων, δεδομένου ότι είναι το πρωταρχικό μέσο για την εκτέλεση αλληλεπιδράσεων υψηλού επιπέδου . Η διαδικασία αυτή

μπορεί να εκτελεστεί παθητικά χωρίς την ανάγκη επαγρύπνησης του υπόπτου και μπορεί να είναι ένα σημαντικό μέρος της ανάπτυξης του πεδίου δράσης της διερεύνησης .

Τέλος, αυτό το είδος δικανικής αποτελεί τον σχετικά πιο πρόσφατο τομέα της έρευνας και της πρακτικής της ψηφιακής δικανικής που έχει εξελιχθεί ως αποτέλεσμα της αυξανόμενης χρήσης του Διαδικτύου και της ραγδαίας ανάπτυξης της εγκληματικής δραστηριότητας. Υποστηρίζεται επίσης ότι το Internet-forensics έχει εξελιχθεί ως απάντηση στην κοινότητα των χάκερ.14

1.5. Οριοθέτηση των εννοιών: «ψηφιακή δικανική» και «ψηφιακά πειστήρια»

Οι θεμελιώδεις αρχές της Δικανικής Επιστήμης δε φαίνεται να παρουσιάζουν μεγάλες διαφορές από τις παραδοσιακές αρχές της εγκληματολογικής επιστήμης. Ο ρόλος του πραγματογνώμονα είναι ουσιαστικός και πρωταγωνιστικός θα τόσο στην παραδοσιακή εγκληματολογία όσο και στην ψηφιακή.15 Σε πρώτο επίπεδο, ο πραγματογνώμονας καλείται να κατανοήσει το είδος των πιθανών στοιχείων που χρειάζονται για να αποτελέσουν αντικείμενο της έρευνας, εν συνεχεία απαραίτητο κρίνεται να προβεί σε μια επισκόπηση των τύπων των εγκλημάτων που είναι πιθανό να περιλαμβάνει ο υπολογιστής, ώστε να διεξαχθεί η έρευνα σύννομα. Εντοπίζει, λοιπόν, ο ερευνητής τα στοιχεία που δύνανται να αποτελέσουν πειστήρια σύμφωνα με το νόμο και τελικά συλλέγονται ακολουθώντας, επίσης, μία σύννομη διαδικασία προκειμένου αυτά να χρησιμοποιηθούν ως νόμιμες και αναλλοίωτες ενδείξεις, αποχρώσες ενδείξεις ή και αποδείξεις σε ένα ποινικό, συνήθως, αλλά και πολιτικό δικαστήριο.16

Πιθανές πηγές ψηφιακών αποδεικτικών στοιχείων είναι οι υπολογιστές, οι συσκευές αποθήκευσης, ακόμη και οι φορητές συσκευές. Η ψηφιακή εγκληματολογία ασχολείται με την ανάκτηση πληροφοριών που δύνανται να αποτελέσουν ηλεκτρονικά αποδεικτικά στοιχεία, ήτοι συλλέγει τα στοιχεία που συγκροτούν κάποιο γεγονός, τα ανακατασκευάζει με απώτερο σκοπό να παρουσιαστούν στο δικαστήριο ως αποδείξεις. Τα αποδεικτικά στοιχεία είναι πιθανό να αποτελούνται από μαρτυρίες, έγγραφα, καθώς και αντικείμενα τα οποία παραδοσιακά συλλέγονται στη φυσική τους μορφή. Οι νέες τεχνολογίες και οι επιπτώσεις τους σχεδόν σε όλες τις πτυχές της ζωής, συμπεριλαμβανομένου του τρόπου τέλεσης των εγκλημάτων θέτουν νέες προκλήσεις όσον αφορά την εξαγωγή αποδείξεων από ηλεκτρονικές συσκευές και έδωσαν αφορμή για μια νέα μορφή αποδεικτικών στοιχείων που ονομάζεται γενικά «ηλεκτρονικά αποδεικτικά στοιχεία» .17

Τα ηλεκτρονικά στοιχεία ως έννοια περικλείουν οποιοδήποτε υλικό σε ηλεκτρονική ή ψηφιακή μορφή που μπορεί να χρησιμοποιηθεί και να γίνει δεκτό ως απόδειξη πραγματικών περιστατικών .[18] Οι ηλεκτρονικές αποδείξεις έχουν σχεδιαστεί ως «οποιαδήποτε πληροφορία που λαμβάνεται από μια ηλεκτρονική συσκευή ή ψηφιακό μέσο και χρησιμεύει για να πείσει την αλήθεια μιας πράξης. Τα ηλεκτρονικά πειστήρια, επομένως, ορίζονται ως οι πληροφορίες και τα δεδομένα που είναι ικανά και χρήσιμα για εξέταση, τα οποία αποθηκεύονται ή διαβιβάζονται από μία ηλεκτρονική συσκευή19.Σημαντικό είναι να αναφερθεί, ότι τα πειστήρια αυτά διακρίνονται για την εξαιρετική ευθραυστότητα που επιδεικνύουν κατά τη διάρκεια της

[14] Maria Karyda and Lilian Mitrou, Internet Forensics: Legal and Technical Issues

[15] http://www.elesme.gr,

[16] http://www.cert.org/tech_tips/FBI_investigates_crime.html

[17] ENISA, Digital Forensics – Handbook, 3 (2013)

[18] Cameron S.D. Brown, Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice, 9(1) Intl. J. Cyber Criminology 83 (January–June 2015)

[19] www.elesme.gr

εξέτασης και συλλογής τους, γεγονός που υποδηλώνει πιθανούς κινδύνους αλλοίωσης του υπό εξέταση υλικού. Η αλλοίωση αυτή δύναται να επέλθει από άγνοια του ειδικού πραγματογνώμονα, από ελλιπή εξέταση του υλικού, ενώ ακόμη κάποιες φορές θεωρείται απαραίτητη κάποια ήσσονος σημασίας αλλοίωση προκειμένου να ελεγχθεί ενδελεχώς ο υλικός φορέας. Στην περίπτωση της ηθελημένης αλλοίωσης, έχουμε να κάνουμε με τροποποιήσεις οι οποίες τίθενται με τη χρήση κάποιων αλγορίθμων που στην πραγματικότητα δεν επηρεάζουν το περιεχόμενο του υλικού φορέα.

Η συλλογή των ηλεκτρονικών αποδεικτικών στοιχείων περιλαμβάνει την αξιολόγηση μιας συγκεκριμένης κατάστασης και τον εντοπισμό και την ανάκτηση των σχετικών πηγών πληροφοριών που θα μπορούσαν να έχουν αποδεικτική αξία σε κάποια ποινική έρευνα. 20Ψηφιακά αποδεικτικά στοιχεία μπορούν να βρεθούν σχεδόν σε όλα τα ηλεκτρονικά δεδομένα επεξεργασίας του συστήματος, δύνανται να υπάρχουν σε μορφή ψηφιακών εγγράφων, e-mail, αρχεία καταγραφής, ψηφιακές φωτογραφίες, προγράμματα λογισμικού, ή άλλα ψηφιακά αρχεία, δεδομένα του δικτύου ή μεταδεδομένα.21

Στη βιβλιογραφία προτείνεται η ταξινόμηση των αποδεικτικών στοιχείων, με βάση μια σειρά ερωτήσεων, για παράδειγμα : ποιος, πότε, τι, γιατί και πώς. 22 Αυτή η ταξινόμηση περιλαμβάνει: α) Τα στοιχεία ταυτότητας, τον εντοπισμό θεμάτων που αποτελούν μέρος ενός γεγονότος που αποτελεί μια επίθεση σε ένα σύστημα πληροφοριών, β)τα αποδεικτικά στοιχεία θέσης, που καθορίζει κατά προσέγγιση ή την ακριβή τοποθεσία, όπου ένα γεγονός λαμβάνει χώρα, γ) το χρόνο που έλαβε χώρα ένα γεγονός , δ) το πλαίσιο των αποδεικτικών στοιχείων, ενέργειες του χρήστη και δραστηριότητες για την περιγραφή του συμβάντος, ή τη φύση του συμβάντος, ε) τα κίνητρα, συμπεριλαμβανομένων των δεδομένων που χρησιμοποιούνται για να καθορίσουν το κίνητρο του γεγονότος και στ) τη σημασία των αποδεικτικών στοιχείων, που περιγράφει τον τρόπο με τον οποίο έλαβε χώρα ένα γεγονός, ή τα μέσα που χρησιμοποιήθηκαν για την επίθεση.23

Συνοψίζοντας, τα ψηφιακά αποδεικτικά στοιχεία που συλλέγονται και τα ψηφιακά πειστήρια που προκύπτουν από την ανάλυση, θεωρούνται ιδιαιτέρως ευαίσθητα, γι' αυτό σημαντικό κομμάτι της ηλεκτρονικής έρευνας αποτελεί η διατήρησή τους και η διασφάλιση της μη αλλοίωσής τους, αυτός είναι και ο λόγος που τα e-πειστήρια μπορούν να δώσουν στους δράστες μια «ευνοϊκή» θέση από νομικής απόψεως.24

Η έρευνα ψηφιακών πειστηρίων, πρέπει να διεξάγεται σύμφωνα με την ισχύουσα κατά περίπτωση νομοθεσία, δοθέντος ότι συχνά εγείρονται αμφιβολίες για την επάρκεια των γνώσεων ενός ερευνητή και για το αν η ανάλυση και διατήρηση των στοιχείων ακολουθεί τις προβλεπόμενες διαδικασίες. Μάλιστα, προτείνεται ένα σύνολο μεθοδολογιών, που θα αναλυθεί παρακάτω, σε κάθε περίπτωση όμως η διεξαγωγή της έρευνας συνδυάζει την ψηφιακή εγκληματολογία και τις παραδοσιακές μεθόδους και τεχνικές.25 Συνεπαγόμενα, πολλές φορές παρατηρείται το φαινόμενο σε μία δίκη να αμφισβητείται είτε η διαδικασία που ακολουθήθηκε κατά την ερευνητική διαδικασία, είτε και τα ίδια τα κατασχεθέντα.

---

[20] ENISA, Electronic Evidence – a Basic Guide for First Responders, 4 (2014).

[21] Philippe Jougleux, Lilian Mitrou, Tatiana-Eleni Synodinou, The Legal Regulation of Cyber Attacks, Edited by Ioannis Iglezakis

[22] C. Blackwell, An Investigative Framework for Incident Analysis In Advances in Digital Forensics,PartVII,22(G.Peterson&S.Shenoieds,Springer2011).

[23]Philippe Jougleux, Lilian Mitrou, Tatiana-Eleni Synodinou, The Legal Regulation of Cyber Attacks, Edited by Ioannis Iglezakis

[24] Internet Forensics: Legal and Technical Issues Maria and Lilian Mitrou.

[25]Philippe Jougleux, Lilian Mitrou, Tatiana-Eleni Synodinou, The Legal Regulation of Cyber Attacks, Edited by Ioannis Iglezakis

Λαμβάνοντας υπόψη τη λειτουργία των αποδεικτικών στοιχείων δεν υπάρχουν εγγενείς διαφορές μεταξύ των ψηφιακών και παραδοσιακών ειδών αποδεικτικών στοιχείων. Επομένως, το παραδεκτό των αποδεικτικών στοιχείων από τα αρχεία ηλεκτρονικών υπολογιστών και ψηφιακών συσκευών στα δικαστήρια εξαρτάται σε μεγάλο βαθμό από τις υποκείμενες βασικές αρχές των αποδεικτικών στοιχείων στην αντίστοιχη χώρα. Στην Ευρώπη, τα ηπειρωτικά νομικά συστήματα λειτουργούν σύμφωνα με την αρχή της ελεύθερης εκτίμησης των αποδείξεων και προβλέπουν ότι όλα τα αποδεικτικά μέσα, ανεξαρτήτως της μορφής που αναλαμβάνουν, μπορούν να γίνουν δεκτοί σε νομικές διαδικασίες.

Συνεπαγόμενα, τα ψηφιακά αποδεικτικά στοιχεία έχουν κάποια ιδιαίτερα χαρακτηριστικά που τα διαχωρίζουν σε κάποιο βαθμό από τις φυσικές αποδείξεις. Χαρακτηρίζονται από ευθραυστότητα, ευπάθεια και πιθανή παροδικότητα κάποιων μορφών. Επομένως, η ψηφιακή εγκληματολογία δίνει ιδιαίτερη έμφαση στη σωστή αντιμετώπιση των πιθανών στοιχείων, προκειμένου να αποτραπεί η οποιαδήποτε αλλοίωση ή παραποίησή τους. 26

Τα δεδομένα, τα οποία μπορούν τελικά να χαρακτηρίζονται ως αποδεικτικά στοιχεία, είναι πτητικά, ήτοι εύκολα μπορούν να τροποποιηθεί, να διαγραφούν ή ακόμη και να εξαφανιστούν, είτε εσκεμμένα είτε ακόμα και μέσω της κανονικής χρήσης.27 Οι ψηφιακές αποδείξεις, όπως και οι παραδοσιακές αποδείξεις, πρέπει να είναι απαλλαγμένες από επεμβάσεις ή αλλοιώσεις.

Ο ερευνητής ενός ηλεκτρονικού εγκλήματος χρησιμοποιεί τα εξειδικευμένα εργαλεία του ακολουθώντας συγκεκριμένα βήματα κατά τη διαδικασία της έρευνας, όπως θα αναλυθεί παρακάτω, καθότι τα αρχεία μπορεί να έχουν διαγραφεί, καταστραφεί, ή να είναι κρυπτογραφημένα, επομένως ο ερευνητής πρέπει να είναι εξοικειωμένος με μια σειρά από μεθόδους για να αποτραπεί η περαιτέρω ζημιά κατά τη διαδικασία αποκατάστασης.

Προσδιορισμός μέσων εγγραφής των δεδομένων και φωτογράφηση ώστε να μπορεί να αποδειχθεί το φυσικό περιβάλλον και η κατάσταση των στοιχείων.
Δημιουργία χώρων ασφάλισης των δεδομένων. Συνήθως χρησιμοποιείται κάποιο ασφαλές ντουλάπι.
Κατάρτιση καταλόγου των στοιχείων που μπορεί να περιλαμβάνει: φορητούς ηλεκτρονικούς υπολογιστές, σκληρούς ή εξωτερικούς δίσκους, μέσα εγγραφής εφεδρικών αντιγράφων, DVD, CD κλπ., κλειδιά USB, υπολογιστές τσέπης, έξυπνα τηλέφωνα, ανάλυση δραστηριοτήτων δικτύου.
Δημιουργία φακέλου εγκληματολογικών αποδεικτικών στοιχείων, που δεν είναι δυνατόν να διαγραφούν ή να απομακρυνθούν, ώστε να διασφαλίζεται η ακεραιότητα των δεδομένων.

[26] Philippe Jougleux, Lilian Mitrou, Tatiana-Eleni Synodinou, The Legal Regulation of Cyber Attacks, Edited by Ioannis Iglezakis

[27] Philippe Jougleux, Lilian Mitrou, Tatiana-Eleni Synodinou, The Legal Regulation of Cyber Attacks, Edited by Ioannis Iglezakis.

Καταχώριση και ασφάλιση της ηλεκτρονικής εικόνας του δίσκου εγκληματολογικών δεδομένων και εργασία του υπευθύνου σε αντίγραφο εργασίας.
Αναζήτηση και άλλων πηγών άντλησης δεδομένων, όπως υποδεικνύει η πορεία της υπόθεσης.
Εξέταση των δεδομένων με το κατάλληλο λογισμικό ώστε να καταστούν αναγνώσιμα τα αναζητούμενα δεδομένα και χρήση π.χ. λέξεων κλειδιών για τον εντοπισμό δεδομένων σχετικών με την υπόθεση. Επιβαρυντικά και μη στοιχεία συλλέγονται και αποκρυπτογραφούνται αρχεία και σπάνε κωδικοί ασφαλείας.
Στη συνέχεια συντάσσεται έκθεση στην οποία καταγράφεται κάθε στάδιο της ηλεκτρονικής εγκληματολογικής έρευνας με τα ευρήματα, η οποία υπογράφεται από τον πελάτη.
Αν θεωρηθεί απαραίτητο, ο ερευνητής παρίσταται ως μάρτυρας στη δικαστική αίθουσα.

Παρά την κατασκευή πολλών εγκληματολογικών εργαλείων, η ικανότητα των ερευνητών να αποκτούν και να χρησιμοποιούν ψηφιακά αποδεικτικά μέσα εγκληματολογίας παραμένει περιορισμένη. Οι ερευνητές αντιμετωπίζουν σταθερά νέες προκλήσεις που δεν σχετίζονται μόνο με την ανάγκη συμμόρφωσης με τις προαναφερόμενες απαιτήσεις της ακεραιότητας, αυθεντικότητας, αξιοπιστίας, πληρότητας και νομιμότητας αλλά και με τα εγγενή χαρακτηριστικά του ψηφιακού περιβάλλοντος. Τα ηλεκτρονικά στοιχεία είναι αόρατα στο ανθρώπινο μάτι ή τουλάχιστον είναι αόρατα για το μη εκπαιδευμένο μάτι και σε κάθε περίπτωση γίνεται ορατά μόνο έμμεσα και αφού ακολουθούνται οι κατάλληλες διαδικασίες.28

Ο υλικός φορέας μέσα στον οποίο συχνά αναζητείται το αποδεικτικό υλικό, συνήθως είναι ο σκληρός δίσκος του υπολογιστή, οι εξυπηρετητές αρχείων (file servers) καθώς επίσης οι συσκευές βοηθητικής μνήμης όπως CD-ROM, DVD-ROM, Flash RAM, δισκέτες και συσκευές εφεδρικής αποθήκευσης όπως οι μονάδες μαγνητικών ταινιών (backup tapes). Αποδεικτικά στοιχεία μπορούν ακόμη να βρεθούν σε τοποθεσίες όπως έξυπνες κάρτες (smart cards), προσωπικοί ψηφιακοί βοηθοί (PDAs), κινητά τηλέφωνα και σε άλλες ηχητικές συσκευές και συσκευές βίντεο.

Ενδεικτικά μια λίστα με τα αρχεία ενός υπολογιστικού συστήματος που πρέπει να ερευνηθούν είναι:

1. Αρχεία που παράγονται από τον υπολογιστή, όπως τα προσωρινά αρχεία (temporary files), τα «cookies» και τα «log» αρχεία.
2. Αρχεία που δημιουργούνται από τον ίδιο τον χρήστη, όπως έγγραφα κειμένου, μηνύματα ηλεκτρονικού ταχυδρομείου, βάσεις δεδομένων, φωτογραφίες και ταινίες.
3. Προστατευμένα και «κρυμμένα» αρχεία, όπως είναι τα κρυπτογραφημένα, τα συμπιεσμένα, αρχεία που απαιτούν την εισαγωγή συνθηματικού για να είναι προσβάσιμα.

[28] Philippe Jougleux, Lilian Mitrou, Tatiana-Eleni Synodinou , The Legal Regulation of Cyber Attacks, Edited by Ioannis Iglezakis

4. Αρχεία που περιλαμβάνουν τα διαγραμμένα αρχεία του υπολογιστή και παραμένουν στο σύστημα (unallocated space), καθώς και τα δεδομένα που πιθανόν να υπάρχουν στην περιοχή (slack space) ανάμεσα στο τέλος ενός αρχείου και στο τέλος ενός «cluster».

Υπάρχουν δύο βασικοί τύποι δεδομένων που συλλέγονται στη διαδικασία των computer forensics, τα persistent data και τα volatile data. Τα «Persistent data»-μόνιμα δεδομένα ορίζονται ως τα δεδομένα που είναι αποθηκευμένα σε έναν τοπικό σκληρό δίσκο (ή άλλο μέσο) και διατηρούνται όταν ο υπολογιστής είναι απενεργοποιημένος. Τα Volatile data είναι όλα τα δεδομένα που είναι αποθηκευμένα στη μνήμη, ή υπάρχει σε transit, και θα χαθούν όταν ο υπολογιστής δεν τροφοδοτείται ή είναι απενεργοποιημένος. Αυτό που είναι σημαντικό να σημειωθεί είναι ότι συχνά υπάρχει η αντίληψη ότι αυτά τα δεδομένα που απαιτείται να ανακτηθούν από έναν υπολογιστή ή μια συσκευή μέσα στην πτητική μνήμη αποθήκευσης καταγράφονται αυτόματα από τη συσκευή σε μακροπρόθεσμες τράπεζες μνήμης, συνεπώς, συχνά θεωρείται ότι αυτά τα πτητικά δεδομένα μπορούν να ανακτηθούν ακόμα και όταν αποσυνδεθούν από μια πηγή ενέργειας. Τα πτητικά δεδομένα είναι αρκετά διαφορετικά, καθώς τα δεδομένα που είναι αποθηκευμένα σε αυτόν τον τύπο μνήμης μπορούν να χαθούν εντελώς, όταν ένας υπολογιστής ή μια κινητή συσκευή χάνει την πηγή τροφοδοσίας του ή είναι απενεργοποιημένη.29 Τα λεγόμενα volatile δεδομένα βρίσκονται στα μητρώα, τη μνήμη cache, και η μνήμη τυχαίας προσπέλασης (RAM). Δοθέντος ότι τα volatile στοιχεία έχουν εφήμερο χαρακτήρα, είναι απαραίτητο ο ερευνητής να γνωρίζει αξιόπιστους τρόπους για να τα ανακτήσει.

Η μεγάλη και σταθερή αύξηση των δυνατοτήτων αποθήκευσης δεδομένων σε συνδυασμό με το ευρύ φάσμα των συσκευών και το εύρος των αποδεικτικών στοιχείων, αυξάνει την πολυπλοκότητα της ψηφιακής εγκληματολογίας και επιβαρύνει τις αρχές επιβολής του νόμου. Επίσης, ανακύπτουν ζητήματα σχετικά με το «μεγάλο όγκο αποδεικτικών στοιχείων», το «σύντομο χρονικό διάστημα κατά το οποίο οι πάροχοι υπηρεσιών αποθηκεύουν τις πληροφορίες που χρειάζονται για σκοπούς έρευνας» και «τη διατήρηση της ακεραιότητας των ηλεκτρονικών αποδεικτικών στοιχείων από τη στιγμή της κατάσχεσης μέχρι τη στιγμή της ολοκλήρωσης της υπόθεσης. Αξιοσημείωτο είναι δε, ότι κάθε υπό εξέταση συσκευή μπορεί τελικά να απαιτεί μια διαφορετική διαδικασία, διαφορετικά εγκληματολογικά εργαλεία και διαφορετικές μεθόδους συλλογής των αποδεικτικών στοιχείων. Για το λόγο αυτό, μία από τις αρχές που συνιστώνται από τον οδηγό συλλογής αποδεικτικών στοιχείων είναι η λεγόμενη «εξειδικευμένη υποστήριξη». Πολύ περισσότερο, επειδή υπάρχουν πολλά διαφορετικά συστήματα και τεχνικές καταστάσεις που είναι σχεδόν αδύνατο για έναν πραγματογνώμονα ψηφιακής δικανικής να έχει τη συγκεκριμένη τεχνογνωσία για τον τρόπο αντιμετώπισης όλων των διαφορετικών ειδών.30

Λαμβάνοντας υπόψη την ευμετάβλητη φύση των ηλεκτρονικών αποδεικτικών στοιχείων, οι ερευνητές οφείλουν να αντιμετωπίσουν πρόσθετα προβλήματα που οφείλονται σε καθυστερήσεις στην πρόσβαση στη «σκηνή του εγκλήματος» ή σε χρονοβόρες διαδικασίες στο εργαστήριο που διεξάγεται η έρευνα και ο έλεγχος των ευρημάτων.31 Ένα ακόμη σημαντικό εμπόδιο για τη διερεύνηση και την επιτυχή δίωξη του εγκλήματος στον κυβερνοχώρο, έγκειται στη δυσκολία να αποδοθεί μια πράξη σε ένα άτομο, ήτοι καθίσταται εξαιρετικά δυσχερές να ταυτοποιηθεί ο τελικός χρήστης. Η δημιουργία μιας μη αμφισβητούμενης σχέσης μεταξύ των ηλεκτρονικών αποδεικτικών στοιχείων και ενός ατόμου είναι ιδιαίτερα δύσκολη, στην περίπτωση που υπάρχουν πολλοί χρήστες της κατασχεμένης συσκευής.

[29] http://www.computerforensicsspecialists.co.uk/blog/what-is-volatile-data

[30] Philippe Jougleux, Lilian Mitrou, Tatiana-Eleni Synodinou ,The Legal Regulation of Cyber Attacks, Edited by Ioannis Iglezakis

[31] A. Mylonas et al., Dynamic Evidence Acquisition for Smartphone Forensics, inProc. of the 27th IFIP International Information Security and Privacy Conference, Springer (IFIP AICT376), Greece (June 2012).

Τα προαναφερόμενα προβλήματα θα μπορούσαν να οδηγήσουν σε αβεβαιότητες και τελικά να υπονομεύσουν την ακρίβεια και την αξιοπιστία των ηλεκτρονικών αποδεικτικών στοιχείων. Για το λόγο αυτό, τα ηλεκτρονικά αποδεικτικά στοιχεία συνήθως συμπληρώνονται με αποδεικτικά στοιχεία που συλλέγονται μέσω παραδοσιακών αστυνομικών ερευνών προκειμένου να αποδειχθεί η σύνδεση των ψηφιακών αποδεικτικών στοιχείων και εν γένει των κατασχεμένων ευρημάτων με το φερόμενο ως δράστη.32

Τέλος, η παρουσίαση των συλλεγόμενων αποδεικτικών στοιχείων στο δικαστήριο έχει εξίσου μεγάλη σημασία για την αξιοπιστία και το παραδεκτό τους. Τα νομικά συστήματα είναι κατά βάση προσαρμοσμένα στις παραδοσιακές μορφές εγκληματικότητας και στις αντίστοιχες διαδικασίες απόδειξης. Η αποδεικτική αξία των ηλεκτρονικών αποδεικτικών στοιχείων φαίνεται να εξαρτάται, επίσης, από τις αντιλήψεις, τις στάσεις και την έλλειψη ή μη εξειδικευμένων γνώσεων των μη τεχνικών φορέων, όπως η αστυνομία, οι εισαγγελείς, οι δικηγόροι και οι δικαστές.33

Κεφάλαιο 2. Νομικό πλαίσιο

2.1. Ελληνική έννομη τάξη

Τα τελευταία χρόνια η χρήση των ηλεκτρονικών υπολογιστών προκάλεσε μια ανυπολόγιστη αύξηση των εγκλημάτων που τελούνται μέσω ηλεκτρονικού υπολογιστή, αλλά οδήγησε και σε νέες μορφές εγκληματικής δράσης, με αποτέλεσμα να γίνονται προσπάθειες αντιμετώπισης της νέας αυτής εγκληματικότητας. Κρίνεται σκόπιμο να παρουσιαστεί το νομικό πλαίσιο σχετικά με το ηλεκτρονικό έγκλημα, όπως αυτό προβλέπεται στην ελληνική έννομη τάξη. Σε συνέδρια τόσο στην Ελλάδα, όσο και παγκοσμίως με κεντρικό θέμα την προστασία των έννομων συμφερόντων των πολιτών έναντι των ηλεκτρονικών εγκλημάτων, έχει τεθεί το ζήτημα σαφούς ποινικής οριοθέτησης των αξιόποινων αυτών πράξεων, αλλά και αντιμετώπισής τους και εξιχνίασής τους με σύννομες διαδικασίες.

Συγκεκριμένα, πραγματοποιήθηκε συνέδριο για το «Ηλεκτρονικό Έγκλημα» στη Βουδαπέστη και υπογράφηκε η συνθήκη, την 23-11-2001, στην οποία εντάσσονται όλα τα σχετικά συμπεράσματα. Τη συνθήκη αυτή υπέγραψαν 26 υπουργοί ευρωπαϊκών κρατών, μεταξύ των οποίων και της Ελλάδας, χωρίς όμως η χώρα μας να την κυρώσει. Αυτή περιλαμβάνει ορισμούς και ρυθμίσεις για όλες τις μορφές ηλεκτρονικής εγκληματικότητας και είναι ως γνωστή ως «Convention on Cyber 2001».

Στην ελληνική έννομη τάξη, ο νόμος 1805/1988 αφορά εγκλήματα που διαπράττονται γενικά με ηλεκτρονικούς υπολογιστές. Συγκεκριμένα με το άρθρο 3 του νόμου προσετέθησαν τρία νέα άρθρα του Ποινικού Κώδικα, τα 370Β, 370Γ, 386Α. Επιπλέον με το Ν. 3625/2007 εισάγεται στον ΠΚ το άρθρο 348Α , ενώ με το νόμο 4411/2016, ο οποίος δημοσιεύθηκε την 3η Αυγούστου του 2016,επιβλήθηκαν σημαντικές αλλαγές ως προς την ποινική αντιμετώπιση του ηλεκτρονικού εγκλήματος. Συγκεκριμένα, με τον τελευταίο νόμο κυρώθηκαν η Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο, γνωστή ως Σύμβαση της Βουδαπέστης και το Πρόσθετο Πρωτόκολλο αυτής, που εστιάζει στην ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, οι οποίες εκδηλώνονται μέσω του διαδικτύου με τη χρήση

[32] Cameron S.D. Brown, Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice, 9(1) Intl. J. Cyber Criminology 86 (January–June 2015).

[33] Philippe Jougleux, Lilian Mitrou, Tatiana-Eleni Synodinou , The Legal Regulation of Cyber Attacks, Edited by Ioannis Iglezakis

υπολογιστών. Επίσης, αξίζει να σημειωθεί η ενσωμάτωση της Οδηγίας 2013/40/ΕΕ που συνδράμει στη βελτίωση της συνεργασίας ανάμεσα στις αρμόδιες αρχές των κρατών-μελών της Ευρωπαϊκής Ένωσης, με απώτερο σκοπό να διευκολυνθεί η πρόληψη των εγκλημάτων που σχετίζονται με τα συστήματα πληροφοριών.

Αξιοσημείωτο είναι δε, ότι η Σύμβαση της Βουδαπέστης υπεγράφη το 2003 και άργησε ιδιαίτερα να ενσωματωθεί στην ελληνική έννομη τάξη, ενώ το Πρόσθετο Πρωτόκολλο επιφέρει τη διεύρυνση του πεδίου εφαρμογής της Σύμβασης για το έγκλημα στον Κυβερνοχώρο, με στόχο να αντιμετωπίζονται και να επιλύονται ζητήματα εκδήλωσης ρατσιστικών ή ξενοφοβικών πράξεων.

Το ελληνικό δίκαιο, λοιπόν, συγκροτείται από διατάξεις που έχουν προστεθεί σε διαφορετικές χρονικές στιγμές και συνήθως αποτελούν αντίδραση του νομοθέτη σε επίκαιρα ζητήματα ή προσαρμόζουν ήδη υπάρχουσες διατάξεις, προκειμένου να ανταποκρίνονται στους καιρούς. Στις μέρες μας έχει λάβει πολύ μεγάλες διαστάσεις το ιδιαίτερα σοβαρό ζήτημα της εκμετάλλευσης ανηλίκων για την παραγωγή πορνογραφικού υλικού και προκαλεί το έντονο ενδιαφέρον των ανθρώπων παγκοσμίως, καθόσον η «παιδική πορνογραφία» προσβάλλει την ατομική αξιοπρέπεια του ανηλίκου και θέτει σε κίνδυνο τη μετέπειτα εξέλιξή του. Η διάταξη του άρθρο 348Α ΠΚ ρυθμίζει την ποινική διάσταση της πορνογραφίας ανηλίκων και στις παραγράφους 2 και 5 με το νόμο 4411/2016 εισάγεται ο όρος «πληροφοριακό σύστημα» σύμφωνα με τον ορισμό που δίνεται στο άρθρο 13 Π.Κ., όπως αναφέρεται παραπάνω, και αυτή η προσθήκη στόχο έχει να αποφευχθεί οποιαδήποτε σύγχυση λόγω ανομοιογένειας στην εννοιολογική προσέγγιση σε διάφορα σημεία του Ποινικού Κώδικα.

Επιπλέον, στη διάταξη του άρθρου 13 Π.Κ. με το νόμο 4411/2016 , μεταφέρεται η οδηγία 2013/40/ΕΕ και εισάγονται στην ελληνική έννομη τάξη οι έννοιες του πληροφοριακού συστήματος και των ψηφιακών δεδομένων και συγκεκριμένα δίνεται η εξής στις περιπτώσεις η και θ : «η) Πληροφοριακό σύστημα είναι συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών μεταξύ τους συσκευών, εκ των οποίων μία ή περισσότερες εκτελούν, σύμφωνα με ένα πρόγραμμα, αυτόματη επεξεργασία ψηφιακών δεδομένων, καθώς και τα ψηφιακά δεδομένα που αποθηκεύονται, αποτελούν αντικείμενο επεξεργασίας, ανακτώνται ή διαβιβάζονται από την εν λόγω συσκευή ή την ομάδα συσκευών με σκοπό τη λειτουργία, τη χρήση, την προστασία και τη συντήρηση των συσκευών αυτών.
θ) 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 μια λειτουργία».

Η προσθήκη του νέου άρθρου 292Β σχετίζεται με την παρακώλυση λειτουργίας των πληροφοριακών συστημάτων, όπως δηλώνει και ο τίτλος του άρθρου και καθώς φαίνεται εναρμονίζεται με την αντίστοιχη ρύθμιση του προηγούμενα άρθρου 292 Α που αφορά σε αντίστοιχη ποινική πρόβλεψη για επιθέσεις όμως σχετικές με την ασφάλεια των τηλεφωνικών επικοινωνιών. Μάλιστα, η τελευταία διάταξη προστέθηκε με την παρ. 3 του άρθρου 9 του ν. 3674/2008 (Α΄ 136/10.7.2008) και ισχύει από 1.9.2008, ενώ αναπροσαρμόσθηκε με το ν. 4055/2012 (Α΄ 51/12.3.2012). Έχοντας ως γνώμονα την αρχή της αναλογικότητας, σύμφωνα με την ένταση της προσβολής που η τελεσθείσα πράξη επιφέρει, η νέα διάταξη ορίζει ότι όποιος χωρίς δικαίωμα παρεμποδίζει σοβαρά ή διακόπτει τη λειτουργία συστήματος πληροφοριών με την εισαγωγή, διαβίβαση, διαγραφή, καταστροφή, αλλοίωση ψηφιακών δεδομένων ή με αποκλεισμό της πρόσβασης στα δεδομένα αυτά, τιμωρείται με φυλάκιση μέχρι τριών (3) ετών. Μάλιστα, η πράξη αυτή σύμφωνα με την ως άνω διάταξη τιμωρείται με φυλάκιση από ένα (1) έως τρία (3) έτη, αν τελέστηκε με τη χρήση εργαλείου που έχει σχεδιαστεί κατά κύριο λόγο για πραγματοποίηση επιθέσεων που επηρεάζουν μεγάλο αριθμό συστημάτων πληροφοριών ή επιθέσεων που προκαλούν σοβαρές ζημίες και ιδίως επιθέσεων που προκαλούν μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών των συστημάτων

πληροφοριών, οικονομική ζημιά ιδιαίτερα μεγάλης αξίας ή σημαντική απώλεια δεδομένων, β) με φυλάκιση τουλάχιστον ενός (1) έτους, αν προκάλεσε σοβαρές ζημίες και ιδίως μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών των συστημάτων πληροφοριών, οικονομική ζημία ιδιαίτερα μεγάλης αξίας ή σημαντική απώλεια δεδομένων και γ) με φυλάκιση τουλάχιστον ενός (1) έτους, αν τελέστηκε κατά συστημάτων πληροφοριών που αποτελούν μέρος υποδομής για την προμήθεια του πληθυσμού με ζωτικής σημασίας αγαθά ή υπηρεσίες. Η ίδια διάταξη προβλέπει ως ζωτικής σημασίας αγαθά ή υπηρεσίες νοούνται ιδίως η εθνική άμυνα, η υγεία, οι συγκοινωνίες, οι μεταφορές και η ενέργεια, και μάλιστα προβλέπεται ως κατ'έγκληση διωκόμενο αδίκημα. Αξιοσημείωτο είναι ότι στην παράγραφο 3 του άρθρου 292 Β Π.Κ. γίνεται αναφορά και στην περίπτωση που οι προηγούμενες πράξεις τελέστηκαν στο πλαίσιο δομημένης και με διαρκή δράση ομάδας τριών ή περισσότερων προσώπων, που επιδιώκει την τέλεση περισσότερων εγκλημάτων του παρόντος άρθρου, τότε η ποινή φυλάκισης είναι τουλάχιστον δύο (2) έτη.

Μετά το άρθρο 381 του Ποινικού Κώδικα προστίθεται το άρθρο 381Α «Φθορά ηλεκτρονικών δεδομένων, εισάγεται, δηλαδή, με το νόμο 4411/2016 το άρθρο 4 της Σύμβασης και το άρθρο 5 της Οδηγίας, συμπληρώνοντας ένα σημαντικό νομικό κενό της ελληνικής έννομης τάξης που αφορούσε στην παράνομη διαγραφή, καταστροφή, αλλοίωση, απόκρυψη δεδομένων ενός πληροφοριακού συστήματος που δύναται να καταστήσει «ανέφικτη τη χρήση τους ή με οποιονδήποτε τρόπο να αποκλείσει την πρόσβαση στα δεδομένα αυτά». Επίσης, με την παράγραφο 10 του δεύτερου άρθρου του νόμου 4411/2016, εισάγεται το άρθρο 381 Β Π.Κ. , με αποτέλεσμα να εντάσσεται στην ελληνική νομοθεσία το άρθρο 7 της Οδηγίας, που αναφέρεται στην παραγωγή, πώληση, προμήθεια προς χρήση, εισαγωγή, κατοχή, ή διανομή : «α) συσκευών ή προγραμμάτων υπολογιστή, σχεδιασμένων ή προσαρμοσμένων κυρίως για το σκοπό της διάπραξης κάποιου από τα εγκλήματα του άρθρου 381Α, β) συνθηματικών ή κωδικών πρόσβασης ή άλλων παρεμφερών δεδομένων με τη χρήση των οποίων είναι δυνατόν να αποκτηθεί πρόσβαση στο σύνολο ή μέρος ενός πληροφοριακού συστήματος».

Αξιοσημείωτη είναι, επίσης, η προσθήκη με την παράγραφο 3 του δεύτερου άρθρου του νόμου 4411/2016, του άρθρου 292 Γ στον Ποινικό Κώδικα, που αποτελεί το άρθρο 7 της Οδηγίας 2013/40/ΕΕ, και προβλέπεται η αυτοτελής ποινικοποίηση της παραγωγής, πώλησης, διανομής , κατοχής κλπ προγραμμάτων ή συσκευών σχεδιασμένων ή προσαρμοσμένων για την τέλεση των πράξεων που αναφέρονται στη διάταξη 292 Β Π.Κ. , όπως παρατέθηκε στην προηγούμενη παράγραφο.

Το άρθρο 386Α «Απάτη με υπολογιστή» καλύπτει τα κενά εφαρμογής των διατάξεων της κλασικής απάτης (386 ΠΚ «Απάτη»),ως προς την προσβολή της περιουσίας με την χρήση ηλεκτρονικού υπολογιστή. Με το νέο νόμο, στη διάταξη αυτή εισάγεται το άρθρο 8 της Σύμβασης και τώρα πια ρητά στους τρόπους πρόκλησης της ζημίας σε ξένη περιουσίας «είτε με τη μη ορθή διαμόρφωση προγράμματος υπολογιστή είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με τη χωρίς δικαίωμα χρήση δεδομένων είτε με τη χωρίς δικαίωμα παρέμβαση σε πληροφοριακό σύστημα».

Στο άρθρο 216 ΠΚ ποινικοποιείται η πλαστογραφία που σχετίζεται άμεσα με το ηλεκτρονικό έγκλημα, λαμβάνοντας υπόψη την έννοια του εγγράφου στο στοιχ. γ) του άρθρου 13 ΠΚ, όπου έγγραφο θεωρείτε και «κάθε μέσο, το οποίο χρησιμοποιείται από υπολογιστή ή από περιφερειακή μνήμη υπολογιστή με ηλεκτρονικό, μαγνητικό ή άλλο τρόπο για εγγραφή αποθήκευση ή αναπαραγωγή στοιχειών που δεν μπορούν να διαβαστούν άμεσα όπως επίσης και κάθε μαγνητικό, ηλεκτρονικό ή άλλο υλικό , στο οποίο εγγράφεται οποιαδήποτε πληροφορία, εικόνα, σύμβολο ή ήχος, αυτοτελώς ή σε συνδυασμό (πχ μαγνητοταινίες, CD, κινηματογραφικές ταινίες, βιντεοκασέτες κα), εφόσον τα μέσα και τα υλικά αυτά προσπορίζονται ή είναι πρόσφορα να αποδείξουν γεγονότα που έχουν έννομη σημασία.»

Αξιοσημείωτη είναι και η παραβίαση του απορρήτου των τηλεφωνημάτων και της προφορικής συνομιλίας. Το απαραβίαστο των επικοινωνιών αρχικά κατοχυρώνεται στο

Σύνταγμα με το άρθρο 19 όπου προστατεύεται η ελεύθερη επικοινωνία και ανταπόκριση. Η προστασία δεν αφορά μόνο τα γραπτά μηνύματα, αλλά και οποιαδήποτε άλλη μορφή ιδιωτικής επικοινωνίας (πχ οι επιστολές, τα τηλεγραφήματα, τα τηλεφωνήματα, τα τέλεξ, τα φαξ, τα e-mails) και η επικοινωνία αρχίζει από τη στιγμή που διατυπώνεται το μήνυμα από τον αποστολέα και τελειώνει μόλις λάβει γνώση του περιεχομένου της και ο παραλήπτης. Το έννομο αγαθό που προστατεύουν οι ποινικές διατάξεις των άρθρων 370 ΠΚ είναι το ιδιωτικό απόρρητο, μέσα στο οποίο εντάσσεται το άρθρο 19 Σ. Μέχρι το 1982 , η ποινική προστασία του απορρήτου της επικοινωνίας, σύμφωνα με όσα ορίζει το άρθρο 370ΠΚ, περιορίζεται μόνο στο απόρρητο των γραπτών κειμένων. Όμως η χρήση της σύγχρονης τεχνολογίας για την παρακολούθηση ιδιωτικών συνομιλιών και την περαιτέρω χρησιμοποίηση του περιεχομένου τους ανάγκασε την επέκταση της ποινικής προστασίας και το απόρρητο των τηλεφωνημάτων. Έτσι θεσπίστηκε με το Ν.1291/1982 το αξιόποινο της παραβίασης του απορρήτου των τηλεφωνημάτων και της προφορικής συνομιλίας με την ψήφιση του όρθρου 370ΑΠΚ για την. Η τελευταία τροποποίηση πραγματοποιήθηκε με τον Ν.3674/2008.

Παραπάνω, έγινε λόγος για τη διάταξη του άρθρου 370Β ΠΚ (Παραβίαση στοιχείων ή προγραμμάτων υπολογιστών που θεωρούνται απόρρητα), η οποία ρυθμίζει την απόκτηση κάθε είδους απορρήτων (πχ στρατιωτικής, επαγγελματικής, οικονομικής φύσης) μέσω ηλεκτρονικών μέσων. Η εφαρμογή της διάταξης αποκλείεται στις περιπτώσεις που οι φορείς δεν έχουν μέτρα ασφαλείας που να εμποδίζουν την κατευθείαν είσοδο σε αυτούς. Αυτό συμβαίνει γιατί η διάταξη απαιτεί τα έγγραφα να είναι προστατευμένα. Επίσης, διαχωρίζεται ότι η αντιγραφή, αποτύπωση, χρησιμοποίηση και αποκάλυψη διαφοροποιούνται από την απλή πρόσβαση στα δεδομένα.

Το άρθρο 370 Γ ΠΚ (Παράνομη αντιγραφή ή χρήση προγραμμάτων υπολογιστών και παράνομη πρόσβαση σε δεδομένα υπολογιστών) προστατεύει το λογισμικό και τα κάθε είδους προγράμματα ή στοιχεία υπολογιστών, καθώς επίσης και τα συναφή συστήματα τηλεπικοινωνιών. Σε αυτό το άρθρο μπορεί να υπαχθούν οι hackers και τα σχετικά περιστατικά hacking. Η διάταξη του άρθρου αυτού τροποποιήθηκε το νόμο 4411/2016, και με τη νέα διατύπωσή του, στη δεύτερη παράγραφό του τιμωρείται η παράνομη πρόσβαση «στο σύνολο ή τμήμα του πληροφοριακού συστήματος ή σε στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών, παραβιάζοντας απαγορεύσεις ή μέτρα ασφαλείας που έχει λάβει ο νόμιμος κάτοχός του».

Μία ακόμη προσθήκη του νέου νόμου 4411/2016 είναι αυτή του άρθρου 370Δ Π.Κ., κατά την οποία εισάγεται αυτοτελώς η παραβίαση του απορρήτου των επικοινωνιών μέσω πληροφοριακών συστημάτων και μάλιστα ορίζεται ότι « 1. Όποιος, αθέμιτα, με τη χρήση τεχνικών μέσων, παρακολουθεί ή αποτυπώνει σε υλικό φορέα μη δημόσιες διαβιβάσεις δεδομένων ή ηλεκτρομαγνητικές εκπομπές από, προς ή εντός πληροφοριακού συστήματος ή παρεμβαίνει σε αυτές με σκοπό ο ίδιος ή άλλος να πληροφορηθεί το περιεχόμενό τους, τιμωρείται με κάθειρξη μέχρι δέκα (10) ετών.

2. Με την ποινή της παραγράφου 1 τιμωρείται όποιος κάνει χρήση της πληροφορίας ή του υλικού φορέα επί του οποίου αυτή έχει αποτυπωθεί με τους τρόπους που προβλέπεται στην παράγραφο 1.

3. Αν οι πράξεις των παραγράφων 1 και 2 συνεπάγονται παραβίαση στρατιωτικού ή διπλωματικού απορρήτου ή αφορούν απόρρητο που αναφέρεται στην ασφάλεια του Κράτους σε καιρό πολέμου τιμωρούνται κατά το άρθρο 146».

Επιπλέον, με τους Ν.2472/97, Ν.3471/2006, εντάσσεται στην ελληνική έννομη τάξη και η ποινική προστασία των προσωπικών δεδομένων. Αναμφισβήτητα, ένας από τους μεγαλύτερους κινδύνους επέμβασης στην προσωπική και ιδιωτική ζωή του άνθρωπο είναι η συγκέντρωση και επεξεργασία δεδομένων προσωπικού χαρακτήρα, ένα στοιχείο το οποίο στην κοινωνία της πληροφορίας καθίσταται εξαιρετικά εύκολο. Καθημερινά ο σύγχρονος άνθρωπος, μέσω των δραστηριοτήτων του γίνεται αντικείμενο επεξεργασίας και ανάλυσης γεγονός που

χρήζει προστασίας και νομική αντιμετώπισης. Στη χώρα μας, το βασικό νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων, καθορίζεται από τους νόμους 2472/97 (Προστασία του ατόμου από την επεξεργασία προσωπικών δεδομένων, ενσωμάτωση Ευρωπαϊκής Οδηγίας 95/46/ΕΚ.) και 3471/2006 (Προστασία προσωπικών δεδομένων και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του Ν.2472/1997, ενσωμάτωση Ευρωπαϊκής Οδηγίας 58/2002). Ιδιαίτερο ενδιαφέρον παρουσιάζει η παράγραφος 4, του άρθρου 22, Ν. 2472/97 σύμφωνα με την οποία τιμωρείται με «φυλάκιση και χρηματική ποινή όποιος χωρίς δικαίωμα επεμβαίνει με οποιονδήποτε τρόπο σε αρχείο δεδομένων προσωπικού χαρακτήρα ή λαμβάνει γνώση τν δεδομένων αυτών ή αφαιρεί, αλλοιώνει, βλάπτει, καταστρέφει, επεξεργάζεται, μεταδίδει ανακοινώνει, τα καθιστά προσιτά σε μη δικαιούμενα πρόσωπα ή επιτρέπει στα πρόσωπα αυτά να λάβουν γνώση των εν λόγω δεδομένων ή τα εκμεταλλεύονται με οποιοδήποτε τρόπο».

Επίσης με σκοπό την προστασία του απορρήτου των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιοδήποτε άλλο τρόπο, καθώς και την ασφάλεια των δικτύων και των πληροφοριών το 2003 με τον Ν. 3115/2003 ιδρύθηκε η «Αρχή Διασφάλισης Του Απόρρητου Των Επικοινωνιών» (ΑΔΑΕ), η οποία είναι Ανεξάρτητη Αρχή που απολαμβάνει διοικητικής αυτοτέλειας, υπόκειται όμως σε κοινοβουλευτικό έλεγχο κατά τον τρόπο και τη διαδικασία που κάθε φορά προβλέπεται από τον κανονισμό της Βουλής.

Στο σημείο αυτό, κρείσσονος σημασίας είναι να αναφερθούν οι περιπτώσεις στις οποίες επιτρέπεται η άρση του απορρήτου των επικοινωνιών , όπως ο νόμος ορίζει (Νόμος 2225/94 και ΠΔ 47/05). Η προστασία της ελεύθερης ανταπόκρισης ή επικοινωνίας, όπως έχει προαναφερθεί, κατοχυρώνεται Συνταγματικά από την πρώτη παράγραφο του άρθρου 19 του Συντάγματος, το οποίο ορίζει: «Το απόρρητο των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο είναι απόλυτα απαραβίαστο. Νόμος ορίζει τις εγγυήσεις υπό τις οποίες η δικαστική αρχή δεν δεσμεύεται από το απόρρητο για λόγους εθνικής ασφάλειας ή για διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων». Η έννοια του απόλυτα απαραβίαστου του αγαθού ενισχύεται ακόμη περισσότερο από το άρθρο 5§1 της οδηγίας 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου με τίτλο «Απόρρητο των επικοινωνιών σχετικά με την επεξεργασία των δεδομένων χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών», η οποία και ενσωματώθηκε στο ελληνικό δίκαιο με το ΠΔ 47/2005. Το Προεδρικό αυτό διάταγμα μαζί με το Ν. 3115/03 που ιδρύει την Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών συμπληρώνουν το Ν. 2225/94, ο οποίος ορίζει περιοριστικά για ποια εγκλήματα επιτρέπεται η άρση του απορρήτου και την διαδικασία αυτής. Τα προβλεπόμενα εγκλήματα για τα οποία δύναται να εκδοθεί άρση του απορρήτου των επικοινωνιών είναι:

α)τα άρθρα 134, 135 παρ. 1, 2, 135Α, 137Α, 137Β, 138, 139, 140, 143, 144, 146, 148 παρ. 2, 150, 151, 157 παρ. 1, 159 παρ. 3, 168 παρ. 1, 187 παρ. 1, 2, 207, 208 παρ. 1, 235 περ. β', 236 περ. β', 237 περιπτώσεις β' των παραγράφων 1 και 2, 264 περ. β', γ', 270, 272, 275 περ. β, 291 παρ. 1 εδ. β, γ, 292 Α, 299, 322, 324 παρ. 2, 3, 342 παρ. 1 και 2, 348, 348Α παρ. 3, 370 Α, 374, 380, 385 του Ποινικού Κώδικα.

β) τα άρθρα 26, 27, 28, 29, 31, 32, 33, 34, 35, 39, 40, 41, 63, 64, 76, 93 και 97 του Στρατιωτικού Ποινικού Κώδικα,

γ) το άρθρο 15 παρ. 1 του ν. 2168/1993,

δ) τα άρθρα 5, 6, 7 και 8 του ν. 1729/1987,

ε) τα άρθρα 89, 90 και 93 του ν.1165/1968

στ) το άρθρο δεύτερο παράγραφος 1 περ. β` του ν. 2656/1998,

ζ) το άρθρο τρίτο παράγραφος 1 περ. β` του ν. 2803/2000,

η) το άρθρο 2 παρ. 1 περ. α` και β` του ν. 2331/199516

θ) Επίσης, επιτρέπεται η άρση του απορρήτου για τη διακρίβωση των προπαρασκευαστικών πράξεων για

το έγκλημα της παραχάραξης νομίσματος κατά το άρθρο 211 του Ποινικού Κώδικα "καθώς επίσης και για τα εγκλήματα των παραγράφων 3 και 4 του άρθρου 342 του ΠΚ και των παραγράφων 1 και 2 του άρθρου 348Α του ΠΚ.
ι) Η άρση του απορρήτου είναι επίσης επιτρεπτή για τη διακρίβωση παραβάσεων των άρθρων 3 έως 7, 29 και 30 του ν. 3340/2005 (ΦΕΚ 112 Α').
ια) το άρθρο 11 του ν. 3917/2011, 15 του ν. 3471/2006 και 10 του ν. 3115/2003
ιβ) Επιτρέπεται, επίσης, η άρση του απορρήτου για τη διακρίβωση των κακουργημάτων που προβλέπονται από το ν. 3028/2002 «Για την προστασία των Αρχαιοτήτων και εν γένει της Πολιτιστικής Κληρονομιάς» (ΦΕΚ 153 Α`), όπως ο νόμος αυτός εκάστοτε ισχύει. Προσφάτως εκφράστηκε για πρώτη φορά η άποψη της διάκρισης της επικοινωνίας σε εξωτερικά και εσωτερικά στοιχεία, από τον Εισαγγελέα του Αρείου Πάγου Γ. Σανιδά (αρ. γνωμ. 9/2009). Όπου εσωτερικά στοιχεία νοείται το περιεχόμενο της επικοινωνίας, που αποτελούν και τον πυρήνα του εννόμου αγαθού, ενώ τα εξωτερικά η ταυτότητα των επικοινωνούντων, ο χρόνος κλήσεως, η γεωγραφική θέση του επικοινωνούντων κλπ. Σύμφωνα λοιπόν με την γνωμοδότηση του Αρείου Πάγου και υπό το πρίσμα, ότι η εγκληματική συμπεριφορά ούτε εμπίπτει ούτε είναι δυνατόν να εμπίπτει στην έννοια των προσωπικών δεδομένων και ότι η αποκάλυψη και επιβεβαίωση της εγκληματικής συμπεριφοράς και του δράστη δεν είναι δυνατόν να θεωρηθεί ότι αποτελεί προσβολή της προσωπικότητας και παραβίαση των προσωπικών δεδομένων, οι πάροχοι υπηρεσιών επικοινωνίας οφείλουν να γνωστοποιούν στις εισαγγελικές, ανακριτικές και προανακριτικές αρχές, πολύ δε περισσότερο τα δικαστικά συμβούλια και τα δικαστήρια, στα πλαίσια των ερευνών για τη διακρίβωση τελέσεως ενός εγκλήματος και του δράστη, τα αιτούμενα εξωτερικά στοιχεία. Την γνωμοδότηση αυτή ο Εισαγγελέας του Αρείου Πάγου την στήριξε στο Σύνταγμα και στη ερμηνεία που δίδεται στα πλαίσια των νέων μορφών επικοινωνίας του Διαδικτύου, γράφοντας δηλαδή το αυτονόητο ότι «Το διαδίκτυο είναι εξ' ορισμού χώρος ελεύθερης έκφρασης και η δημιουργία ή άλλως κατασκευή ιστοσελίδας σ' αυτό είναι ελεύθερη σε οποιονδήποτε», πχ έκφραση ιδιωτικών απόψεων σε ιστολόγια, που θεμιτά βρίσκονται σε δημόσια θέα, συνεπώς δεν υπάρχει θέληση να διατηρηθεί η μυστικότητα. Με απλά λόγια το ΠΔ 47/2005 κρίθηκε αντισυνταγματικό.

Αξιοσημείωτο είναι ότι με το τρίτο άρθρο του νόμου 4411/2016 εισάγονται νέες ρυθμίσεις στο νόμο 2225/1995, όπως προαναφέρθηκαν, χρίζουν, ωστόσο, περαιτέρω αναφοράς. Συγκεκριμένα, οι περιπτώσεις για τις οποίες αίρεται το απόρρητο επεκτείνονται στα νεοεισαχθέντα άρθρα του νόμου, όπως αναλύθηκαν παραπάνω, δοθέντος ότι η ίδια η φύση των ηλεκτρονικών εγκλημάτων είναι τέτοια που θεωρείται αδήριτη ανάγκη η άρση του απορρήτου της επικοινωνίας προκειμένου να εξιχνιασθεί η τέλεσή τους και να εντοπιστούν αποδεικτικά στοιχεία.

Επίσης, με το νόμο 4411/2016 προστίθεται το τελευταίο εδάφιο του άρθρου 5 παράγραφος 11 του νόμου 2225/1994, όπου προβλέπεται τιμωρία σε όποιον γνωστοποιεί σε τρίτους το γεγονός της άρσης απορρήτου, και όποιος παραβιάζει την υποχρέωση εχεμύθειας κατά τη διαδικασία της άρσης απορρήτου.

Το τέταρτο άρθρο του νόμου 4411/2016 προβλέπει διοικητικές κυρώσεις κατά νομικών προσώπων, εντάσσοντας στην ελληνική έννομη τάξη το άρθρο 10 της Οδηγίας και το άρθρο 12 της Σύμβασης. Και τέλος, το πέμπτο άρθρο, ορίζει ως αρμόδια αρχή για την αμοιβαία δικαστική συνδρομή το Υπουργείο Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων και στο έκτο άρθρο η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας υπό την εποπτεία του Εισαγγελέα Εφετών ως σημείο επαφής για την εκπλήρωση των σκοπών του άρθρου 35 της Σύμβασης «Δίκτυο 24/7» και του άρθρου 13 παράγραφος 1 της Οδηγίας.

Σημαντικό είναι να αναφερθούν κάποιες διατάξεις που προβλέπονται στο στρατιωτικό ποινικό κώδικα και τη στρατιωτική ποινική δικονομία. Συγκεκριμένα, τα εγκλήματα που διαπράττονται σε ένα στρατιωτικό περιβάλλον κατά απορρήτων εγγράφων ή πληροφοριών, τιμωρούνται σύμφωνα με τις διατάξεις των άρθρων 140, 141, 142. Στη διάταξη του άρθρου 140

γίνεται λόγος για την αποσφράγιση, υπεξαγωγή ή καταστροφή εγγράφων ή άλλων αντικειμένων και ορίζεται ότι όποιος χωρίς δικαίωμα ανοίγει, υπεξάγει ή καταστρέφει έγγραφο ή άλλο αντικείμενο οποιασδήποτε στρατιωτικής ή διπλωματικής υπηρεσίας του οποίου ανέλαβε τη φύλαξη ή μεταφορά ή εν γνώσει επιτρέπει σε άλλον την επιχείρηση τέτοιας πράξης ή βοηθά την τέλεσή της ή γνωστοποιεί σε τρίτο το περιεχόμενο εγγράφου που ο ίδιος γνωρίζει λόγω της υπηρεσίας του ή της εργασίας του, τιμωρείται, αν η πράξη δεν επισύρει βαρύτερη ποινή κατ` άλλη διάταξη: α) Σε ειρηνική περίοδο, με φυλάκιση τουλάχιστον έξι μηνών. β) Σε πολεμική περίοδο, με φυλάκιση τουλάχιστον δύο ετών. Επίσης, στη δεύτερη παράγραφο της ίδιας διάταξης, προβλέπεται βαρύτερη ποινή στην περίπτωση που το έγγραφο ή αντικείμενο έχει νομίμως χαρακτηρισθεί ως απόρρητο, τότε επιβάλλεται σε ειρηνική περίοδο φυλάκιση τουλάχιστον δύο ετών και σε πολεμική περίοδο κάθειρξη.

Κατά τη διάταξη του άρθρου 141, προβλέπεται η περίπτωση της απώλειας απορρήτων εγγράφων ή αντικειμένων οποιασδήποτε στρατιωτικής υπηρεσίας, τα οποία χαρακτηρίσθηκαν νομίμως ως απόρρητα και παραδόθηκαν σε αυτόν για μεταφορά, φύλαξη ή διαχείριση, τιμωρείται. Συγκεκριμένα, σε ειρηνική περίοδο, η απώλεια αυτή επισύρει ποινή φυλάκισης μέχρι έξι μηνών, ενώ σε πολεμική περίοδο, ορίζεται φυλάκιση μέχρι δύο ετών. Το άρθρο 142, αφορά στην παράλειψη διασφάλισης απορρήτων σε πολεμική περίοδο, κατά τη διάρκεια της οποίας απαιτείται η προσπάθεια απόκρυψης εγγράφων ή άλλων αντικειμένων οποιασδήποτε στρατιωτικής υπηρεσίας, που χαρακτηρίσθηκαν νομίμως ως απόρρητα. Στη διάταξη του άρθρου 143 ορίζεται το περιεχόμενο των μυστικών πληροφοριών : α) Στην κατάσταση γενικά του στρατού και του πολεμικού υλικού , στα έργα οχύρωσης, στα κρυπτογραφικά μέσα συνεννόησης, στο δίκτυο των στρατιωτικών συγκοινωνιών, στις θέσεις του στρατού, στους τόπους ανεφοδιασμού και στην κατάσταση των προμηθειών σε όπλα, πολεμοφόδια, καύσιμα, τρόφιμα ή χρήματα. β) Στο σχέδιο οργάνωσης ή σύνθεσης του στρατού, στο σχέδιο και τα προπαρασκευαστικά μέτρα επιστράτευσης ή κινητοποίησης του στρατού και στα σχέδια στρατιωτικής επιχείρησης. γ) Σε στρατιωτικές μετακινήσεις ή μεταφορές που εκτελούνται ή σχεδιάζονται. δ) Στην κατάσταση της υγείας ή του φρονήματος και πειθαρχίας του στρατού ή στον αριθμό των τραυματιών, νεκρών ή αιχμαλώτων. ε) Σε κάθε αντικείμενο που χαρακτηρίσθηκε νομίμως ως απόρρητο.

Στη διάταξη του άρθρου 144, η μετάδοση στρατιωτικών μυστικών κρίνεται παράνομη στην περίπτωση που στρατιωτικός και όποιος ανήκει στην υπηρεσία του στρατού, παράνομα και με πρόθεση παραδίδει ή ανακοινώνει σε άλλον ή αφήνει με οποιονδήποτε τρόπο να περιέλθουν στην κατοχή ή στη γνώση άλλου μυστικές πληροφορίες στρατιωτικής σημασίας. Στο άρθρο 145, επισύρει ποινή φυλάκισης μέχρι έξι μηνών η ανακοίνωση στρατιωτικών πληροφοριών χωρίς έγκριση της στρατιωτικής αρχής, εφόσον αυτές οι πληροφορίες είναι ικανές να κλονίσουν την εμπιστοσύνη του κοινού σε αυτόν.

Η αντιμετώπιση περιστατικών από εσωτερικές αιτίες, προβλέπονται στο στρατιωτικό ποινικό κώδικα στη διάταξη του άρθρου, όπου γίνεται λόγος για τη βλάβη ηλεκτρονικών και άλλων μέσων πληροφοριών με ποινή πρόσκαιρης κάθειρξης για περίοδο πολέμου, με ισόβια κάθειρξη σε περίπτωση που τελέστηκε η βλάβη στα πλαίσια της μαχητικής ικανότητας του στρατεύματος και με ποινή φυλάκισης εάν η βλάβη προκλήθηκε από αμέλεια.

2.1.1 Διατάξεις ποινικής δικονομίας

Ως επιταγή της προπεριγραφείσας πραγματικότητας ανέκυψε η ψηφιακή δικανική με τους επιμέρους κλάδους της. Πρόκειται για το είδος εγκληματολογίας που αναζητά ψηφιακά πειστήρια. Το είδος αυτό πειστηρίων αποτελεί αποδεικτικό μέσο με το οποίο εισφέρονται γνώσεις ειδικής πείρας, εμπειρίας, τέχνης ή επιστήμης προς απόδειξη των αποδεικτικών

ζητημάτων. Απαιτείται, λοιπόν, πραγματογνωμοσύνη (369ΚΠολΔ), οι ειδικοί πραγματογνώμονες βοηθούν τους δικαστές, δεν δικαιοδοτούν οι ίδιοι, ενώ εφαρμόζεται και το γενικό μέρος της απόδειξης. Ο διορισμός του πραγματογνώμονα γίνεται από το δικαστήριο. Καταρτίζονται κατάλογοι ανάλογα με συγκεκριμένες ιδιότητες. Ο πραγματογνώμονας είναι υποχρεωμένος να εκτελέσει τα καθήκοντα του εκτός εάν τις αποποιηθεί, πριν ορκιστεί. Η αντικατάσταση πριν ή μετά απ' την ορκωμοσία.
Πρέπει να γνωμοδοτήσει εγγράφως, κατάθεση εγγράφου στο δικαστήριο. Αντίδικη πλευρά με δικαίωμα ανταπόδειξης μπορεί να ζητήσει διορισμό τεχνικού συμβούλου (έξοδα αντίδικης πλευράς, 391ΚΠολΔ). Πραγματογνώμονες και τεχνικοί σύμβουλοι: δικαίωμα να παρίστανται σε κάθε πράξη και να παρίστανται στο δικαστήριο και να υποστηρίζουν την άποψη τους. Οι πραγματογνωμοσύνες εκτιμώνται ελεύθερα και οι πραγματογνώμονες διορίζονται από το δικαστήριο από την μεριά αυτού που φέρει το βάρος απόδειξης (390 κ 387 ΚΠολΔ : το δικαστήριο εκτιμά ελεύθερα την γνωμοδότηση του πραγματογνώμονα).

Σύμφωνα με τον ΚΠολΔ διαπιστώνουμε ότι για να ξεκινήσει μια έρευνα από έναν ειδικό πραγματογνώμονα, η πραγματογνωμοσύνη διατάσσεται είτε αυτεπάγγελτα είτε κατόπιν αιτήσεως διαδίκου, όταν πρόκειται για διάγνωση γεγονότος για την οποία απαιτούνται ειδικές γνώσεις επιστήμης ή τέχνης και η επιλογή πραγματογνώμονα γίνεται από τον πίνακα πραγματογνωμόνων που τηρείται σε κάθε Πρωτοδικείο όσον αφορά τα πολιτικά δικαστήρια και σε κάθε Εισαγγελία όσον αφορά τα ποινικά δικαστήρια.

Είναι γνωστό ότι στη μεν πολιτική διαδικασία ισχύει η αρχή της ελεύθερης εκτίμησης των αποδείξεων στη δε ποινική η αρχή της ηθικής απόδειξης, που σημαίνει ότι το δικαστήριο κρίνει ελεύθερα τα αποδεικτικά μέσα και αποφασίζει κατά συνείδηση χωρίς να δεσμεύεται απόλυτα από κανένα αποδεικτικό μέσο αλλά καταλήγει στην οριστική του κρίση συνεκτιμώντας το σύνολο των αποδείξεων που διαθέτει. Ουσιαστικά καλούνται ειδικοί επιστήμονες κατά περίπτωση (π.χ. γιατροί, πολιτικοί μηχανικοί, βιολόγοι, γεωλόγοι, τεχνικοί υπολογιστών και ένα μεγάλο πλήθος ακόμα ειδικοτήτων) να καταθέσουν την εξειδικευμένη γνώση τους για να μη ληφθεί τελικά υπόψη σε πολλές περιπτώσεις από τους δικαστές; Για ποιο λόγο υπάρχει η εν λόγω διαδικασία που και χρόνο απαιτεί και σε πολλές περιπτώσεις καθυστερεί την υπόθεση (ιδιαίτερα στα ποινικά δικαστήρια που η ανάκριση παραμένει εκκρεμής μέχρι να ολοκληρωθεί η εκάστοτε πραγματογνωμοσύνη) αλλά και χρήμα δαπανάται από το κράτος για την αμοιβή των πραγματογνωμόνων, εάν η επιστημονική γνώση που καταθέτουν κατ' ουσία πηγαίνει στα αζήτητα; Από τη στιγμή που οι δικαστές πέραν της νομική επιστήμης κατέχουν και όλες τις υπόλοιπες, γιατί πρέπει οι διάδικοι να μπαίνουν σε μια δαιδαλώδη διαδικασία και να στηρίζουν τις ελπίδες τους για δικαίωση εκεί χωρίς αποτέλεσμα;

Έχει κριθεί από τον Άρειο Πάγο ότι η έκθεση πραγματογνωμοσύνης εκτιμάται μεν ελεύθερα από το Δικαστήριο της ουσίας, πλην όμως πρέπει να αιτιολογείται η αντίθετη δικαστική κρίση αυτού. Στην πράξη τα πρωτοβάθμια δικαστήρια και σε πολλές περιπτώσεις και τα δευτεροβάθμια δεν ενστερνίζονται αυτή την άποψη και απορρίπτουν με πλημμελείς αιτιολογίες τις πραγματογνωμοσύνες κάθε είδους.

Εδώ ακριβώς τίθεται το ερώτημα κατά πόσο οι θεμελιώδεις αυτές αρχές της απόδειξης πρέπει να τυγχάνουν εφαρμογής και αναφορικά προς το αποδεικτικό μέσο της πραγματογνωμοσύνης; Μήπως ο νομοθέτης θα έπρεπε να εισαγάγει κάποια εξαίρεση και να καταστήσει την εκτίμηση του ως άνω αποδεικτικού μέσου από τα δικαστήρια απόλυτα δεσμευτική; Πρόκειται για αμερόληπτη και εξειδικευμένη επιστημονική γνώση την οποία προσφέρει επιλεγμένο από τις δικαστικές αρχές πρόσωπο (δε μιλάμε για τεχνικό σύμβουλο) και δε μπορεί να δοθεί από τον καθένα και όχι για μια απλή μαρτυρική κατάθεση που τείνει προς την υπεράσπιση του διαδίκου. Κατόπιν επανειλημμένων περιστατικών που παρατηρούνται στη δικαστική καθημερινότητα, θεωρείται αναγκαιότητα η έναρξη διαβούλευσης γύρω από το ζήτημα της δεσμευτικότητας της πραγματογνωμοσύνης στα ελληνικά δικαστήρια, με απώτερο

σκοπό τη μεταβολή του υφιστάμενου νομοθετικού καθεστώτος, που εξισώνει με ισοπεδωτικό τρόπο όλα τα αποδεικτικά μέσα.

Από την άλλη πλευρά, στα αμιγώς ποινικά ζητήματα, όπου τίθεται και περισσότερο το ζήτημα παραβίασης της ιδιωτικότητας των φερόμενων ως δραστών, αξίζει να σημειωθεί ότι η έρευνα διενεργείται όπως κάθε άλλη μορφή έρευνας προς εξιχνίαση κάποιας αξιόποινης πράξης. Συγκεκριμένα, απαιτείται ένταλμα έρευνας, κατάσχεσης υλικών φορέων κλπ. ή σε άλλη περίπτωση η έγκριση του κατόχου/ιδιοκτήτη του υλικού φορέα. Επομένως, ακολουθείται μία σύννομη πορεία κατά την έναρξη της διαδικασίας, ενώ κατά τη διάρκεια διεξαγωγής της έρευνας καταγράφονται όλες οι διαδικασίες προκειμένου να τηρηθεί η αξιοπιστία των πειστηρίων.

Στη στρατιωτική ποινική δικονομία οι διαδικασίες της ανάκρισης-προανάκρισης καθώς επίσης και η αυτόφωρη σύλληψη ρυθμίζονται από το άρθρο 201. Συγκεκριμένα, για τα εγκλήματα αρμοδιότητας των στρατοδικείων ενεργούν αξιωματικοί με παραγγελία του αρμόδιου εισαγγελέα του στρατοδικείου, ο οποίος κατ' εξαίρεση μπορεί να αναθέτει την ενέργεια προανάκρισης και σε γενικό ή ειδικό προανακριτικό υπάλληλο (άρθρα 33 και 34 ΚΠΔ), εκτός από τους πταισματοδίκες και ειρηνοδίκες. Οι προανακριτικοί υπάλληλοι της προηγούμενης παραγράφου, καθώς και οι διοικητές σωμάτων με διοικητική αυτοτέλεια ή οι αξιωματικοί τους οποίους αυτοί ορίζουν, ενεργούν προανάκριση, χωρίς παραγγελία του εισαγγελέα, για τα εγκλήματα που διαπράττουν οι στρατιωτικοί στην περίπτωση που πρόκειται για αυτόφωρα εγκλήματα ή αν από την αναβολή υπάρχει κίνδυνος να ματαιωθεί η δυσχερανθεί η βεβαίωση του εγκλήματος ή η ανακάλυψη του δράστη ή η αποκατάσταση της βλάβης. Στις περιπτώσεις αυτές ειδοποιούν με το ταχύτερο δυνατό μέσο τον αρμόδιο εισαγγελέα του στρατοδικείου και ενεργούν σύμφωνα με τις εντολές και οδηγίες του. Η προανάκριση και η ανάκριση γίνονται με την παρουσία γραμματέα. Ως γραμματέας μπορεί να χρησιμοποιηθεί δικαστικός γραμματέας ή άλλος στρατιωτικός ή υπάλληλος της στρατιωτικής υπηρεσίας και σε περίπτωση που αυτοί δεν υπάρχουν, ενήλικος ιδιώτης κατάλληλος κατά την κρίση του ανακριτή.

2.2 Τοπική δωσιδικία μιας υπόθεσης

Το ζήτημα της φορητότητας, της συνδεσιμότητας των συστημάτων πληροφορικής και γενικότερα ότι το ηλεκτρονικό έγκλημα τελείται οπουδήποτε, δύναται να οδηγήσει σε προβληματισμούς σχετικά με την κατά τόπον αρμοδιότητα. Το νομικό σύστημα διαφέρει σε κάθε χώρα, με αποτέλεσμα το νομικό πλαίσιο σχετικά με το ηλεκτρονικό έγκλημα να παρουσιάζει διαφορές. Σε κάθε περίπτωση, όμως, τα ψηφιακά αποδεικτικά στοιχεία είναι απαραίτητο να πληρούν κάποιες τυπικές προϋποθέσεις προκειμένου να χρησιμοποιηθούν παραδεκτά στην ακροαματική διαδικασία.34 Το διεθνές δίκαιο προβλέπει ορισμένες βάσεις για τη δικαιοδοσία σχετικά με πράξεις εγκληματικότητας στον κυβερνοχώρο, που περιλαμβάνει πρωτίστως την εθνικότητα. Η εδαφικότητα και η εθνικότητα στηρίζονται στην κυριαρχία ενός κράτους που υποδηλώνει το δικαίωμα να ασκεί όλες τις λειτουργίες ενός κράτους σε σχέση με ένα καθορισμένο φυσικό χώρο και πλαισιώνει επίσης τις μορφές και τα όρια της διεθνούς συνεργασίας.35

[34] , James Tetteh Ami-Narh , Edith Cowan University, Patricia A.H. Williams, Edith Cowan University Digital forensics and the legal system: A dilemma of our times, 2008

[35] Philippe Jougleux, Lilian Mitrou, Tatiana-Eleni Synodinou The Legal Regulation of Cyber Attacks, Edited by Ioannis Iglezakis

Αξιοσημείωτο είναι ότι μια πράξη μπορεί να αποτελέσει έγκλημα μέσω υπολογιστή σε μία χώρα , δύναται να είναι νομικά αποδεκτή σε μια άλλη. Σημαντικό παράδειγμα αποτελεί μία υπόθεση ορόσημο, κατά την οποία ένας Αυστραλός επιχειρηματίας υπέβαλε μήνυση για συκοφαντική δυσφήμιση στο αυστραλιανό Ανώτατο Δικαστήριο σχετικά με ένα άρθρο που δημοσιεύθηκε μέσω διαδικτύου στις Ηνωμένες Πολιτείες (OUT-LAW.COM News, 2002). Στην περίπτωση Braintech εναντίον Kostiuk το δευτεροβάθμιο δικαστήριο έχει τη δικαιοδοσία του Ανωτάτου Δικαστηρίου του Καναδά προκειμένου να αποφανθεί για μια υπόθεση που αφορά την προβαλλόμενη παράνομη πράξη από κάτοικο της Κολομβίας, μέσω της χρήσης του διαδικτύου. Το Δικαστήριο έκρινε ότι η παρουσίαση πληροφοριών μέσω του Διαδικτύου, το οποίο είναι προσβάσιμο σε χρήστες σε ξένες δικαιοδοσίες δεν παρέχει επαρκείς λόγους για να επιτρέψει σε μια άλλη χώρα να διεκδικήσει την κατά τόπον δικαιοδοσία. Ως εκ τούτου, το δικαστήριο του Τέξας κρίθηκε κατά τόπον αναρμόδιο στην περίπτωση αυτή (Zorzi, 2000).36

Η σύμβαση για το έγκλημα στον κυβερνοχώρο και η οδηγία 2013/40 / ΕΚ προβλέπουν δικαιοδοσία **βάσει της ιθαγένειας**. Σύμφωνα με το άρθρο 22 παράγραφος 1 στοιχείο δ της σύμβασης της Βουδαπέστης, κάθε συμβαλλόμενο μέρος καθορίζει τη δικαιοδοσία όταν το αδίκημα διαπράττεται από έναν από τους υπηκόους του και εάν θεωρείται αδίκημα κατά το ποινικό νομικό πλαίσιο του τόπου τέλεσης. Η οδηγία 2013/40 / ΕΚ στο άρθρο 12 ορίζει ότι η τοπική δικαιοδοσία σχετίζεται με την ιθαγένεια τουλάχιστον στις περιπτώσεις όπου η πράξη θεωρείται αδίκημα στον τόπο τέλεσής του.

Όσον αφορά τα θέματα επιβολής της ποινικής δικαιοσύνης, η τοπική δωσιδικία συνδέεται αποκλειστικά με τη γεωγραφική επικράτεια του τόπου τέλεσης. Συνεπαγόμενα, η κατά τόπον αρμοδιότητα στις διάφορες έννομες τάξεις καθιερώνεται σύμφωνα με τον τόπο που υπέστη κάποια ζημία ή τον τόπο που τελέσθηκε το αδίκημα.37 Από την άλλη, όμως, η ίδια η φύση των ηλεκτρονικών εγκλημάτων δημιουργεί ζητήματα στον καθορισμό του τόπου, δοθέντος ότι σε σχέση με έναν δράστη που ενεργεί μέσω διαδικτυακής σύνδεσης συχνά δεν είναι σαφές σε ποια τοποθεσία έχει εκτελεστεί μια πράξη.38 Ευκολότερο είναι να προσδιοριστεί συνήθως ο τόπος που επέρχεται το αποτέλεσμα της ζημίας που προκλήθηκε, με αμφιβολίες μόνο στην περίπτωση της νεφουπολογιστικής, όπου δύσκολα μπορεί να αναδειχθεί ο τόπος λόγω συχνής αλλαγής του κέντρου δεδομένων.

Σύμφωνα με τη Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο ένα συμβαλλόμενο μέρος θα μπορούσε να διεκδικήσει την εδαφική αρμοδιότητα και να εκδικάσει ένα αδίκημα εάν το άτομο που επιτίθεται σε ένα ηλεκτρονικό σύστημα και αντίστοιχα το ηλεκτρονικό σύστημα του θύματος βρίσκεται στο έδαφός του, ακόμη και αν ο εισβολέας δεν είναι. 39 Επιπλέον, σύμφωνα με την οδηγία 2013/40/ΕΚ , τα κράτη-μέλη έχουν δικαιοδοσία να εφαρμόσουν το ποινικό νομικό πλαίσιο όταν: α) ο δράστης βρισκόταν φυσικά στην επικράτειά του όταν διέπραξε το αδίκημα, ανεξάρτητα από το αν η παραβίαση αυτή είναι ενάντια σε ένα σύστημα πληροφοριών στο έδαφός του · ή β) το αδίκημα είναι ενάντια σε ένα σύστημα πληροφοριών στο έδαφός του, ανεξάρτητα από το αν ο δράστης διαπράττει το αδίκημα όταν βρίσκεται φυσικά στην επικράτειά του. Συνεπώς, εξάγεται το συμπέρασμα ότι δεν απαιτείται να εκφράζονται όλα τα στοιχεία ενός αδικήματος στο κράτος-μέλος που διεκδικεί την τοπική δωσιδικία, ήτοι η τέλεση του εγκλήματος και τα αποτέλεσμα αυτού, όπως συχνά

[36] James Tetteh Ami-Narh , Edith Cowan University, Patricia A.H. Williams, Edith Cowan University
Digital forensics and the legal system: A dilemma of our times, 2008

[37] Philippe Jougleux, Lilian Mitrou, Tatiana-Eleni Synodinou The Legal Regulation of Cyber Attacks, Edited by Ioannis Iglezakis.

[38] Philippe Jougleux, Lilian Mitrou, Tatiana-Eleni Synodinou The Legal Regulation of Cyber Attacks, Edited by Ioannis Iglezakis.

[39]Philippe Jougleux, Lilian Mitrou, Tatiana-Eleni Synodinou The Legal Regulation of Cyber Attacks, Edited by Ioannis Iglezakis.

συμβαίνει δεν συμπίπτουν, χωρίς αυτό να εμποδίζει το εκάστοτε κράτος-μέλος στο οποίο διετελέστηκε είτε το αδίκημα είτε εκφράστηκε το αποτέλεσμα αυτού, να εφαρμόσει τις ποινικές κυρώσεις που προβλέπονται.

Αξιοσημείωτο είναι βέβαια, το γεγονός, ότι στο διαδικτυακό κόσμο, δύναται να προκύψει δικαστική σύγκρουση , αφού συχνά περισσότερες από μία χώρες διεκδικούν τη δικαιοδοσία για ένα ηλεκτρονικό έγκλημα. Σε περιπτώσεις «παράλληλης» δικαιοδοσίας, η ευρωπαϊκή προσέγγιση επικεντρώνεται στη συνεργασία ή τη διαβούλευση μεταξύ των ενδιαφερομένων κρατών.40 Συγκεκριμένα, στόχος είναι να συγκεντρωθούν οι δικαστικές διαδικασίες σε ένα μόνο κράτος-μέλος κατόπιν συνεργασίας των ενδιαφερόμενων κρατών. Η οδηγία 2013/40 / ΕΕ εισάγει το ρόλο της Ευρωπαϊκής Επιτροπής ως σημείο ενημέρωσης σχετικά με την πρόθεση ενός κράτους μέλους να καθορίσει τη δικαιοδοσία για ένα αδίκημα που διαπράχθηκε εκτός του εδάφους του (άρθρο 10 παράγραφος 3), χωρίς να διευκρινίζει περαιτέρω εάν η Επιτροπή θα πρέπει να ενεργεί ως Συντονιστικό όργανο.

Η απόφαση-πλαίσιο 2009/948/ΔΕΥ του Συμβουλίου της 30ης Νοεμβρίου 2009 στοχεύοντας να αποφευχθεί η σύγκρουση δικαιοδοσίας στον τομέα της ποινικής διαδικασίας, προωθεί τη στενότερη συνεργασία μεταξύ των αρμοδίων αρχών δύο ή περισσοτέρων κρατών μελών που διεξάγουν ποινικές διαδικασίες για την πρόληψη καταστάσεων κατά τις οποίες το ίδιο πρόσωπο υπόκειται σε παράλληλες ποινικές διαδικασίες σε διαφορετικά κράτη μέλη για τα ίδια πραγματικά περιστατικά. Η απόφαση πλαίσιο θεσπίζει ένα πρότυπο συνεργασίας που βασίζεται στην ενημέρωση, τη διαβούλευση και την παραπομπή της υπόθεσης στην Eurojust όταν οι αρμόδιες αρχές δεν είναι σε θέση να καταλήξουν σε συναίνεση.41 Η Eurojust συνιστά έναν οργανισμό της Ευρωπαϊκής Ένωσης, ο οποίος συστάθηκε το 2002. Σκοπός της είναι να προάγει την εύρυθμη διεξαγωγή των ερευνών και των διώξεων, βελτιώνοντας τη συνεργασία μεταξύ των αρμόδιων δικαστικών αρχών των κρατών μελών της Ευρωπαϊκής Ένωσης, στις περιπτώσεις που, όπως προαναφέρθηκε, αντιμετωπίζουν σοβαρές μορφές διασυνοριακού και οργανωμένου εγκλήματος.42

Ένα σημαντικό πρόβλημα που ανακύπτει στην αρχή της εδαφικότητας, όπως αυτή εφαρμόζεται στον ψηφιακό κόσμο, είναι ότι τα δεδομένα είναι δυναμικά και μετακινούνται ή αποθηκεύονται σε διακομιστές που εμπίπτουν σε πολλαπλές δικαιοδοσίες. Επιπρόσθετα, δύναται να ανακύψει αδυναμία προσδιορισμού του τόπου στον οποίο ανήκουν τα υπό εξέταση δεδομένα. Από την άλλη πλευρά, στην υπόθεση "Lotus" (France v. Turkey), ορίστηκε ότι « ο πρώτος και κυριότερος περιορισμός που επιβάλλεται από το διεθνές δίκαιο σε ένα κράτος είναι ότι - ελλείψει της ύπαρξης αντίθετης διάταξης - δεν μπορεί να ασκήσει την εξουσία του υπό οποιαδήποτε μορφή στο έδαφος άλλου κράτους.» Στην ίδια απόφαση, επίσης, αναγνωρίζεται η δικαιοδοσία ως εδαφική με αποτέλεσμα να είναι αδύνατο να ασκηθεί από κάποιο κράτος εκτός της επικράτειάς του παρά μόνο βάσει ενός επιτρεπτού κανόνα που απορρέει από διεθνές έθιμο ή σύμβαση.

Σε κάθε περίπτωση, δοθέντος ότι ανακύπτουν σοβαρά ζητήματα στον προσδιορισμό της τοπικής δωσιδικίας, η διεθνής δικαιοδοσία βασίζεται στην αμοιβαιότητα και κυρίως στις ποινικές διαδικασίες βασίζεται στην αμοιβαία δικαστική συνδρομή, όπως θα αναλυθεί και παρακάτω. Ωστόσο, όσον αφορά την εγκληματικότητα στον κυβερνοχώρο, είναι εξαιρετικά αμφισβητήσιμο εάν η παραδοσιακή διαδικασία δικαστικής συνδρομής είναι επαρκής για την εξυπηρέτηση των σκοπών της ποινικής έρευνας. Το ζήτημα αυτό προκύπτει ιδιαίτερα όσον αφορά την ανάγκη εξασφάλισης στοιχείων που σχετίζονται με ποινικές παραβάσεις εκτείνονται

[40] Article22(5)oftheCouncilofEuropeCybercrimeConventionor Article 10(4) of the Decision on Attacks against Information System.

[41]Philippe Jougleux, Lilian Mitrou, Tatiana-Eleni Synodinou, The Legal Regulation of Cyber Attacks, Edited by Ioannis Iglezakis,

[42] https://e-justice.europa.eu/content_eurojust-23-el.do

διασυνοριακά και απαιτείται η λήψη άμεσων μέτρων καταστολής ή ενεργειών για τη διετέλεση έρευνας.

2.3 Δικαστική συνδρομή

Στα πλαίσια εξέτασης των δομών ενός εργαστηρίου ψηφιακής εγκληματολογίας, σημαντικό είναι να γίνει μνεία για τη δικαστική συνδρομή. Δοθέντος, ότι ο τόπος τέλεσης εγκλήματος μέσω διαδικτύου είναι αβέβαιος, συχνά η δικαστική συνδρομή συνιστά αδήριτη ανάγκη. Προσέτι, η ανίχνευση και δίωξη των μορφών αυτών συμπεριφοράς από ανεξάρτητες μεταξύ τους υπηρεσίες, όπως είναι η αστυνομία και η ποινική δικαιοσύνη, που εδράζονται σε διαφορετικές χώρες, έρχεται αντιμέτωπη με προσκόμματα που θέτει η ανάγκη διασυνοριακής συνεργασίας. Οι διαδικασίες, μάλιστα, που χρειάζεται να ακολουθηθούν είναι εξαιρετικά χρονοβόρες.

Η παραδοσιακή διεθνής συνδρομή, έδινε ιδιαίτερη έμφαση στη σχέση εκζητούντος κράτους και εκζητούμενου, δηλαδή, αντιμετωπιζόταν ως μία διεθνής σχέση, με το εκζητούμενο κράτος να έχει την ευχέρεια να αποδεχθεί ή να απορρίψει κάποιο αίτημα δικαστικής συνδρομής. Το πιο σημαντικό είναι η προϋπόθεση του διπλού αξιοποίνου, με αποτέλεσμα να καθίσταται δυσχερής σε κάποιες περιπτώσεις η διεθνής συνδρομή σε ποινικές υποθέσεις.[43] Ήδη με την εμφάνιση της εγκληματικότητας στο κυβερνοχώρο, τόσο οι μελετητές όσο και οι επαγγελματίες του κυβερνοχώρου έχουν αναγνωρίσει την πρόκληση της εξωεδαφικής συλλογής δεδομένων που ελέγχονται από τρίτους και έχει γίνει πλέον κατανοητή η ανάγκη δικαστικής συνδρομής πέραν της κλασικής. Το θέμα της διασυνοριακής πρόσβασης σε ηλεκτρονικά αποδεικτικά στοιχεία τέθηκε από τα δεκαετία του 80 στο πλαίσιο των συζητήσεων στο Συμβούλιο της Ευρώπης στην σύσταση R (89) 9 για την εγκληματικότητα στον κυβερνοχώρο. Η σύσταση του υπουργικού συμβουλίου με αριθ. 95 (13) σχετικά με την σκοπιμότητα αναζήτησης διασυνοριακών δικτύων αντικατοπτρίζει την κοινή αντίληψη ότι μια ερευνητική δραστηριότητα σε διεθνή δίκτυα ή και συστήματα ηλεκτρονικών υπολογιστών που βρίσκονται σε ξένη επικράτεια δεν θα μπορούσε να ξεκινήσει χωρίς προηγουμένως να έχει τη συγκατάθεση του ενδιαφερόμενου κράτους.[44] Συνακόλουθα, επαφίεται στα κράτη-μέλη η δυνατότητα να διαπραγματευτούν τη δωσιδικία και να επιτύχουν διασυνοριακές αναζητήσεις.

Για την επίλυση των δυσκολιών, αρχικά δημιουργήθηκαν οι διμερείς συμβάσεις έκδοσης εγκληματιών και δικαστικής συνδρομής σε ποινικές υποθέσεις, με τις οποίες δεν παρεχόταν ευρεία ευχέρεια απόρριψης των αιτήσεων, ανάμεσα στα κράτη. Αργότερα, θεσπίσθηκαν οι διμερείς συμβάσεις, όπως η Ευρωπαϊκή Σύμβαση περί Εκδόσεως Εγκληματιών της 13-12-1957 και το από 20-4-1959 συμπλήρωμά της, η Ευρωπαϊκή Σύμβαση περί Αμοιβαίας Δικαστικής Συνδρομής επί Ποινικών Υποθέσεων, καθώς και τα δύο πρόσθετα πρωτόκολλά της. Ωστόσο, δεδομένου ότι το ηλεκτρονικό έγκλημα εξελίσσεται σε ένα παγκόσμιο επίπεδο, διαπιστώνεται ότι χρειάζεται διεθνής συνεργασία και όχι μόνο σε ευρωπαϊκό επίπεδο.

Είναι βέβαιο, ότι οι διωκτικές αρχές, οι δικαστικές αρχές και συνακόλουθα και ο στρατός αδυνατεί να επιλύσει τα όποια συμβάντα ανακύπτουν, ενόσω πρόκειται για διασυνοριακή εγκληματικότητα, χωρίς μια συνεργασία σε παγκόσμιο επίπεδο. Ως αποτέλεσμα αυτής της διαπίστωσης, είναι η ευρωπαϊκή προσπάθεια για επίτευξη συνεργασίας σε διεθνές επίπεδο με στόχο την καταπολέμηση των διασυνοριακών μορφών εγκληματικότητας. Στο πλαίσιο αυτό διατυπώνονται νέα συμβατικά κείμενα, προκειμένου να καλύψουν ανακύπτοντα κενά και να διορθώσουν πρακτικά προβλήματα.

[43] Διονύσιος Δ. Σπινέλλης, Η δικαστική συνεργασία σε ποινικές υποθέσεις στην Ευρώπη και ειδικότερα η ευρωπαϊκή εντολή έρευνας, Ιανουάριος 2016, σελ.12

[44] Philippe Jougleux, Lilian Mitrou, Tatiana-Eleni Synodinou, The Legal Regulation of Cyber Attacks, Edited by Ioannis Iglezakis

Αξιοσημείωτη είναι η Συνθήκη του Amsterdam της 1-5-1999, διακηρύσσοντας (άρθρο 29), ότι σκοπός της ΕΕ είναι η δημιουργία ενός "χώρου ελευθερίας, ασφάλειας και δικαιοσύνης". Η Συνθήκη της Λισσαβόνας για τη Λειτουργία της ΕΕ της 13-12-2007 (παρακάτω: ΣΛΕΕ) στο άρθρο 3 §2 ανέφερε εκ νέου το σκοπό της Ευρωπαϊκής Ένωσης και προς επίρρωση τούτου, στο άρθρο της 67 § 3 υποστηρίζει ότι υιοθετεί μέτρα που επιδιώκουν :

1. την πρόληψη και καταπολέμηση της εγκληματικότητας
2. το συντονισμό και τη συνεργασία των οργάνων απονομής της δικαιοσύνης,
3. την αμοιβαία αναγνώριση των ποινικών αποφάσεων και
4. ενδεχομένως, αν καταστεί αναγκαίο, και τη θέσπιση ελάχιστων κανόνων για την προσέγγιση των διαφόρων νομοθεσιών.45

Τα κράτη μέλη στο πλαίσιο της Σύμβασης για την εγκληματικότητα στο κυβερνοχώρο δέχτηκαν τη διασυνοριακή πρόσβαση σε υπολογιστή με αποθηκευμένα δεδομένα που βρίσκεται σε άλλη χώρα χωρίς την εξουσιοδότηση του τελευταίου σε δύο περιπτώσεις: α) όταν τα δεδομένα που έχουν πρόσβαση είναι δημόσια διαθέσιμα, ανεξάρτητα από το πού αποθηκεύονται γεωγραφικά β) όταν η αρχή διερεύνησης έχει αποκτήσει πρόσβαση σε δεδομένα που βρίσκονται εκτός της επικράτειάς της με τη συγκατάθεση του δικαιούχου, άρα διεξάγει νόμιμο και εξουσιοδοτημένο έλεγχο.46

Η Σύμβαση για το έγκλημα στον κυβερνοχώρο περιλαμβάνει διάταξη σχετικά με τη διασυνοριακή πρόσβαση σε δημόσια διαθέσιμα δεδομένα, στο άρθρο 32, ορίζοντας ότι οι αρμόδιες αρχές έχουν άμεση πρόσβαση σε πληροφορίες σχετικά με διαθέσιμες στο κοινό πηγές, όπως πληροφορίες που δημοσιεύονται σε έναν κάποιο ιστότοπο. Επιπλέον, μπορούν να αποθηκεύσουν δεδομένα (download), να τραβήξουν στιγμιότυπα ή να εξασφαλίσουν σε κάθε περίπτωση παρόμοια δεδομένα με στόχο να τα χρησιμοποιήσουν ως αποδεικτικά στοιχεία χωρίς να χρειάζεται να ζητήσουν αμοιβαία δικαστική συνδρομή ή την άδεια του κράτους στο οποίο βρίσκεται το σύστημα που φιλοξενεί τα δεδομένα. Όπως υποδεικνύεται στο έγγραφο καθοδήγησης σχετικά με το άρθρο 32 της επιτροπής για τα εγκλήματα στον κυβερνοχώρο (CoE), είναι άκρως κατανοητό και σίγουρα νόμιμο, τα δημοσίως προσβάσιμα δεδομένα να χρησιμοποιούνται ως αποδεικτικά στοιχεία, υπό την προϋπόθεση ότι ο εθνικός νόμος δεν περιορίζει την πρόσβαση ή / και τη χρήση τέτοιων δεδομένων. Ωστόσο, διευκρινίζεται ότι εάν ένα μέρος του δημόσιου δικτυακού τόπου, υπηρεσίας ή παρόμοιου είναι κλειστό για το κοινό, τότε δεν θεωρείται ότι είναι δημόσια διαθέσιμο κατά την έννοια του άρθρου 32α, παράγραφος 4.47

Το άρθρο 32β της σύμβασης συνιστά τη σημαντικότερη διάταξη όσον αφορά τη διασυνοριακή πρόσβαση στα δεδομένα για σκοπούς επιβολής και συλλογής αποδεικτικών στοιχείων και μάλιστα αντιμετωπίζει την κατάσταση κατά την οποία μια αρχή επιβολής του νόμου έχει πρόσβαση σε δεδομένα αποθηκευμένα σε άλλο κράτος έχοντας τη συγκατάθεση του νόμιμου εξουσιοδοτημένου να αποκαλύψει τα δεδομένα. Η σύμβαση και η αιτιολογική έκθεση, ωστόσο, δεν καθορίζουν τα κριτήρια για τη νόμιμη εξουσιοδότηση του προσώπου.48 Τόσο ο νόμος όσο και οι λοιποί κανονισμοί, συμπεριλαμβανομένων των συμβάσεων, είναι αποδεκτοί ως βάση. Σε κάθε περίπτωση, όμως, η νομιμότητα καθορίζεται από το εθνικό νομικό πλαίσιο, το οποίο μπορεί να ποικίλει σημαντικά μεταξύ των κομματικών κρατών.49

[45]Bernd Hecker, in: Kai Amboss (Hg), Europäisches Strafrecht post Lissabon, στο Europäisches Strafrecht post Lissabon

[46] https://ccdcoe.org/transborder-data-access-quo-vadis-council-europe.html

[47] Philippe Jougleux, Lilian Mitrou, Tatiana-Eleni Synodinou, The Legal Regulation of Cyber Attacks, Edited by Ioannis Iglezakis

[48] Philippe Jougleux, Lilian Mitrou, Tatiana-Eleni Synodinou, The Legal Regulation of Cyber Attacks, Edited by Ioannis Iglezakis

[49] B.-J. Koops & M. Goodwin, Cyberspace, the Cloud, and Cross-Border Criminal Investigation the Limits and Possibilities of International Law, ibid.

Η Σύμβαση δεν ρυθμίζει τον τρόπο απόκτησης της «συναίνεσης». Ωστόσο, για να λειτουργήσει ως νόμιμη η συναίνεση αυτή θα πρέπει να είναι ελεύθερη, ενημερωμένη, ρητή και να αποκτάται πριν από την πρόσβαση στα δεδομένα.50 Σύμφωνα με την αιτιολογική έκθεση (294), υπάρχουν περιπτώσεις που για παράδειγμα τα δεδομένα ηλεκτρονικού ταχυδρομείου είναι αποθηκευμένα σε κάποιο πάροχο (provider) άλλου κράτους ή και σκόπιμα κάποιος να τα αποθηκεύσει σε άλλη χώρα, εν προκειμένω, εφόσον δοθεί η συγκατάθεση του υποκειμένου που φέρει τη νόμιμη εξουσία, οι ερευνητές αποκτούν νόμιμη πρόσβαση σε αυτά.

Το πλαίσιο πρόσβασης που προβλέπεται στο άρθρο 32β της σύμβασης για το κυβερνοέγκλημα, δεν χρησιμοποιήθηκε πολύ συχνά από τις αρχές επιβολής του νόμου. Αντ'αυτού προτιμούν να έχουν άμεση πρόσβαση μέσω παρόχων υπηρεσιών ή άλλων φορέων του ιδιωτικού τομέα, ωστόσο, η άμεση επαφή με αλλοδαπούς παρόχους υπηρεσιών δημιούργησε ανησυχίες και δεν είναι το είδος της διασυνοριακής πρόσβασης σε δεδομένα που γενικά ενθαρρύνονται ή γίνονται δεκτά στο διεθνές δίκαιο. Ενώ το Συμβούλιο της Ευρώπης αποτρέπει τη "άμεση πρόσβαση σε ξένες ISPs και συνιστά να κάνουν χρήση των διαδικασιών που περιγράφονται στις διεθνείς συνθήκες, όπως η Σύμβαση για την εγκληματικότητα στον κυβερνοχώρο. Επιπλέον, η ομάδα εργασίας για την προστασία δεδομένων του άρθρου 29 συνέστησε να θεσπιστούν νομοθετικά μέτρα για την απαγόρευση στους υπευθύνους επεξεργασίας δεδομένων που δραστηριοποιούνται στην ΕΕ να αποκαλύπτουν δεδομένα προσωπικού χαρακτήρα σε τρίτη χώρα, εάν το ζητήσει η δικαστική ή διοικητική αρχή τρίτης χώρας, εκτός εάν υπάρχει ρητή άδεια από διεθνή συμφωνία ή προβλέπεται από τις συνθήκες αμοιβαίας δικαστικής συνδρομής ή έχει εγκριθεί από εποπτική αρχή.51

Όσον αφορά τη διασυνοριακή πρόσβαση σε δεδομένα για σκοπούς έρευνας, βάσει της Οδηγίας 2013/40/ΕΕ, ο ευρωπαίος νομοθέτης υιοθέτησε μια εντελώς διαφορετική προσέγγιση. Δεν υπάρχουν ειδικοί κανόνες σχετικά με τους τρόπους και τους όρους πρόσβασης σε δεδομένα σε άλλη χώρα. Η συνεργασία, ο συντονισμός και η προσέγγιση του ποινικού δικαίου φαίνεται να αποτελούν τις κύριες επιλογές της οδηγίας 2013/40 / ΕΕ σχετικά με τις επιθέσεις κατά των συστημάτων πληροφοριών όσον αφορά τις επιθέσεις με διασυνοριακή διάσταση.

Η σύμβαση εισάγει την υποχρέωση ενός κράτους μέλους να ενημερώνει την Επιτροπή, όταν αποφασίζει να εξετάσει το ζήτημα της δικαιοδοσίας του για αδίκημα που διαπράχθηκε εκτός του εδάφους του. Η ανταλλαγή πληροφοριών ρυθμίζεται στο άρθρο 13 και συνίσταται στην καθιέρωση και χρήση λειτουργικών εθνικών σημείων επαφής και στην υποχρέωση θέσπισης διαδικασιών για την αντιμετώπιση επειγόντων αιτημάτων συνδρομής. Η απόφαση-πλαίσιο 2009/948/ΔΕΥ επικεντρώνεται στην πρόληψη καταστάσεων κατά τις οποίες το ίδιο πρόσωπο μπορεί να υποβληθεί σε παράνομες εγκληματικές πράξεις σε διαφορετικά κράτη μέλη. 52Προκειμένου να αποφευχθούν οι δυσμενείς συνέπειες που προκύπτουν από παράλληλες διαδικασίες, η απόφαση-πλαίσιο θεωρεί τη συγκέντρωση της διαδικασίας σε ένα κράτος ή την αναφορά στην Eurojust.

Η ανταλλαγή πληροφοριών μεταξύ αρμόδιων αρχών και η απάντηση σε αιτήσεις που υποβάλλονται από αρμόδιες αρχές άλλου κράτους μέλους θεωρούνται υποχρέωση των κρατών μελών. Ωστόσο, δεν διατίθεται μια συνολική ρύθμιση για τη διασυνοριακή συνεργασία, δοθέντος ότι τα κράτη-μέλη που στηρίζονται τη Σύμβαση για την εγκληματικότητα στον κυβερνοχώρο απέφυγαν τη λεπτομερή ρύθμιση και επέλεξαν μια "εποικοδομητική ασάφεια" ώστε να μπορούν να αντιμετωπίσουν διαφορετικές καταστάσεις. Η προσέγγιση της ΕΕ

[50] Philippe Jougleux, Lilian Mitrou, Tatiana-Eleni Synodinou, The Legal Regulation of Cyber Attacks, Edited by Ioannis Iglezakis

[51] Philippe Jougleux, Lilian Mitrou, Tatiana-Eleni Synodinou, The Legal Regulation of Cyber Attacks, Edited by Ioannis Iglezakis

[52] Philippe Jougleux, Lilian Mitrou, Tatiana-Eleni Synodinou , The Legal Regulation of Cyber Attacks, Edited by Ioannis Iglezakis

προέβλεπε τη συνεργασία και τη συντονισμένη συνεργασία, η οποία ενισχύθηκε και βελτιστοποιήθηκε.

Λόγω των δυσχερειών των διαδικασιών αμοιβαίας δικαστικής συνδρομής, οι ερευνητές μερικές φορές προχωρούν εξ αποστάσεως σε δραστηριότητες έρευνας σε ξένο έδαφος χωρίς την επίσημη εξουσιοδότηση. Οι διαδικασίες αμοιβαίας δικαστικής συνδρομής, αν και πιο ευέλικτες και λιγότερο χρονοβόρες από τις παραδοσιακές αμοιβαίες σχέσεις βοήθειας, υποβαθμίζουν τις απαιτήσεις για την απόκτηση και διαφύλαξη πτητικών ηλεκτρονικών αποδεικτικών στοιχείων. Για τη μονομερή πρόσβαση σε αποδεικτικά στοιχεία που βρίσκονται σε άλλη περιοχή, απαιτεί από τα κράτη να θυσιάσουν ένα μέρος της κυριαρχίας τους, και ζήτημα γεννάται ως προς τις επιπτώσεις που θα είχε κάτι τέτοιο. Από την άποψη αυτή, η μονομερής απομακρυσμένη πρόσβαση θα πρέπει να επιτευχθεί κατά τρόπο που να ικανοποιεί τα θεμελιώδη δικαιώματα της ελευθερία επικοινωνίας, προστασία δεδομένων και τα δικαιώματα ιδιοκτησίας καθώς επίσης και να ευθυγραμμίζεται με τους κανόνες του ποινικού δικαίου.

Τον Ιούνιο του 2013, πραγματοποιήθηκε δημόσια ακρόαση στο Στρασβούργο για να συζητηθούν τα πιθανά στοιχεία ενός πρόσθετου πρωτοκόλλου και έγινε οι ακόλουθες πέντε προτάσεις: διασυνοριακή πρόσβαση με συγκατάθεση χωρίς περιορισμό στα αποθηκευμένα δεδομένα "σε άλλο μέρος" · διασυνοριακή πρόσβαση χωρίς συγκατάθεση, αλλά με έγκυρα διαπιστευτήρια · διασυνοριακή πρόσβαση χωρίς συγκατάθεση σε απαιτητικές ή άλλες περιστάσεις · επέκταση της έρευνας χωρίς τον περιορισμό «στην επικράτειά του» στο άρθρο 19.3 · και η εξουσία διάθεσης ως συνδετικού νομικού παράγοντα. Οι βασικές επικρίσεις, πάνω σε αυτές τις προτάσεις αφορούσαν τις απαιτήσεις προστασίας της ιδιωτικής ζωής και της έννοιας της συγκατάθεσης ενός υποκειμένου δεδομένων αντί του υπεύθυνου επεξεργασίας δεδομένων. Οι πτυχές που σχετίζονται με την προστασία των δεδομένων είναι ακόμη πιο δύσκολες, δεδομένου ότι τα συμβαλλόμενα μέρη της Σύμβασης για την εγκληματικότητα στον κυβερνοχώρο εκτείνονται και πέρα από την επικράτεια του Συμβουλίου της Ευρώπης. 53 Υπάρχουν επίσης και άλλα ζητήματα σχετικά με τη νομιμότητα της έγκρισης πρόσβασης σε διασυνοριακό επίπεδο, την αμφισβητούμενη ερμηνεία των όρων όπως «καλή τη πίστει ή σε επιτακτικές περιστάσεις» και «η εξουσία διάθεσης δεδομένων» στο πλαίσιο της διασυνοριακής πρόσβασης.54

Τα συμβατικά κείμενα που αφορούν σε ποινικές υποθέσεις και συνδέουν τα κράτη μέλη της Ευρωπαϊκής Ένωσης είναι τα κάτωθι:

1) Η Ευρωπαϊκή Σύμβαση περί Εκδόσεως Εγκληματιών της 13-12-1957, και το από 20-4-1959 συμπλήρωμά της, η Ευρωπαϊκή Σύμβαση περί Αμοιβαίας Δικαστικής Συνδρομής επί ποινικών υποθέσεων, καθώς και τα δύο πρόσθετα πρωτόκολλά της.
2) Τμήματα της Συνθήκης Schengen της 14 -6-1985.
3) Η Ευρωπαϊκή Σύμβαση της 29-5-2000 για την Αμοιβαία Δικαστική Συνδρομή σε Ποινικές Υποθέσεις (ΑΔΣΠΥ/ΕΕ) και το πρόσθετο πρωτόκολλό της, που όμως δεν την έχει κυρώσει η Ελλάδα.
4) Η Απόφαση-Πλαίσιο 2002/584/JI της 13-6-2002 για το Ευρωπαϊκό Ένταλμα Σύλληψης.
5) Η Απόφαση-πλαίσιο 2003/577/ΔΕΥ του Συμβουλίου της 22/7/ 2003 σχετικά με την εκτέλεση των αποφάσεων δέσμευσης περιουσιακών ή αποδεικτικών στοιχείων στην ΕΈ (ΕΑΔΠΑ).
6) Η Απόφαση-Πλαίσιο 2008/978/ JI για την Ευρωπαϊκή Εντολή για τη συλλογή αντικειμένων, εγγράφων και στοιχείων σε ποινικές υποθέσεις (ΕΕΣΑ).
7) Η Οδηγία 2010/64/EU για το δικαίωμα διερμηνείας και μετάφρασης σε ποινικές διαδικασίες.
8) Η Οδηγία 2012/13/EU για το δικαίωμα πληροφόρησης σε ποινικές διαδικασίες.

[53] https://ccdcoe.org/transborder-data-access-quo-vadis-council-europe.html

[54] http://www.coe.int/en/web/corruption/home

9) Η Οδηγία 2013/48/EU για το δικαίωμα πρόσβασης σε δικηγόρο και το δικαίωμα επικοινωνίας των στερημένων της ελευθερίας τους.
10) Τέλος, σημαντικό σταθμό πρόκειται να αποτελέσει η Οδηγία 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 3-4-2014, περί Ευρωπαϊκής Εντολής Έρευνας σε ποινικές υποθέσεις, η οποία πρόκειται να αρχίσει να ισχύει από την 22/5/2017 (βλ. πιο κάτω) (ΕΕΕ).55

Η αίτηση δικαστικής συνδρομής ιδιαίτερα στα εγκλήματα μέσω διαδικτύου είναι συνηθισμένη. Οι αιτήσεις αυτές διαβιβάζονται από κάποιο δικαστή ή εισαγγελέα ενός κράτους μέλους (ΚΜ) σε δικαστή ή εισαγγελέα άλλου κράτους μέλους.56 Το πρώτο ευρωπαϊκό μέσο που ρύθμιζε θέματα σχετικά με αιτήσεις αυτού του είδους ήταν η Σύμβαση του Συμβουλίου της Ευρώπης του 1959 και το Πρωτόκολλο του 1978 και, αργότερα, η Σύμβαση του 1990. Το 2000, τα κράτη μέλη της Ευρωπαϊκής Ένωσης υπέγραψαν Σύμβαση για την αμοιβαία δικαστική συνδρομή επί ποινικών υποθέσεων προς συμπλήρωση και διευκόλυνση της εφαρμογής αυτών των συμβάσεων. Η σύμβαση του 2000 ενισχύθηκε το 2001 από Πρωτόκολλο, το οποίο επικεντρώνεται στην αμοιβαία νομική συνδρομή για πληροφορίες σχετικά με τραπεζικούς λογαριασμούς ή τραπεζικές συναλλαγές.
Δυνάμει της συμβάσεως του 2000, παρέχεται αμοιβαία συνδρομή για:

1. ποινικές διαδικασίες,
2. διαδικασίες που κινούνται από διοικητικές αρχές όταν η απόφαση μπορεί να δικαιολογήσει προσφυγή ενώπιον ποινικού δικαστηρίου,
3. διαδικασίες που αφορούν αδικήματα ή παραβάσεις τα οποία συνεπάγονται ευθύνη νομικού προσώπου (εταιρείας ή φορέα, όχι «προσώπου») στο αιτούν κράτος μέλος.

Η συνεργασία δύναται να πραγματοποιείται μέσω «αυθόρμητης» ανταλλαγής πληροφοριών ή κατόπιν αιτήματος κράτους μέλους. Ο γενικός κανόνας είναι ότι οι αιτήσεις θα πρέπει να διαβιβάζονται απευθείας μεταξύ των δικαστικών αρχών που είναι κατά τόπον αρμόδιες για την υποβολή και τη διεκπεραίωσή τους και να επιστρέφονται δια της αυτής οδού. Το κράτος μέλος προς το οποίο απευθύνεται η αίτηση οφείλει να συμμορφώνεται προς τις διατυπώσεις και τις διαδικασίες που υπέδειξε ρητά το αιτούν κράτος μέλος. Για να διευκολυνθεί η στενότερη συνεργασία μεταξύ των αρχών επιβολής του νόμου, των δικαστικών αρχών και των λοιπών αρμόδιων αρχών, η Σύμβαση του 2000 προβλέπει τη χρήση τεχνολογικών εργαλείων όπως η εικονοδιάσκεψη, η τηλεφωνική συνδιάλεξη και η παρακολούθηση των τηλεπικοινωνιών.

Από το 2001 τα κράτη μέλη συνεργάζονται όλο και περισσότερο χρησιμοποιώντας μέσα τα οποία εφαρμόζουν την αρχή της αμοιβαίας αναγνώρισης. Η αμοιβαία αναγνώριση σημαίνει ότι οι δικαστικές αρχές (δικαστήρια, δικαστές, εισαγγελείς) ενός κράτους μέλους αναγνωρίζουν τις αποφάσεις των δικαστικών αρχών άλλου κράτους μέλους ως ισοδύναμες εκείνων που λαμβάνονται στο κράτος τους.

Τέλος οι διατάξεις της Οδηγίας 2014/41/ΕΕ, αποτελούν μια πρόοδο στον τομέα της ασφάλειας και της απονομής δικαιοσύνης στην ΕΕ, διευκολύνοντας τη δικαστική συνεργασία σχετικά με τα διασυνοριακά εγκλήματα. Η ως άνω Οδηγία αντικαθιστά τα διάφορα προηγούμενα νομικά κείμενα που ρύθμιζαν θέματα δικαστικής συνδρομής με ένα ενιαίο κείμενο, ενώ παραμένουν κάποιες μόνο εξαιρέσεις που προβλέπονται από ειδικές ρυθμίσεις. Στο κανονιστικό πλαίσιο της Οδηγίας ενισχύεται η θέση του κράτους που δίνει την εντολή, ενώ ταυτόχρονα αναγνωρίζει και στο κράτος εκτέλεσης σημαντικούς λόγους να αρνηθεί την αιτούμενη δικαστική συνδρομή. Εν μέρει τουλάχιστον, διατηρεί και αυτή η οδηγία την απαίτηση του διπλού αξιοποίνου. Το κράτος εντολής έχει τον κύριο λόγο για τον καθορισμό του επιτρεπτού πλαισίου εκτέλεσης των ερευνών. Η ρύθμιση αυτή των σχετικών ζητημάτων

[55]Διονύσιος Δ. Σπινέλλης, Η δικαστική συνεργασία σε ποινικές υποθέσεις στην Ευρώπη και ειδικότερα η ευρωπαϊκή εντολή έρευνας, Ιανουάριος 2016
[56]https://e-justice.europa.eu/content_request_for_judicial_assistance-91-el.do

δικαιολογείται από το γεγονός ότι το αποτέλεσμα των ανακριτικών ενεργειών θα χρησιμοποιηθεί σε ποινική διαδικασία του κράτους αυτού (του κράτους εντολής). Τα κυριότερα ζητήματα που ενδιαφέρουν κατά τη μεταφορά των διατάξεων της Οδηγίας στο Ελληνικό Δίκαιο αφορούν την τήρηση ενός υψηλού βαθμού δικονομικών εγγυήσεων. Η διαδικασία της έκδοσης και εκτέλεσης του ΕΕΕ γίνεται προσπάθεια να επιταχυνθεί με δυο τουλάχιστον τρόπους: Πρώτον, προβλέπεται ότι η εκτέλεση του ΕΕΕ θα πρέπει να γίνεται "το ταχύτερο", και αφετέρου προβλέπονται ειδικές προθεσμίες γι αυτό: 30 ημέρες για ν' αποφασίσει το κράτος εκτέλεσης για την εκτέλεση της ΕΕΕ (ά. 12 παρ. 3) και 90 ημέρες για να πραγματοποιηθεί η εκτέλεση του ανακριτικού μέτρου (ά. 12 παρ. 4). Στην πράξη, για διάφορους λόγους, οι προθεσμίες συχνά δεν τηρούνται. Η πρόβλεψη αυτή, όμως, στόχο έχει να ασκήσει σε κάποιο βαθμό πίεση για την επιτάχυνση των διαδικασιών.57

Λαμβάνοντας υπόψη τα προβλήματα που ανακύπτουν λόγω της ανταλλαγής δεδομένων σε διαφορετικές δικαιοδοσίες σχετικά με την ποινική διαδικασία, σχεδιάστηκε το «έργο της απόδειξης»-"the evidence project". Το σχέδιο αυτό κατέληξε στο συμπέρασμα ότι η Ευρωπαϊκή Ένωση πρέπει να αναπτύξει ένα καλύτερο μέσο για την ταχεία ανταλλαγή πληροφοριών και αποδεικτικών στοιχείων από τη μία χώρα στην άλλη σχετικά με τα εγκλήματα με σκοπό την έγκαιρη διερεύνηση της εγκληματικότητας. Η ανταλλαγή είναι αδήριτη ανάγκη να είναι αμεσότερη ιδίως για τις αντιτρομοκρατικές επιχειρήσεις με σκοπό την αντιμετώπιση παγκόσμιων εγκλημάτων. Ταυτόχρονα, μια ασφαλής και αξιόπιστη ανταλλαγή πληροφοριών και ηλεκτρονικών αποδεικτικών στοιχείων σχετικά με εγκλήματα αποτελεί σημαντικό στοιχείο για την προώθηση της δικαστικής συνεργασίας σε ποινικές υποθέσεις καθώς και για την αποτελεσματική και συνεπή εφαρμογή της αμοιβαίας δικαστικής συνδρομής της Ευρωπαϊκής Ένωσης και των διαδικασιών ευρωπαϊκής διερεύνησης.[58]

Η αντιμετώπιση της τρομοκρατίας και των οργανωμένων εγκλημάτων, συμπεριλαμβανομένου του εγκλήματος στον κυβερνοχώρο, μπορεί να βελτιωθεί σημαντικά, επιτρέποντας την αποτελεσματική, ασφαλή και αξιόπιστη ανταλλαγή εξειδικευμένων πληροφοριών και ηλεκτρονικών αποδεικτικών στοιχείων μεταξύ των εισαγγελέων και των υπηρεσιών επιβολής του νόμου των κρατών μελών, υιοθετώντας μια τυποποιημένη γλώσσα και διαδικασία για την προώθηση της συνεργασίας ποινικά θέματα. Στο πλαίσιο αυτό, η πρόκληση είναι να διευκολυνθεί η ανταλλαγή ηλεκτρονικών αποδεικτικών στοιχείων στο πλαίσιο της Ευρωπαϊκής Ένωσης, καθιστώντας δυνατή την επίτευξη βελτιωμένης διεθνούς συνεργασίας στον εγκληματικό τομέα, με την ενσωμάτωση ειδικού πλαισίου στις διαδικασιών δικαστικής συνδρομής που θα επιτρέπουν καλύτερη συνεργασία και αμεσότητα.

Δύο νομικά πλαίσια της ΕΕ είναι σημαντικό να εξεταστούν στα πλαίσια της προσπάθειας ενίσχυσης της δικαστικής συνεργασίας στον ποινικό τομέα, αφενός οι υφιστάμενες διαδικασίες δικαστικής συνδρομής, όπως προαναφέρθηκαν και αφετέρου τα νέα σύνορα της ευρωπαϊκής εντολής έρευνας. Δοθέντος ότι σε ποινικές υποθέσεις δεν υπάρχουν καθολικά μέσα που να διέπουν μια άμεση συνεργασία καθότι οι διαδικασίες δικαστικής συνδρομής δεν έχουν προσαρμοστεί στην πολυπλοκότητα των σημερινών εγκλημάτων, δύναται να επηρεάσουν αρνητικά τις δυνατότητες ταχείας και αποτελεσματικής μεταφοράς ηλεκτρονικών αποδεικτικών στοιχείων. Συνεπαγόμενα, τον Ιούνιο του 2016, οι Υπουργοί του Συμβουλίου Δικαιοσύνης και Εσωτερικών Υποθέσεων συνέστησαν να μεταρρυθμιστούν οι διαδικασίες αυτές, με σκοπό την αμεσότερη ανταλλαγή ηλεκτρονικών αποδεικτικών στοιχείων. Η προσέγγιση μιας τέτοιας μεταρρυθμιστικής προσπάθειας θα μπορούσε να είναι είτε αποκεντρωμένη είναι κεντρική, συγκεκριμένα, θα μπορούσε η κεντρική πύλη της ΕΕ να λειτουργεί ως κέντρο επεξεργασίας

[57]Διονύσιος Δ. Σπινέλλης, Η δικαστική συνεργασία σε ποινικές υποθέσεις στην Ευρώπη και ειδικότερα η ευρωπαϊκή εντολή έρευνας, Ιανουάριος 2016

[58] A proposed electronic evidence exchange across the European Union By Maria Angela Biasiotti

αιτήσεων αμοιβαίας δικαστικής συνδρομής με μία κεντρική εγκατάσταση αποθήκευσης ψηφιακών αποδεικτικών στοιχείων ή θα μπορούσε να υιοθετηθεί μια εφαρμογή αναφοράς για τις αιτήσεις, η οποία θα εγκαθίσταται χωριστά στα κράτη-μέλη, παρέχοντας αναφορά για τη μονάδα αποθήκευσης.[59]

Όσον αφορά τη συνεργασία μεταξύ των αρχών επιβολής του νόμου και των παρόχων, η Επιτροπή περιέγραψε τις κυριότερες ανησυχίες σχετικά με τη διαφάνεια της διαδικασίας, την αξιοπιστία των ενδιαφερομένων, τον εντοπισμό και την επαφή των αρμόδιων παρόχων υπηρεσιών, τη γνησιότητα και τη νομιμότητα ενός αιτήματος από μια αρχή, την άνιση μεταχείριση των αρχών σε όλα τα κράτη-μέλη και το παραδεκτό των αποδεικτικών στοιχείων σε μια ακροαματική διαδικασία. Μάλιστα η Επιτροπή έδωσε ιδιαίτερη έμφαση στο ζήτημα της πολυπλοκότητας που δημιουργείται από τις διαφορετικές κι ενίοτε αντιφατικές προσεγγίσεις των κρατών-μελών στο πεδίο των ερευνών.[60]

2.4 Η διεύθυνση IP και τα ζητήματα της απόδειξης

Η εφαρμογή της νομοθεσίας για το έγκλημα στον κυβερνοχώρο και, ειδικότερα, το θέμα της συλλογής και της χρήσης αποδεικτικών στοιχείων σε ποινικές διαδικασίες που σχετίζονται με το έγκλημα στον κυβερνοχώρο, έχουν μεγάλη σημασία για την καταπολέμηση της εγκληματικότητας στον κυβερνοχώρο. Ο εντοπισμός των εγκληματιών στον κυβερνοχώρο βασίζεται σχεδόν αποκλειστικά σε ψηφιακά στοιχεία, μάλιστα, η διεύθυνση IP αποτελεί την κύρια πηγή αναγνώρισης των εγκληματιών στον κυβερνοχώρο. Επιπλέον, στην πλειονότητα των περιπτώσεων, το μόνο ίχνος μιας επιθέσεις στον κυβερνοχώρο παίρνει τη μορφή της διεύθυνσης IP. (Οι υπολογιστές στο Διαδίκτυο αναγνωρίζουν ο ένας τον άλλο μέσω διευθύνσεων IP. Κάθε υπολογιστής συνδεδεμένος στο Διαδίκτυο έχει τη δική του διεύθυνση IP που του χορηγείται μόνιμα ή προσωρινά. Η διεύθυνση IP έχει τη μορφή μιας σειράς αριθμών).61

Όπως αναφέρεται στην Ειδική Έκθεση του Υπουργείου Δικαιοσύνης των ΗΠΑ σχετικά με τις έρευνες που αφορούν το Διαδίκτυο και τα Δίκτυα Υπολογιστών: Το Διαδίκτυο και τα δίκτυα βασίζονται σε μια διεύθυνση IP για να φτάσουν στον προορισμό τους. Το κλειδί για τη διερεύνηση των εγκλημάτων που σχετίζονται με το Διαδίκτυο και τα δίκτυα είναι η αναγνώριση της προέλευσης διεύθυνσης IP και η ανίχνευσή της σε μια πηγή. Αυτές οι δεξιότητες επιτρέπουν σε έναν ερευνητή να εντοπίσει πρόσθετες πηγές αποδεικτικών στοιχείων, να επιβεβαιώσει τις καταθέσεις του θύματος και των μαρτύρων και να εντοπίσει ενδεχομένως τον ύποπτο. »62 Οι πάροχοι υπηρεσιών Διαδικτύου έχουν την υποχρέωση να διατηρούν το ημερολόγιο των διευθύνσεων IP που τους έχουν κατανεμηθεί σε κάθε δεδομένη στιγμή, επίσης, υπάρχουν στατικές και δυναμικές διευθύνσεις IP, με τις στατικές να προσφέρουν στο χρήστη τη δυνατότητα δημιουργίας προσωπικού διακομιστή. 63

Η χρήση της διεύθυνσης IP ως ψηφιακών στοιχείων εγείρει το θέμα της επιτήρησης του Διαδικτύου και την παρακολούθηση των επικοινωνιών που συνδέονται με έναν ύποπτο, καθώς και την αποκάλυψη πληροφοριών από τα ISP logs σχετικά με τους πελάτες τους. Δοθέντος ότι

[59] A proposed electronic evidence exchange across the European Union By Maria Angela Biasiotti

[60] Technical Document: Measures to improve cross-border access to electronic evidence for criminal investigations following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace, 2017

[61] G. Smith, Internet Law and Regulation

[62] Alberto R. Gonzales, Regina B. Schofield, David W. Hagy, US. Department of Justice, Special Report on Investigations Involving the Internet and Computer Networks, January 2007

[63] Philippe Jougleux, Lilian Mitrou, Tatiana-Eleni Synodinou, The Legal Regulation of Cyber Attacks, Edited by Ioannis Iglezakis

μέσω των ISP logs, δίνεται η δυνατότητα να συνδεθεί μια συγκεκριμένη διεύθυνση IP με κάποιο χρήστη.

Το ζήτημα της νομικής φύσης της διεύθυνσης IP δεν αφορά μόνο τις επιθέσεις στον κυβερνοχώρο, αλλά και τα εγκλήματα στον κυβερνοχώρο, όπως η παιδική πορνογραφία, η επιβολή της πνευματικής ιδιοκτησίας, η δυσφήμιση κ.λ.π., και γενικότερα την εφαρμογή νομικών κανόνων στο διαδίκτυο. Πράγματι, χωρίς τον εντοπισμό του δράστη μιας εγκληματικής δραστηριότητας, δεν μπορεί να υπάρξει καταστολή κάποια παράνομης πράξης και, συνακόλουθα, δε δύναται να εφαρμοστεί κάποιο νομικό πλαίσιο και αντίστοιχα κάποια κύρωση.

Ένα σοβαρό ζήτημα που γεννάται είναι η φύση της διεύθυνσης IP ως προσωπικών δεδομένων, ωστόσο, μέσω αυτής δεν καθίσταται απόλυτα δυνατή και βέβαιη η σύνδεση με τον τελικού χρήστη που διέπραξε κάποια παραβατική συμπεριφορά. Το πρόβλημα γίνεται περίπλοκο στην περίπτωση που κάποια συσκευή μοιράζεται σε πολλά φυσικά πρόσωπα χωρίς εγγραφή και αναγνώριση πριν από οποιαδήποτε χρήση. Επίσης, ο εντοπισμός του τελικού χρήστη καθίσταται δυσχερής στην περίπτωση χρήσης VPN, ή τεχνολογιών ανωνυμοποίησης, όπως είναι το TOR.

Το νομικό πλαίσιο που εφαρμόζεται στις διευθύνσεις IP σχετίζεται με το διττό χαρακτήρα των διευθύνσεων αυτών, ήτοι προστατεύονται τόσο με βάση το νόμο για τα δεδομένα προσωπικού χαρακτήρα, όσο και με βάση την προστασία του απορρήτου της επικοινωνίας. Η διπλή ταυτότητα που φαίνεται να διατίθεται από τη νομοθεσία της ΕΕ για το ιδιωτικό απόρρητο σε διευθύνσεις IP έχει ως αποτέλεσμα την ταυτόχρονη εφαρμογή διαφορετικών νομικών πηγών και κανόνων, γεγονός που περιπλέκει ακόμη περισσότερο το ζήτημα του προσδιορισμού της νομικής φύσης της διεύθυνσης IP και συνεπώς παρεμβαίνει επιβολή του νόμου.64

Οι διευθύνσεις IP δύνανται να θεωρηθούν, όπως προαναφέρθηκε, προσωπικά δεδομένα, υπό αυτή την έννοια εφαρμόζεται το προστατευτικό καθεστώς της νομοθεσίας της ΕΕ για την προστασία των δεδομένων, γεγονός που συζητήθηκε στη θεωρία και τη νομολογία με την υιοθέτηση της Οδηγίας 95/46 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Πράγματι, ο ευέλικτος ορισμός των δεδομένων προσωπικού χαρακτήρα στην οδηγία 95/46 / ΕΚ δίνει περιθώριο για μια ερμηνεία υπέρ του χαρακτηρισμού των διευθύνσεων IP ως δεδομένων προσωπικού χαρακτήρα. Στην πράξη, αυτή η προσέγγιση ακολουθήθηκε και από τα εθνικά δικαστήρια, ενώ υπήρξε στον αντίποδα ένα σημαντικό ρεύμα νομολογίας που διαφώνησε με την εφαρμογή του νομικού καθεστώτος των προσωπικών δεδομένων στις διευθύνσεις IP.65 Το κύριο επιχείρημα που ευνοεί μια προσέγγιση υπέρ των προσωπικών δεδομένων είναι ότι μια διεύθυνση IP αποτελεί μια σειρά αριθμών, που θεωρούνται ως προσωπικά δεδομένα σχετικά με ένα άτομο, στο βαθμό που σχετίζονται με ένα μηχάνημα και όχι με το άτομο που χρησιμοποιεί τον υπολογιστή. Αξιοσημείωτη είναι η απόφαση του περιφερειακού δικαστηρίου στις ΗΠΑ , την 19η Μαρτίου 2014, σχετικά με την επεξεργασία διευθύνσεων IP από χρήστες του BitTorrent σε συνδυασμό με τη χρήση λογισμικού γεωγραφικής τοποθεσίας , χαρακτηριστικά αναφέρθηκε ότι "δεν υπάρχει τίποτα που να συνδέει τη θέση της διεύθυνσης IP με την ταυτότητα του ατόμου που κατεβάζει και προβάλλει τα βίντεο , ακόμη και άν αυτό το άτομο ζει σε αυτήν την περιοχή".

Σύμφωνα με το άρθρο 2 στοιχείο α) της οδηγίας 95/46 / ΕΚ, τα δεδομένα προσωπικού χαρακτήρα ορίζονται ως : κάθε πληροφορία σχετικά με αναγνωρισμένο ή αναγνωρίσιμο φυσικό πρόσωπο ("υποκείμενο των δεδομένων") · Ένα αναγνωρίσιμο άτομο μπορεί να αναγνωριστεί

[64]Lilian Mitrou, Tatiana-Eleni Synodinou, The Legal Regulation of Cyber Attacks, Edited by Ioannis Iglezakis

[65] Philippe Jougleux, Lilian Mitrou, Tatiana-Eleni Synodinou, Study of Case Law on the Circumstances in Which IP Addresses are Considered Personal Data, Final Report, May 2, 2011 & The Legal Regulation of Cyber Attacks, Edited by Ioannis Iglezakis

άμεσα ή έμμεσα, ιδίως με αναφορά σε αριθμό αναγνώρισης ή σε έναν ή περισσότερους παράγοντες που σχετίζονται με τη φυσική, φυσιολογική, πνευματική, οικονομική, πολιτιστική ή κοινωνική του ταυτότητα.

Επιπλέον, η αιτιολογική σκέψη 26 της οδηγίας ορίζει ότι «πρέπει να λαμβάνονται υπόψη όλα τα μέσα που είναι δυνατόν να χρησιμοποιηθούν είτε από τον υπεύθυνο επεξεργασίας είτε από οποιοδήποτε άλλο πρόσωπο για να προσδιορίσει το εν λόγω πρόσωπο». Επομένως, ένα κεντρικό στοιχείο αυτού του ορισμού είναι η ικανότητα των πληροφοριών να αποκαλύπτουν την ταυτότητα του προσώπου με το οποίο σχετίζονται οι πληροφορίες, ανεξάρτητα από το αν η αναγνώριση αυτή γίνεται άμεσα ή έμμεσα. Είναι γνωστό ότι η διεύθυνση IP διατίθεται σε μια συγκεκριμένη συσκευή και αποκαλύπτει την ταυτότητα του χρήστη της συσκευής σε μεταγενέστερο στάδιο όταν συνδυάζεται με άλλα στοιχεία, όπως τα δεδομένα κίνησης (τα στοιχεία σύνδεσης χρήστη και τα αρχεία καταγραφής). Συνεπαγόμενα, θα μπορούσε να υποστηριχθεί ότι η διεύθυνση IP εμπίπτει στην κατηγορία πληροφοριών που μπορεί να οδηγήσει έμμεσα στην ταυτότητα ενός χρήστη του Διαδικτύου.66 Ωστόσο, η διεύθυνση IP δεν εντοπίζει ένα φυσικό πρόσωπο, αλλά μια συγκεκριμένη συσκευή και μάλιστα εκδίδεται μόνο προσωρινά. Επομένως, μια πολύ στενή ανάγνωση της αιτιολογικής σκέψης 26 μπορεί να οδηγήσει στην αντίθετη διαπίστωση, που σημαίνει ότι η διεύθυνση IP τυπικά δεν μπορεί να χρησιμοποιηθεί για την αναγνώριση ενός φυσικού προσώπου, αλλά μόνο για τη δημιουργία και την καταγραφή ηλεκτρονικής επικοινωνίας μεταξύ δύο συσκευών δικτύου.67

Η ομάδα εργασίας του άρθρου 29, με την απόφαση 4/2007 σχετικά με τα προσωπικά δεδομένα, ζητά ευρεία, ευέλικτη και μη κυριολεκτική ερμηνεία της αιτιολογικής σκέψης 26 της οδηγίας 95/46. Μάλιστα, όπως αναφέρεται στη γνωμοδότηση, "στην πραγματικότητα, αμφισβητώντας ότι τα άτομα δεν μπορούν να εξακριβωθούν, αν και ο σκοπός της επεξεργασίας είναι ακριβώς να τα αναγνωρίσουν, συνιστά μια τεράστια αντίφαση. Ως εκ τούτου, οι πληροφορίες πρέπει να θεωρούνται ότι σχετίζονται με αναγνωρίσιμα άτομα και η επεξεργασία πρέπει να υπόκειται στους κανόνες περί προστασίας των δεδομένων. " Η ομάδα εργασίας του άρθρου 29 καθιέρωσε, επομένως, την αρχή της τελεολογικής ερμηνείας.

Το νομικό καθεστώς της διεύθυνσης IP συμπληρώνεται από την αναγνώριση της διεύθυνσης IP ως εξωτερικής συνιστώσας των ιδιωτικών ηλεκτρονικών επικοινωνιών υπό το φως της προστασίας του απορρήτου των επικοινωνιών. Στο πλαίσιο αυτό, οι κύριες νομικές προκλήσεις δεν αφορούν το νομικό χαρακτηρισμό της διεύθυνσης IP, αλλά τη σωστή βαθμονόμηση της εμπιστευτικότητας της διεύθυνσης IP με άλλα αντικρουόμενα συμφέροντα, όπως η εθνική ασφάλεια και η καταστολή του εγκλήματος.68

Η οδηγία 2002/58 / ΕΚ ορίζει τα «δεδομένα κίνησης» ως δεδομένα που υποβάλλονται σε επεξεργασία για τη μεταφορά μιας επικοινωνίας σε δίκτυο ηλεκτρονικών επικοινωνιών ή για τη χρέωση της. Στην αιτιολογική σκέψη 15 της οδηγίας εξηγείται περαιτέρω η έννοια των δεδομένων κίνησης ως μια επικοινωνία που μπορεί να περιλαμβάνει οποιαδήποτε πληροφορία ονομασίας, αρίθμησης ή διεύθυνσης που παρέχεται από τον αποστολέα μιας επικοινωνίας ή από τον χρήστη μιας σύνδεσης . Τα δεδομένα κυκλοφορίας μπορούν, μεταξύ άλλων, να συνίστανται σε δεδομένα σχετικά με τη δρομολόγηση, τη διάρκεια, τον χρόνο ή τον όγκο μιας επικοινωνίας, το χρησιμοποιούμενο πρωτόκολλο, τη θέση του τερματικού εξοπλισμού του αποστολέα ή του παραλήπτη, το δίκτυο από το οποίο προέρχεται η επικοινωνία , την αρχή, το τέλος ή τη διάρκεια

[66] J. Frayssinet, in: Lucas, Frayssinet, Deveze, Droit de l'informatique et de l'Internet 78 (PUF 2001).

[67] Philippe Jougleux, Lilian Mitrou, Tatiana-Eleni Synodinou , Study of Case Law on the Circumstances in Which IP Addresses are Considered Personal Data, Final Report, May 2, 2011 & The Legal Regulation of Cyber Attacks, Edited by Ioannis Iglezakis.

[68] Philippe Jougleux, Lilian Mitrou, Tatiana-Eleni Synodinou,Study of Case Law on the Circumstances in Which IP Addresses are Considered Personal Data, Final Report, May 2, 2011 & The Legal Regulation of Cyber Attacks, Edited by Ioannis Iglezakis.

μιας σύνδεσης. Μπορούν επίσης να αποτελούνται από τη μορφή στην οποία μεταδίδεται η επικοινωνία από το δίκτυο.69

Οι διευθύνσεις IP εμπίπτουν, λοιπόν, σε αυτόν τον ευρύ ορισμό των δεδομένων κίνησης. Τα δεδομένα κίνησης καλύπτονται από το προστατευτικό πέπλο του εμπιστευτικού χαρακτήρα της επικοινωνίας που θεσπίζεται στο άρθρο 5 της οδηγίας, το οποίο αναφέρει τα εξής:
«Τα κράτη μέλη μεριμνούν για την εμπιστευτικότητα των επικοινωνιών και των σχετικών δεδομένων κίνησης μέσω δημόσιου δικτύου επικοινωνιών και διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών μέσω της εθνικής νομοθεσίας. Ειδικότερα, απαγορεύουν την ακρόαση, την υποκλοπή, την αποθήκευση ή άλλα είδη παρακολούθησης των επικοινωνιών και των σχετικών δεδομένων κίνησης από πρόσωπα διαφορετικά από τους χρήστες, χωρίς τη συγκατάθεση των ενδιαφερομένων χρηστών.»

Παρόλα αυτά, εξαιρέσεις από τον κανόνα αυτό μπορούν να εισαχθούν βάσει του άρθρου 15 παράγραφος 1 της οδηγίας, το οποίο επιτρέπει στα κράτη μέλη να περιορίσουν το πεδίο εφαρμογής των δικαιωμάτων και υποχρεώσεων που προβλέπονται στο άρθρο 5, όταν ο περιορισμός αυτός είναι αναγκαίος, κατάλληλος και ανάλογος (δηλ. Της κρατικής ασφάλειας), της άμυνας, της δημόσιας ασφάλειας και της πρόληψης, διερεύνησης, διαπίστωσης και δίωξης ποινικών αδικημάτων ή της μη εξουσιοδοτημένης χρήσης του συστήματος ηλεκτρονικών επικοινωνιών, όπως αναφέρεται στο άρθρο 13, 1 της οδηγίας 95/46 / ΕΚ. Για το σκοπό αυτό, τα κράτη μέλη μπορούν, μεταξύ άλλων, να θεσπίζουν νομοθετικά μέτρα που προβλέπουν τη διατήρηση δεδομένων για περιορισμένο χρονικό διάστημα, που δικαιολογούνται για συγκεκριμένους λόγους.

Το άρθρο 15 παράγραφος 1 της οδηγίας 2002/58 / ΕΚ είναι ισοδύναμο με το άρθρο 13 της οδηγίας για την προστασία των δεδομένων. Όπως αναφέρεται στην αιτιολογική σκέψη 11 της οδηγίας 2002/58 / ΕΚ:
«Όπως η οδηγία 95/46 / ΕΚ, η παρούσα οδηγία δεν εξετάζει ζητήματα προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών που συνδέονται με δραστηριότητες που δεν διέπονται από το κοινοτικό δίκαιο. Επομένως, δεν μεταβάλλει την υφιστάμενη ισορροπία μεταξύ του δικαιώματος της ιδιωτικής ζωής και της δυνατότητας των κρατών μελών να λαμβάνουν τα μέτρα που αναφέρονται στο άρθρο 15 παράγραφος 1 της παρούσας οδηγίας, τα οποία είναι αναγκαία για την προστασία της δημόσιας ασφάλειας, της άμυνας, της ασφάλειας του κράτους, της οικονομικής ευημερίας του κράτους όταν οι δραστηριότητες σχετίζονται με θέματα κρατικής ασφάλειας και της επιβολής του ποινικού δικαίου. Κατά συνέπεια, η παρούσα οδηγία δεν επηρεάζει την ικανότητα των κρατών μελών να πραγματοποιούν νόμιμη παρακολούθηση των ηλεκτρονικών επικοινωνιών ή να λαμβάνει άλλα μέτρα, εφόσον είναι αναγκαίο για οποιονδήποτε από αυτούς τους σκοπούς και σύμφωνα με την Ευρωπαϊκή Σύμβαση για την Προάσπιση των Δικαιωμάτων του Ανθρώπου και των Θεμελιωδών Ελευθεριών όπως ερμηνεύονται από τις αποφάσεις του Ευρωπαϊκού Δικαστηρίου Ανθρωπίνων Δικαιωμάτων.» Τα μέτρα αυτά πρέπει να είναι κατάλληλα και αναλογικά με τον επιδιωκόμενο σκοπό, καθώς , επίσης και αναγκαία σε μια δημοκρατική κοινωνία, παρακάτω θα γίνει αναφορά στους λόγους άρσης απορρήτου.

2.5. Καθ'ύλην αρμοδιότητα-σύγκρουση αρμοδιότητας

Στις περιπτώσεις όπου μεταξύ των κοινών ποινικών δικαστηρίων και των στρατιωτικών δημιουργήθηκε σύγκρουση αρμοδιότητας, ο Άρειος Πάγος, που συνέρχεται σε συμβούλιο, προσδιορίζει το αρμόδιο δικαστήριο με αίτηση του κατηγορουμένου, του πολιτικώς ενάγοντος ή

[69] Philippe Jougleux, Lilian Mitrou, Tatiana-Eleni Synodinou,Study of Case Law on the Circumstances in Which IP Addresses are Considered Personal Data, Final Report, May 2, 2011 & The Legal Regulation of Cyber Attacks, Edited by Ioannis Iglezakis.

του εισαγγελέα ή του επιτρόπου. "Στη δικαιοδοσία των στρατιωτικών ποινικών δικαστηρίων υπάγονται όσοι είναι στρατιωτικοί κατά το χρόνο τέλεσης της πράξης καθώς και οι αιχμάλωτοι πολέμου. Αν στο έγκλημα συμμετέχουν στρατιωτικοί και ιδιώτες, αρμόδια είναι α) τα κοινά ποινικά δικαστήρια, αν το έγκλημα είναι του κοινού ποινικού δικαίου, β) τα στρατοδικεία για τους στρατιωτικούς και τα κοινά ποινικά δικαστήρια για τους ιδιώτες αν το έγκλημα είναι στρατιωτικό." 70 Μάλιστα, αποκλείεται η παραπομπή ιδιώτη σε στρατιωτικά ποινικά δικαστήρια για οποιοδήποτε έγκλημα.

Συγκεκριμένα, κατά τις διατάξεις των παρ.1 και 2 του άρθρου 132 ΚΠοινΔ στην περίπτωση που μεταξύ δικαστηρίων εξ ίσου αρμοδίων αλλά μη υπαγομένων το ένα στο άλλο ή μεταξύ ανακριτικών υπαλλήλων τίθεται ζήτημα αμφισβήτησης της αρμοδιότητας, τότε η αρμοδιότητα καθορίζεται όπως προσδιορίζεται στην παράγραφο 2, ειδικότερα αν η σύγκρουση δημιουργήθηκε μεταξύ των κοινών ποινικών δικαστηρίων και των στρατιωτικών, τότε το ανώτατο δικαστήριο του Αρείου Πάγου, κατόπιν αιτήσεως των διαδίκων, ήτοι της πολιτικής αγωγής ή του κατηγορούμενου, και κατόπιν αιτήσεως ακόμη και του εισαγγελέως ή του επιτρόπου του Δικαστηρίου (στρατιωτικού Ν.2287/1995 ή πολιτικού), θα συγκροτηθεί σε συμβούλιο, προκειμένου να αποφανθεί.

Αξίζει να σημειωθεί ότι σύμφωνα με το άρθρο 193 παρ.1 του Στρατιωτικού Ποινικού Κώδικα στη δικαιοδοσία των στρατιωτικών ποινικών δικαστηρίων υπάγονται "όσοι είναι στρατιωτικοί κατά το χρόνο τέλεσης της πράξεως καθώς και οι αιχμάλωτοι πολέμου". Στη διάταξη του άρθρου 5 παρ.1 του Στρατιωτικού Ποινικού Κώδικα ορίζεται ότι "στρατός είναι ο ελληνικός στρατός της ξηράς, της θάλασσας και του αέρα και στρατιωτικές υπηρεσίες είναι οι υπηρεσίες που ανήκουν σε αυτόν, στρατιωτικοί δε είναι όσοι ανήκουν στο στρατό και στο λιμενικό σώμα". Με το άρθρο 167 του ως άνω Κώδικα ορίζεται ότι η ποινική δικαιοσύνη στο στρατό απονέμεται από τα στρατιωτικά δικαστήρια και τον Άρειο Πάγο. Προσέτι, το άρθρο 213 του Στρατιωτικού Ποινικού Κώδικα σημειώνει ότι "οι διατάξεις του Κώδικα Ποινικής Δικονομίας και οι λοιπές διατάξεις που εφαρμόζονται στις διαδικασίες ενώπιον των κοινών ποινικών δικαστηρίων και αρχών εφαρμόζονται και στις διαδικασίες ενώπιον των στρατιωτικών ποινικών δικαστηρίων και αρχών, εκτός αν ο Κώδικας αυτός ή άλλος ειδικός νόμος ορίζουν διαφορετικά".

Με τη διάταξη του άρθρου 96 παρ. 4 εδάφιο α του ισχύοντος Συντάγματος του 1975 (όπως αυτό ισχύει μετά την αναθεώρηση του 1986 και την αναθεώρηση του έτους 2001), ορίζεται ότι "ειδικοί νόμοι ορίζουν: α) τα σχετικά με τα στρατοδικεία, ναυτοδικεία και αεροδικεία, στην αρμοδιότητα των οποίων δεν μπορεί να υπαχθούν ιδιώτες". Ο Στρατιωτικός Ποινικός Κώδικας που κυρώθηκε με το Ν. 2287/1995 εναρμονίζεται απόλυτα με την προαναφερόμενη συνταγματική επιταγή , η οποία οριζει ότι οι ιδιώτες απαγορεύεται να υπαχθούν σε στρατιωτικά ποινικά δικαστήρια. Ειδικότερα με τις διατάξεις του Κώδικα αυτού ορίζονται μεταξύ των άλλων και τα εξής:

α) Με το άρθρο 5 παρ.1 εδάφιο α ότι "στρατός είναι ο ελληνικός στρατός της ξηράς, της θάλασσας και του αέρα και στρατιωτικές υπηρεσίες είναι οι υπηρεσίες που ανήκουν σ' αυτόν", με το εδάφιο β ότι "στρατιωτικοί είναι όσοι ανήκουν στον στρατό και το λιμενικό σώμα ...".

β) Με το άρθρο 167 παρ.1 ότι " η ποινική δικαιοσύνη στον στρατό απονέμεται από τα στρατιωτικά δικαστήρια και τον Άρειο Πάγο …"

γ)Με το άρθρο 193 παρ.1 (δικαιοδοσία των στρατιωτικών ποινικών δικαστηρίων) αναφέρεται ότι "στη δικαιοδοσία των στρατιωτικών ποινικών δικαστηρίων υπάγονται όσοι είναι στρατιωτικοί κατά τον χρόνο τέλεσης της πράξης, καθώς και οι αιχμάλωτοι πολέμου ...".

δ) Με το άρθρο 195 (συμμετοχή στρατιωτικών και ιδιωτών), ότι "αν στο έγκλημα συμμετέχουν στρατιωτικοί και ιδιώτες, αρμόδια είναι: α) τα κοινά ποινικά δικαστήρια, αν το έγκλημα είναι

[70] Απόφαση 984/2013, Άρειος Πάγος

του κοινού ποινικού δικαίου β) τα στρατοδικεία για τους στρατιωτικούς και τα κοινά ποινικά δικαστήρια για τους ιδιώτες, αν το έγκλημα είναι στρατιωτικό ...".
ε) Με το άρθρο 197 παρ.1 (αρμοδιότητα επί συναφών, κατ' εξακολούθηση και διαρκών εγκλημάτων), ότι "αν συρρέουν εγκλήματα που υπάγονται άλλα σε στρατιωτικά δικαστήρια και άλλα σε κοινά ποινικά δικαστήρια, δικάζονται από το δικαστήριο που έχει δικαιοδοσία για το βαρύτερο έγκλημα. Κατ' εξαίρεση η λιποταξία δικάζεται πάντοτε από τα στρατιωτικά δικαστήρια", με την παρ. δε 2 του ιδίου άρθρου ότι "αν από τις μερικότερες πράξεις ενός κατ' εξακολούθηση εγκλήματος, άλλες τελέσθηκαν σε χρόνο που ο δράστης ήταν στρατιωτικός και άλλες σε χρόνο που ήταν ιδιώτης, δικάζουν για όλες τα κοινά ποινικά δικαστήρια. Η διάταξη αυτή εφαρμόζεται και στα διαρκή εγκλήματα",
στ) Στη διάταξη του άρθρου 213 (εφαρμογή του Κώδικα Ποινικής Δικονομίας), ορίζεται ότι "οι διατάξεις του Κ.Π.Δ και οι λοιπές διατάξεις που εφαρμόζονται στις διαδικασίες ενώπιον των κοινών ποινικών δικαστηρίων και αρχών, εφαρμόζονται και στις διαδικασίες ενώπιον των στρατιωτικών δικαστηρίων και αρχών, εκτός αν ο Κώδικας αυτός ή άλλος ειδικός νόμος ορίζουν διαφορετικά".

Συνακόλουθα, κατόπιν των προεκτεθέντων διατάξεων και ιδίως των 195 και 197 παρ.2 του Σ.Π.Κ, εξάγεται σαφώς και ανενδοιάστως το συμπέρασμα ότι στις περιπτώσεις διαπιστώνεται συμμετοχή ιδιωτών και στρατιωτικών στο ίδιο έγκλημα, και μάλιστα πρόκειται για εγκλήματα που γίνονται κατ' εξακολούθηση και χαρακτηρίζονται ως διαρκή, αποκλείεται η υπαγωγή ιδιωτών στην αρμοδιότητα στρατιωτικών ποινικών δικαστηρίων. Το ίδιο ισχύει και για την διάταξη του άρθρου 197 παρ.1 του ιδίου Κώδικα που ρυθμίζει την αρμοδιότητα σε περίπτωση συρροής εγκλημάτων, ορισμένα εκ των οποίων υπάγονται στην αρμοδιότητα των κοινών ποινικών δικαστηρίων και ορισμένα στην αρμοδιότητα των στρατιωτικών δικαστηρίων. Μολονότι, ο υπέρτιτλος του τελευταίο αυτού άρθρου αναφέρεται σε αρμοδιότητα "επί συναφών εγκλημάτων", διαπιστώνουμε ότι στη διάταξη του άρθρου ρυθμίζονται τα ζητήματα αρμοδιότητας σε περίπτωση συρροής και όχι συνάφειας (Α.Π 1373/2000 ΠοινΧρον ΝΑ 521). Παρά το γεγονός ότι στην ως άνω διάταξη δε γίνεται αναφορά στην ιδιότητα του υπαιτίου της διάπραξης των εγκλημάτων που συρρέουν αληθώς, καθίσταται πρόδηλο ότι πρόκειται για στρατιωτικούς, δοθέντος ότι είναι μια διάταξη εντεταγμένη στον Σ.Π.Κ, και ερμηνεύεται συναρτήσει της βασικής διάταξης του άρθρου 193 παρ.1 του ιδίου Κώδικα. Στην αντίθετη περίπτωση που από τον υπέρτιτλο του σχετικού άρθρου προκύπτει η βούληση του νομοθέτη να ρυθμίσει με αυτήν ζητήματα αρμοδιότητας σε περίπτωση συνάφειας, είναι προφανές ότι η διάταξη αυτή αναφέρεται μόνο στην περίπτωση α του άρθρου 129 του Κ.Π.Δ, την περίπτωση δηλαδή εγκλημάτων που τελούνται είτε συγχρόνως είτε σε διαφορετικούς τόπους και χρόνους από το ίδιο πρόσωπο που έχει την ιδιότητα του στρατιωτικού και από την περίπτωση γ του ιδίου άρθρου, την περίπτωση εγκλημάτων που τελούνται (από το αυτό βεβαίως πρόσωπο που έχει την στρατιωτική ιδιότητα) με σκοπό να διευκολύνουν ή να κάνουν περισσότερο εύστοχη ή να αποκρύψουν ένα από αυτά (βλ. σχετ. Α.Π 794/2004).

Συνακόλουθα ο ισχύων Σ.Π.Κ αποκλείει την παραπομπή ιδιώτη σε στρατιωτικά ποινικά δικαστήρια, για οποιοδήποτε έγκλημα και για οποιοδήποτε λόγο. Ενόψει των ανωτέρω καθίσταται σαφές ότι ακόμη και η διάταξη του άρθρου 7 του Α.Ν. 376/1936, που παραπέμπει σε στρατιωτικά δικαστήρια ιδιώτη πρέπει να ερμηνευθεί υπό το πρίσμα του ισχύοντος Συντάγματος και του εναρμονισμένου με αυτό μεταγενέστερου Στρατιωτικού Ποινικού Κώδικα πού ήδη ισχύει. Σύμφωνα με την απόφαση 984/2013 του Αρείου Πάγου, μια τέτοια ερμηνεία οδηγεί στο συμπέρασμα ότι η διάταξη αυτή, στο μέτρο που προβλέπει την παραπομπή ιδιώτη σε στρατιωτικά ποινικά δικαστήρια, είναι **αντισυνταγματική** και συνεπώς μη εφαρμοστέα κατά το άρθρο 93 παρ. 4 του Συντάγματος.

Σημαντικό είναι να διευκρυνισθεί ότι την ιδιότητα του "στρατιωτικού των ελληνικών ενόπλων δυνάμεων", την αποκτά όποιος κατατάσσεται σ' αυτές προς εκπλήρωση στρατιωτικής υποχρέωσης κατά τις προβλέψεις του ειδικού περί στρατολογίας των Ελλήνων νόμου (Ν

3421/2005), είτε με την απόκτηση της ιδιότητας του μόνιμου στρατιωτικού (με την εισαγωγή και φοίτηση του σε παραγωγικές σχολές αξιωματικών και υπαξιωματικών ή με την απευθείας ονομασία του σε αξιωματικό (βλ. σχετικά άρθρο 4 του στρατιωτικού κανονισμού 20-1 που κυρώθηκε με το Π.Δ 130/1984), με δεδομένο ότι κάποιος δεν είναι στρατιωτικός υπό την ανωτέρω εκτεθείσα έννοια, είναι προφανές ότι αρμόδιο στην προκειμένη περίπτωση είναι το κοινό δικαστήριο(βλ Α.Π 530/1992 Ποιν.Χρον ΜΒ 571, με την οποία δεν αναιρέθηκε για υπέρβαση εξουσίας αλλά για άλλο λόγο, απόφαση κοινού ποινικού δικαστηρίου που είχε κρίνει υπόθεση παράβασης του Α.Ν. 376/1936 από ιδιώτη). Δεν υπάρχει, επομένως, περιθώριο να εμφιλοχωρήσει κάποια σύγκρουση δικαιοδοσίας σύμφωνα με τα προεκτεθέντα.

Από τα παραπάνω έπεται ότι η διάταξη του άρθρου 7 του διατηρηθέντος κατά τα προαναφερθέντα σε ισχύ Α.Ν. 376/1936 πρέπει να ερμηνευθεί υπό τις προαναφερθείσες ρυθμίσεις του ισχύοντος Συντάγματος και του ισχύοντος Στρατιωτικού Ποινικού Κώδικα και να θεωρηθεί ότι η εν λόγω διάταξη κατά το μέρος που προβλέπει ότι για τις παραβάσεις των άρθρων 4 και 5 του ως άνω αναγκαστικού νόμου αρμόδια είναι τα στρατιωτικά ποινικά δικαστήρια και στην περίπτωση που ο παραβάτης είναι ιδιώτης, ως αντίθετη προς τη διάταξη του άρθρου 96 παρ.4 του Συντάγματος, είναι μη εφαρμοστέα κατ' άρθρο 93 παρ.4 αυτού, που ορίζει ότι τα δικαστήρια υποχρεούνται να μην εφαρμόζουν νόμο που το περιεχόμενό του είναι αντίθετο προς το Σύνταγμα.

2.6. Προστασία ιδιωτικής ζωής- ένταλμα έρευνας ή κατάσχεσης

Η κατάσχεση ψηφιακών αποδεικτικών στοιχείων συνδέεται στενά με το ζήτημα της προστασίας της ιδιωτικής ζωής, μάλιστα, σύμφωνα με το άρθρο 12 της Διακήρυξης του ΟΗΕ για τα Ανθρώπινα Δικαιώματα, προστατεύεται το δικαίωμα της ιδιωτικής ζωής του καθενός (CRL, 2006). Ως εκ τούτου, οι άνθρωποι έχουν το δικαίωμα να είναι ασφαλείς στο σπίτι τους και στην εργασία τους. Σε μία δικαστική υπόθεση των Ηνωμένων Πολιτειών κατά της Triumph Capital, η κυβέρνηση ζήτησε και έλαβε ένταλμα έρευνας για να αναζητήσει και να κατάσχει ένα φορητό υπολογιστή να αποφευχθεί η παραβίαση της ιδιωτικής ζωής και της νόθευσης των αποδεικτικών στοιχείων. Η διαδικασία της κατάσχεσης, ωστόσο, συχνά πάσχει από νομιμότητα και αποτελεί ένα από τα πιο σημαντικά στάδια συλλογής των αποδεικτικών στοιχείων, ώστε αυτά αφενός να μην αλλοιωθούν και αφετέρου να συγκεντρωθούν νομότυπα ώστε να μην απορριφθούν για τυπικούς λόγους.71

Ο τρόπος που πραγματοποιείται η έρευνα και το νομότυπο της κατάσχεσης των ψηφιακών αποδεικτικών στοιχείων αποτελούν τα πιο συχνά αμφισβητούμενα σημεία στις δικαστικές υποθέσεις. Κατά τη διάρκεια αυτής της αρχικής διαδικασίας της εγκληματολογικής έρευνας, η χρήση μιας ακατάλληλης μεθοδολογίας ή παράνομης κατάσχεσης μπορεί να επηρεάσει αρνητικά το παραδεκτό των αποδεικτικών στοιχείων. Σε κάθε έρευνα, κρείσσονος σημασίας είναι να διασφαλίζεται η προστασία της ιδιωτικής ζωής του κατηγορούμενου, επομένως η νομική διαδικασία που επιβάλλεται να ακολουθηθεί για την αναζήτηση και την κατάσχεση στοιχείων, πρέπει να γίνεται κατόπιν εντάλματος, γεγονός που αντανακλά το νομικό πλαίσιο που καλύπτει τις ως άνω διαδικασίες.

Οι ερευνητές, επομένως, πρέπει όχι μόνο να εντοπίσουν αλλά και να αρθρώσουν τα πιθανά αίτια στα οποία θα στηριχθεί η έκδοση εντάλματος έρευνας ή κατάσχεσης. Επιπλέον, σημαντικό είναι να γνωρίζουν τα όρια μέσα στα οποία μπορεί να διεξαχθεί μια έρευνα ή κατάσχεση κατόπιν εντάλματος. Ένα ωραίο παράδειγμα αποτελεί η κατάσχεση της ηλεκτρονικής αλληλογραφίας των κατηγορουμένων από τους τεχνικούς του Yahoo, με την κατηγορία της

[71] James Tetteh Ami-Narh , Edith Cowan University, Patricia A.H. Williams Digital forensics and the legal system: A dilemma of our times, 2008, Edith Cowan University

παιδικής πορνογραφίας κατόπιν βεβαίως έκδοσης του σχετικού εντάλματος. Ωστόσο, υπήρξαν δύο αντικρουόμενες αποφάσεις, ήτοι, το μεν πρωτοβάθμιο δικαστήριο έκρινε ότι η ανάκτηση των e-mails από τους τεχνικούς του Yahoo χωρίς την παρουσία της αστυνομίας ήταν παράνομη. Από την άλλη, το δευτεροβάθμιο δικαστήριο, έκρινε ότι η αναζήτηση των e-mails του κατηγορουμένου χωρίς την παρουσία αστυνομικού ήταν νομότυπη κατά την τέταρτη τροποποίηση της αμερικανικής νομοθεσίας και ως εκ τούτου τα δικαιώματα της ιδιωτικής ζωής του κατηγορούμενου δεν παραβιάστηκαν.

Για να διασαφηνιστούν τα όρια του εντάλματος, θα μπορούσαμε να αναφέρουμε δύο χαρακτηριστικά παραδείγματα. Στην υπόθεση Wisconsin εναντίον Schroeder, χρειάστηκε η έκδοση δεύτερου εντάλματος κατά τη διάρκεια διεξαγωγής της έρευνας. Συγκεκριμένα, αρχικά εκδόθηκε ένταλμα έρευνας για την απόδειξη online παρενοχλήσεων που δόθηκε στις αρμόδιες αρχές προκειμένου να αναζητήσουν αποδεικτικά στοιχεία και να κατάσχουν τον υπολογιστή του κατηγορουμένου. Ωστόσο, όσο διαρκούσε η έρευνα ανακαλύφθηκαν πορνογραφικές εικόνες παιδιών, με αποτέλεσμα να χρειαστεί η έκδοση καινούριου εντάλματος προκειμένου να συνεχιστεί η έρευνα σχετικά με το έγκλημα της παιδικής πορνογραφίας. Στο δεύτερο παράδειγμα, ο κατηγορούμενος κατόρθωσε ακυρώσει τη συλλογή των αποδεικτικών στοιχείων, καθότι το ένταλμα που εκδόθηκε αφορούσε στον έλεγχο λειτουργίας ενός cable box και η αστυνομία υπερέβη τις εξουσίες της επιθεωρώντας αρχεία που αφορούσαν σε παράνομες δραστηριότητες, αλλά δεν αναφέρονταν στο ένταλμα. Για να συνεχιστεί νομότυπα, λοιπόν, η ως άνω διαδικασία έπρεπε να εκδοθεί ένα καινούριο ένταλμα.

2.6.1. Η επιτήρηση των ηλεκτρονικών επικοινωνιών στο χώρο εργασίας-αρχή της ιδιωτικότητας

Ο ελληνικός νόμος για την προστασία των προσωπικών δεδομένων είναι ο Ν. 2472/1997 προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα" , ο οποίος υιοθετήθηκε προκειμένου να εφαρμοστεί στη χώρα μας η κοινοτική οδηγία 95/46/ΕΚ που αφορά στα προσωπικά δεδομένα, ορίζει σε τι συνίσταται η επεξεργασία, παρέχει ασφαλιστικές δικλείδες και κυρώσεις σε περίπτωση παραβίασής τους.72 Επομένως, στο ως άνω νομοθετικό πλαίσιο θα βασιστούμε για να καθορίσουμε το περιθώριο επεξεργασίας των προσωπικών δεδομένων ακόμη και στο χώρο εργασίας που μας απασχολεί στην προκειμένη περίπτωση. Ένα κρίσιμο ζήτημα, όμως, θέτει η αρχή της ιδιωτικότητας, δοθέντος ότι από τη μία πρέπει να οριοθετηθεί η επεξεργασία και συλλογή των προσωπικών δεδομένων προκειμένου να μην τίθεται ζήτημα παραβίασης της ιδιωτικότητας των εργαζομένων από την άλλη όμως να μην περιορίζεται σε σημείο που να αποκλείεται η άσκηση του διευθυντικού δικαιώματος.

Σε μια προσπάθεια να εξισορροπηθούν οι δύο αντικρουόμενες πλευρές και να προασπιστούν ισότιμα, στηριζόμαστε τόσο στο νόμο 2472/97 όσο και στην Οδηγία 115/2001 της Ελληνικής Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ). Σε αυτό το σημείο, σημαντικό είναι να προσδιοριστούν οι δύο πόλοι που τίθενται σε κίνδυνο από την πλευρά του εργαζομένου, ήτοι στα πλαίσια της εργασιακής σχέσης σημαντικό είναι να διαφυλάσσεται σφαιρικά η προσωπικότητά του, τόσο δηλαδή η έκφραση των ατομικών ελευθεριών του εργαζομένου μέσα στην επιχείρηση υπό την έννοια της εξωεπαγγελματικής σφαίρας όσο και η ίδια προσωπικότητα του εργαζομένου.

Ένα σημαντικό άρθρο του ως άνω νόμου, είναι το 7Α παρ.1 το οποίο ορίζει τα πλαίσια απαλλαγής υποχρέωσης σε γνωστοποίηση και λήψη άδειας και συγκεκριμένα αναφέρει : "α) Όταν η επεξεργασία πραγματοποιείται αποκλειστικά για σκοπούς που συνδέονται άμεσα με σχέση εργασίας ή έργου ή με παροχή υπηρεσιών στο δημόσιο τομέα και είναι αναγκαία για την

[72]Ιγγλεζάκης Ι., Ευαίσθητα προσωπικά δεδομένα , έκδοση. Σάκκουλα, Αθήνα Θεσσαλονίκη, 2003, σελ. 11

εκπλήρωση υποχρέωσης που επιβάλλει ο νόμος ή για την εκτέλεση των υποχρεώσεων από τις παραπάνω σχέσεις και το υποκείμενο έχει προηγουμένως ενημερωθεί.” Ένα κρίσιμο σημείο είναι όταν έχει υποβληθεί αίτηση από τους υποψήφιους αλλά δεν έχει πραγματοποιηθεί η πρόσληψη, σε αυτή την περίπτωση, οι εργοδότες χρειάζονται τη συγκατάθεση των υποψηφίων για την επεξεργασία των προσωπικών τους δεδομένων και καλούνται να γνωστοποιήσουν την ως άνω επεξεργασία.

Η χρήση της τεχνολογικής υποδομής στο χώρο εργασίας είναι τόσο υπηρεσιακή όσο και προσωπική.73 Αυτό σημαίνει ότι οι εργαζόμενοι κάνουν χρήση του διαδικτύου τόσο στα πλαίσια των καθηκόντων τους όσο και για προσωπικούς λόγους. Σημαντικό είναι να καθοριστεί η έννοια της υπηρεσιακής χρήσης. Συγκεκριμένα, όταν γίνεται χρήση του διαδικτύου σχετική με τα καθήκοντα του εργαζομένου, όπως αυτά ορίζονται από σαφώς στη σύμβαση εργασίας, τότε αναμφισβήτητα η χρήση είναι υπηρεσιακή, ωστόσο, υπάρχουν κάποιες περιπτώσεις που πρέπει να προσεχθούν. Η χρήση δύναται να θεωρηθεί υπηρεσιακή ακόμη και αν πρόκειται για ιδιωτική επικοινωνία στην περίπτωση που ο εργαζόμενος θα προβεί σε κάποια ενέργεια ιδιωτικού περιεχομένου, ορμώμενη από κάποιο γεγονός στο εργασιακό περιβάλλον. Σε αυτή την περίπτωση, όπως χαρακτηριστικά αναφέρεται στην “Επιτήρηση και παρακολούθηση των τηλεπικοινωνιών στο χώρο εργασίας” ΔιΜΕΕ 2005, του Ι.Ιγγλεζάκη “είναι δυνατό να θεωρηθεί υπηρεσιακή και επικοινωνία ιδιωτικής φύσης, όταν αυτή θα γίνει με αφορμή κάποιο υπηρεσιακό γεγονός, όπως για παράδειγμα όταν ο εργαζόμενος αναγκάζεται να ενημερώσει κάποιους δικούς του ανθρώπους για την αναβολή προγραμματισμένων σχεδίων επειδή θα πρέπει να παραμείνει στην εργασία του”.

Στις περιπτώσεις που ο εργαζόμενος χρησιμοποιεί για προσωπικούς λόγους την τεχνολογική υποδομή του εργασιακού του περιβάλλοντος και το διαδίκτυο, οφείλει να έχει προηγουμένως λάβει ρητή ή και σιωπηρή συγκατάθεση του εργοδότη του. Ως ρητή θεωρείται η συγκατάθεση που περιλαμβάνεται στην έγγραφη σύμβαση εργασίας ή όταν ο εργοδότης παρέχει δύο ηλεκτρονικές διευθύνσεις, μία για τις προσωπικές του επικοινωνίες και μία για την εκπόνηση των εργασιακών του καθηκόντων. Από την άλλη πλευρά, σε κάποιες εταιρίες διατίθενται υπολογιστές, στους χώρους που πραγματοποιούνται τα διαλείμματα των εργαζομένων, τότε πρόκειται για μία σιωπηρή συγκατάθεση, που παρέχει τη δυνατότητα στους εργαζομένους να επικοινωνούν για προσωπικούς τους λόγους από συγκεκριμένους υπολογιστές κατά τη διάρκεια του διαλείμματος.

Ένα σημαντικό ζήτημα που γεννάται όταν ο εργαζόμενος κάνει προσωπική χρήση στον επαγγελματικό υπολογιστή του, είναι η μεγάλη πιθανότητα πρόκλησης βλάβης στους ηλεκτρονικούς υπολογιστές, με τους γνωστούς ιούς. Συχνά, λοιπόν, σε πολλές εταιρίες και υπηρεσίες, η χρήση του διαδικτύου και του ηλεκτρονικού ταχυδρομείου παρακολουθείται προκειμένου να αποφευχθούν οι όποιοι κίνδυνοι, δημιουργώντας όμως σοβαρούς κλυδωνισμούς στην αρχή της ιδιωτικότητας.

2.7. Πιστοποίηση ISO

Σημαντικό είναι να αναφερθεί ότι τα εργαστήρια, χρειάζεται να πιστοποιούνται σύμφωνα με διεθνή πρότυπα προκειμένου να καθορίζονται κάποιες κατευθυντήριες γραμμές λειτουργίας τους που λειτουργούν ως δικλείδες ασφαλείας για τη σωστή διεξαγωγή των ερευνών. Συγκεκριμένα, προτείνεται το ISO1779974 και COBIT.75 Τα πρότυπα αυτά δεν καλύπτουν μια

[73] Ι . Ιγγλεζάκης σελ. Επιτήρηση και παρακολούθηση των τηλεπικοινωνιών στο χώρο εργασίας, ΔιΜΕΕ 2005, 57

[74] Information Technology – Security techniques – Codes of Practice for information security management. International Organisation for Standardization and the International Electrotechnical Commission. ISO/IEC 17799. 2005.

εγκληματολογική έρευνα, αλλά θα μπορούσαν να συνδράμουν στην αποδεκτή διεξαγωγή τους. Αξιοσημείωτο είναι ότι χρειάζεται να υιοθετηθούν εσωτερικά πρότυπα και πολιτικές σύμφωνες με τις εσωτερικές διαδικασίες του στρατού. Ένα παράδειγμα είναι στη Νότια Αφρική, όπου υπάρχουν μια σειρά από σημαντικές νομοθετικές ρυθμίσεις, οι οποίες επιτρέπουν την υιοθέτηση εσωτερικών προτύπων και πολιτικών, και αφορούν τις ηλεκτρονικές επικοινωνίες και συναλλαγές και την προώθηση της πρόσβασης σε πληροφοριακά δεδομένα. Παρ' όλ'αυτά δεν παρέχουν σαφείς οδηγίες για τον τρόπο που θα πρέπει να διεξαχθεί η έρευνα.

Συνακόλουθα, ένας σημαντικός τρόπος για τους περισσότερους οργανισμούς και ειδικότερα για το στρατό να προστατεύσει τον εαυτό του ενάντια στις κυβερνοεπιθέσεις είναι να καθιερώσει εσωτερικές πολιτικές και διαδικασίες που προσδιορίζουν ακριβώς το τι συνιστά επιβλαβή δράση και το πλαίσιο στο οποίο δύναται να κινηθεί.76

Μέχρι στιγμής έχει διαπιστωθεί ότι η εφαρμογή ορισμένων προτύπων, όπως του προαναφερθέντος ISO17799, μπορεί να είναι ένα χρήσιμο πρώτο βήμα από έναν οργανισμό για την αποτελεσματική προστασία των πληροφοριών και τη νομότυπη διεξαγωγή της έρευνας, δοθέντος ότι ακολουθείται μια θεωρητικά πιο τυποποιημένη και ελεγχόμενη διαδικασία.77 Πολλώ δε μάλλον, οι συγκεκριμένες πολιτικές και διαδικασίες που τυγχάνουν εφαρμογής μέσα σε κάποιο οργανισμό, στοχεύουν στην προστασία της εσωτερικής ακεραιότητας των πληροφοριών και των στοιχείων του οργανισμού. Ο απότοκος της πιστοποίησης, τελικά είναι η συγκέντρωση αποδείξεων που συλλέχτηκαν νομότυπα, διατηρήθηκαν ακέραιες και δύνανται να χρησιμοποιηθούν σε κάποιο δικαστήριο εάν χρειασθεί.

Το λεξικό της Οξφόρδης ορίζει ως πλαίσιο ένα σύνολο κανόνων που «υποστηρίζει μια δομή». Ένα τέτοιο πλαίσιο μπορεί να οριστεί ως μια δομή που στόχο έχει να υποστηρίξει μια επιτυχημένη εγκληματολογική έρευνα. Ένα πλαίσιο εξαρτάται από μια σειρά από δομές, στην περίπτωση της ψηφιακής εγκληματολογίας ή γενικότερα της εγκληματολογίας, η νομοθεσία πρέπει να θεωρείται ότι είναι εξέχουσας σημασίας. Μια εγκληματολογική έρευνα χρειάζεται να διεξαχθεί με επιστημονικό τρόπο και παράλληλα να συμμορφώνεται με όλες τις νομικές απαιτήσεις. Τα στοιχεία θα πρέπει να συλλέγονται σε κάθε περίπτωση σύννομα, ανεξαρτήτως του σκοπού δηλαδή αν πρόκειται για εσωτερική έρευνα, πειθαρχική ακρόαση ή δίκη.

Επιπλέον, η Διεύθυνση Εγκληματολογικών Ερευνών της Ελληνικής Αστυνομίας , η οποία συνιστά την Εθνική Εγκληματολογική Υπηρεσία της χώρας και μάλιστα έχει ενταχθεί στο Δίκτυο Εγκληματολογικών Ινστιτούτων (ENFSI) και παρέχει σημαντική υποστήριξη και βοήθεια στο έργο όλων των διωκτικών Αρχών της χώρας, έχει πιστοποιηθεί σύμφωνα με το διεθνές πρότυπο ISO 9001:2008, ISO 17025:2005 και ISO 17020:2004.78

Κεφάλαιο 3ο: Μεθοδολογίες forensics

3.1 Απαιτήσεις στα εργαλεία ψηφιακής δικανικής

---

[75]Information Security, Audit and Control Association (ISACA). July 2000. COBIT 3rd Edition Control Objectives. http://isaca.org.

[76]Framework for a Digital Forensic Investigation Michael Kohn1, JHP Eloff2 and MS Olivier3
1mkohn@cs.up.ac.za, 2eloff@cs.up.ac.za, 3molivier@cs.up.ac.za

[77]Framework for a Digital Forensic Investigation Michael Kohn1, JHP Eloff2 and MS Olivier3
1mkohn@cs.up.ac.za, 2eloff@cs.up.ac.za, 3molivier@cs.up.ac.za

[78]http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=48&Itemid=39&lang

Στην αμερικάνικη έννομη τάξη, προκειμένου να γίνουν αποδεκτά στο δικαστήριο ψηφιακά αποδεικτικά στοιχεία, ελέγχεται η αξιοπιστία τους από τις Daubert κατευθυντήριες γραμμές, οι οποίες υποστηρίζουν ότι τα ανοιχτού κώδικα εργαλεία δύνανται να παρέχουν με μεγαλύτερη σαφήνεια στοιχεία και σε γενικές γραμμές είναι ισάξια με τα εργαλεία κλειστού κώδικα.79

Η συζήτηση σχετικά με το λογισμικό ανοιχτού και κλειστού κώδικα έχει θέσει πολλά ζητήματα στην ασφάλεια ψηφιακών συστημάτων και στην αξιοπιστία των ψηφιακών αποδεικτικών στοιχείων που μας αφορά εν προκειμένω. Τα εργαλεία ψηφιακής εγκληματολογίας αποτελούν ένα από τα πιο σημαντικά σημεία της έρευνας, δοθέντος ότι παρέχουν τα στοιχεία που θα χρησιμοποιηθούν στην ακροαματική διαδικασία, επομένως, πέραν της νομότυπης διαδικασίας που θα ακολουθηθεί στην έρευνα, κρείσσονος σημασίας είναι να εξετασθούν οι διαφορές μεταξύ εργαλείων ανοιχτού και κλειστού κώδικα και σε τι βαθμό τα αποτέλεσματά τους θεωρούνται αξιόπιστα. Για πολλά χρόνια, η ψηφιακή εγκληματολογία αποτελούσε κατά κύριο λόγο αντικείμενο των κρατικών φορέων, ωστόσο τώρα πια δημιουργούνται ιδιωτικά εργαστήρια ψηφιακής εγκληματολογίας, ενώ επίσης, ο κάθε κρατικός φορέας, εφόσον, η φύση της λειτουργίας του το επιτάσσει δύναται να ιδρύσει δικό του εργαστήριο, όπως για παράδειγμα αποτελεί ο στρατός ή κάποιο εκπαιδευτικό ίδρυμα. Συνακόλουθα, η παροχή πολλών επιλογών στα εργαλεία ψηφιακής δικανικής και κυρίως αυτών του ανοιχτού κώδικα, ίσως θεωρούνται καλή και αξιόπιστη επιλογή, συγκρίσιμη με τα αντίστοιχα κλειστού κώδικα.

3.2 Παραδεκτό ψηφιακών αποδεικτικών στοιχείων

Οι προτεινόμενες ψηφιακές αποδείξεις για την εισαγωγή στο δικαστήριο πρέπει να πληρούν αυστηρά τις δύο κάτωθι προϋποθέσεις :

1]αρχικά πρέπει να είναι σχετικές με το υπό κρίση ζήτημα, ήτοι να τελούν σε αιτιώδη συνάφεια με το υπό εξέταση αδίκημα

2]είναι πολύ σημαντικό να προέρχονται από νομικά αναγνωρισμένη επιστημονική μέθοδο, η οποία να υποδεικνύεται και να υποστηρίζεται από κατάλληλη επικύρωση, ένταλμα ή εξουσιοδότηση.

Πιο αναλυτικά, τα πειστήρια που συλλέγονται με στόχο να αποτελέσουν αποδείξεις σε μια επ'ακροατηρίω διαδικασία, χρειάζεται να πληρούν κάποιες βασικές προϋποθέσεις. Αρχικά, απαιτείται η αυθεντικότητα του υλικού που εξετάζεται, είναι κρείσσονος σημασίας, λοιπόν, το εξεταζόμενο στοιχείο να προέρχεται από την πηγή που εξετάστηκε χωρίς να χωρά καμία αμφιβολία για το αντίθετο. Αξιοσημείωτο είναι δε ότι το Συμβούλιο της Ευρώπης στην επεξηγηματική έκθεση για το έγκλημα στον κυβερνοχώρο, χαρακτηριστικά αναφέρει ότι πρέπει τα στοιχεία να είναι «αδιάσειστα αυθεντικά», δηλαδή να είναι δυνατό να συνδεθούν τα αποδεικτικά στοιχεία με το υπό κρίση συμβάν.80 Επίσης, η αξιόπιστη συλλογή των δεδομένων αποτελεί μία σημαντική παράμετρο, η οποία ορίζει ότι πρέπει να χρησιμοποιούνται τρόποι νομικά αποδεκτοί. Η τρίτη προϋπόθεση αφορά στην πληρότητα των στοιχείων, η οποία εισάγει την έννοια του βαθμού ευρωστίας που απορρέει από τον έλεγχο ενός υλικού φορέα. Τέλος, η ακεραιότητα των δεδομένων, αποτελεί ίσως και το πιο ευαίσθητο σκέλος στη συλλογή των πειστηρίων, καθότι δε γίνονται δεκτά από τις δικαστικές αρχές στοιχεία τα οποία είναι πιθανό να έχουν τροποποιηθεί ουσιωδώς. Η αυθεντικότητα συνδέεται με την απαίτηση της ακεραιότητας. Ίσως το πιο σημαντικό στοιχείο στην ψηφιακή εγκληματολογία είναι να διατηρηθεί η ακεραιότητα των ψηφιακών αποδεικτικών στοιχείων, ήτοι τα δεδομένα που

[79]Open Source Digital Forensics Tools: The Legal Argument, By Brian Carrier, October 2002

[80] http://www.coe.int

συλλέχθηκαν πρέπει να είναι ίδια με εκείνα που αρχικά ανακαλύφθηκαν. Οι αποδείξεις, επομένως, πρέπει να εξεταστούν και να αξιολογηθούν, αλλά στις περισσότερες επιθέσεις κατά των πληροφοριακών συστημάτων δεν υπάρχουν φυσικές αποδείξεις, επομένως, οι ηλεκτρονικές συσκευές και τα δεδομένα χρειάζεται να παραμείνουν αμετάβλητα σε σχέση είτε με το hardware είτε με το software.81

Οι ψηφιακές ενδείξεις πρέπει, επίσης, να έχουν όλα τα χαρακτηριστικά των συμβατικών στοιχείων, κάθε εργαλείο, μέθοδος ή διαδικασία που χρησιμοποιείται κατά τη διάρκεια της έρευνας χρειάζεται να πληρούν αυστηρές προδιαγραφές. Οι ερευνητές, επομένως, οφείλουν να διασφαλίσουν ότι η κατοχή και η πρόσβαση σε ηλεκτρονικές αποδείξεις είναι σύννομες, και σε κάθε περίπτωση οι διαδικασίες που εφαρμόζονται είναι συμβατές με την εκάστοτε νομοθεσία. Άλλωστε, η νομιμότητα αποτελεί μία από τις πέντε κύριες αρχές που υιοθετήθηκαν ως μέρος του προγράμματος της ΕΕ και του Συμβουλίου της Ευρώπης για την ανάπτυξη ενός οδηγού για την κατάσχεση των ηλεκτρονικών αποδείξεων. Συνακόλουθα χρειάζεται να αποδεικνύεται η συμμόρφωση με το ισχύον νομικό πλαίσιο, καθότι τόσο τα ψηφιακά όσο και τα φυσικά στοιχεία που έχουν συλλεχθεί είναι πιθανό να απορριφθούν ως απαράδεκτα στο δικαστήριο.82

Κατά τη διεξαγωγή μιας έρευνας σε ηλεκτρονικά δεδομένα, είναι σημαντικό να μην παραβιάζεται η ιδιωτικότητα του ατόμου κατά την εύρεση κάποιου ψηφιακού πειστηρίου. Κατόπιν τούτου, απαιτείται η χορήγηση εντάλματος που θα καθορίζει με ακρίβεια τα αντικείμενα που μπορούν να ερευνηθούν, μάλιστα ακόμη και στην περίπτωση που ο ερευνητής θεωρήσει ότι μπορεί να αντλήσει στοιχεία και από άλλα αντικείμενα εκτός των καθορισμένων, τα στοιχεία αυτά δεν θα έχουν αποδεικτική αξία στη δικαστική αίθουσα και θα απορριφθούν.

Κάνοντας μια επισκόπηση στην αμερικάνικη έννομη τάξη, διαπιστώνουμε ότι για να είναι παραδεκτά στο δικαστήριο τα ψηφιακά αποδεικτικά στοιχεία πρέπει να είναι σχετικά επί του υπό κρίση ζητήματος και αξιόπιστα. Το αξιοσημείωτο είναι ότι η προϋπόθεση της αξιοπιστίας εξετάζεται σε μια άγνωστη για την ελληνική έννομη τάξη διαδικασία, το προδικαστικό "Daubert ακροατήριο". Ο δικαστής στην προδικαστική αυτή διαδικασία επιφορτίζεται με τον έλεγχο της μεθοδολογίας που αποφασίστηκε να ακολουθεί, ήτοι τα βήματα στη διεξαγωγή της έρευνας, καθώς επίσης και να διατυπώσει γνώμη επί της τεχνικής. Τόσο η μεθοδολογία όσο και η τεχνική πρέπει να δίνουν ακέραια και τελικά αξιόπιστα στοιχεία. Η διαδικασία Daubert καθορίζει τέσσερις κατευθυντήριες γραμμές που ακολουθούνται στην αξιολογική διαδικασία.

1. Δοκιμή: η διαδικασία πρέπει να έχει προηγουμένως δοκιμαστεί
2. Ποσοστό λάθους : Αφού έχει δοκιμαστεί θα δοθεί και το ποσοστό σφαλμάτων στα εξαγόμενα αποτελέσματα.
3. Δημοσίευση: Είναι σημαντικό να έχει δημοσιευθεί τόσο η μεθοδολογία όσο και η τεχνική (εργαλείο) και να έχει υποβληθεί σε μελέτες και πιθανόν σε διορθώσεις από την επιστημονική κοινότητα.
4. Αποδοχή: Η μεθοδολογία και το εργαλείο ψηφιακής εγκληματολογίας πρέπει σε κάθε περίπτωση να είναι αποδεκτά από την επιστημονική κοινότητα.

Αρχικά τα αμερικάνικα δικαστήρια αποδέχονταν μία τεχνική ως αξιόπιστη, εφόσον ήταν δημοσιευμένη σε κάποιο επιστημονικό περιοδικό. Επομένως, οι δοκιμές Daubert, κατάφεραν να διευρύνουν το πλαίσιο των αποδεκτών τεχνικών, ορίζοντας κάποιες κατευθυντήριες.

Η κατευθυντήρια γραμμή ορίζει ότι οι δοκιμές θα υποδείξουν εάν η εκάστοτε διαδικασία δύναται να παρέχει ακριβή αποτελέσματα. Οι δοκιμές επιμερίζονται σε δύο κατηγορίες, στις «ψευδώς αρνητικές» (false negative) και «ψευδώς θετικές» (false positive). Συγκεκριμένα, τα ψευδώς αρνητικά (false negative) τεστ διασφαλίζουν ότι το χρησιμοποιούμενο εργαλείο παρέχει

[81] ENISA, Digital Forensics – Handbook, 4 (2013).

[82] Cameron S.D. Brown, Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice, 9(1) Intl. J. Cyber Criminology 87 (January–June 2015)

όλα τα δεδομένα εισάγονται. Με τις ψευδώς θετικές (false positive) δοκιμές ελέγχεται ότι δεν εισάγονται νέα δεδομένα στο αποτέλεσμα. Η δεύτερη κατηγορία είναι δύσκολο να ελεγχθεί και συνήθως γίνεται με τη χρήση δεύτερου εργαλείου.

Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) έχει μια ειδική ομάδα εργασίας για τα εργαλεία ψηφιακής εγκληματολογίας (CFTT). Οι δοκιμές εφαρμόστηκαν σε πολλά εργαλεία και εξέτασαν τα αποτελέσματα σύμφωνα με τα δεδομένα που εισήχθησαν, χωρίς ωστόσο, να έχει αναπτυχθεί τελικά μια μεθοδολογία δοκιμών για τα εργαλεία ανάλυσης.83 Πριν από τα αποτελέσματα NIST CFTT, είχε δημοσιευθεί στο SC Magazine μία σύγκριση μεταξύ των εργαλείων ψηφιακής εγκληματολογίας κλειστού κώδικα, η οποία επιχείρησε να τοποθετήσει δεδομένα σε διάφορα σημεία του δίσκου και προσπάθησε να ελέγξει την αξιοπιστία των εργαλείων με το ποσοστό των δεδομένων που ανέκτησαν. Ως αποτέλεσμα, ήταν να βρεθούν αρκετά τρωτά σημεία σε κάθε ένα από τα εργαλεία, γεγονός που οδήγησε στο συμπέρασμα ότι τα εργαλεία ανοιχτού κώδικα δύνανται να προσφέρουν επαρκή βοήθεια στις νομικές διαδικασίες δοθέντος όντως ελέγχονται ευρέως από την επιστημονική κοινότητα.84

Χρήσιμο θα ήταν να δημιουργηθεί μία σουίτα δοκιμών που θα έχει τη δυνατότητα να επικυρώνει την αξιοπιστία των εργαλείων ανάλυσης. Το εργαλείο ανάλυσης καλείται να χειριστεί κάθε πιθανή κατάσταση και μάλιστα ένα σύνηθες επιχείρημα κατά των εφαρμογών ανοιχτού κώδικα είναι ότι οι κακόβουλοι χρήστες θα είναι σε θέση να εντοπίσουν τα τρωτά τους σημεία και να καλύψουν τα ίχνη τους εκμεταλλευόμενοι τις ευπάθειες αυτές. Ωστόσο, ένα μεγάλο μέρος της επιστημονικής κοινότητας, υποστηρίζει ότι σε κάθε περίπτωση, ακόμη και στα εργαλεία κλειστού κώδικα, οι δράστες θα στοχεύουν να εντοπίσουν και να εκμεταλλευτούν τις ευπάθειες, με τη μόνη διαφορά ότι στις εφαρμογές ανοιχτού κώδικα αυτές θα είναι ευρέως γνωστές και θα γίνονται προσπάθειες αντιμετώπισης και βελτίωσής τους από τους προγραμματιστές. Έχοντας πρόσβαση στον πηγαίο κώδικα ενός εργαλείου βελτιώνεται τελικά η ποιότητα της διαδικασίας ελέγχου, διότι τα σφάλματα μπορούν να εντοπιστούν μέσω μιας αναθεώρησης του κώδικα. Σημαντικό είναι οι ερευνητές-προγραμματιστές να διεξάγουν ελέγχους στα εργαλεία και να δημοσιεύουν τα αποτελέσματα, από την άλλη στα εργαλεία κλειστού κώδικα θα ήταν ωφέλιμο να δημοσιεύονται οι προδιαγραφές σχεδιασμού, ώστε να δοκιμάζονται και να ελέγχονται οι διαδικασίες του εργαλείου.

Η κατευθυντήρια γραμμή που αφορά στα ποσοστά σφαλμάτων προσδιορίζει το αντίστοιχο ποσοστό του κάθε εργαλείου, στα εργαλεία ψηφιακής εγκληματολογίας συνήθως τα δεδομένα επεξεργάζονται μέσα από μια σειρά κανόνων. Επίσης, εξίσου σημαντική θεωρείται η δημοσίευση των εργαλείων, παλαιότερα μάλιστα αποτελούσε και τη βασική προϋπόθεση για την αποδοχή αποδεικτικών στοιχείων. Μάλιστα το FBI ήδη το 1999 είχε δημοσιεύσει κείμενό του σχετικά με την εγκληματολογία και συγκεκριμένα με την ψηφιακή φωτογραφία, όπου τοποθετούσε μια εξαιρετικά σημαντική νομική υποσημείωση στην ενότητα οδηγίες λογισμικού "Οι κατασκευαστές του λογισμικού που χρησιμοποιείται για την επεξεργασία εικόνας οφείλουν να καθιστούν γνωστό τον πηγαίο κώδικα στους διαδίκους. Η αποτυχία από την πλευρά του κατασκευαστή να παρέχει αυτές τις πληροφορίες στους διαδίκους θα μπορούσε να οδηγήσει στον αποκλεισμό της απεικόνισης ως αποδεικτικό στοιχείο στις δικαστικές διαδικασίες. Αυτό πρέπει να λαμβάνεται υπόψη κατά την επιλογή του λογισμικού".85

Στους ομοσπονδιακούς κανόνες περί αποδείξεως, ο κανόνας 901 ορίζει ότι μια διαδικασία δύναται να επικυρωθεί με «ενδείξεις που περιγράφουν μια διαδικασία ή κάποιο σύστημα που χρησιμοποιείται για την παραγωγή ενός αποτελέσματος και αποδεικνύει ότι η διαδικασία ή το

[83]NIST. Computer Forensics Tool Testing. Available at http://www.cftt.nist.gov/

[84] James Holley. Computer Forensics Market Survey. SC Magazine September 2000. Available at: http://www.scmagazine.com/scmagazine/2000_09/survey/survey.html

[85]Guidance Software. EnCase Legal Journal, Second Edition. March 2002. Available at: http://www.encase.com/support/downloads/LegalJournal.pdf

σύστημα παράγει ακριβή αποτελέσματα». Ο ως άνω κανόνας ευθυγραμμίζεται πλήρως με τις κατευθυντήριες γραμμές για τη δημοσίευση και το ποσοστό λάθους των δοκιμών Daubert. Αξιοσημείωτο είναι δε, ότι ο κανόνας εξετάζει την κατευθυντήρια γραμμή των δοκιμών, διότι είναι αναγκαίο να αναπτυχθεί μια μεθοδολογία δοκιμών προτού υπολογιστεί το ποσοστό σφάλματος. Επιπλέον, οι βασικές έννοιες των κατευθυντήριων γραμμών Daubert εφαρμόζονται στα ψηφιακά αποδεικτικά στοιχεία, ανεξάρτητα αν θεωρούνται μη-επιστημονικές τεχνικές μαρτυρίες ή επιστημονικά στοιχεία.

Χρησιμοποιώντας τις οδηγίες των δοκιμών Daubert, αποδείχθηκε ότι τα εργαλεία ανοικτού κώδικα ευθυγραμμίζονται σε μεγαλύτερο ποσοστό με τις επιταγές του νόμου. Επιπλέον, προτείνει την υιοθέτηση των ακόλουθων μέτρων προκειμένου να γίνουν αποδεκτά από το νόμο αυτά τα εργαλεία.

1. Ανάπτυξη ολοκληρωμένων δοκιμών για τα εργαλεία ανάλυσης.
2. Δημοσίευση σχεδιασμού εργαλείου για να βοηθήσει στη δημιουργία πιο αποτελεσματικών εξετάσεων.
3. Δημιουργία ενός προτύπου για τον υπολογισμό των ποσοστών σφάλματος των εργαλείων.
4. Δημοσίευση συγκεκριμένων διαδικασιών που χρησιμοποιεί ένα εργαλείο. Ενώ τα εργαλεία ανοικτού κώδικα έχουν ήδη δημοσιεύσει τον πηγαίο κώδικά τους, θα ήταν πολύ χρήσιμο να περιγράφεται ρητά η διαδικασία που ακολουθούν.
5. Δημόσια συζήτηση σχετικά με τις διαδικαστικές λεπτομέρειες προκειμένου να εξασφαλιστεί σύμπνοια και ταύτιση ανάμεσα σε νομικού και τεχνικούς.86

Υποστηρίζεται, επομένως, ότι στόχος ενός εργαλείου ψηφιακής εγκληματολογίας είναι η ωρίμανση της επιστήμης, η οποία δύναται να προωθηθεί από τα open source εργαλεία, με τη δημοσίευση των διαδικασιών που ακολουθούν και κατ'επέκταση τον επανέλεγχο και τη διεπιστημονική συζήτηση.

Η έρευνα ψηφιακών πειστηρίων πρέπει να πραγματοποιείται βάσει των κάτωθι αρχών:

1. Καμία ενέργεια δε δύναται να μεταβάλει δεδομένα που τηρούνται σε υπολογιστή ή μέσο αποθήκευσης, τα οποία μπορεί να προσκομισθούν στο δικαστήριο.
2. Χρήση αρχέτυπων δεδομένων από τρίτο άτομο, κατόπιν εξουσιοδότησης.
3. Δημιουργία ιστορικού ελέγχου των διαδικασιών.
4. Το άτομο που έχει οριστεί ως υπεύθυνος της έρευνας, επιφορτίζεται με τη γενική ευθύνη για τη διασφάλιση τήρησης της επικείμενης νομοθεσίας και των εν λόγω αρχών.

[86]Open Source Digital Forensics Tools: The Legal Argument, By Brian Carrier, October 2002

Η διαδικασία χειρισμού των ηλεκτρονικών αποδεικτικών στοιχείων μπορεί να διαιρεθεί σε διάφορες σε διάφορες φάσεις. Η πρώτη φάση περιλαμβάνει την ταυτοποίηση και τη συλλογή των στοιχείων, καταπολεμώντας τυχόν ιούς και προφυλάσσοντας τα στοιχεία, ενώ παράλληλα δημιουργούνται και έγγραφα, όπως αυτά που προτείνονται στο τέταρτο κεφάλαιο και αναφέρουν τις δραστηριότητες που εκτελούνται σε κάθε βήμα. Στη δεύτερη φάση, προσδιορίζονται τα στοιχεία που είναι πιθανότερο να εξυπηρετήσουν τους σκοπούς της έρευνας, δίνοντας μεγαλύτερη έμφαση σε αυτά που δύνανται να αλλοιωθούν με την πάροδο του χρόνου. Κατά την Τρίτη φάση τα ευρήματα αξιολογούνται και ερμηνεύονται, ενώ κατά την τέταρτη φάση παρουσιάζονται τα αποτελέσματα σε μια έκθεση, η οποία περιλαμβάνει πραγματικά περιστατικά, ερμηνεία και γνώμη ειδικού πραγματογνώμονα. Η έκθεση και η παρουσίαση συνιστούν βασικά βήματα στον κύκλο ζωής των ψηφιακών πειστηρίων, δεδομένου ότι το δικαστήριο εξετάζει την έκθεση και τα τεχνικά επιστημονικά ευρήματα όπως αυτά συνοδεύονται από τις ανάλογες αναφορές. Σε κάθε περίπτωση όλες οι ενέργειες και τα συμπεράσματα πρέπει να τεκμηριώνονται (πώς βρέθηκαν τα αποδεικτικά στοιχεία, σε τι κατάσταση βρέθηκαν, το μοντέλο, οι σειριακοί αριθμοί κλπ). [87]Παρακάτω στην εικόνα 1 απεικονίζονται οι διαφορετικές φάσεις των αποδεικτικών στοιχείων.

Εικόνα 1[88]

[87] The Evidence Project will be part of the DG Home Annual Report as a 'success story', Maria Angela Biasiotti, 2017

[88] The Evidence Project will be part of the DG Home Annual Report as a 'success story', Maria Angela Biasiotti, 2017

Πίνακας 1: Τα υπάρχοντα ψηφιακά πλαίσια Εγκληματολογικών Ερευνών

1. Διαδικασία δικανικής υπολογιστών (M.Pollitt, 1995) 4 διαδικασίες
2. Γενική ερευνητική διαδικασία (Palmer, 2001) 7 επίπεδα
3. Αφηρημένο μοντέλο της Ψηφιακής δικανικής (Reith, Carr, & Gunsch, 2002) 9 βήματα
4. Η διαδικασία της ολοκληρωμένης ψηφιακής έρευνας (Carrier & Spafford, 2003) 17 φάσεις
5. End-to-End Ψηφιακή δικανική (Stephenson, 2003) 9 βήματα
6. Ενίσχυση της ολοκληρωμένης ψηφιακής έρευνας(Baryamureeba & Tushabe, 2004) 21 φάσεις
7. Εκτεταμένο μοντέλο των ψηφιακών ερευνών (Ciardhuain, 2004) 13 δραστηριότητες
8. Ιεραρχικό πλαίσιο βασισμένο στο στόχο (Beebe & Clark, 2004) 6 φάσεις
9. Πλαίσιο ψηφιακών εγκληματολογικών ερευνών βασισμένο στο γεγονός (Carrier & Spafford, 2004) 16 φάσεις
10. Διαδικασία ψηφιακής δικανικής (Kent K, Chevalier, Grance, και Dang, 2006) 4 διαδικασίες
11. Πλαίσιο έρευνας (Kohn, Eloff, & Oliver, 2006) 3 στάδια
12. Δικανική υπολογιστών, μοντέλο διαλογής στοιχείων(K.Rogers, Goldman, Mislan, Wedge, και Debrota, 2006) 4 φάσεις
13. Ερευνητικό μοντέλο (Freiling & Schwittay, 2007) 4 φάσεις

3.3 Προτεινόμενα πλαίσια ερευνών στην ψηφιακή δικανική

Η έρευνα που διεξάγεται στα πλαίσια της ψηφιακής εγκληματολογίας, θα πρέπει να ακολουθείται από κάποιες βασικές αρχές, οι οποίες θα διέπουν όλες τις διαδικασίες. Συγκεκριμένα, υποστηρίζεται ότι όλες οι διαδικασίες θα πρέπει να ακολουθούν το τρίπτυχο : αναγνώριση, αξιοπιστία, σχετικότητα. Κατά μία άλλη άποψη, όλες οι μεθοδολογίες οφείλουν να παρουσιάζουν τέσσερα διακριτά βήματα, τα οποία είναι η απόκτηση, η αναγνώριση, η αξιολόγηση και τελικά η αποδοχή των συλλεγέντων στοιχείων ως αποδεικτικών. Απότοκος των τεσσάρων διακριτών βημάτων είναι δεδομένα, πληροφορίες και τελικά τα ίδια τα αποδεικτικά στοιχεία.

Ειδικότερα, με την έννοια αναγνώριση, ορίζεται ότι ο ερευνητής στα πλαίσια μιας διαδικασίας ψηφιακής εγκληματολογίας, πρέπει να εξαντλήσει διαφορετικές μεθόδους, πρακτικές και εργαλεία, ώστε να εξετάσει το συγκεκριμένο λειτουργικό περιβάλλον και τελικά να συλλέξει, ανακτήσει, αποκωδικοποιήσει, εξάγει και τελικά αναλύσει τα δεδομένα που διατηρούνται σε διαφορετικά μέσα αποθήκευσης με σκοπό τα χρησιμοποιηθούν ως νόμιμα ψηφιακά πειστήρια. 89

Επίσης η αξιοπιστία θεωρείται βασικό χαρακτηριστικό της διαδικασίας, δοθέντος ότι στόχος είναι τα πειστήρια να γίνουν δεκτά από το δικαστήριο. Συνεπαγόμενα, είναι αδήριτη

[89]IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.10, October 2008

ανάγκη κατά τη συλλογή, ανάλυση, μεταφορά των δεδομένων να τηρείται η γνησιότητα και η ακεραιότητά τους. Τέλος, ο όρος σχετικότητα αφορά στην αιτιώδη συνάφεια που υπάρχει μεταξύ μιας αξιόποινης πράξης και των ψηφιακών στοιχείων, ήτοι τα πειστήρια θα πρέπει να σχετίζονται άμεσα με το υπό κρίση ζήτημα.

Οι πρακτικές της ψηφιακής εγκληματολογίας αριθμούνται σε εκατοντάδες, ήτοι ανά τον κόσμο έχουν αναπτυχθεί διαφορετικές διαδικασίες έρευνας ψηφιακής εγκληματολογίας και κάθε οργανισμός παρουσιάζει την τάση να αναπτύσσει τις δικές του διαδικασίες. Μάλιστα, άλλοι επικεντρώνονται στην τεχνολογία και στον τρόπο απόκτησης των δεδομένων, άλλοι δίνουν έμφαση στην ανάλυση των δεδομένων σε μεγάλο τμήμα της έρευνας (Brill και Pollitt, 2006). Μεταξύ αυτών των διαδικασιών, οι ακόλουθες είναι οι πιο γνωστές, Lee (Lee et al., 2001), Casey (Casey, 2003a), DFRWS (DFRWS, 2001) και Reith, Carr και Gunsch (Reith et al., 2002). Αξιοσημείωτο είναι δε, ότι κάθε οργανισμός έχει την τάση να αναπτύσσει τις δικές του διαδικασίες. Μέχρι σήμερα, η διαδικασία της ψηφιακής έρευνας έχει κατευθυνθεί από την ίδια την τεχνολογία και τα διαθέσιμα εργαλεία. Συνεπαγόμενα, όταν η υποκείμενη τεχνολογία εξελιχθεί ή τροποποιηθεί, νέες διαδικασίες πρέπει θα χρειαστεί να αναπτυχθούν. Παρά το γεγονός ότι με Ciardha δημιουργείται ένα μοντέλο, κατά το οποίο οι διαδικασίες ψηφιακής εγκληματολογίας έχουν επεκταθεί για να καλύψουν τα περισσότερα τεχνικά κενά, ωστόσο εξακολουθεί να υπάρχει χάσμα μεταξύ των τεχνικών πτυχών της ψηφιακής εγκληματολογίας και της δικαστικής διαδικασία (Losavio και Adams, 2006). Σύμφωνα με τους Losavio και Adams, υποστηρίζεται ότι υπάρχει ένα μεγάλο χάσμα μεταξύ των τεχνικών εμπειρογνωμόνων και των νομικών επαγγελμάτων.90

Πίνακας 2 [91]

Table 1 – A comparison table between different digital forensics investigation model extracted from Séamus Ó Ciardhuáin's analysis

Term in new model	Model			
	Lee et al.	Casey	DFRWS	Reith et al.
Awareness				Identification
Authorisation				
Planning				Preparation
Notification				
Search/identification	Recognition, identification	Recognition	Identification	
Collection	Collection and preservation	Preservation, collection, documentation	Preservation, collection	Preservation, collection
Transport				
Storage				
Examination	Individualization	Classification, comparison, individualization	Examination	Examination
Hypothesis	Reconstruction	Reconstruction	Analysis	Analysis
Presentation	Reporting and presentation		Presentation	Presentation
Proof/defence			Decision	
Dissemination				

Αξιοσημείωτη είναι η συνεισφορά των Brungs και Jamieson, οι οποίοι διεξήγαγαν έρευνα σχετικά με τις προτεραιότητες του νομικού πλαισίου της Αυστραλίας στην ψηφιακή

[90]Forza, Digital forensics investigation framework that incorporate legal issues

[91] Forza, Digital forensics investigation framework that incorporate legal issues

δικανική. Η μελέτη τους, η οποία προσδιορίζεται σε δεκαεπτά νομικά ζητήματα και καλύπτει τρεις κατηγορίες, ήτοι το δικαστικό σκέλος , την ιδιωτικότητα και το ζήτημα της πολλαπλής δικαιοδοσίας, έθεσε τις βάσεις για την ταξινόμηση των νομικών ζητημάτων που αφορούν στην ψηφιακή εγκληματολογία. Η μελέτη των Brungs-Jamieson καλύπτει τη νομοθεσία της Αυστραλίας στον τομέα των τηλεπικοινωνιών, δηλαδή το νόμο περί τηλεπικοινωνιών του 1979 και την ερμηνεία του. Η μελέτη αυτή προσδιόρισε την ανάγκη για την προστασία της ιδιωτικής ζωής των φυσικών προσώπων και των επιχειρήσεων κατά τη διάρκεια των ερευνών ως μια μεγάλη πρόκληση. Άλλοι ερευνητές έχουν επίσης επισημάνει ότι αυτό είναι ένα από τα σημαντικότερα ζητήματα στην ψηφιακή εγκληματολογία.92

Ένα ακόμη κρίσιμο ζήτημα είναι η παρουσίαση των ψηφιακών αποδεικτικών στοιχείων σε νομικές διαδικασίες. Το γεγονός ότι οι δικηγόροι, οι δικαστές και οι ένορκοι συνήθως διαθέτουν περιορισμένες τεχνικές γνώσεις, επισύρει την ανάγκη η παρουσίαση των ψηφιακών αποδεικτικών στοιχείων να γίνεται κατά τρόπο σαφή και εύκολα κατανοητό. Οι Broucek και Turner, μάλιστα, υποστήριξαν ότι οι περισσότεροι επαγγελματίες νομικοί έχουν περιορισμένη κατανόηση της τεχνολογίας και τείνουν να επιδεικνύουν περιορισμένη εμπιστοσύνη στην ικανότητα των τεχνικών πραγματογνωμόνων να προσκομίσουν αποδεικτικά στοιχεία παραδεκτά κατά την ακροαματική διαδικασία. Τέλος, οι Brungs και Jamieson έθεσαν το ζήτημα των βέλτιστων πρακτικών, του ελέγχου των ψηφιακών εργαλείων και της αξιοπιστίας των πραγματογνωμόνων. Σήμερα, οδηγοί βέλτιστων πρακτικών είναι διαθέσιμοι, ωστόσο δεν υπάρχουν δημοσιευμένες τιμές σφαλμάτων ή αποτελέσματα δοκιμών για τα εργαλεία που εφαρμόζονται στην ψηφιακή δικανική. Τα προσόντα και οι δεξιότητες των πραγματογνωμόνων είναι ακόμη ένα σοβαρό ζήτημα, και μάλιστα οι Meyers και Rogers έθεσαν το ερώτημα αν κάποιος δύναται να θεωρηθεί ένας εμπειρογνώμονας βασιζόμενος στην ικανότητα να χρησιμοποιεί ένα πακέτο εργαλείων ή κάποιο λογισμικό, χωρίς , όμως, να καθορίζεται με σαφήνεια σε τι συνίσταται η δυνατότητα λειτουργίας κάποιου εργαλείου ή η αναθεώρηση του κώδικα. Έτσι, λοιπόν, γίνονται προσπάθειες για την ανάπτυξη προτύπων σχετικά με τα προσόντα των εμπειρογνωμόνων. 93

Η σημερινή χρυσή εποχή της ψηφιακής εγκληματολογίας γρήγορα θα πλησιάσει στο τέλος της. Χωρίς μια σαφή στρατηγική για τη διευκόλυνση των ερευνητικών προσπαθειών η εγκληματολογική έρευνα θα τελματώσει. Η εφαρμογή της ψηφιακής εγκληματολογίας στο στρατό και σε άλλους οργανισμούς, χρειάζεται την υιοθέτηση τυποποιημένων διαδικασιών, προκειμένου να ανακύπτουν αξιόπιστες πληροφορίες-αποδεικτικά στοιχεία τα οποία έχουν συλλεγεί με μία σύννομη διαδικασία.94

Το 2001, η εγκληματολογική ερευνητική ομάδα ψηφιακής δικανικής όρισε μια γενική διαδικασία έρευνας που μπορούσε να εφαρμοστεί στην πλειοψηφία των ερευνών που αφορούσαν σε ψηφιακά συστήματα και διαδίκτυο. Οι διαδικασίες που όρισαν ήταν εντοπισμός στοιχείων, συντήρηση, συλλογή, εξέταση, ανάλυση, παρουσίαση στο δικαστήριο και έκδοση απόφασης. Σε αυτό το πλαίσιο οι διαδικασίες ονομάζονται "τάξεις των εργασιών" και οι επιμέρους εργασίες ονομάζονται "φάσεις" ή "επιμέρους στάδια της διαδικασίας". Το πλαίσιο αυτό έθεσε μια σημαντική βάση για τις μελλοντικές εργασίες πάνω στις ψηφιακές έρευνες.

Το 2002, προτείνεται ένα πλαίσιο που ονομάζεται αφηρημένο πλαίσιο ψηφιακής εγκληματολογίας, αποτελείται από έντεκα φάσεις οι οποίες περιλαμβάνουν τον εντοπισμό, την προετοιμασία, τη στρατηγική προσέγγιση, τη συντήρηση, συλλογή, εξέταση, ανάλυση και παρουσίαση των αποδεικτικών στοιχείων. Αυτή η διαδικασία είναι ολοκληρωμένη και

[92] Marcus Rogers and Marianne Hoebich , Chapter 20, , Sydney Liles, Marcus Rogers and Marianne Hoebich

[93] Marcus Rogers and Marianne Hoebich , Chapter 20, a survey of the legal issues facing digital forensics experts , Sydney Liles

[94] Digital forensics research: The next 10 years, Simson L. Garfinkel Validhtml, Naval Postgraduate School, Monterey, USA, , 2 August 2010

προσέφερε μια σειρά πλεονεκτημάτων, συγκεκριμένα έθεσε το μηχανισμό για την εφαρμογή του ίδιου πλαισίου στις μεταγενέστερες ψηφιακές τεχνολογίες. Αξιοσημείωτο είναι δε ότι αυτό το πλαίσιο, δίνει έμφαση στο στάδιο της προετοιμασίας και συγκεκριμένα στην επιμέρους φάση αυτή που είναι η στρατηγική προσέγγιση των στοιχείων.

Το 2003, προτείνεται ένα πλαίσιο ερευνητικής διαδικασίας, το οποίο κατά κύριο λόγο βασίζεται στη διερεύνηση του φυσικού τόπου του εγκλήματος και ονομάζεται "διαδικασία της ολοκληρωμένης ψηφιακής έρευνας". Το ως άνω πλαίσιο, ορίζει ως τόπο τέλεσης του ψηφιακού εγκλήματος, το εικονικό περιβάλλον του ψηφιακού εγκλήματος (π.χ. το λογισμικό) και στην έννοια του τόπου τέλεσης συμπεριλαμβάνονται τα υλικά αντικείμενα που θα βρεθούν και θα χρησιμοποιηθούν ως ψηφιακές αποδείξεις του συμβάντος. Το πλαίσιο αυτό επιμερίζει τη διαδικασία σε πέντε ομάδες οι οποίες διαχωρίζονται συνολικά σε δεκαεπτά (17) περαιτέρω φάσεις. Οι ομάδες αποτελούνται από φάσεις ετοιμότητας, φάσεις ανάπτυξης, φάσεις έρευνας στο φυσικό τόπο του εγκλήματος, φάσεις έρευνας στο εικονικό περιβάλλον του ψηφιακού εγκλήματος και τέλος φάση αναθεώρησης. Η συγκεκριμένη πρόταση διεξαγωγής της έρευνας εστιάζει κυρίως στην ανασύνθεση των γεγονότων που οδήγησαν στο περιστατικό, μάλιστα υποστηρίζεται ότι η δημιουργία αυτού του μηχανισμού δύναται να οδηγήσει σε ταχύτερη διεκπεραίωση της έρευνας.

Αξιοσημείωτο είναι ένα ακόμη πλαίσιο η λεγόμενη end-to-end ψηφιακή έρευνα - διατερματική ψηφιακή έρευνα, η οποία αποτελείται από εννέα βήματα. Τα βήματα αυτά τελούνται από τον εκάστοτε ερευνητή, ο οποίος συλλέγει τα ευρήματα, τα διατηρεί, τα εξετάζει και τελικά αναλύει τις ψηφιακές ενδείξεις. Επίσης, ο ερευνητής θα καθορίσει τις κρίσιμες δραστηριότητες στη διαδικασία συλλογής, μερικές από τις οποίες είναι η συλλογή στοιχείων από τους υπό εξέταση υπολογιστές, η συλλογή των logs-αρχείων καταγραφής στις ενδιάμεσες συσκευές, ιδίως εκείνες που είναι συνδεδεμένες στο διαδίκτυο, με στόχο τον εντοπισμό πιθανών εισβολών που θα έχουν ανιχθευθεί από τα συστήματα ανίχνευσης ιών και τα firewalls.

Εν συνεχεία, το 2004, ενισχύεται το προαναφερθέν πλαίσιο "διαδικασία της ολοκληρωμένης ψηφιακής έρευνας" , το οποίο ονομάζεται ενισχυμένο πλαίσιο της ψηφιακής έρευνας (EIDIP). Το ενισχυμένο πλαίσιο διαχωρίζει τις έρευνες στην πρωτογενή και δευτερογενή σκηνή του εγκλήματος, ως πρωτογενής σκηνή θεωρείται ο υπολογιστής και ως δευτερογενής ο φυσικός τόπος τέλεσης. Προσέτι, απεικονίζει τις φάσεις ως επαναληπτικές και όχι γραμμικές, ο στόχος του ενισχυμένου μοντέλου είναι να ανακατασκευάσει τα δύο σκηνές εγκλήματος ταυτόχρονα ώστε να αποφευχθούν τυχόν ασυνέχειες στη ροή τέλεσης του εγκλήματος.

Η ομάδα των Carrier και Spafford πρότεινε το 2004 ένα ακόμη πλαίσιο βασισμένο κυρίως στο ίδιο το γεγονός, απλοποιώντας τη διαδικασία στη φάση της διατήρησης, αναζήτησης και ανασυγκρότησης. Αυτό το απλό πλαίσιο βασίζεται στις γενεσιουργές αιτίες του συμβάντος και τις συνέπειες αυτού. ένα τρωτό σημείο, ωστόσο, της ως άνω διαδικασίας είναι οι φάσεις δεν είναι σαφώς ορισμένες και τελικά το πλαίσιο κρίθηκε ανεπαρκές για την ψηφιακή εγκληματολογική έρευνα.

Το εκτεταμένο μοντέλο ψηφιακών ερευνών, από την άλλη, προτείνει σαφή βήματα που πρέπει να ακολουθηθούν κατά τη διάρκεια της διαδικασίας, περιλαμβάνει φάσεις, όπως είναι η ευαισθητοποίηση, ο σχεδιασμός των φάσεων, η αναζήτηση και ο εντοπισμός στοιχείων, η συλλογή τους, η μεταφορά συσκευών-αποδεικτικών στοιχείων, η αποθήκευσή τους, η εξέταση των ευρημάτων, η παρουσίασή τους και τέλος η απόδειξή τους στην επ ακροατηρίω διαδικασία. Το πλαίσιο προβλέπει επίσης τη βάση για την ανάπτυξη τεχνικών και εργαλείων με στόχο την υποστήριξη του έργου των ερευνητών. Συνεπαγόμενα, το πλαίσιο αυτό θεωρείται η πιο ολοκληρωμένη μέχρι σήμερα προτεινόμενη διαδικασία.

Το 2006, προτείνεται η διαδικασία ψηφιακής δικανικής η οποία αποτελείται από τέσσερις φάσεις, τη συλλογή των στοιχείων, την εξέτασή τους, την ανάλυση των ευρημάτων και την συνακόλουθη υποβολή εκθέσεων. Σε αυτό το πλαίσιο, συλλέγονται τα δεδομένα, εξετάζονται

και μετατρέπονται σε τέτοια μορφή, ώστε να μπορούν να επεξεργαστούν από τα εργαλεία ψηφιακής δικανικής. Στη συνέχεια, τα δεδομένα μετατρέπεται σε πληροφορίες μέσω της ανάλυσης και τελικά οι πληροφορίες μετατρέπονται στα αποδεικτικά στοιχεία κατά τη φάση της υποβολής των εκθέσεων.95

Το πλαίσιο έρευνας, αποτελεί ένα μοντέλο που συγχωνεύει όλα τα άλλα υφιστάμενα προταθέντα πλαίσια στοχεύοντας να συγκεράσει τα πλεονεκτήματα των προγενέστερων σχεδίων. Κρείσσονος σημασίας είναι ότι σε αυτό το πλαίσιο τονίστηκε η ιδιαίτερη σημασία της κατανόησης της νομικής πραγματικότητας που περιβάλει τις διαδικασίες αυτές. Η εις βάθος γνώση της νομικής βάσης πριν τη δημιουργία του σχεδίου έρευνας θεωρήθηκε, όπως και πράγματι είναι, αδήριτη ανάγκη, δεδομένου ότι θα διατρέχει όλα τα στάδιά της. Η υπό κρίση διαδικασία περιλαμβάνει τρία στάδια, την προετοιμασία, την έρευνα και την παρουσίαση, οι οποίες οφείλουν να πληρούν τις απαιτήσεις του νόμου. Αντιλαμβανόμαστε, επομένως, ότι οι προαναφερθέντες φάσεις έχουν ομαδοποιηθεί στα τρία αυτά στάδια, τα οποία ακολουθούν μία προβλεπόμενη νομική βάση, σύμφωνα με το πλαίσιο, ώστε να είναι προκαθορισμένες οι νομικές απαιτήσεις σε κάθε βήμα. Το γεγονός ότι, το σχέδιο αυτό δίνει μεγάλη βαρύτητα στη σύννομη πορεία της ερευνητικής διαδικασίας το ανυψώνει στα βασικά πλαίσια εφαρμογής, πάνω στο οποίο δύνανται να προστεθούν κι άλλες φάσεις ή ακόμη και να βελτιωθούν οι ήδη υπάρχουσες.

Σημαντικό είναι να αναφερθεί ότι η πρόταση σχεδίου έρευνας από όγδοο μοντέλο, το ιεραρχικό, εισήγαγε ένα νέο πλαίσιο διαδικασίας για τη διερεύνηση των περιστατικών ασφάλειας υπολογιστών με βασικό στόχο το συνδυασμό του "incident response" με τη δικανική υπολογιστών. Το πλαίσιο, λοιπόν, αυτό δίνει ιδιαίτερη έμφαση στην ανάλυση των περιστατικών, διακρίνοντάς την σε τρεις επιμέρους φάσεις, το προπαρασκευαστικό στάδιο της ανάλυσης, τον κύριο κορμό της ανάλυσης και τελικά το στάδιο μετά την ανάλυση. Το προγενέστερο βήμα περιέχει όλα τα βήματα και τις δραστηριότητες που πραγματοποιούνται πριν από την πραγματική έναρξη της ανάλυσης, ενώ η "μέτα-ανάλυση" φάση αφορά στην έγγραφη τεκμηρίωση-αναφορά του συνόλου των δραστηριοτήτων κατά τη διάρκεια της έρευνας. Η πραγματική ανάλυση λαμβάνει χώρα στον κύριο κορμό, όπως προαναφέρθηκε. Παρατηρώντας την ιδιαίτερη έμφαση στο incident response του συγκεκριμένου πλαισίου, συνακόλουθα προκύπτει ότι το σχέδιο αυτό οδηγεί σε τρόπους αντιμετώπισης των περιστατικών ασφάλειας που ανακύπτουν.

Το δωδέκατο πλαίσιο "δικανική υπολογιστών, μοντέλο διαλογής στοιχείων" (CFFTPM) προτείνει μια επιτόπια προσέγγιση της ερευνητικής διαδικασίας προκειμένου να επιτευχθεί η ταυτοποίηση, η ανάλυση και η ερμηνεία των ψηφιακών αποδεικτικών στοιχείων σε σύντομο χρονικό διάστημα χωρίς να κρίνεται απαραίτητη η εξέταση σε κάποιο εργαστήριο ψηφιακής εγκληματολογίας, καθότι υποστηρίζει ότι ο επιτόπιος έλεγχος δύναται να οδηγήσει σε πλήρη και αποτελεσματικά ευρήματα. Αυτό το πλαίσιο περιλαμβάνει φάσεις, κατά τις οποίες γίνεται σχεδιασμός της έρευνας, διαλογή στοιχείων, υποβολή χρονοδιαγράμματος και ελέγχεται η όποια διαδικτυακή δραστηριότητα. Το ως άνω πλαίσιο προσομοιάζει με τις κλασικές έρευνες και το μεγάλο πλεονέκτημά του είναι ότι θεωρείται πιο ρεαλιστική μέθοδος από τις προηγούμενες αφού στηρίζεται ιδιαίτερα στον τόπο τέλεσης των παράνομων πράξεων. Στον αντίποδα, υποστηρίζεται ότι δε δύναται μια τέτοια μέθοδος να καλύψει όλες τις περιπτώσεις διεξαγωγής ερευνών.96

Καταλήγοντας, μέχρι σήμερα δεν υπάρχει ενιαίο πλαίσιο που θα μπορούσε να θεωρηθεί ως μια γενική κατευθυντήρια γραμμή για τη διερεύνηση όλων των περιστατικών. Από τα υπάρχοντα προτεινόμενα πλαίσια ή μοντέλα που προαναφέρθηκαν, μπορεί να φανεί ξεκάθαρα ότι κάθε ένα βασίζεται στην εμπειρία που παρείχε το προηγούμενο, μερικά από τα πλαίσια

[95]IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.10, October 2008
[96]IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.10, October 2008

έχουν παρόμοιες προσεγγίσεις, ενώ άλλα έχουν δώσει έμφαση σε διαφορετικούς τομείς της έρευνας.

3.4 Χαρτογράφηση πλαισίου

Σε μία προσπάθεια να χαρτογραφήσουμε ένα πλαίσιο ερευνών ψηφιακής εγκληματολογίας, επιτυγχάνοντας το συγκερασμό όλων των θετικών στοιχείων των προτεινόμενων μοντέλων σε ένα.

Βήμα 1 - Προσδιορισμός των υφιστάμενων πλαισίων
Σε αυτό το βήμα περιγράφονται οι φάσεις, οι δραστηριότητες / διεργασίες και τα αποτελέσματα για κάθε πλαίσιο.

Προετοιμασία
Στο σημείο αυτό λαμβάνεται η άδεια για την πραγματοποίηση έρευνας, ήτοι το ένταλμα έρευνας. Επίσης, ο ερευνητής φροντίζει να διαθέτει την υποδομή που απαιτείται για τη διεξαγωγή της.
Σε αυτό το στάδιο προσχεδιάζεται η διαδικασία που θα ακολουθηθεί για να διεξαχθεί η έρευνα, καθορίζεται η στρατηγική, το πλαίσιο και ελέγχεται το ιστορικό της υπόθεσης.
Τα ενδιαφερόμενα μέρη ενημερώνονται για τη διεξαγωγή της έρευνας.

Το αποτέλεσμα του σταδίου προετοιμασίας είναι η δημιουργία σχεδίου, η χορήγηση εντάλματος, η κοινοποίηση αυτού και η έναρξη της διαδικασίας.

Συλλογή και διατήρηση στοιχείων

Στο στάδιο της συλλογής των στοιχείων, κατά κύριο λόγο οριοθετείται η έννοια των ψηφιακών αποδεικτικών στοιχείων, ποια αφορούν το αντικείμενο της έρευνας και ποιες θα αποτελέσουν τις πηγές των δεδομένων που θα αναζητηθούν. Συνακόλουθα, καθορίζονται τα αποδεικτικά στοιχεία που θα εξετασθούν ή θα φανούν χρήσιμα στη φυσική τοποθεσία τέλεσης του εγκλήματος. Τα στοιχεία που θα συλλέξουν οι ερευνητές, πρέπει να παραμείνουν ακέραια και να αποθηκευθούν κατάλληλα. Ο φυσικός τόπος τέλεσης περιγράφεται και καταγράφεται στην έκθεση έρευνας προκειμένου να τηρείται η διαφάνεια της διαδικασίας, αλλά και να συμπληρωθεί η έρευνα εάν κριθεί απαραίτητο μεταγενέστερα.

Σε κάθε περίπτωση για τις ψηφιακές αποδείξεις θα ληφθούν αντίγραφα μέσω αποδεκτών διαδικασιών προκειμένου να διασφαλιστεί η εγκυρότητα και η ακεραιότητά τους. Το αποτέλεσμα αυτής της φάσης είναι να έχει κατανοηθεί σε ένα σημαντικό βαθμό το είδος του εγκλήματος που τελέσθηκε, οι πιθανές πηγές αποδεικτικών στοιχείων έχουν προσδιοριστεί και συλλεγεί και τελικά το περιστατικό έχει κατηγοριοποιηθεί επαρκώς.

Παρουσίαση και έγγραφη αναφορά

Οι πληροφορίες που προέκυψαν από τη φάση της συλλογής παρουσιάζονται σε αυτό το στάδιο. Καθορίζονται και αποσαφηνίζονται τα αποτελέσματα της συλλογής στοιχείων και τεκμηριώνονται με τα αποδεικτικά στοιχεία πλέον που θα αναφερθούν στην έγγραφη αναφορά. Σημαντικό είναι να αναφερθεί ότι εξάγονται συμπεράσματα από την έρευνα τα οποία, παράλληλα με τα φυσικά και αποδεικτικά στοιχεία περικλείονται στην παρουσίαση ενώπιον του δικαστηρίου. Κρείσσονος σημασίας είναι να αποδεικνύεται στην επ' ακροατηρίω διαδικασία η εγκυρότητα της διαδικασίας συλλογής στοιχείων και η σύννομη διεξαγωγή της έρευνας. Το αποτέλεσμα του ως άνω σταδίου είναι η εξαγωγή των αποδεικτικών στοιχείων και η αποτύπωσή

τους εγγράφως, παρουσιάζοντας το πρότυπο που επιλέχθηκε να ακολουθηθεί για τη διεκπεραίωση της υπόθεσης, τα βήματα που υιοθετήθηκαν, τα στοιχεία που αποκαλύφθηκαν και χρησιμοποιούνται με τη δυναμική της απόδειξης τέλεσης ή μη τέλεσης κάποιου εγκλήματος.

Σχηματισμός της υπόθεσης

Έχοντας σχηματίσει μια εικόνα της υπόθεσης, διασφαλίζοντας τα φυσικά και ψηφιακά στοιχεία ακέραια, είναι δυνατό να επανεξεταστούν τα κρίσιμα σημεία της έρευνας, να βελτιωθούν κάποιες διαδικασίες και τελικά να οδηγηθεί η έρευνα να τερματίσει, παρέχοντας πλήρη αποδεικτικά στοιχεία, ακέραια και κατόπιν νομότυπης συλλογής. Τέλος, αυτή η φάση δύναται να οδηγήσει σε νέες πολιτικές και διαδικασίες έρευνας.

Βήμα 2 - Κατασκευή της φάσης

Σε αυτό το βήμα, κατασκευάζεται η κάθε φάση, οι διαδικασίες και οι δραστηριότητες που θα αναπτυχθούν σε κάθε φάση και καθορίζεται το αναμενόμενο αποτέλεσμα. Στο δεύτερο βήμα ορίζονται οι κάτωθι πέντε φάσεις.

Φάση 1 : Προετοιμασία
Η προετοιμασία περιλαμβάνει τη δημιουργία πλάνου, την έκδοση εντάλματος έρευνας-κατάσχεσης-σύλληψης, την κοινοποίηση.
Φάση 2 : Συλλογή-διατήρηση
Η φάση αυτή οριοθετεί τον τύπο του εγκλήματος, τις πιθανές πηγές αποδιεκτικών στοιχείων, τα φυσικά αντικείμενα που θα εξετασθούν και πλέον έχουμε ένα σαφή καθορισμό του συμβάντος.
Φάση : 3 Εξέταση και Ανάλυση
Στο σημείο αυτό συλλέγονται τα αρχεία καταγραφής logs και γενικότερα οι ψηφιακές πληροφορίες που αφορούν κάποια τελεσθείσα πράξη.
Φάση : 4
Παρουσίαση και αναφορά
Τα αποδεικτικά στοιχεία έχουν πλέον σχηματιστεί και εντάσσονται σε μία έγγραφη αναφορά.
Φάση : 5
Παρουσίαση-διάδοση της υπόθεσης
Τώρα πια υπάρχει μια υπόθεση που έχει εξετασθεί και μελετηθεί και το αποτέλεσμά της δύναται να οδηγήσει σε βελτιώσεις, νέες πολιτικές, νέες διαδικασίες.

Αφού λοιπόν έχει προηγηθεί μια εκτενής ανάλυση, συγκεκριμένα στη φάση ένα έχουν μελετηθεί γενικότερα οι προτεινόμενες φάσεις και οι διαδικασίες που τις απαρτίζουν, στη φάση δύο έχει σχεδιαστεί το πλαίσιο που θα ακολουθηθεί γνωρίζοντας τις ανάγκες της υπό κρίση υπόθεσης. Σε αυτό σημείο σημαντικό είναι να αναφερθεί το αποτέλεσμα της έρευνας όπως απεικονίζεται στον παρακάτω πίνακα.

Πίνακας 1

Phase / Output	**1**	**2**	**3**	**4**	**5**
Pollitt, 1995					
Acquisition		√			
Identification		√			
Evaluation			√		
Admission as Evidence				√	
Kent et. al, 2006					
Collection		√			
Examination			√		
Analysis			√		
Reporting				√	√
Freiling and Schwittay, 2007					
Pre-Incident Preparation	√				
Pre-Analysis		√			
Analysis			√		
Post-Analysis				√	√

3.5 Εφαρμοσμένες μεθοδολογίες

Το Υπουργείο Δικαιοσύνης των ΗΠΑ τον Ιούλιο του 2001 δημοσίευσε ένα μοντέλο έρευνας του τόπου διάπραξης ηλεκτρονικού εγκλήματος η οποία που αποτελείται από τέσσερις φάσεις:

Συλλογή: η πρώτη φάση περιλαμβάνει την αναζήτηση, την αναγνώριση, τη συλλογή αποδεικτικών στοιχείων και την καταγραφή τους. Ανάλογα με το είδος της έρευνας, αυτά

μπορεί να είναι σκληροί δίσκοι, οπτικά μέσα, κάρτες αποθήκευσης από ψηφιακές φωτογραφικές μηχανές, κινητά τηλέφωνα, chips από φορητές συσκευές, ή
ακόμα και μεμονωμένα αρχεία. Αφού τα μέσα αυτά συλλεχθούν, δημιουργείται ένα ακριβές αντίγραφο τους (forensic duplicate) με κατάλληλα εργαλεία υλικού ή λογισμικού και συνήθως χρησιμοποιείται και μία συσκευή write-blocking η οποία αποτρέπει τυχόν τροποποιήσεις στα αρχικά δεδομένα. Η διαδικασία αυτή συχνά ονομάζεται και imaging. Να σημειωθεί ότι οποιαδήποτε εξέταση πραγματοποιείται επί του αντιγράφου και όχι επί του πρωτότυπου πειστηρίου, έτσι ώστε να αποφευχθεί οποιαδήποτε μεταβολή στα αυθεντικά ψηφιακά δεδομένα, η οποία θα καθιστούσε την όλη έρευνα αναξιόπιστη ώστε να σταθεί ως αποδεικτικό στοιχείο σε μια δικαστική διαμάχη. Στη συνέχεια, το αρχικό ψηφιακό μέσο τοποθετείται σε ένα ασφαλές μέρος ώστε να αποφευχθούν αλλοιώσεις. Τέλος, για το αποκτηθέν αντίγραφο καθώς και για το αρχικό ψηφιακό μέσο, πρέπει να υπολογιστεί μία κρυπτογραφική σύνοψη (με χρήση για παράδειγμα των συναρτήσεων MD5, SHA-1 και SHA-256). Οι δύο τιμές που θα προκύψουν συγκρίνονται ώστε να πιστοποιηθεί ότι το αντίγραφο είναι ακριβές. Σε κρίσιμα σημεία της ανάλυσης, υπολογίζεται πάλι η σύνοψη του ψηφιακού μέσου έτσι ώστε να επιβεβαιωθεί ότι τα δεδομένα δεν έχουν υποστεί αλλοιώσεις.

Εξέταση: στη φάση αυτή εξηγείται η προέλευση και η σημασία των πειστηρίων για την υπόθεση, ενώ περιλαμβάνει και την αποκάλυψη κρυφών πληροφοριών και σχετικών εγγράφων.

Ανάλυση: στο σημείο αυτό εξετάζονται τα αποτελέσματα της εξέτασης και αναδεικνύεται η αποδεικτική τους αξία για την υπό κρίση υπόθεση, πρόκειται για την πραγματική εξέταση του ψηφιακού μέσου. Μετά την απόκτηση, το περιεχόμενο των ψηφιακών αντιγράφων αναλύεται με σκοπό την εύρεση αποδείξεων που είτε υποστηρίζουν είτε αντικρούουν μία υπόθεση, ή στοιχείων που υποδεικνύουν αλλοιώσεις (με σκοπό την απόκρυψη δεδομένων). Το 2002, το International Journal of Digital Evidence αναφέρθηκε στο συγκεκριμένο στάδιο σαν ” μία σε βάθος συστηματική αναζήτηση στοιχείων που να σχετίζονται με το υποπτευόμενο έγκλημα”. Αντίθετα, ο Brian Carrier το 2005, περιέγραψε μία πιο διαισθητική διαδικασία κατά την οποία προφανή δεδομένα προσδιορίζονται πρώτα και στη συνέχεια πραγματοποιούνται πιο διεξοδικές αναζητήσεις για να καλυφθούν τα διάφορα κενά. Κατά τη διάρκεια της ανάλυσης, ένας ερευνητής συνήθως ανακτά αποδεικτικό υλικό χρησιμοποιώντας πολλές διαφορετικές μεθοδολογίες (και εργαλεία), συνήθως ξεκινώντας από τις πιο συνηθισμένες τοποθεσίες ανάλογα με το είδος της έρευνας. Για παράδειγμα, αν μελετώνται περιηγήσεις ιστού ενός χρήστη, η έρευνα ξεκινά από το ιστορικό, τους σελιδοδείκτες και την προσωρινή μνήμη του περιηγητή (web browser cache.) Οι εξεταστές χρησιμοποιούν ειδικά εργαλεία για να βοηθήσουν την προβολή και ανάκτηση δεδομένων. Το είδος των δεδομένων που ανακτάται ποικίλει ανάλογα με την έρευνα και παραδείγματα αποτελούν e-mail, logs συνομιλιών, εικόνες, ιστορικό διαδικτύου ή αρχεία κειμένου. Οι αποδείξεις μπορούν να ανακτηθούν όχι μόνο από τον προσβάσιμο χώρο ενός ψηφιακού μέσου αλλά και από τον ελεύθερο χώρο του ή από αρχεία λανθάνουσας μνήμης ενός λειτουργικού συστήματος (cache files). Αφού ανακτηθούν τα στοιχεία, οι πληροφορίες αναλύονται με σκοπό την αναπαράσταση γεγονότων ή ενεργειών και την κατάληξη σε συμπεράσματα.

Αναφορά/παρουσίαση: στο τελευταίο στάδιο είναι κρείσσονος σημασίας η σύνταξη μιας έκθεσης που περιγράφει τη διαδικασία εξέτασης και τα δεδομένα που έχουν ανακτηθεί από τη συνολική έρευνα. Πρόκειται για τη διαδικασία κατά την οποία ο εξεταστής μοιράζεται τα αποτελέσματα της ανάλυσής του με τους ενδιαφερόμενους. Αυτό περιλαμβάνει την δημιουργία αναφοράς με τα βήματα που ακολούθησε, τα στοιχεία που σύλλεξε καθώς και την ερμηνεία τους. Πολλές φορές η φάση της παρουσίασης περιλαμβάνει επίσης την υπεράσπιση των ευρημάτων από τον εξεταστή.

Φάση πρώτη: Προετοιμασία

Η φάση της προετοιμασίας εξελίσσεται πριν από την έρευνα. Σε αυτήν συμπεριλαμβάνεται η κατανόηση της φύσης του εγκλήματος και η συγκέντρωση των υλικών-εργαλείων που θα χρησιμοποιηθούν στην συλλογή και συσκευασία των αποδείξεων. Επίσης κατά την διάρκεια της προετοιμασίας θα πρέπει να έχουν εξεταστεί όλα τα νομικά ζητήματα και να έχουν ξεπεραστεί όλα τα εμπόδια που τυχόν προκύψουν, σύμφωνα με τα όσα ορίζει το εκάστοτε δικονομικό σύστημα μιας χώρας, όπως για παράδειγμα η προστασία των δικαιωμάτων των υπόπτων. Τέλος αφού έχει γίνει μια σωστή εκτίμηση των συνθηκών του εγκλήματος και έχουν ξεπεραστεί τα νομικά ζητήματα, πρέπει να αναπτυχθεί μια κατάλληλη στρατηγική για την διεξαγωγή της έρευνα. Έχοντας, λοιπόν, μια διεξοδική προετοιμασία αυξάνεται η ποιότητα των αποδεικτικών στοιχείων και ελαχιστοποιούνται οι κίνδυνοι και οι απειλές που συνδέονται με την έρευνα.

Φάση δεύτερη: Εξασφάλιση της σκηνής

Αυτό το στάδιο ασχολείται κυρίως με την εξασφάλιση της σκηνής του εγκλήματος από οποιαδήποτε μη εξουσιοδοτημένη πρόσβαση και την διατήρηση των αποδεικτικών στοιχείων ανέπαφων. Πρώτο μέλημα θα πρέπει να είναι ο προσδιορισμός του χώρου της σκηνής του εγκλήματος και η δημιουργία μια σαφής περιμέτρου. Επίσης θα πρέπει να ληφθούν μέτρα για την προστασία της ακεραιότητας όλων των αποδεικτικών στοιχείων και να υπάρχει ο απόλυτος έλεγχος της σκηνής αποτρέποντας οποιαδήποτε παρέμβαση από τους ανεπιθύμητους ανθρώπους. Πρώτη προτεραιότητα πρέπει να δοθεί σε αυτό το στάδιο στην ελαχιστοποίηση της διαφθοράς των αποδεικτικών στοιχείων. Η φάση αυτή παίζει σημαντικό ρόλο στη συνολική ερευνητική διαδικασία που καθορίζει την ποιότητα των αποδεικτικών στοιχείων.

Φάση τρίτη: Έρευνα και Αναγνώριση

Σε αυτό το στάδιο ξεκινά η έρευνα με την αξιολόγηση της σκηνής, τη διαμόρφωση κατάλληλου σχεδίου αναζήτησης και τον εντοπισμό πηγών από όπου θα εξαχθούν τα αποδεικτικά στοιχεία. Σε ένα σύνθετο περιβάλλον, αυτό μπορεί να μην είναι απλό. Σε αυτή την διαδικασία σημαντικό ρόλο μπορεί να παίξει η ανακριτική διαδικασία όπου μέσω ερωτήσεων που θα γίνουν στους ιδιοκτήτες ή τους χρήστες των ηλεκτρονικών συσκευών ή των διαχειριστών του συστήματος θα εξαχθούν πολύτιμες πληροφορίες, που αφορούν σε διάφορες εφαρμογές που υπάρχουν στο συσκευές, λεπτομέρειες κρυπτογράφησης κλπ. χωρίς να παραβιάζεται το απόρρητο των επικοινωνιών και άλλων δικαιωμάτων όπου ο νόμος ορίζει αντίστοιχα.

Φάση τέταρτη: Καταγραφή της σκηνής

Αυτό το στάδιο πρέπει να καταγραφούν όλα τα αντικείμενα που στοιχειοθετούν την σκηνή του εγκλήματος και να φωτογραφηθούν. Συνεπώς κατά την φωτογράφηση ηλεκτρονικών συσκευών θα πρέπει να φωτογραφηθούν μαζί τους και οι μετασχηματιστές ρεύματος, τα καλώδια, οι βάσεις κα. Κατά την καταγραφή χρήσιμο είναι να σημειωθεί ο τύπος του πειστηρίου (cd, κασέτα), ο κατασκευαστής του κλπ. Σκοπός αυτής της καταγραφής είναι η δυνατότητα δημιουργίας εκ νέου της σκηνής κάθε στιγμή με σκοπό την επανεξέτασή της, καθώς και την παρουσίασή της σε μια αίθουσα δικαστηρίου σε μεταγενέστερο χρόνο. Κατά την καταγραφή θα πρέπει να προσδιορίζεται η ημέρα, η ώρα και οι συμμετέχοντες στην σκηνή του εγκλήματος.

Φάση πέμπτη: Θωράκιση Επικοινωνίας

Το βήμα αυτό συμβαίνει πριν από τη συλλογή αποδεικτικών στοιχείων. Σε αυτό το στάδιο, πραγματοποιείται η απενεργοποίηση όλων των συσκευών και ο αποκλεισμό τους με οποιαδήποτε δυνατή επικοινωνία ενσύρματα ή ασύρματα. Σε αντίθετη περίπτωση υπάρχει πιθανότητα αλλοίωσης αυτών.

Φάση έκτη: Συλλογή αποδεικτικών στοιχείων

Τα αποδεικτικά στοιχεία που μπορούν να συλλεχθούν από τις ψηφιακές συσκευές διακρίνονται σε δύο κατηγορίες:

• Πτητικές συσκευές

Η απόφαση για το εάν η συλλογή των αποδεικτικών στοιχείων θα γίνει στον τόπο του εγκλήματος ή αργότερα σε ένα ασφαλές εγκληματολογικό εργαστήριο εξαρτάται από την τρέχουσα κατάσταση. Εάν η συσκευή βρίσκεται σε λειτουργία με χρήση μπαταρίας, το σύνολο των πληροφοριών κινδυνεύει να χαθεί σύντομα. Σε αυτή την περίπτωση, θα πρέπει να χρησιμοποιηθεί ο μετασχηματιστής ρεύματος ή να αντικατασταθεί η μπαταρία. Εάν δεν είναι δυνατή η παροχή επαρκούς ηλεκτρικού ρεύματος, η συσκευή πρέπει να απενεργοποιηθεί ώστε να διατηρηθεί η ποσότητα ισχύος της μπαταρίας και το περιεχόμενο της μνήμης. Επίσης η παρουσία του κάθε κακόβουλου λογισμικού που έχει εγκατασταθεί από τον χρήστη, θα πρέπει να ελέγχεται στο παρόν στάδιο.

• Μη -πτητικές συσκευές

Η φάση αυτή περιλαμβάνει τη συλλογή αποδεικτικών στοιχείων από μη-πτητικές συσκευές, όπως MMC cards, compact flash (CF) cards, memory sticks, secure digital (SD) cards, USB memory sticks κα. Επίσης πρέπει να συλλέγονται όλα τα καλώδια τροφοδοσίας και τα λοιπά εξαρτήματα. Τα εργαλεία που χρησιμοποιούνται για τη συλλογή των αποδεικτικών στοιχείων πρέπει να εξασφαλίζουν ότι θα είναι αποδεκτά σε ένα δικαστήριο καθώς θα προστατεύουν την ακεραιότητα και την αυθεντικότητα των συλλεγόμενων στοιχείων. Επίσης θα πρέπει να συλλέγεται και οποιοδήποτε στοιχείο μη-ηλεκτρονικής φύσεως που όμως συνδέεται άμεσα με τις ενδιαφερόμενες μηχανές, όπως σημειώσεις με κωδικούς πρόσβασης, εγχειρίδια λογισμικού και σχετικά έγγραφα, εκτυπώσεις ηλεκτρονικών υπολογιστών κ.α.

Φάση έβδομη: Διατήρηση

Η διατήρηση αποδεικτικών στοιχείων είναι μια άλλη σημαντική πτυχή της εγκληματολογικής έρευνας. Δεδομένης της δυναμικής φύσης των ηλεκτρονικά αποθηκευμένων πληροφοριών και του γεγονότος ότι η καθημερινή λειτουργία των υπολογιστών δύναται να προκαλέσει αλλοίωση , τροποποίηση ή και διαγραφή των πληροφοριών, κρίνεται ως ζωτικής σημασίας η διατήρηση ακέραιων των αποδεικτικών στοιχείων στο πρώιμο στάδιο της έρευνας, ήτοι ο ερευνητής οφείλει να διατηρεί αποδεδειγμένα αναλλοίωτα τα ψηφιακά στοιχεία (Alan & McCort, 2007). Είναι κοινώς αποδεκτό, λοιπόν, ότι οι ψηφιακές αποδείξεις είναι εγγενώς εύθραυστες συγκριτικά με τα ευρήματα των παραδοσιακών ερευνών (Kornblum, 2002). Συγκεκριμένα, τα τρωτά σημεία εντοπίζονται στο γεγονός ότι τα στοιχεία δύνανται να χαθούν κατά τον τερματισμό, οι ψηφιακές αποδείξεις μπορούν να αλλοιωθούν κατά τη συλλογή, ανάλυση και παρουσίασή τους και μάλιστα χωρίς να είναι εύκολο να εντοπισθούν τα ίχνη της αλλοίωσης. Επίσης, είναι δύσκολο να ταυτοποιηθεί ο τελικός χρήστης στα ψηφιακά αποδεικτικά στοιχεία, γεγονός που συνιστά ένα από τα πιο σημαντικά μειονεκτήματά τους.

Τα ψηφιακά στοιχεία πρέπει να προστατεύονται από ιούς, επομένως, οι ερευνητές οφείλουν να αποδεικνύουν ανά πάσα στιγμή ότι αυτά παραμένουν αναλλοίωτα τόσο κατά τη διάρκεια της συλλογής όσο και μεταγενέστερα. Στην υπόθεση Kucala Enterprises, Ltd εναντίον Auto Wax Co., Inc., το δικαστήριο απέρριψε τα αποδεικτικά στοιχεία γιατί ο ενάγων είχε καταστρέψει μέρος αυτών με τη χρήση Eliminator.(Patzakis, 2008).

Η φάση αυτή περιλαμβάνει τη συσκευασία, τη μεταφορά και την αποθήκευση. Κατάλληλες διαδικασίες θα πρέπει να ακολουθούνται και να τεκμηριώνονται για να εξασφαλιστεί ότι τα στοιχεία δεν μεταβλήθηκαν ή καταστράφηκαν. Όλες οι πιθανές πηγές των αποδεικτικών στοιχείων θα πρέπει να προσδιορίζονται και να επισημαίνονται κατάλληλα πριν από την συσκευασία. Η πιο γνωστή διαδικασία που ακολουθείται κατά την καταγραφή των ψηφιακών πειστηρίων είναι η ακόλουθη. Σε κάθε πειστήριο εφαρμόζεται ένας κανόνας «EX-MEDIA» . Ο πρώτος χαρακτήρας είναι «E» όταν πρόκειται για πρωτότυπο πειστήριο ενώ «C» όταν πρόκειται για κλώνο. Ο δεύτερος χαρακτήρας «X» παίρνει τιμές 1, 2, 3..... με βάση την

αρίθμηση των πειστηρίων . Το «MEDIA» σημαίνει ο τύπος του πειστηρίου , δηλαδή HD για σκληρό δίσκο, CD ή DVD για οπτικό ψηφιακό δίσκο, MC για κάρτα μνήμης.
Για παράδειγμα το αναγνωριστικό E1-CD σημαίνει το πρώτο πειστήριο, το οποίο πρόκειται για πρωτότυπο και είναι τύπο cd.

Σε περιπτώσεις ηλεκτρονικών πειστηρίων όπως cd, dvd, κάρτα μνήμης κλπ είναι πολύ σημαντικό να υπολογιστεί και ο μοναδικός αναγνωριστικός αριθμός hash value για κάθε αρχείο. Συνήθως υπολογίζεται αυτός ο αριθμός με τον αλγόριθμο MD-5, αλλά πολλές φορές μπορεί να προκύψουν προβλήματα κατά την διαδικασία του δικαστηρίου, διότι ο αλγόριθμος MD5 είναι δυνατόν για δύο διαφορετικά αρχεία με διαφορετικό περιεχόμενο να δώσει ίδιο hash value αυτό είναι το λεγόμενο «MD5 – collision», γι' αυτό συνήθως χρησιμοποιείται το SHA1. Η χρήση των κοινών πλαστικών σακούλων μπορεί να προκαλέσει στατικό ηλεκτρισμό. Ως εκ τούτου, η χρήση αντιστατικών (anti-static) συσκευασιών είναι απαραίτητη. Επίσης η συσκευασία με τα αποδεικτικά στοιχεία πρέπει να διατηρείται σε δοχείο απομονωμένο από επίδραση ραδιοσυχνότητας για να αποφευχθεί η περαιτέρω επικοινωνία με οποιαδήποτε άλλη συσκευή. Όλα τα δοχεία που περιέχουν αυτές τις σακούλες και τα αποδεικτικά στοιχεία πρέπει επίσης να φέρουν την κατάλληλη σήμανση. Στη συνέχεια τα στοιχεία θα πρέπει να αποθηκεύονται σε ασφαλή χώρο και θα πρέπει να προστατεύονται από τις ηλεκτρομαγνητικές ακτινοβολίες, τη σκόνη, τη θερμότητα και την υγρασία. Μη εξουσιοδοτημένα άτομα θα πρέπει να μην έχουν πρόσβαση στο χώρο αποθήκευσης.

Φάση όγδοη: Εξέταση

Η φάση αυτή περιλαμβάνει την εξέταση του περιεχομένου των αποδεικτικών στοιχείων που συλλέγονται και την εξαγωγή πορίσματος, η οποία είναι κρίσιμη για την απόδειξη της υπόθεσης. Κατάλληλος αριθμός αντιγράφων των αποδεικτικών στοιχείων πρέπει να δημιουργηθεί πριν την εξέταση. Αυτή η φάση στοχεύει στο να καταστήσει τα στοιχεία ορατά, εξηγώντας παράλληλα τη σημασία τους. Τεράστιοι όγκοι δεδομένων που συλλέγονται κατά τη διάρκεια των πτητικών και μη πτητικών φάσεων συλλογής πρέπει να μετατραπούν σε ένα διαχειρίσιμο μέγεθος και σε μορφή ικανή για μελλοντική ανάλυση. Φιλτράρισμα δεδομένων, αναζήτηση συγκεκριμένων λέξεων-κλειδιών σε σχέση με τη φύση του εγκλήματος, ταίριασμα με επιλογές κλπ. είναι μερικά από τα σημαντικά βήματα που εκτελούνται κατά τη διάρκεια αυτής της φάση. Το ημερολόγιο, το πρόγραμμα του υπόπτου, τα μηνύματα κειμένου, τα φωνητικά μηνύματα, τα έγγραφα και τα ηλεκτρονικά ταχυδρομεία είναι μερικές από τις πηγές οι οποίες πρέπει να εξεταστούν λεπτομερώς. Τα δεδομένα πρέπει να ερευνούνται εξονυχιστικά για την ανάκτηση των κωδικών πρόσβασης, την εύρεση κρυφών αρχείων ή καταλόγων, την επέκταση αρχείων κλπ. Επίσης οι πραγματογνώμονες είναι υποχρεωμένοι να αποδεικνύουν ότι τα αποδεικτικά στοιχεία δεν έχουν μεταβληθεί.

Φάση ένατη: Ανάλυση

Σε αυτή την φάση εντοπίζεται η σχέση μεταξύ των δεδομένων, αναλύοντας κρυφά δεδομένα, καθορίζοντας την σημασία των πληροφοριών που λαμβάνονται από την φάση της εξέτασης, ανασυνθέτοντας τα στοιχεία με βάση τα δεδομένα που εξάγονται για να επιτευχθούν ορθά συμπεράσματα κ.λπ. Τα αποτελέσματα της φάσης ανάλυσης μπορεί να δείχνουν την ανάγκη για επιπρόσθετα μέτρα ανάλυσης. Τα αποτελέσματα της ανάλυσης πρέπει να είναι πλήρως και με ακρίβεια τεκμηριωμένα.

Φάση δέκατη: Παρουσίαση

Εφόσον πρόκειται για αστυνομική έρευνα τα πορίσματα πρέπει να παρουσιάζονται σε ένα δικαστήριο. Σε αυτή την φάση πρέπει να επιβεβαιωθεί ή να απορριφθεί ο ισχυρισμός σχετικά με το συγκεκριμένο έγκλημα και την ενοχή του υπόπτου. Τα αποτελέσματα της εξέτασης και της ανάλυσης πρέπει να επανεξετασθούν στο σύνολό τους για να υπάρχει μια πλήρη εικόνα. Μαζί με το πόρισμα, θα πρέπει επίσης να παρουσιαστούν τα αντίγραφα των ψηφιακών στοιχείων, οι εκτυπώσεις των διαφόρων στοιχείων κλπ.

Φάση ενδέκατη: Αποτελέσματα & κριτική

Το τελικό στάδιο είναι της αναθεώρησης. Αυτό περιλαμβάνει την εξέταση όλων των σταδίων της έρευνα και τον εντοπισμό των τομέων βελτίωσης. Στο πλαίσιο της φάσης αναθεώρησης, τα αποτελέσματα και η μεταγενέστερη ερμηνεία τους μπορεί να χρησιμοποιηθεί για την συλλογή, την εξέταση και την ανάλυση των αποδεικτικών στοιχείων σε μελλοντικές έρευνες. Αυτές οι πληροφορίες θα επίσης να συμβάλλουν στην καθιέρωση καλύτερων πολιτικών και διαδικασιών του στο μέλλον.

β. Μεθοδολογία Hershensohn, 2005, Ryder, 2002, Yeager 2006 97

Ταυτοποίηση :
Αναγνωρίζεται το περιστατικό που χρήζει διερεύνησης. Το περιστατικό προκλήθηκε κατόπιν ανίχνευσης ανωμαλιών σε ένα σύστημα. Στο σημείο αυτό συλλέγονται πληροφορίες για το τελεσθέν έγκλημα.
Έρευνα και κατάσχεση στοιχείων :
Στο δεύτερο στάδιο απαιτείται ένταλμα έρευνας και προετοιμασία των κατάλληλων τεχνικών και εργαλείων. Η στρατηγική που θα υιοθετηθεί στόχο έχει να συλλέξει τα περισσότερα στοιχεία χωρίς αυτά να αλλοιωθούν, καθώς, επίσης, και να υπάρχει ο μικρότερος δυνατός αντίκτυπος στο θύμα.
Διατήρηση :
Το ως άνω στάδιο περιλαμβάνει τη λήψη μέτρων για να αποφευχθεί οποιαδήποτε δραστηριότητα που δύναται να βλάψει τις ψηφιακές πληροφορίες που συλλέγονται.
Εξέταση :
Στην εξέταση γίνεται συστηματική αναζήτηση των αποδεικτικών στοιχείων για το περιστατικό που ερευνάται, ήτοι αναζητούνται δισκέτες, σκληροί δίσκοι, ταινίες αντιγράφων ασφαλείας, CD-ROM, καθώς και κάθε άλλο μέσο που χρησιμοποιείται για την αποθήκευση δεδομένων. Τα αντικείμενα δεδομένων μπορεί να περιλαμβάνουν χρονικές σφραγίδες, log files, αρχεία δεδομένων που περιέχουν συγκεκριμένες φράσεις κ.λπ.
Ανάλυση :
Στο στάδιο της ανάλυσης, αναζητούνται οι αποδείξεις για να εντοπιστεί ο δράστης του εγκλήματος. Επίσης, γίνεται ανακατασκευή δεδομένων που ενδεχομένως αλλοιώθηκαν και τελικά διατυπώνονται κάποια συμπεράσματα με βάση τα στοιχεία που συλλέγονται. Αξιοσημείωτο είναι ότι απαιτείται η χρήση εργαλείων και εξειδικευμένων τεχνικών γνώσεων για την αποτελεσματικότητα της διαδικασίας.
Αναφορά :
Συνοψίζοντας παρέχονται κάποια συμπεράσματα σχετικά με την ανάλυση των αποδεικτικών στοιχείων. Και τέλος, ακολουθείται η παρουσίαση αυτών σε συνδυασμό με τις τεχνικές που χρησιμοποιήθηκαν.

3.6 Η ψηφιακή δικανική ως σουρεαλιστική αφήγηση

Υποστηρίζεται από τον Mark Pollitt ότι ο σουρεαλισμός δύναται να ωφελήσει την ψηφιακή δικανική, αξιοποιώντας τις πληροφορίες προκειμένου να εκτελέσει τις εξετάσεις και αναλύσεις πιο αποτελεσματικά και αποδοτικά.

Χρησιμοποιούνται ως βασικές έννοιες η αφήγηση και το μοντάζ, οι οποίες συνιστούν τα ισχυρά εργαλεία της μεθόδου αυτή. Ο σχεδιασμός ενός συστήματος που εκμεταλλεύεται αυτές οι έννοιες απαιτεί κάποιες βασικές αρχές. Πρώτον, τα ηλεκτρονικά δεδομένα πρέπει να

[97] James Tetteh Ami-Narh, Edith Cowan University, Patricia A.H. Williams, Edith Cowan University
2008, Digital forensics and the legal system: A dilemma of our times

αναλυθούν σε αφηγήσεις. Δεύτερον, αυτές οι αφηγήσεις και το πλαίσιο της έρευνας θα πρέπει να κωδικοποιηθεί για να ενεργοποιηθούν υπολογιστικές λύσεις. Τρίτον, είναι απαραίτητο να κατανοήσουμε πως υπάρχουν διαφορετικά επίπεδα αφήγησης. Οι τρεις αυτες αρχές δεν είναι ασήμαντες και απαιτούν πολύ διαφορετικές προσεγγίσεις από εκείνες που παραδοσιακά έχουν χρησιμοποιηθεί στην έρευνα της επιστήμης των υπολογιστών.

Η έννοια της αξιοποίησης των σουρεαλιστικών τεχνικών παιγνίων ως μέθοδο ψηφιακής εγκληματολογικής έρευνας δεν είναι τόσο απίθανη όσο φαίνεται. Οι σουρεαλιστική τεχνικές δεν εξηγούν τη γνωστική λειτουργία, μάλλον, μας παρέχουν έναν ακόμη τρόπο να "διαβάσματος" του σκληρού δίσκου. Τελικά, ο συνδυασμός αφήγησης και μοντάζ μπορεί να οδηγήσει σε ένα νέο είδος τεχνικών ψηφιακής εγκληματολογίας.98

3.7 Προτεινόμενο μοντέλο

Κατόπιν όλων των προεκτεθέντων, διαπιστώνουμε ότι τα περισσότερα πλαίσια αποτελούνται από τις κρίσιμες φάσεις της συλλογής και της διατήρησης των στοιχείων, τη φάση της εξέτασης και ανάλυσης, την τέταρτη φάση της παρουσίασης και αναφοράς και δεν ακολουθούν την πρώτη και την τελευταία, δύο φάσεις που συμβάλλουν σημαντικά στην πληρότητα της έρευνας. Συγκεκριμένα, η πρώτη φάση αποτελεί το προστάδιο για μια σωστή εκκίνηση στην έρευνα, ώστε να υιοθετηθούν οι κατάλληλες διαδικασίες σύμφωνα μην την εκάστοτε περίπτωση και να διαφυλαχθούν τα ευρήματα. Επίσης, η πέμπτη φάση που είναι και η τελευταία, συμβάλλει στη βελτίωση των μετέπειτα ερευνών και πολιτικών.

Προτεινόμενο μοντέλο-συνοψίζοντας όλα τα προηγούμενα

Παρατηρώντας όλα τα προηγούμενα προτεινόμενα πρωτόκολλα ψηφιακής έρευνας, διαπιστώνονται κοινά βήματα, τα οποία είναι αφηρημένα μέχρι ενός σημείου προκειμένου να καλύψουν και να τύχουν εφαρμογής σε όσο το δυνατόν περισσότερα και διαφορετικής φύσης περιστατικά, ώστε τελικά να μην υπάρχει άρρηκτη σύνδεση μιας μεθοδολογίας με συγκεκριμένες και μόνο τεχνολογίες ή εγκλήματα. Η πρόταση ενός κοινού πλαισίου που συγκεντρώνει τις βασικές πτυχές όλων των προηγούμενων, ενώ επίσης περιλαμβάνει και μεθοδολογίες έρευνας της κλασικής εγκληματολογίας δύναται να φανεί χρήσιμη, αφού πετυχαίνει το συγκερασμό της ψηφιακής δικανικής με την κλασική.99 Τα βασικά συστατικά αυτού του μοντέλου περιλαμβάνουν τα ακόλουθα στοιχεία :

1.Αναγνώριση - η αναγνώριση του περιστατικού
2.Προετοιμασία - καθορισμός εργαλείων και τεχνικών, χορήγηση εντάλματος έρευνας και αδειών.
3.Στρατηγική προσέγγιση - Ο στόχος της στρατηγικής είναι να συλλεχθούν ακέραια τα αποδεικτικά στοιχεία, χωρίς να γίνουν νομικές παραβάσεις.
4.Διατήρηση - Σημαντική είναι η ασφαλής διατήρηση της κατάστασης των φυσικών και ψηφιακών αποδεικτικών στοιχείων.
5.Συλλογή - Στο σημείο αυτό καταγράφεται η πραγματική σκηνή και διπλές οι ψηφιακές αποδείξεις χρησιμοποιώντας τυποποιημένες και αποδεκτές διαδικασίες.
6.Εξέταση - Τα ευρήματα εξετάζονται σε βάθος προκειμένου να οριστούν ως αποδεικτικά στοιχεία ή μη και κυρίως για την νομότυπη εξαγωγή τους. Αφού οριοθετηθούν τα αποδεικτικά στοιχεία κατασκευάζεται μια λεπτομερής τεκμηρίωσης για ανάλυση.

[98] Mark Pollitt , Digital forensics as a surreal narrative
[99]FBI Crime Scene Search. http://www.fbi.gov/hq/lab/handbook/scene1.htm

7.Ανάλυση - Αναλύονται τα ευρήματα και εξάγονται συμπεράσματα για τα αποδεικτικά στοιχεία. Το στάδιο αυτό απαιτεί υψηλές τεχνικές δεξιότητες.
8.Παρουσίαση - Σε αυτό το σημείο συνοψίζονται τα συμπεράσματα και παρέχονται εξηγήσεις σχετικά με τα αποδεικτικά στοιχεία.
9.Επιστροφή ευρημάτων - Επιστρέφονται τα φυσικά στοιχεία στον ιδιοκτήτη τους, αναλόγως με το αποτέλεσμα. Πρόκειται για ένα στάδιο που δεν υιοθετείται, ωστόσο, συχνά.

Τα παραπάνω βήματα συμφωνούν σε μεγάλο βαθμό με τις παραδοσιακές μεθόδους που χρησιμοποιούνται για τη νομότυπη συλλογή των φυσικών αποδείξεων. «Ένα μεγάλο σώμα των αποδεδειγμένων τεχνικών έρευνας υπάρχει στους παραδοσιακούς κλάδους της εγκληματολογίας κλάδους. Ωστόσο, οι περισσότεροι αν και έχουν τύχει εφαρμογής στον κυβερνοχώρο, δεν έχουν ακόμη ληφθεί σοβαρά υπόψη». 100 Αξιοσημείωτο είναι ότι στα παραπάνω βήματα, δημιουργείται μια τυποποιημένη διαδικασία χωρίς να προσδιορίζει συγκεκριμένα εγκλήματα και τεχνολογίες. Ο αφηρημένος τρόπος προσδιορισμού του πρωτοκόλλου, επιτρέπει τη χρήση του σε πολλά διαφορετικά μεταξύ τους περιστατικά. Αυτό το μοντέλο δύναται να χρησιμοποιηθεί ακόμη και σε μελλοντικές διαφοροποιημένες τεχνολογίες. Αυτό το πλαίσιο θεωρείται ότι ενισχύει την επιστήμη της εγκληματολογίας καθότι παρέχει τα θεμέλια για την ανάλυση ακόμη και κάποιας νέας ψηφιακής εγκληματολογίας, ενώ παράλληλα δίνει τη δυνατότητα να χρησιμοποιείται ένα κοινό πλαίσιο με στόχο τις νομότυπες διαδικασίες κατά τη διάρκεια της έρευνας.

3.8 Ρόλοι σε μια διαδικασία ψηφιακής εγκληματολογίας

Σε μια τυπική έρευνα ψηφιακής εγκληματολογίας, αναμένεται να συμμετέχουν τόσο τεχνικοί όσο και νομικοί σύμβουλοι. Ωστόσο, αν διαχωριστούν περαιτέρω οι ρόλοι και οι αρμοδιότητες αυτών των συμμετεχόντων, θα μπορούσαν να ταξινομηθούν σε οκτώ επιμέρους ρόλους. Αυτοί οι ρόλοι είναι διαφορετικής φύσης, ωστόσο, είναι δυνατό να συγκεντρωθούν όλες οι αρμοδιότητες στο ίδιο πρόσωπο, εφόσον αυτό απαιτείται.

Πιο συγκεκριμένα οι ρόλοι διακρίνονται στους κάτωθι:
1. Υπεύθυνος έρευνας
2. Νομικός σύμβουλος
4. Ελεγκτής συστήματος
5. Ειδικός ψηφιακής εγκληματολογίας
6. Ερευνητής ψηφιακής εγκληματολογίας
7. Αναλυτής ψηφιακής εγκληματολογίας
8. Εισαγγελέας

[100]Digital Forensics Research Workshop. “A Road Map for Digital Forensics Research” 2001. www.dfrws.org

Κεφάλαιο 4

4.1 Προτεινόμενα έγγραφα

Παρακάτω παρατίθενται προτεινόμενη μορφή εγγράφων που κρίνεται σκόπιμο να συμπληρώνονται κατά τη διεξαγωγή οποιασδήποτε έρευνας, προκειμένου να αποτυπώνονται εγγράφως οι ενέργειες που έλαβαν χώρα, με ακριβή χρονική σειρά, ώστε να δύνανται αφενός να αξιοποιηθούν δικαστηριακά εάν κριθεί απαραίτητο, και αφετέρου να αποδεικνύεται η σύννομη πορεία της έρευνας.

ΕΚΘΕΣΗ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΠΕΡΙΣΤΑΤΙΚΟΥ ΑΣΦΑΛΕΙΑΣ
Στον ..... σήμερα την ..... ημέρα ..... και ώρα ..... ο υπογράφων ……μέλος της Ομάδας Αντιμετ.ώπισης Περιστατικών του Γενικού Επιτελείου
Στρατου……..... παρουσιάστηκε το κάτωθι περιγραφόμενο περιστατικό
:……
……
……
Ενεργήσαμε ως εξής και παρατηρήσαμε ότι :
.....
.....
.....
.....
.....
.....
.....
.....
....
....
.....
Η αντιμετώπιση του παραπάνω περιστατικού άρχισε στις ..... και τελείωσε στις .....
Για τούτο συντάχθηκε η έκθεση αυτή και υπογράφεται.
Ο Διοικητής

…….

Ο επικεφαλής της Ομάδας Αντιμετώπισης Περιστατικών ασφαλείας

…….

ΕΚΘΕΣΗ ΠΡΑΓΜΑΤΟΓΝΩΜΟΣΥΝΗΣ

Στον ..... σήμερα την ..... ημέρα ..... και ώρα ..... οι υπογράφοντες..... .....
.....
……
…… ως μέλη της Ομάδας Αντιμετώπισης Περιστατικών Ασφαλείας του Γενικού Επιτελείου Στρατού.
Αφού παραλάβαμε τα .....
.....
.....
.....και μετά από επισταμένη εξέταση σύμφωνα με τα άρθρα 183 και εξής του Κ.Π.Δ. και με βάση τα ερωτήματα που μας τέθηκαν, παρατηρήσαμε .....
....
....
Επομένως, καταλήγουμε στα κάτωθι συμπεράσματα :
.....
……
……
……
……

Ο Διοικητής
……..
Ο επικεφαλής της Ομάδας Αντιμετώπισης Περιστατικών
……..

ΕΚΘΕΣΗ ΠΑΡΑΔΟΣΗΣ ΠΡΑΓΜΑΤΟΓΝΩΜΟΣΥΝΗΣ

Η έκθεση αυτή παραδόθηκε στον κ .... σήμερα την ..... ημέρα ..... και ώρα ....., παρισταμένου και του κ. ..... από εμάς τους ιδίους τους
....και τους βεβαιώσαμε και προφορικά για το περιεχόμενό της.

Για το σκοπό αυτό συντάχθηκε η παρούσα, η οποία διαβάστηκε παρουσία των ως άνω και υπογράφεται:

Ο Διευθυντής

Ο Διοικητής

Ο επικεφαλης της Ο.Α.Π.Α. του Γ.Ε.Σ.

Επίλογος

Τα τελευταία χρόνια η χρήση των ηλεκτρονικών υπολογιστών προκάλεσε μια ανυπολόγιστη αύξηση των εγκλημάτων που τελούνται μέσω ηλεκτρονικού υπολογιστή, αλλά οδήγησε και σε νέες μορφές εγκληματικής δράσης. Η δημιουργία εργαστηρίων ψηφιακής εγκληματολογίας κυρίως σε περιβάλλοντα που διακινούνται απόρρητες πληροφορίες, όπως είναι το στρατιωτικό περιβάλλον, συνιστά αδήριτη ανάγκη. Εξετάσαμε τοζήτημα της φορητότητας, της συνδεσιμότητας των συστημάτων πληροφορικής και γενικότερα ότι το ηλεκτρονικό έγκλημα τελείται οπουδήποτε, γεγονός που επισύρει προβληματισμούς σχετικά με την κατά τόπον αρμοδιότητα. Το διεθνές δίκαιο προβλέπει ορισμένες βάσεις για τη δικαιοδοσία σχετικά με πράξεις εγκληματικότητας στον κυβερνοχώρο, που περιλαμβάνει πρωτίστως την εθνικότητα. Σχετικά με τη δικαστική συνδρομή για την επίλυση των δυσκολιών, έχουν θεσπιστεί οι διμερείς συμβάσεις, όπως η Ευρωπαϊκή Σύμβαση περί Εκδόσεως Εγκληματιών της 13-12-1957 και το από 20-4-1959 συμπλήρωμά της, η Ευρωπαϊκή Σύμβαση περί Αμοιβαίας Δικαστικής Συνδρομής επί Ποινικών Υποθέσεων, καθώς και τα δύο πρόσθετα πρωτόκολλά της. Ωστόσο, δεδομένου ότι το ηλεκτρονικό έγκλημα εξελίσσεται σε ένα παγκόσμιο επίπεδο, διαπιστώνεται ότι χρειάζεται διεθνής συνεργασία και όχι μόνο σε ευρωπαϊκό επίπεδο. Είναι βέβαιο, ότι οι διωκτικές αρχές, οι δικαστικές αρχές και συνακόλουθα και ο στρατός αδυνατεί να επιλύσει τα όποια συμβάντα ανακύπτουν, ενόσω πρόκειται για διασυνοριακή εγκληματικότητα, χωρίς μια συνεργασία σε παγκόσμιο επίπεδο. Ως αποτέλεσμα αυτής της διαπίστωσης, είναι η ευρωπαϊκή προσπάθεια για επίτευξη συνεργασίας σε διεθνές επίπεδο με στόχο την καταπολέμηση των διασυνοριακών μορφών εγκληματικότητας. Στο πλαίσιο αυτό διατυπώνονται νέα συμβατικά κείμενα, προκειμένου να καλύψουν ανακύπτοντα κενά και να διορθώσουν πρακτικά προβλήματα.

Μάλιστα, τον Ιούνιο του 2016, οι Υπουργοί του Συμβουλίου Δικαιοσύνης και Εσωτερικών Υποθέσεων συνέστησαν να μεταρρυθμιστούν οι διαδικασίες αυτές, με σκοπό την αμεσότερη ανταλλαγή ηλεκτρονικών αποδεικτικών στοιχείων. Η προσέγγιση μιας τέτοιας μεταρρυθμιστικής προσπάθειας θα μπορούσε να είναι είτε αποκεντρωμένη είναι κεντρική, συγκεκριμένα, θα μπορούσε η κεντρική πύλη της ΕΕ να λειτουργεί ως κέντρο επεξεργασίας αιτήσεων αμοιβαίας δικαστικής συνδρομής με μία κεντρική εγκατάσταση αποθήκευσης ψηφιακών αποδεικτικών στοιχείων ή θα μπορούσε να υιοθετηθεί μια εφαρμογή αναφοράς για τις αιτήσεις, η οποία θα εγκαθίσταται χωριστά στα κράτη-μέλη, παρέχοντας αναφορά για τη μονάδα αποθήκευσης. Τα εμπόδια που τίθενται σχετικά με την πρόσβαση στα ψηφιακά πειστήρια δύνανται να περιπλέξουν τις έρευνες, δεδομένου ότι η απόκτησή τους θέτει ζητήματα διασυνοριακά. Οι αρχές , επομένως, χρειάζεται να βασίζονται σε μηχανισμούς δικαστικής συνεργασίας όπως είναι η αμοιβαία δικαστική συνδρομή, ή η αμοιβαία αναγνώριση στην Ευρωπαϊκή Ένωση, με άμεση συνεργασία των παρόχων και άμεση πρόσβαση στις ηλεκτρονικές πληροφορίες.[101]

[101] Technical Document: Measures to improve cross-border access to electronic evidence for criminal investigations following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace

Η διασυνοριακή πρόσβαση στα ψηφιακά πειστήρια δύναται να επιτευχθεί με τρεις τρόπους, είτε μέσω διαύλων συνεργασίας μεταξύ των αρμόδιων αρχών των εμπλεκόμενων χωρών (συνήθως μέσω της δικαστικής συνδρομής ή μέσω συνεργασίας της αστυνομίας των χωρών), είτε μέσω της άμεσης συνεργασίας μεταξύ των αρχών επιβολής του νόμου μια χώρας, σε εθελοντική ή υποχρεωτική βάση. Το γεγονός ότι ορισμένα κράτη μέλη και τρίτες χώρες έχουν αναπτύξει ή αναπτύσσουν εθνικές λύσεις, είναι πολύ πιθανό να δημιουργήσουν αβεβαιότητα στο νομικό πλαίσιο που αφορά στις αρχές και τους παρόχους.[102] Συνεπώς, η Επιτροπή εύλογα ξεκίνησε μια διαδικασία εμπειρογνωμοσύνης με ευρύ φάσμα ενδιαφερομένων, συμπεριλαμβανομένων και των υπουργείων δικαιοσύνης των κρατών-μελών, τις αρχές επιβολής του νόμου και του ακαδημαϊκού τομέα, προκειμένου να μεταρρυθμιστεί το πλαίσιο της δικαστικής συνδρομής σύμφωνα με τις σύγχρονες επιταγές.

Επιπρόσθετα, εξετάσαμε το ζήτημα του εντοπισμού των εγκληματιών στον κυβερνοχώρο, το οποίο βασίζεται σχεδόν αποκλειστικά σε ψηφιακά στοιχεία, μάλιστα, η διεύθυνση IP αποτελεί την κύρια πηγή αναγνώρισης των εγκληματιών στον κυβερνοχώρο. Το νομικό πλαίσιο που εφαρμόζεται στις διευθύνσεις IP σχετίζεται με το διττό χαρακτήρα των διευθύνσεων αυτών, ήτοι προστατεύονται τόσο με βάση το νόμο για τα δεδομένα προσωπικού χαρακτήρα, όσο και με βάση την προστασία του απορρήτου της επικοινωνίας. Η διπλή ταυτότητα που φαίνεται να διατίθεται από τη νομοθεσία της ΕΕ για το ιδιωτικό απόρρητο σε διευθύνσεις IP έχει ως αποτέλεσμα την ταυτόχρονη εφαρμογή διαφορετικών νομικών πηγών και κανόνων, γεγονός που περιπλέκει ακόμη περισσότερο το ζήτημα του προσδιορισμού της νομικής φύσης της διεύθυνσης IP και συνεπώς παρεμβαίνει επιβολή του νόμου.

Αξιοσημείωτο είναι το ζήτημα που προκύπτει στην περίπτωση συμμετοχής ιδιωτών και στρατιωτικών στο ίδιο έγκλημα, όπου καταλήξαμε σύμφωνα με τις διατάξεις 195 και 197 παρ.2 του Σ.Π.Κ, ότι αποκλείεται η υπαγωγή ιδιωτών στην αρμοδιότητα στρατιωτικών ποινικών δικαστηρίων. Το ίδιο ισχύει και για την διάταξη του άρθρου 197 παρ.1 του ιδίου Κώδικα που ρυθμίζει την αρμοδιότητα σε περίπτωση συρροής εγκλημάτων, ορισμένα εκ των οποίων υπάγονται στην αρμοδιότητα των κοινών ποινικών δικαστηρίων και ορισμένα στην αρμοδιότητα των στρατιωτικών δικαστηρίων.

Αφού παρουσιάστηκε το νομικό πλαίσιο σχετικά με το ηλεκτρονικό έγκλημα και εκτέθηκαν μερικοί σημαντικοί προβληματισμοί προκειμένου να εξαχθεί κάποιο συμπέρασμα όπως και έγινε, στο τρίτο κεφάλαιο έγινε λόγος για τις μεθόδους εξιχνίασής τους με σύννομες διαδικασίες. Μάλιστα, διαπιστώθηκε ότι τα περισσότερα πλαίσια αποτελούνται από τις κρίσιμες φάσεις της συλλογής και της διατήρησης των στοιχείων, τη φάση της εξέτασης και ανάλυσης, την τέταρτη φάση της παρουσίασης και αναφοράς και δεν ακολουθούν την πρώτη και την τελευταία, δύο φάσεις που συμβάλλουν σημαντικά στην πληρότητα της έρευνας. Αναφέροντας προτεινόμενα πρωτόκολλα ψηφιακής έρευνας, καταλήξαμε στην παρουσίαση ενός κοινού πλαισίου που συγκεντρώνει τις βασικές πτυχές όλων των προηγούμενων, ενώ επίσης περιλαμβάνει και μεθοδολογίες έρευνας της κλασικής εγκληματολογίας, η οποία δύναται να φανεί χρήσιμη, αφού πετυχαίνει το συγκερασμό της ψηφιακής δικανικής με την κλασική.

Τέλος, κρίναμε σημαντικό να προτείνουμε κάποια έγγραφα που δύνανται να συνοδεύουν τη διεξαγωγή της έρευνας, προκειμένου να διασφαλίζεται η σύννομη πορεία των ενεργειών και να αποδεικνύονται με χρονική ακολουθία οι έλεγχοι που διενεργήθηκαν.

[102] Non-paper from the Commission services, This document is a document prepared by the Commission services and cannot be considered as stating an official position of the Commission, 2017

Βιβλιογραφία

1.Απόφαση 984/2013, Άρειος Πάγος

2.Διονύσιος Δ. Σπινέλλης, «Η δικαστική συνεργασία σε ποινικές υποθέσεις στην Ευρώπη και ειδικότερα η ευρωπαϊκή εντολή έρευνας», Ιανουάριος 2016

3.Επιστημονική Διεύθυνση: Ένωση Ελλήνων Νομικών e-ΘΕΜΙΣ , «Αντιμέτωποι με τις σύγχρονες τεχνολογικές εξελίξεις»

4.Επιστημονική Διεύθυνση: Ένωση Ελλήνων Νομικών e-ΘΕΜΙΣ, «LegalTech & Data Protection» (4ο Πανελλήνιο Συνέδριο)

5.Ιγγλεζάκης, «Επιτήρηση και παρακολούθηση των τηλεπικοινωνιών στο χώρο εργασίας», υποσημείωση 16, ΔιΜΕΕ 2005.

6.Κων/νος Λαμπρινουδάκης, Λίλιαν Μήτρου, Στέφανος Γκρίτζαλης, Σωκράτης Κάτσικας, «Προστασία της ιδιωτικότητας & Τεχνολογίες Πληροφορικής και επικοινωνιών . Τεχνικά και νομικά θέματα».

7.Ν. Αντωνίου, Ε. Βαγενά, Μ. Ζούλοβιτς, Π. Καλαμπούκα-Γιαννοπούλου, Χρ. Καπαρτζιάνη, Λ. Κοτσίρης, Σπ. Λειβαδόπουλος, Κ. Μαργέλλου, Ε. Παναγιωτίδου, Φ. Παναγοπούλου - Κουτνατζή, Γ. Παπαδόπουλος, Α. Παπαθανασίου, Α. Παπακωνσταντίνου, Β. Παπακωνσταντίνου, Ε. Περάκης, Γ. Ραυτογιάννης, Κ. Ρόκας, Β. Σαμαρτζή, Σ. Τάσσης, Π. Τσουγκριάνης, Β. Τσουκαλά, Γ. Φιτσιάλος, Θ. Χίου, «Innovation law»

8.Alexios Mylonas, Vasilis Meletiadis, Lilian Mitrou, Dimitris Gritzalis, «Smartphone sensor data as digital evidence».

9.A. Mylonas et al, «Dynamic Evidence Acquisition for Smartphone Forensics», inProc. of the 27th IFIP International Information Security and Privacy Conference, Springer (IFIP AICT376), Greece., June 2012.

10.Alberto R. Gonzales, Regina B. Schofield, David W. Hagy, US. Department of Justice, «Special Report on Investigations Involving the Internet and Computer Networks», January 2007

11.Article22(5)of the Council of Europe Cybercrime Conventionor Article 10(4) of the Decision on Attacks against Information System

12.Brian Carrier, «Open Source Digital Forensics Tools: The Legal Argument», October 2002

13.Cameron S.D. Brown, «Investigating and Prosecuting Cyber Crime. Forensic, Dependencies and Barriers to Justice», 9(1) Intl. J. Cyber Criminology 83, January–June 2015

14.Cameron S.D. Brown, «Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice», 9(1) Intl. J. Cyber Criminology 86, January–June 2015.

15.C. Blackwell, G.Peterson&S.Shenoieds, «An Investigative Framework for Incident Analysis In Advances in Digital Forensics»,PartVII,22,2011.

16.Digital Forensics Research Workshop. «A Road Map for Digital Forensics Research» 2001. www.dfrws.org(last retrieved 4/2015)

17.EnCase Legal Journal, Second Edition. March 2002, Guidance Software. Available at: http://www.encase.com/support/downloads/LegalJournal.pdf(last retrieved 4/2016)

18.ENISA, Electronic Evidence – a Basic Guide for First Responders, 4, 2014

19.FBI Crime Scene Search. http://www.fbi.gov/hq/lab/handbook/scene1.htm(last retrieved 4/2017)

20.Forza , «Digital forensics investigation framework that incorporate legal issues».

21.Frayssinet, in: Lucas, Frayssinet, Deveze, «Droit de l'informatique et de l'Internet», 78 J, 2001.

22.Ioannis Iglezakis, Philippe Jougleux, Lilian Mitrou, Tatiana-Eleni Synodinou, «The Legal Regulation of Cyber Attacks».

23.ISACA, Information Security, Audit and Control Association (ISACA). COBIT 3rd Edition Control Objectives. http://isaca.org, July 2000, (last retrieved 4/2015)

24.ISO/IEC 17799. 2005, Information Technology – Security techniques – Codes of Practice for information security management. International Organisation for Standardization and the International Electrotechnical Commission.

25.James Holley, «Computer Forensics Market Survey», SC Magazine September 2000 , Available at: http://www.scmagazine.com/scmagazine/2000_09/survey/survey.html

26.James Tetteh Ami-Narh , Edith Cowan University , Patricia A.H. Williams , Edith Cowan University, «Digital forensics and the legal system: A dilemma of our times».

27.JCSNS International Journal of Computer Science and Network Security, VOL.8 No.10, October 2008

28.Van Solms, SH. and Lourens, CP. IFIP 11.9, «A Control Framework for Digital Forensics», 2006

29.Sydney Liles, Marcus Rogers and Marianne Hoebich, «A survey of legal issues facing digital forensic experts», Chapter 20

30.Maria Karyda and Lilian Mitrou, «Internet Forensics: Legal and Technical Issues».

31.Maria Angela Biasiotti, «The evidence project will be part of the DG Home Annual Report as a 'success story'», 2017

32.Mark Pollitt, «Digital forensics as a surreal narrative».

33.Mark Reith, Clint Carr, Gregg Gunsch Department of Electrical and Computer Engineering Graduate School of Engineering and Management Air Force Institute of Technology Wright-Patterson AFB, «An Examination of Digital Forensic Models», OH 45433-7765

34.Mark Reith, Clint Carr, Gregg Gunsch Department of Electrical and Computer Engineering Graduate School of Engineering and Management Air Force Institute of Technology Wright-Patterson AFB Bernd Hecker, in: Kai Amboss (Hg), Europäisches Strafrecht post Lissabon, στο Europäisches Strafrecht post Lissabon, «An Examination of Digital Forensic Models», International Journal of Digital Evidence Fall 2002, Volume 1, Issue 3, σ. 15

35.Michael Kohn1, JHP Eloff2 and MS Olivier, «Framework for a Digital Forensic Investigation».

36.NIST, Computer Forensics Tool Testing, Available at http://www.cftt.nist.gov/ (last retrieved 4/2017)

37.Non-paper from the Commission services, «This document is a document prepared by the Commission services and cannot be considered as stating an official position of the Commission», 2017

38.Simson L. Garfinkel Valightml, Naval Postgraduate School, Monterey, USA, , «Digital forensics research: The next 10 years», 2 August 2010

39.Siti Rahayu Selamat1, Robiah Yusof2, Shahrin Sahib3, Faculty of Information Technology and Communication, University Teknikal Malaysia Melaka, Ayer Keroh, Melaka, Malaysia, «Mapping Process of Digital Forensic Investigation Framework»

40.Technical Document: «Measures to improve cross-border access to electronic evidence for criminal investigations following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace»

41.http://www.cybercrimejournal.com/broadhurstetalijcc2014vol8issue1.pdf (last retrieved 9/2016)

42.http://www.britannica.com/EBchecked/topic/1017431/phishing(last retrieved 8/2016)

43.http://www.reuters.com/article/2014/06/09/us-cybersecurity-mcafee-csis-idUSKBN0EK0SV20140609 (last retrieved 8/2016)

44.http://www.usnews.com/news/articles/2014/06/09/study-hackers-cost-more-than-445-billion-annually (last retrieved 8/2016)

45.http://internet-safety.sch.gr/index.php/ekp/171-chprn(last retrieved 8/2016)

46.http://www.emc.com/collateral/white-paper/rsa-cyber-crime-report-0414.pdf (last retrieved 9/2016)

47.http://www.webopedia.com/TERM/S/software_piracy.html(last retrieved 9/2016)

48.http://resources.infosecinstitute.com/dangerous-ddos-distributed-denial-of-service-on-the-rise/(last retrieved 9/2016)

49.http://krebsonsecurity.com/all-about-skimmers (last retrieved 12/2016)

50.http://www.computerforensicsspecialists.co.uk/blog/what-is-volatile-data (last retrieved 10/2016)

51.http://us.norton.com/cyberstalking/article(last retrieved 10/2016)

52.http://www.pcmag.com/encyclopedia/term/51693/software-piracy(last retrieved 10/2016)

53.https://www.europol.europa.eu/content/organised-crime-groups-exploiting-hidden-internet-online-criminal-service-industr(last retrieved 4/2017)

54.http://resources.infosecinstitute.com/cybercrime-as-a-service/(last retrieved 4/2017)

55.http://www.scmagazineuk.com/cybercrime-as-a-service-the-new-criminal-business-model/article/374124/(last retrieved 4/2017)

56.http://readwrite.com/2012/11/15/botclouds-how-botnets-now-offer-crime-as-a-service(last retrieved 5/2015)

57.http://www.computing.co.uk/ctg/news/2372724/-crime-as-a-service-exploited-by-criminal-gangs-warns-europol-iocta-report(last retrieved 4/2017)

58.http://www.statetechmagazine.com/article/2012/11/why-crime-service-next-big-cybersecurity-threat(last retrieved 5/2015)

59.http://www.computerweekly.com/news/2240231663/Service-model-driving-cyber-crime-says-Europol-report(last retrieved 4/2017)

60.http://www.cyberskillscentre.com/crime-service-lowers-entry-barriers-cybercrime-world/(last retrieved 4/2017)

61.http://securityaffairs.co/wordpress/28750/cyber-crime/europol-i2014-iocta-report.html(last retrieved 5/2015)

62.http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG(last retrieved 4/2017)

63.http://aut.researchgateway.ac.nz/bitstream/handle/10292/1633/Frantzeskou%2c%20Gritzalis%20and%20MacDonell%20%282004%29%20ICETE.pdf?sequence=2&isAllowed=y
http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime(last retrieved 4/2017)
64.https://blog.malwarebytes.org/intelligence/2013/10/cryptolocker-ransomware-what-you-need-to-know/(last retrieved 5/2015)

65.http://tech.in.gr/consult/article/?aid=1231103537(last retrieved 4/2017)

66.http://www.haltabuse.org/(last retrieved 4/2017)

67.http://threatpost.com/how-much-does-botnet-cost-022813/77573

68.http://www.nist.gov/forensics/mobile_forensics2.cfm(last retrieved 4/2017)

69.http://cgi.di.uoa.gr/~xenakis/Published/53-COSE-2014/Mobile-forensics.pdf(last retrieved 5/2015)

70.http://en.wikipedia....puter_forensics(last retrieved 5/2016)

71.http://www.fbi.gov/a...00/computer.htm(last retrieved 4/2015)

72.https://e-justice.europa.eu/content_request_for_judicial_assistance-91-el.do (last retrieved 4/2017)

73.http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=48&Itemid=39&lang(last retrieved 5/2016)

74.https://e-justice.europa.eu/content_eurojust-23-el.do (last retrieved 4/2017)

75.https://ccdcoe.org/transborder-data-access-quo-vadis-council-europe.html (last retrieved 4/2017)

76.http://www.coe.int/en/web/corruption/home(last retrieved 4/2017)