ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΚΑΙ ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ ΤΜΗΜΑ ΝΟΜΙΚΗΣ

“Ψηφιακά πειστήρια και αποδεικτικές απαγορεύσεις στην ποινική δίκη σε εθνικό και υπερεθνικό επίπεδο”

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ ΤΗΣ

Ελπίδας Γ. Ματάμη

ΘΕΣΣΑΛΟΝΙΚΗ, ΦΕΒΡΟΥΆΡΙΟΣ 2022

“Ψηφιακά πειστήρια και αποδεικτικές απαγορεύσεις στην ποινική δίκη σε εθνικό και υπερεθνικό επίπεδο”

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ ΤΗΣ

Ελπίδας Γ. Ματάμη

ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΦΟΙΤΗΤΡΙΑΣ

ΑΠΟΦΟΙΤΟΥ ΝΟΜΙΚΗΣ ΣΧΟΛΗΣ ΑΠΘ (2017)

ΥΠΟΒΑΛΛΟΜΕΝΗ ΠΡΟΣ ΜΕΡΙΚΗ ΕΚΠΛΗΡΩΣΗ ΤΩΝ ΑΠΑΙΤΗΣΕΩΝ ΤΟΥ

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ “ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ”

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ

ΘΕΟΧΑΡΗΣ Ι. ΔΑΛΑΚΟΥΡΑΣ

ΕΓΚΡΙΘΗΚΕ ΑΠΟ ΤΡΙΜΕΛΗ ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ ΤΗΝ

……../……/2022

ΟΝΟΜΑΤΕΠΩΝΥΜΟ 1	ΟΝΟΜΑΤΕΠΩΝΥΜΟ 2	ΟΝΟΜΑΤΕΠΩΝΥΜΟ 3
……	……	……

ΜΑΤΑΜΗ Γ. ΕΛΠΙΔΑ

(Υπογραφή) .....

ΜΑΤΑΜΗ ΕΛΠΙΔΑ

Δικηγόρος, Απόφοιτος Νομικής Σχολής ΑΠΘ, Μεταπτυχιακή Φοιτήτρια ΔΠΜΣ Δίκαιο και Πληροφορική, (ΠΑΜΑΚ - Νομική σχολή ΔΠΘ)

Αφιερωμένη,

Στους αγαπημένους μου γονείς μου

Γιώργο και Δήμητρα

για όλα όσα έκαναν προκειμένου

να φτάσω ως εδώ σήμερα

Θεσσαλονίκη 2022,

Ελπίδα Γ. Ματάμη

ΠΡΟΛΟΓΟΣ - ΕΥΧΑΡΙΣΤΙΕΣ

Ως μεταπτυχιακή φοιτήτρια του Διϊδρυματικού Προγράμματος Μεταπτυχιακών Σπουδών (ΔΠΜΣ) «Δίκαιο και Πληροφορική», πλησιάζοντας πλέον προς το τέλος αυτής της διαδρομής νιώθω την ανάγκη να ευχαριστήσω ορισμένα πρόσωπα, που υπήρξαν αρωγοί στην διαδρομή αυτή. Για αρχή θα ήθελα να ευχαριστήσω τη Διευθύντρια του Προγράμματος και Καθηγήτρια μου ***κα Αλεξανδροπούλου – Αιγυπτίαδου Ευγενία,*** *αλλά και όλους τους διδάσκοντες για υποστήριξη, την καθοδήγηση, και τις πολύτιμες γνώσεις που μου παρείχαν καθ' όλη την διάρκεια της φοίτησης μου.*

Εν συνεχεία, νιώθω την ηθική υποχρέωση να θα ευχαριστήσω ξεχωριστά τον επιβλέποντα Καθηγητή κ. ***Δαλακούρα Θεοχάρη,*** *ειδικότερα για την υποστήριξή του κατά την εκπόνηση της παρούσας διπλωματικής εργασίας και γενικότερα για τις πολύτιμες γνώσεις που μου παρείχε καθ' όλη τη διάρκεια των μεταπτυχιακών μου σπουδών.*

Το πιο μεγάλο ευχαριστώ όμως νιώθω ότι οφείλω στους αγαπημένους μου ***γονείς*** *, Γιώργο και Δήμητρα* ***και στην αδερφή μου*** *Αγγελική, οι οποίοι βρίσκονται πάντα στο πλευρό μου και δεν παραλείπουν να με στηρίζουν σε κάθε μου βήμα.*

Δεν μπορώ βέβαια να παραλείψω να ευχαριστήσω ***τις φίλες μου,*** *Μαρία και Λίνα, οι οποίες στήριξαν με τον δικό τους τρόπο, μέσα από πολύωρες συζητήσεις μας στην εκπόνηση της παρούσας.Τέλος ένα μεγάλο ευχαριστώ οφείλω στον Δημήτρη, για την σημαντική ψυχολογική στήριξη που μου παρείχε ώστε να καταφέρω πράγματι να ολοκληρώσω την παρούσα, ανταποκρινόμενη στην πίεση των τελευταίων ημερών.*

ΠΕΡΙΛΗΨΗ

Ο ρυθμός εξέλιξης της τεχνολογίας, σε συνάρτηση με την διαρκώς αυξανόμενη ενσωμάτωση αυτής στην εγκληματική δράση, έχουν καταστήσει τη συλλογή και ανάλυση των ψηφιακών δεδομένων, σημαντικό εργαλείο για τις ανακριτικές αρχές. Οι προκλήσεις στον τομέα της ψηφιακής Εγκληματολογίας είναι πολλές και ενδεικτικά θα μπορούσαν να κατηγοριοποιηθούν σε τεχνικές, επιχειρησιακές και νομικές. Δεν έχει έως σήμερα κατοχυρωθεί παγκοσμίως μια κοινά αποδεκτή μεθοδολογία ψηφιακής εγκληματολογίας. Τα προτεινόμενα στην βιβλιογραφία μοντέλα ποικίλλουν, ωστόσο οι παραλλαγές αυτών παρουσιάζουν κάποια κοινά βασικά βήματα και διαδικασίες.

Σε εθνικό επίπεδο, με τον νέο Κώδικα Ποινικής δικονομίας θεσμοθετήθηκε για πρώτη φορά η κατάσχεση ψηφιακών πειστηρίων, με το άρθρο 265. Νομοθετικό φραγμό στην προσπάθεια αναζήτησης της αντικειμενικής αλήθειας μέσω των διενεργούμενων ανακριτικών πράξεων, αποτελούν οι αποδεικτικές απαγορεύσεις, ως εξαίρεση στον κανόνα της ηθικής απόδειξης. Τα ψηφιακά πειστήρια που κατάσχονται, δηλαδή αφαιρούνται, αντιγράφονται και επαληθεύονται κατά παράβαση του νόμου, οδηγούν σε αποδεικτική απαγόρευση.

Σε υπερεθνικό επίπεδο, τόσο η “CLOUD ACT” των ΗΠΑ όσο και η Ευρωπαϊκή πρόταση “E-Evidence”, επιδιώκουν να ανταποκριθούν στην αυξανόμενη ψηφιοποίηση των πληροφοριών, στον ρόλο τρίτων παρόχων στον έλεγχο αυτών και στο γεγονός ότι οι πάροχοι και τα δεδομένα ενδιαφέροντος διατηρούνται ολοένα και περισσότερο εκτός συνόρων.

Με την παρούσα μελέτη επιχειρείται η υπαγωγή των πραγματοποιηθέντων σε εθνικό και υπερεθνικό επίπεδο νομοθετικών κινήσεων, στις υφιστάμενες στον χώρο της ψηφιακής εγκληματολογίας προκλήσεις· η αξιολόγηση αυτών με γνώμονα τα υποστηριζόμενα από την θεωρία μοντέλα και τις αρχές που αυτά έχουν διαμορφώσει· και τέλος η άσκηση κριτικής με σκοπό την πλήρωση νομοθετικών κενών.

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: ψηφιακά πειστήρια, παρανόμως κτηθέντα αποδεικτικά μέσα, κατάσχεση, Cloud Act, E - Evidence

Abstract

Due to the pace of technology development, and its ever-increasing integration into criminal activity, the collection and analysis of digital data has become an important tool for investigators. There are many challenges in the field of digital criminology potentially categorized into technical, operational and legal. A digital forensic methodology has not yet been universally accepted and established. Although the models proposed in the literature vary, their variations seem to have adapted some common basic steps and procedures.

For the first time, the new Code of Criminal Procedure instituted the seizure of digital evidence at national level, under Article 265. The evidentiary prohibitions, as an exception to the rule of "moral proof", make up a legislative barrier in the attempt to seek objective truth. Digital evidence , confiscated, namely removed, copied and verified in violation of the law, leads to an evidentiary prohibition.

At supranational level, both the US CLOUD ACT and the European E-Evidence proposal, seek to respond to the increasing digitization of information, to the management of them through the role of third-party providers and to the fact that providers and data of interest are retained more and more abroad.

The present study attempts to subordinate the legislative moves, made at national and supranational level, to the existing challenges in the field of digital criminology; to evaluate them through the models supported by the theory and the principles that they have formed; and finally to exercise criticism at them, aiming at a possible filling of legislative gaps.

Keywords: digital forensics, Admissible evidence, seizure, Cloud Act, E – Evidence

ΠΕΡΙΕΧΟΜΕΝΑ

Εισαγωγή 11

1.1 Πρόβλημα – Σημαντικότητα του θέματος 11

1.2 Προβληματισμοί 13

1.3 Σκοπός – Στόχοι 15

1.4 Η ερευνητική πρόκληση 16

1.5 Βασική Ορολογία 18

i. Ψηφιακά Πειστήρια - Δεδομένα 19

ii. **Ηλεκτρονικά αποδεικτικά στοιχεία** 21

iii. Ηλεκτρονικό Έγκλημα 21

iv. Αποδεικτικές Απαγορεύσεις 22

v. Κατάσχεση 23

1.6 Διάρθρωση της μελέτης 24

Κύριο Μέρος 25

2. **Ψηφιακές Εγκληματολογικές Προκλήσεις** 25

i.Τεχνικές Προκλήσεις 26

ii. Επιχειρησιακές / Λειτουργικές Προκλήσεις 27

iii. Νομικές προκλήσεις 27

3. Θεωρίες/Μοντέλα Μεθοδολογίας Ψηφιακής Εγκληματολογίας 28

i. **National Institute of Standards and Technology (NIST)** 28

ii. Computer Forensic Investigative Process 31

iii. **DFRWS Investigative Model** 31

iv. **Abstract Digital Forensic Model (ADFM)** 32

v. **The Integrated Digital Investigation Process Model (IDIP)** 32

vi. **The Enhanced Integrated Digital Investigation Process (EIDIP)** 33

vii. **Digital Forensics Investigation Model (DFIM)** 34

viii. Model for Hybrid Evidence Investigation 34

4. Το Ισχύον νομοθετικό καθεστώς σε Εθνικό Επίπεδο 35

4.1 Τα δικονομικά χαρακτηριστικά – Αρχές της Ανακριτικής Διαδικασία 35

4.2 Παραγγελία για ποινική έρευνα και κίνηση ποινικής δίωξης 37

4.3 Η αστυνομική έρευνα 38

4.4 Ανακριτικές Πράξεις 39

i. Έρευνα 39

ii. Άσυλο κατοικίας - Έρευνες 41

iii. Κατάσχεση 42

- Κατάσχεση "πραγμάτων" 42
- Κατάσχεση ψηφιακών πειστηρίων 43
- Φύλαξη και σφράγιση των κατασχεθέντων πραγμάτων και ψηφιακών δεδομένων 49
- Πρόσβαση σε κατασχεθέντα ψηφιακά δεδομένα 51

4.5. Ειδικές Ανακριτικές Πράξεις 52

4.6. Απόδειξη 57

i. Αρχή Ηθικής Απόδειξης 57

ii. Περιορισμοί στην αρχή Ηθικής Απόδειξης - Αποδεικτικές Απαγορεύσεις 58

(α) Νομοθετικές διατάξεις - Ιστορική προσέγγιση 58

(β) Ερμηνεία του άρθρου 177 παράγραφος 2 ΚΠΔ : περί αποδεικτικών απαγορεύσεων 62

- Η έννοια της αξιόποινης πράξης 62
- Αιτιώδης σύνδεσμος 63
- Απώτερη Επενέργεια - "Μέσω" αξιόποινης πράξης 63
- Αξιόποινη απόκτηση από διωκτικές αρχές 64

iii. Απόλυτη Ακυρότητα 65

iii. Αποδεικτικές Απαγορεύσεις και Κατάσχεση Ψηφιακών Πειστηρίων 65

5. Νομοθετικές Κινήσεις σε Υπερεθνικό Επίπεδο 66

5.1. Νομολογιακές Περιπτώσεις 66

5.2.Cloud Act 71

5.3."E-Evidence" 74

5.4. Συγκριτική Προσέγγιση 76

Συμπεράσματα 77

6.1 Σύνοψη και συμπεράσματα 77

6.2 Όρια και περιορισμοί της έρευνας 79

6.3 Μελλοντικές Επεκτάσεις 79

ΒΙΒΛΙΟΓΡΑΦΙΑ 81

i. Ελληνική 81

ii. Ξενόγλωσση 83

iii. Νομολογιακές Αποφάσεις 85

iv. Υπερσύνδεσμοι Ιστοσελίδων 85

Κυρώσεις για λογοκλοπή 87

Εισαγωγή

1.1 Πρόβλημα – Σημαντικότητα του θέματος

Η συνεχώς αυξανόμενη χρήση των πληροφοριακών συστημάτων και εν γένει των σύγχρονων τεχνολογιών από τους πολίτες - ιδιώτες στην σύγχρονη καθημερινότητα, δεν δύναται σε καμία περίπτωση να αφήσει ανεπηρέαστη την “εγκληματική εφευρετικότητα”. Νέες μορφές εγκληματικών συμπεριφορών, όπως επί παραδείγματι το hacking, cracking και malware infection, αλλά και παραδοσιακές εγκληματικές ενέργειες τελούμενες πλέον με χρήση νέων τεχνολογικών μέσων, απασχολούν όλο και περισσότερο τις δικαστικές και ανακριτικές αρχές.

Ενώ η νομική επιστήμη ακολουθεί ασθμαίνοντας, προσπαθώντας να προλάβει τις εξελίξεις, η ανάγκη για πρόληψη, εξιχνίαση και καταστολή της νέας “βελτιωμένης” εγκληματικότητας, έχει πλέον καταστήσει, επιβεβλημένη την “πλήρη” αξιοποίηση των ίδιων τεχνολογικών μέσων απο τις ανακριτικές αρχές. Το δε αναμφίβολα δύσκολο εγχείρημα της ομαλής συμπόρευσης και αλληλεπίδρασης μεταξύ της νομικής και των τεχνολογικών επιστημών, λαμβανομένου υπόψη και του χρονικού παράγοντα, ήτοι από την μία την ραγδαία εξέλιξη της τεχνολογικής επιστήμης και από την άλλη τα περιορισμένα χρονικά όρια αντίδρασης στην διερεύνηση μιας εγκληματικής συμπεριφοράς, αναπόφευκτα διευκολύνει την από μέρους των δραστών ανάπτυξη δραστηριοτήτων και τεχνικών συγκάλυψης και αποφυγής σύλληψης.

Η διαρκής αυτή εξέλιξη της τεχνολογικής επιστήμης και η καταστρατήγηση αυτής από τους εκάστοτε δράστες, συνεπάγεται πιο αποδοτικές και εξελιγμένες εγκληματικές ενέργειες και δράσεις, τις οποίες δεν δύναται πλέον να εντοπίσουν, να αναστείλουν και να παρεμποδίσουν οι παραδοσιακές ανακριτικές ενέργειες και η δια αυτών συγκέντρωση, αξιολόγηση και αξιοποίηση αποκλειστικά παραδοσιακών πειστηρίων. Αντιθέτως απαιτείται

η ανάπτυξη σύγχρονων και προηγμένων τεχνικών ανίχνευσης και καταστολής κυβερνοεγκλημάτων.

Η τέλεση επομένως τόσο "εγκληματικών πράξεων νέας μορφής", όσο και παραδοσιακών εγκλημάτων, με την αξιοποίηση σύγχρονων τεχνολογικών μέσων, συνεπάγονται και την δημιουργία "νέας μορφής πειστηρίων". Τα ψηφιακά αυτά πειστήρια, δεν θα πρέπει να αγνοηθούν, καθώς δύνανται να οδηγήσουν στην εξιχνίαση της τελεσθείσας εγκληματικής ενέργειας. Τόσο η κατάληψη ψηφιακών ιχνών, οσο και η αξιοποίηση σύγχρονων τεχνολογικών μέσων κατά την εξέταση παραδοσιακών ψηφιακών πειστηρίων μπορεί να οδηγήσει σε προσφορότερη αντιμετώπιση και καταστολή της αλματικά αυξανόμενης εγκληματικότητας. Στην προκειμένη περίπτωση όμως θα εστιάσουμε στην πρώτη εκδοχή, αυτή που αφορά μια "νέα μορφή πειστηρίων", αυτή των "ψηφιακών πειστηρίων".

Έργο όμως της δικαιοσύνης πέραν την υποχρέωσης προστασίας των έννομων αγαθών και της καταστολής των εγκληματικών πράξεων, αποτελεί συγχρόνως και η προστασία θεμελιωδών δικαιωμάτων του φερόμενου δράστη και των λοιπών εμπλεκόμενων μερών. Αφ' ης στιγμής τα ψηφιακά πειστήρια λαμβάνουν σημαντικό ρόλο στην εξιχνίαση και καταστολή των ποινικών αδικημάτων, χρέος της δικαιοσύνης αποτελεί και η θωράκιση των δικαιωμάτων των εμπλεκόμενων υποκειμένων, από τυχόν καταστρατήγηση αυτών από μέρους των ανακριτικών αρχών. Αδήριτη λοιπόν καθίσταται η ανάγκη πρόβλεψης αρχών, κανόνων και άκρων ορίων στην συλλογή, επεξεργασία και αξιοποίηση των ψηφιακών πειστηρίων, η υπέρβαση των οποίων θα οδηγήσει σε αποδεικτικές απαγορεύσεις και ακυρότητες.

Πιο συγκεκριμένα, στην παρούσα μελέτη θα επιχειρηθεί η προσέγγιση νομοθετικά προβλεπόμενων ανακριτικών πράξεων, τόσο από θεωρητική νομική σκοπιά όσο και από πρακτική, σε πεδίο εφαρμογής τους και η δι αυτών εξαγωγή, συλλογή και αξιολόγηση ψηφιακών πειστηρίων, σε άμεση συνάρτηση με τους κανόνες περί αποδεικτικών απαγορεύσεων. Κεντρικό ζήτημα θα αποτελέσει η έρευνα, κατάσχεση, ανάλυση, αξιολόγηση και αξιοποίηση ψηφιακών πειστηρίων κατά την ποινική προδικασία και την κύρια διαδικασία ενώπιον του Δικαστηρίου. Καίριος άξονας, γύρω από τον οποίο θα εξεταστεί η αποτελεσματικότητα υφιστάμενων και προτεινόμενων ανακριτικών πράξεων και η

αξιοπιστία των ψηφιακών πειστηρίων, είναι αυτός της δικαιοδοσίας των εθνικών και υπερεθνικών ανακριτικών αρχών.

1.2 Προβληματισμοί

Η δαιδαλώδης διαδρομή προς την αναζήτηση, ανάκτηση και συλλογή ψηφιακών πειστηρίων, στην οποία εμπλέκονται **διαφορετικά δικαϊκά συστήματα** δημιουργεί **συγκρούσεις** που συνδεονται με σύνθετα πραγματικά και νομικά ζητήματα. Πιο συγκεκριμένα, τίθεται θέμα εφαρμογής διαφορετικών δικαιικών συστημάτων, τόσο ως προς την **θεμελίωση του αξιοποίνου** της εκάστοτε φερόμενης εγκληματικής δράσης όσο και ως προς την ίδια την **διαχείριση και ανάκτηση των ψηφιακών πειστηρίων**, προς στοιχειοθέτηση των εγκληματικών πράξεων. Οι συγκρούσεις αυτές δύναται να εξισορροπηθούν μέσω θέσπισης και εφαρμογής **κοινών νομοθετημάτων και γενικών αρχών.**

Την αναπόφευκτα συγκρουσιακή αυτή σχέση, ως ένα βαθμό έρχεται να εξομαλύνει η χρήση μιας "**κοινής ψηφιακής γλώσσας"**. Η ψηφιακή γλώσσα είναι μια διεθνής γλώσσα. Το Χ πληροφοριακό σύστημα επιτελεί ακριβώς τις ίδιες λειτουργίες, με τον ίδιο τρόπο και έχει την ίδια λειτουργική προσέγγιση είτε βρίσκεται στο κράτος Α είτε στο Β είτε είναι διασυνδεδεμένο σ΄ένα τοπικό ή υπερ τοπικό δίκτυο είτε όχι · αντίστοιχα μία παραμένει η έννοια και η τεχνολογική δομή της ασύρματης ή της ενσύρματης δικτύωσης, με διαφοροποιήσεις ανάλογα με την τεχνική δομή. Έτσι λοιπόν το πρόβλημα της εφαρμογής διαφορετικών δικαιικών συστημάτων σχετικά με το αξιόποινο συμπεριφορών στον ψηφιακό χώρο αλλά και την διαχείριση των ψηφιακών στοιχείων σε μια ποινική δίκη, ισορροπείται κατά κάποιον τρόπο από το γεγονός της κοινής ψηφιακής γλώσσας, η οποία επιτρέπει αναπαραγωγή μεθοδολογίας αλλά και επεξηγηματικές αναφορές, μέσα από την διακρατική συνεργασία των αρμοδίων και σχετιζομένων με το ηλεκτρονικό έγκλημα υπηρεσιών, σε σταθερό και τεχνολογικά ασφαλές έδαφος.

Ωστόσο, η αποδοχή κοινών κανόνων και αρχών στην διαχείριση και επεξεργασία των ψηφιακών δεδομένων, που προκύπτουν κατά την διενέργεια των σχετικών ανακριτικών πράξεων, είναι αυτή η οποία δύναται σταδιακά να γεφυρώσει πράγματι το χάσμα μεταξύ

των περισσότερων εμπλεκόμενων στην ίδια περίπτωση δικαιικών τάξεων. Έτσι, η αποδοχή κοινών κανόνων στην διαχείριση των δεδομένων, που προκύπτουν από την διενέργεια ανακριτικής έρευνας, είναι ένα πρώτο βήμα αναφορικά με τον καθορισμό προϋποθέσεων χρήσης ενός πειστηρίου από ένα δικαιικό σύστημα όπου λαμβάνει χώρα η τεχνική του διαχείριση, σε ένα άλλο δικαιικό σύστημα όπου τελικά θα λάβει χώρα η δικαστική του αξιοποίηση. Επί του παρόντος τέτοια δικαιική ταύτιση δεν προκύπτει από το συγκριτικό δίκαιο. Δεν υπάρχει τέτοια αναφορά στην επιλογή των δικαιικών κανόνων που πλαισιώνουν την όλη ανακριτική διαδικασία.

Αναμφίβολα, κοινή παραδοχή για όλα τα Κράτη, αποτελεί η **αντιστροφή της σχέσης εξαίρεση - κανόνα,** στην εμπλοκή περισσότερων κρατών στην αξιολόγηση μιας ποινικά ενδιαφέρουσας συμπεριφοράς και δράσης. Έτσι, κατά κανόνα πλέον παρατηρείται το φαινόμενο της **ανάγκης για διακρατική συνεργασία**, που εκ προοιμίου συνεπάγεται ως ένα βαθμό παραίτηση από εξουσίες της "απόλυτης κρατικής κυριαρχίας", μέσω αμοιβαίων υποχωρήσεων, χάριν του κοινού συμφέροντος καταπολέμησης της σύγχρονης εγκληματικότητας, η οποία αγνοεί τα κρατικά σύνορα και εκμεταλλεύεται την "αδυναμία" των κρατών να συνεργαστούν αποτελεσματικά. Σε κάθε δε περίπτωση κοινό τόπο θα πρέπει να αποτελεί η διαχείριση των ψηφιακών πειστηρίων, ως βάση για την εξαγωγή αποδεικτικών στοιχείων.

Εν κατακλείδι, ενώ για τους δράστες η τέλεση μιας εγκληματικής ενέργειας σε υπερεθνικό επίπεδο, στο οποίο δύναται να εμπλέκονται δυο ή και πολλές περισσότερες έννομες τάξεις, *(άλλος/-οι ο/οι τόπος/-οι ενέργειας της εγκληματικής πράξης άλλος/-οι ο/οι τόπος/-οι επέλευσης του αποτελέσματος)* άλλοτε συνιστά μέθοδο συγκάλυψης, με τεχνητή δημιουργία μιας σύνθετης διαδρομής αναζήτησης πειστηρίων δια μέσου περισσότερων εννόμων τάξεων και άλλοτε τρόπο εκμετάλλευσης ευμενέστερης ποινικής μεταχείρισης, για τα κράτη εξακολουθεί ως σήμερα σε μεγάλο βαθμό να αποτελεί τροχοπέδη στην αντιμετώπιση μιας ποινικά κολάσιμης συμπεριφοράς.

1.3 Σκοπός – Στόχοι

Βασικός στόχος, η επίτευξη του οποίου επιδιώκεται μέσω του παρόντος πονήματος είναι η διενέργεια ενός εποικοδομητικού διαλόγου μεταξύ θεωρητικών και πρακτικών ζητημάτων, νομικής και πληροφορικής επιστήμης. Ο ως άνω δε στόχος, κατά την γνώμη της γράφουσας αντανακλά σε σημαντικό βαθμό και την φιλοσοφία και λογική του ίδιου του διιδρυματικού μεταπτυχιακού προγράμματος σπουδών, στο πλαίσιο του οποίου το παρόν εκπονείται.

Ειδικότερα, αφού **προηγηθεί μια ανάλυση των προκλήσεων** - T*εχνικών, Επιχειρησιακών / Λειτουργικών, Νομικών και Ερευνητικών* - που αναφύονται σε εθνικό αλλά και διεθνές περιβάλλον γύρω από τα ψηφιακά πειστήρια, θα ακολουθήσει μια καταγραφή των προτεινόμενων από την θεωρία **μοντέλων ανάκτησης και διαχείρισης ψηφιακών πειστηρίων**, μέσα από τα οποία σκοπός είναι να συναχθούν βασικές αρχές και να χαραχθούν κατευθυντήριες γραμμές.

Εν συνεχεία, αφού προηγουμένως προχωρήσουμε σε καταγραφή των υφιστάμενων στην ελληνική έννομη τάξη βασικών **διατάξεων ποινικής δικονομίας** που ρυθμίζουν τις ανακριτικές πράξεις και τους βασικούς κανόνες της αποδεικτικής διαδικασίας, θα επιχειρηθεί **κριτική θεώρηση** αυτών σε σχέση με τις προκλήσεις και τις αρχές που θα αναπτυχθούν παραπάνω. Ειδικότερα, σκοπός της παρούσας είναι να επιχειρηθεί θεωρητική - *νομική αλλά και τεχνολογική* - και στο μέτρο του δυνατού πρακτική προσέγγιση, των αναφυόμενων από τις νέες διατάξεις του Κώδικα Ποινικής Δικονομίας και από την διαμορφωθείσα πρακτική, ζητημάτων, που αφορούν στις προβλεπόμενες σ΄αυτόν ανακριτικές πράξεις και δη στην κατάσχεση ψηφιακών πειστηρίων, ορώμενων μέσω των ρητά θεσμοθετημένων και καθιερωμένων αποδεικτικών απαγορεύσεων και ακυροτήτων.

Ακολούθως, θα επιχειρηθεί μια **νομολογιακή επισκόπηση σε διεθνές επίπεδο** του ζητήματος της αξιοποίησης των ψηφιακών πειστηρίων, μέσω της οποίας αναμένεται να αναδειχθεί τόσο **η σημαντικότητα αυτών στην ποινική διαδικασία** όσο και οι **νομικοί και και πρακτικοί προβληματισμοί,** που ανακύπτουν σε διεθνές περιβάλλον. Κατόπιν, θα ακολουθήσει σύντομη καταγραφή και αξιολόγηση νομοθετικών κινήσεων που έχουν πραγματοποιηθεί ήδη σε διεθνές επίπεδο προς την κατεύθυνση επίλυσης των σχετικών

προβλημάτων και πάντως ως ένδειξη αναγνώρισης της σημαντικότητας των ψηφιακών πειστηρίων στην σύγχρονη ποινική διαδικασία.

Συνοψίζοντας, στόχος της παρούσας είναι η υπαγωγή των νομοθετικών κινήσεων, που έχουν γίνει σε εθνικό και υπερεθνικό επίπεδο, **στις υφιστάμενες στον χώρο της ψηφιακής εγκληματολογίας προκλήσεις**, **η αξιολόγηση αυτών** με γνώμονα τα υποστηριζόμενα από την θεωρία μοντέλα και τις αρχές που αυτά έχουν διαμορφώσει και τέλος **η άσκηση εποικοδομητικής κριτικής προς τον σκοπό κάλυψης κενών και αναγκών.**

1.4 Η ερευνητική πρόκληση

Η **ταχεία εξέλιξη της τεχνολογικής επιστήμης**, σε συνάρτηση με την διαρκώς αυξανόμενη ενσωμάτωση αυτής τόσο στην καθημερινότητα των υποκειμένων εν γένει, όσο και αναπόφευκτα στην εγκληματική δράση, που κατά κάποιο τρόπο συνιστά μέρος της καθημερινότητας, αναντίρρητα έχουν καταστήσει τη συλλογή και ανάλυση των ψηφιακών δεδομένων, όλο και πιο σημαντικό εργαλείο, αναφορικά με την ενίσχυση του αποδεικτικού υλικού ή την κατάστρωση της υπερασπιστικής στρατηγικής στις περιπτώσεις των ηλεκτρονικών εγκλημάτων και την διεκπεραίωση δικαστικών υποθέσεων.

Τόσο η **ευελιξία των νέων τεχνολογιών,** που ενσωματώνουν στοιχεία όπως η φορητότητα και η απομακρυσμένη πρόσβαση όσο και **διαρκώς αυξανόμενη ισχύς** αυτών από πλευράς δυνατοτήτων, που παρέχονται προς τους χρήστες, όπως επί παραδείγματι η ταχύτητα και ο όγκος δεδομένων που δημιουργούνται, αποθηκεύονται και προσπελάζονται, καθιστούν τα ψηφιακά πειστήρια ένα κρίσιμο ερευνητικό μέγεθος. Οι σύγχρονες συσκευές μπορούν να χρησιμεύσουν ως αποθετήριο τεράστιου όγκου προσωπικών πληροφοριών και δεδομένων. Κι ενώ από την μία δημιουργείται ένα σαφές πλεονέκτημα υπερ των ανακριτικών αρχών από την διαχείριση πολλών πόρων πληροφόρησης για την εξιχνίαση μια εγκληματικής δράσης και ενδεχόμενα για την αιτιολόγηση καταδικαστικών αποφάσεων και γενικά για την εφαρμογή κι επιβολή του νόμου, από την άλλη κρίνεται αναγκαία η προσεκτική διαχείριση της δυνατότητας αυτής από εκείνους, που θεσμικά εμπλέκονται στην διαχείριση των αποδεικτικών αυτών στοιχείων, των οποίων η προσοχή πρέπει να εστιάσει στην διατήρηση της νομιμότητας αναφορικά με την άντληση των ψηφιακών δεδομένων αλλά και στην διατήρηση ακέραιου του περιβάλλοντος προστασίας των προσωπικών δεδομένων, όπου με

τις ενέργειές τους ελλοχεύει κίνδυνος προσβολής του σκληρού πυρήνα κάποιας ατομικής ελευθερίας.

Κρίσιμη επομένως, καθίσταται *η "**εξισορρόπηση ανάμεσα στην διαδικασία ανάκτησης, συλλογής, και αποθήκευσης των πειστηρίων και συνεπώς στο παραδεκτό της χρήσης και αξιοποίησης των ψηφιακών στοιχείων και στην εύλογη ανησυχία σχετικά με την ανάγκη προστασίας της ιδιωτικής ζωής"*[1], ατομικών ελευθεριών και συναφών δικαιωμάτων, είτε αφορά αποκλειστικά το πρόσωπο του ίδιου του κατηγορουμένου είτε πολύ περισσότερο όταν η αναφορά σχετίζεται με αμέτοχα τρίτα πρόσωπα.

Η δικαστική αξιοποίηση των ψηφιακών πειστηρίων είναι ένα **σχετικά νέο εργαλείο** για το δίκαιο, σχεδόν σε όλα τα δικαιικά συστήματα των ανεπτυγμένων κοινωνιών, ωστόσο η εφαρμογή του νόμου μέσα από την τα διατακτικά των δικαστικών αποφάσεων βασίζεται ολοένα και περισσότερο στα ψηφιακά στοιχεία για σημαντικές πληροφορίες σχετικά με την εξεύρεση της ουσιαστικής αλήθειας και την αξιολόγηση των ισχυρισμών τόσο του δράστη όσο και του θύματος.

Κατά την συγγραφή του παρόντος πονήματος, **πέραν των ανωτέρω γενικότερων προκλήσεων,** οι οποίες μάλιστα κρίνεται σκόπιμο να αναλυθούν και περαιτέρω στο κυρίως μέρος του παρόντος, καθώς μέσω αυτών θεωρείται οτι θα καταστούν σαφέστερα τα κενά τα οποία χρήζουν νομικής ρυθμίσεως και θεωρητικής εποικοδομητικής συζητήσεως, α**ναμένεται να συναντηθούν και κάποιες επιπλέον πρακτικές προκλήσεις.**

Πιο συγκεκριμένα, όπως και για κάθε "νέο" θέμα, που απασχολεί τόσο εν γένει την επιστημονική κοινότητα όσο και συγκεκριμένα την νομική επιστήμη, έτσι και για το συγκεκριμένο **η ύπαρξη περιορισμένου συγγραφικού έργου** πάνω στο οποίο μπορεί ένας νέος επιστήμονας να στηριχθεί προκειμένου να το εξελίξει δυσχεραίνει την προσπάθεια του.

Παρότι η ίδια η έννοια των **ψηφιακών πειστηρίων, δεν αποτελεί κάτι νέο για την επιστημονική κοινότητα, οι νομοθετικές προσπάθειες που γίνονται προς ρύθμιση αυτών** σε εθνικό και διεθνές επίπεδο, **δεν έχουν ακόμα ωριμάσει** · η ίδια η πράξη μέσω της εφαρμογής τους **δεν έχει ακόμα καταφέρει να αναδείξει όλα τα προβλήματα και τα κενά**

[1] S. E. Goodison, R. C. Davis, and Br. A. Jackson, "*Digital Evidence and the U.S. Criminal Justice System, Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence*", (2015)

τους · η νομολογία δεν έχει ακόμα σχηματίσει κατευθυντήριες γραμμές ως προς την ερμηνεία τους · **ενώ τέλος δεν έχουν ακόμα αποτελέσει αντικείμενο θεωρητικών αντιπαραθέσεων και διαλόγων αλλά μόνο μεμονωμένων θεωρητικών προσεγγίσεων.**

Στον αντίποδα βέβαια της αναντίρρητης αυτής ερευνητικής δυσκολίας, η ύπαρξη "εδάφους" για διατύπωση νέων ιδεών και απόψεων έρχεται να ενισχύσει την προσπάθεια αυτή. Ο υφιστάμενος αυτός "χώρος", αποτελεί γόνιμο έδαφος και αφήνει ακόμα και σε έναν "άπειρο", "νέο" επιστήμονα το περιθώριο να επιχειρήσει να παράγει το δικό του θεωρητικό έργο · να προσπαθήσει να περάσει το δικό του στίγμα σε ζητήματα "μη χιλιοειπωμένα", που δεν έχουν ακόμη αποτελέσει αντικείμενο πολλών ερευνητικών έργων. Έτσι το έδαφος αυτό αποτελεί κίνητρο και κινητήρια δύναμη και στην παρούσα συγγραφική προσπάθεια.

Πέραν αυτής, σημαντική πρόκληση για την γράφουσα η οποία ενυπάρχει και ως βασική πρόκληση στην αντιμετώπιση εν γένει των ψηφιακών πειστηρίων από τους νομικούς, είναι η ανάγκη **προηγούμενης κατανόησης της ίδιας της φύσης των ψηφιακών πειστηρίων αλλά και των βασικών τεχνολογιών μέσω των οποίων αυτά παράγονται, κατάσχονται, επεξεργάζονται αποθηκεύονται και επαληθεύονται.** Είναι αδύνατον να ασκηθεί εποικοδομητική κριτική σε υφιστάμενες νομοθετικές διατάξεις ή να διατυπωθούν προτάσεις για νέες νομοθετικές προσεγγίσεις χωρίς προηγουμένως να διασφαλιστεί η "κατανόηση" του ρυθμιζόμενου αντικειμένου. Η δε ταχεία εξέλιξη του συγκεκριμένου "ρυθμισταίου αντικειμένου" που αποτελεί σύμφυτη ιδιότητα του, σε συνδυασμό με την "πολυπλοκότητα", απαιτούν μεταξύ άλλων μια διεπιστημονική προσέγγιση και συνεργασία πληροφορικών και νομικών αυξάνοντας έτι περεταίρω τον ήδη μεγάλο βαθμό δυσκολίας.

1.5 Βασική Ορολογία

Αμέσως πριν το κύριο μέρος του παρόντος πονήματος, κρίνεται σκόπιμο να προηγηθεί μια ερμηνευτική προσέγγιση και οριοθέτηση ορισμένων βασικών εννοιών, που πρόκειται να μας απασχολήσουν παρακάτω. Τέτοιες κρίσιμες έννοιες είναι αυτή των "ψηφιακών πειστηρίων " ή κατ' άλλο νομοθετικό κείμενο των "ηλεκτρονικών αποδεικτικών στοιχείων", του "ηλεκτρονικού εγκλήματος", των "αποδεικτικών απαγορεύσεων" και της "κατάσχεσης".

i. Ψηφιακά Πειστήρια - Δεδομένα

Ο Ποινικός Κώδικας (Π.Κ.) στα πλαίσια της συμμόρφωσης της χώρας μας, ουσιαστικά μέσα από τις επιταγές της Σύμβασης της Βουδαπέστης για το Κυβερνοέγκλημα[2] και τεχνικά μέσα από τις διατάξεις του Ν 4411/2016[3], ορίζει στο άρθρο 13 περ. θ΄ ότι τα *«**Ψηφιακά δεδομένα** είναι η παρουσίαση **γεγονότων, πληροφοριών ή εννοιών** σε μορφή κατάλληλη προς επεξεργασία από πληροφοριακό σύστημα, συμπεριλαμβανομένου προγράμματος που παρέχει τη δυνατότητα στο πληροφοριακό σύστημα να εκτελέσει λειτουργία.[4]»*. Ο ορισμός αυτός διατηρήθηκε αναλλοίωτος και στην πρόσφατη θεμελιώδη τροποποίηση του Ποινικού Κώδικα, που συντελέστηκε με το νόμο 4619/2019. Κατά τον ορισμό αυτό, *τα ψηφιακά δεδομένα μπορούν να συνίστανται στο γεγονότα, πληροφορίες ή έννοιες*,[5] που παρουσιάζονται δηλαδή αναπαρίστανται σε γλώσσα κατανοητή σε πληροφοριακό σύστημα, δηλαδή στο δυαδικό σύστημα. Η ίδια η διάταξη περιλαμβάνει ρητά στην έννοια των ψηφιακών δεδομένων και τα προγράμματα υπολογιστή.

Ο Κώδικας Ποινικής Δικονομίας, δεν περιλαμβάνει ορισμό της έννοιας των ψηφιακών δεδομένων, ούτε κατηγοριοποιεί αυτά περαιτέρω, με αποτέλεσμα να επιφυλάσσεται για τα τελευταία ενιαία αντιμετώπιση παρά την εγγενή διαφορετικότητα τους.

Τα ψηφιακά δεδομένα κατ' αρχήν αποτελούν **άυλα στοιχεία,** δηλαδή δεν έχουν απτή υλική μορφή και υπόσταση. Το βασικό αυτό χαρακτηριστικό τους μάλιστα αποτέλεσε αφορμή διατύπωσης πλείστων θεωρητικών ενστάσεων, σε σχέση με τον τρόπο διαχείρισής τους υπό το προϊσχύσαν δικονομικό καθεστώς αλλά και έναυσμα για την νέα χωριστή ρύθμιση της διαδικασίας κατάσχεσης τους. Ειδικότερα, υπό το προϊσχύσαν δίκαιο, τα ψηφιακά δεδομένα καίτοι διακριτά και αυτοτελή σε σχέση με τα υλικά μέσα, που αποτελούν τους φορείς αποθήκευσης, απαρέγκλιτα ακολουθούσαν την τύχη των υλικών φορέων τους.

---

[2] Στο άρθρο 1 της Σύμβασης για το έγκλημα στον Κυβερνοχώρο, τα "δεδομένα υπολογιστών" ορίζονται *ως "αναπαράσταση γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη για να υποστεί επεξεργασία σε ένα σύστημα υπολογιστή, περιλαμβανομένου και ενός προγράμματος κατάλληλου για να προκαλέσει την εκτέλεση μιας λειτουργίας από ένα σύστημα υπολογιστή."*

[3] Νόμος υπ' αριθμ. 4411 ΦΕΚ 142/03.08.2016 "*Κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο και του Προσθέτου Πρωτοκόλλου της, σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, που διαπράττονται μέσω Συστημάτων Υπολογιστών Μεταφορά στο ελληνικό δίκαιο της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης – πλαισίου 2005/222/ΔΕΥ του Συμβουλίου, ρυθμίσεις σωφρονιστικής και αντεγκληματικής πολιτικής και άλλες διατάξεις*"

[4] Άρθρο 13 - Ποινικός Κώδικας (Νόμος 4619/2019)

[5] "Εδώ εντοπίζεται βέβαια εν μέρει μια ταυτολογία και εν μέρει μια αλληλοεπικάλυψη, λαμβανομένου υπόψη ότι "πληροφορία" δεν είναι τίποτε περισσότερο από ένα δεδομένο. - Γ. Ναζίρης, " Η κατάσχεση ψηφιακών Δεδομένων", Ποινική Δικαιοσύνη, Τεύχος Φεβρουάριος 2020

Επρόκειτο δε για μια λύση ανάγκης, μια θεωρητική κατασκευή, η οποία στερείτο νομικής ορθότητας και δικαιολογημένα διέγειρε θεωρητικές ενστάσεις και πρακτικούς προβληματισμούς. Η ιδιαίτερη μορφή των ψηφιακών δεδομένων επιβάλλει διαχειριστικές μεθόδους και προσεγγίσεις διαφορετικές από τις συνήθεις παραδοσιακές πρακτικές στα πλαίσια της ανακριτικής έρευνας.

Κατά κοινά παραδεδεγμένη εννοιολογική προσδιοριστική θέση, **ως ψηφιακά πειστήρια,** νοούνται "*τα **δεδομένα (ευρήματα) τα οποία βρίσκονται σε ψηφιακή μορφή και εντοπίζονται, εξάγονται και ερμηνεύονται κατά την διαδικασία της ψηφιακής σήμανσης (digital forensics) με επιστημονικά αποδεκτές μεθόδους, προκειμένου να αξιοποιηθούν σε ποινική διαδικασία."***[6]. Σύμφωνα με μια άλλη εννοιολογική προσέγγιση, πρόκειται για ***"τα αντικείμενα εκείνα που λειτουργούν ως υλικές συσκευές, που μπορούν να φιλοξενήσουν και να αποθηκεύσουν στο ψηφιακή μορφή δεδομένα"***. Αν και κρατούσα, η τελευταία κατά την γνώμη της γράφουσας, συνιστά παρωχημένη και μονοδιάστατη προσέγγιση, η οποία βρίσκεται πιο κοντά στην υλική, ενσώματη μορφή των παραδοσιακών πειστηρίων, καθώς φαίνεται να εστιάζει μόνο στους υλικούς φορείς και όχι στα ίδια τα δεδομένα.

Επιχειρώντας λοιπόν, μια περαιτέρω αποδόμηση και κατανόηση του όρου, ορώμενα από μια άλλη ερμηνευτική σκοπιά και ξεκινώντας από το αποτέλεσμα προς την διενεργούμενη ανακριτική πράξη, τα ψηφιακά πειστήρια, δεν παύουν να αποτελούν τα στοιχεία εκείνα, που συνιστούν την βάση και το ερευνητικό αντικείμενο, για την διεξαγωγή ειδικής πραγματογνωμοσύνης, την οποία συναντούμε κυρίως ως ανακριτική πράξη κατά την διερεύνηση των συνθηκών τέλεσης μιας εγκληματικής πράξης και την ανάδειξη ή υπόδειξη του προσώπου, που σχετίζεται με την διάπραξη αυτής. Άλλως πρόκειται για ***"τις πληροφορίες και τα δεδομένα εκείνα, που αποθηκεύονται, λαμβάνονται ή μεταδίδονται από μια εν ευρεία εννοία ηλεκτρονική συσκευή και σχετίζονται με την διάπραξη εγκληματικής συμπεριφοράς".***[7]

Με την σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο, αναγνωρίζονται τρεις κατηγορίες ψηφιακών δεδομένων, τα δεδομένα συνδρομητή/ χρήστη

[6] Θ. Δαλακούρας, «Το Ηλεκτρονικό έγκλημα», εκδόσεις Νομική Βιβλιοθήκη, 2019

[7] M. B. Mukasey, J. L. Sedgwick, D. W. *«Electronic Crime Scene Investigation, A Guide for First Responders, Second Edition»,* U.S. Department of Justice, Office of Justice Programs, National Institute of Justice

ή δεδομένα καταλόγου (subscriber data)[8], τα δεδομένα περιεχομένου (content data)[9] και τα δεδομένα κίνησης (traffic data)[10]

ii. **Ηλεκτρονικά αποδεικτικά στοιχεία**

Ως ταυτόσημη έννοια, κρίνεται σκόπιμο να αναφερθεί και αυτή των **"Ηλεκτρονικών αποδεικτικών στοιχείων («e-evidence»)"**, που κατά την Ευρωπαϊκή Επιτροπή, συνιστούν τα *"ψηφιακά εκείνα δεδομένα που χρησιμοποιούνται για τη διερεύνηση και τη δίωξη ποινικών αδικημάτων.Στα στοιχεία αυτά περιλαμβάνονται, μεταξύ άλλων:*

- *τα μηνύματα ηλεκτρονικού ταχυδρομείου*
- *τα γραπτά μηνύματα (SMS) ή το περιεχόμενο από εφαρμογές ανταλλαγής μηνυμάτων*
- *το οπτικοακουστικό περιεχόμενο*
- *οι πληροφορίες για τον ηλεκτρονικό λογαριασμό ενός χρήστη"*[11]

Τέτοιου είδους δεδομένα μπορούν να χρησιμοποιηθούν για την ταυτοποίηση ενός προσώπου ή για τη συγκέντρωση περισσότερων πληροφοριών σχετικά με τις δραστηριότητές του."[12]

iii. Ηλεκτρονικό Έγκλημα

Διάφορες εννοιολογικές προσεγγίσεις της έννοιας του ηλεκτρονικού εγκλήματος έχουν διατυπωθεί από την θεωρία σε βάθος χρόνου. Η Ελληνική Δίωξη Ηλεκτρονικού Εγκλήματος, διατύπωσε τον ορισμό ότι ηλεκτρονικό έγκλημα αποτελούν ***« οι αξιόποινες εγκληματικές πράξεις που τελούνται με τη χρήση ηλεκτρονικών υπολογιστών και συστημάτων επεξεργασίας δεδομένων και τιμωρούνται με συγκεκριμένες ποινές από την ελληνική νομοθεσία».***

[8] Πρόκειται για δεδομένα που φυλάσσονται από τους παρόχους υπηρεσιών και αφορούν τους συνδρομητές των υπηρεσιών τους, εξαιρουμένων των στοιχείων κίνησης ή περιεχομένου - Νάιντος, "Η κατάσχεση ψηφιακών Δεδομένων", Ποινική Δικαιοσύνη, Τεύχος Φεβρουάριος 2020

[9] Σε αυτή την κατηγορία εμπίπτει το περιεχόμενο των αρχείων κειμένου, ήχου, εικόνας κ.α. - Γ. Ναζίρης " Η κατάσχεση ψηφιακών Δεδομένων", Ποινική Δικαιοσύνη, Τεύχος Φεβρουάριος 2020

[10] Πρόκειται για δεδομένα υπολογιστή που σχετίζονται με την επικοινωνία μέσω ενός πληροφοριακού συστήματος και καταδεικνύουν την προέλευση, τον προορισμό, την διαδρομή, τον χρόνο, την ημερομηνία, το μέγεθος, την διάρκεια ή τον τύπο της υφιστάμενης υπηρεσίας της επικοινωνίας - Γ. Ναζίρης, " Η κατάσχεση ψηφιακών Δεδομένων", Ποινική Δικαιοσύνη, Τεύχος Φεβρουάριος 2020

[11] https://www.consilium.europa.eu/el/policies/e-evidence/

[12] https://ec.europa.eu/home-affairs/what-we-do/cybercrime/e-evidence_el

Οι Forester and Morrison, από την άλλη, το 1994, όρισαν το ηλεκτρονικό έγκλημα ως ***«μια εγκληματική πράξη στην οποία ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως το κυριότερο μέσο τέλεσής της».***

Ο Grabosky, το 2007, επιχειρώντας να κατατάξει τα ηλεκτρονικά εγκλήματα σε επιμέρους κατηγορίες, κατέληξε σε τρεις διαφορετικές κατηγορίες. Πιο συγκεκριμένα διέκρινε τα ηλεκτρονικά εγκλήματα σε (α) αυτά στα οποία χρησιμοποιείται ως μέσο τέλεσης του εγκλήματος χρησιμοποιείται ο υπολογιστής, (β) στο αυτά όπου ο υπολογιστής συνεπικουρεί στο αδίκημα και (γ) στο αυτά όπου ο υπολογιστής είναι ο στόχος του εγκλήματος[13]. Ακόμη, οι McGuire και Dowling, το 2013 κατηγοριοποίησαν το ψηφιακό έγκλημα σε έγκλημα «ενεργοποιημένο στον κυβερνοχώρο» και έγκλημα «εξαρτώμενο από τον κυβερνοχώρο».[14]

iv. Αποδεικτικές Απαγορεύσεις

Σύμφωνα με τον Ν. Δημητράτο μέσω του θεσμού των **«αποδεικτικών απαγορεύσεων»** τίθενται περιορισμοί στην ποινική αποδεικτική διαδικασία, ήτοι στην συγκέντρωση και αξιοποίηση αποδεικτικών στοιχείων.[15] Σύμφωνα με άλλη θεωρητική εννοιολογική προσέγγιση ως **«αποδεικτικές απαγορεύσεις»** ορίζονται «*οι περιορισμοί της αποδεικτικής διαδικασίας που αφορούν είτε στην απόκτηση, είτε στην αξιοποίηση ορισμένου αποδεικτικού μέσου»*[16]. Κατά δε άλλη διατυπωθείσα στην θεωρία άποψη οι αποδεικτικές απαγορεύσεις συνιστούν περιορισμοί αυτόνομους κανόνες, μέσω των οποίων τίθενται περιορισμοί στην ουσιαστική διερεύνηση της αλήθειας σε όλο το φάσμα της Ποινικής Διαδικασίας[17]. Από άλλους θεωρητικούς έχει διατυπωθεί η άποψη ότι οι αποδεικτικές απαγορεύσεις, συνίστανται στους κανόνες εκείνους που περιορίζουν την διακρίβωση των

[13] Peter Grabosky, "Security in the 21st Century, Security Journal" (2007)
[14] Mike Mcguire, S. Dowling, "Cyber crime: A review of the evidence Research Report 75 Chapter 2: Cyber-enabled crimes -fraud and theft" (2013)
[15] Ν. Δημητράτος, «Περί των αποδεικτικών απαγορεύσεων στην ποινική δίκη», εκδόσεις Αντ. Ν. Σάκκουλα Αθήνα- Κομοτηνή, 1992
[16] Θ. Δαλακούρας, «Απαγορευμένα αποδεικτικά μέσα : δογματικές βάσεις για την θεμελίωση των αποδεικτικών απαγορεύσεων στην Ποινική Δίκη» , ΠοινΧρ ΜΣΤ/1996
[17] Χ. Νάϊντος, «Αποδεικτικές Απαγορεύσεις στην Ποινική Δίκη», Εκδόσεις Α. Σάκκουλα, Αθήνα – Θεσσαλονίκη, 2010

συνθηκών τέλεσης ενός εγκλήματος στον βωμό της υπηρέτησης άλλων αξιών τις οποίες ένα Κράτος Δικαίου οφείλει να θέτει υπό προτεραιότητα[18]. Σε κάθε όμως περίπτωση, κοινώς αποδεκτό στην νομική θεωρία και πράξη είναι ότι οι αποδεικτικές απαγορεύσεις αποτελούν φραγμό και όριο στην αναζήτηση άνευ ετέρου αναζήτηση αλήθειας [19] .

Έχει επικρατήσει στην νομική βιβλιογραφία, η περαιτέρω κατηγοριοποίηση των αποδεικτικών απαγορεύσεων σε **"μη αυτοτελείς ή εξαρτημένες"** και σε **"αυτοτελείς ή ανεξάρτητες".** Στις μη αυτοτελείς αποδεικτικές απαγορεύσεις απαραίτητη προϋπόθεση συνιστά η προηγούμενη παράνομη συλλογή του αποδεικτικών στοιχείων. Άλλως, εξαρτημένες είναι αυτές που από την φύση του προϋποθέτουν προηγούμενη παράνομη απόκτηση. Έτσι, επί παραδείγματι μη αυτοτελή αποδεικτική απαγόρευση καθιερώνεται από τη διάταξη του άρθρου 177 παρ. 2 ΚΠΔ.

Από την άλλη, οι ανεξάρτητες αποδεικτικές απαγορεύσεις, είναι αποσυνδεδεμένες από τυχόν πρότερη παράνομη δραστηριότητα των ανακριτικών οργάνων ή άλλου υποκειμένου που διενεργήθηκε για την ανάκτηση, η αξιοποίηση αυτών και η οποία δίχως άλλο από μόνη της θα προσέβαλε θεμελιώδη έννομα αγαθά του ατόμου[20].

ν. Κατάσχεση

Η κατάσχεση αποτελεί επίσης μία από τις νομοθετικά προβλεπόμενες στον Κώδικα Ποινικής Δικονομίας, ανακριτικές πράξεις. Η πράξη αυτή συνίσταται στην από ορισμένο πρόσωπο, **αφαίρεση της κατοχής πραγμάτων**, τα οποία συνδεόνται με συγκεκριμένη εγκληματική πράξη, ως αντικείμενα αυτής, ή ως μέσα διάπραξης ή ως προϊόντα της. Η αφαίρεση δε αυτή συντελείται προκειμένου να καλυφθούν οι ανάγκες της ανακριτικής διαδικασίας, ήτοι να επιτευχθεί συγκέντρωση και διατήρηση αποδεικτικών στοιχείων ή να διασφαλιστεί τυχόν διενεργηθείσα δήμευση ή καταστροφής επιβεβλημένη από τον νόμο.

[18] Α. Καρράς, *«Ποινικό Δικονομικό Δίκαιο»*, Εκδόσεις Ά. Σάκκουλα, Αθήνα , 2011

[19] Ν. Κ Ανδρουλάκης , «Θεμελιώδεις έννοιες της Ποινικής Δίκης» ,Εκδόσεις Α. Σάκκουλας, Αθήνα- Κομοτηνή, 2007

[20] Ν. Ανδρουλάκης, «Θεμελιώδεις έννοιες της ποινικής δίκης», Εκδόσεις Α. Σάκκουλας, Αθήνα- Κομοτηνή, 2007

1.6 Διάρθρωση της μελέτης

Στο **Εισαγωγικό μέρος** της παρούσας, που αποτελείται από έξι κεφάλαια, συμπεριλαμβανομένου του παρόντος επιχειρήθηκε η ανάδειξη του προβλήματος που καλούμαστε να λύσουμε στο πλαίσιο της παρούσας · διατυπώθηκαν γενικοί γύρω από το πραγματευόμενο ερευνητικό αντικείμενο προβληματισμοί αλλά και ειδικοί στο πλαίσιο εκπόνησης της παρούσας · τέθηκαν ερωτήματα · αναλύθηκαν οι στόχοι, η επίτευξη των οποίων επιδιώκεται με την συγγραφή της παρούσας· και τέλος προσεγγίστηκαν εννοιολογικά βασικές έννοιες.

Το **κύριο μέρος** της παρούσας μελέτης διαρθρώνεται σε τέσσερα (4) βασικά κεφάλαια. Κύριο άξονα γύρω από τον οποίο εξετάζονται οι επιμέρους έννοιες των ανακριτικών πράξεων και των αποδεικτικών απαγορεύσεων είναι η έννοια των "ψηφιακών πειστηρίων". Πιο συγκεκριμένα, το πρώτο κεφάλαιο φέρει επικεφαλίδα "Ψηφιακές Εγκληματολογικές Προκλήσεις". Σε αυτό το αρχικό στάδιο της έρευνας επιδιώκεται ο εντοπισμός και η κατηγοριοποίηση των υφιστάμενων προκλήσεων στο χώρο της ψηφιακής εγκληματολογίας, προκειμένου μέσω αυτών να εξετασθούν εν συνεχεία οι υφιστάμενες νομοθετικές διατάξεις. Το κεφάλαιο αυτό διακρίνεται περεταίρω σε τρία υποκεφάλαια αυτά των Τεχνικών, Επιχειρησιακών/ Λειτουργικών και Νομικών προκλήσεων.

Στο δεύτερο κεφάλαιο με τίτλο "Θεωρίες/Μοντέλα Μεθοδολογίας Ψηφιακής Εγκληματολογίας", επιχειρείται να χαραχθεί ένα θεωρητικό πλαίσιο εξέτασης των ψηφιακών πειστηρίων και να καταγραφούν ορισμένες βασικές αρχές που η θεωρία έχει έως σήμερα αναδείξει. Προς την κατεύθυνση αυτή ακολουθεί επιγραμματική καταγραφή βασικών μοντέλων που έχουν προταθεί από την θεωρία με χρονολογική σειρά : National Institute of Standards and Technology (NIST), DFRWS Investigative Model, Abstract Digital Forensic Model (ADFM, The Integrated Digital Investigation Process Model (IDIP), The Enhanced Integrated Digital Investigation Process (EIDIP), Digital Forensics Investigation Model (DFIM) και Model for Hybrid Evidence Investigation.Στο επόμενο κεφάλαιο με τίτλο "Το Ισχύον νομοθετικό καθεστώς σε Εθνικό Επίπεδο" ακολουθεί σύντομη παρουσίαση και σχολιασμός ισχύοντος στο εθνικό επίπεδο νομοθετικού πλαισίου των ανακριτικών πράξεων και των αποδεικτικών απαγορεύσεων. Ειδικότερα, σε αυτό επιχειρείται ο εννοιολογικός προσδιορισμός και η κατηγοριοποίηση των θεσμοθετημένων ανακριτικών και ειδικών ανακριτικών πράξεων, με

βαρύτητα στην νέα νομοθετικά κατοχυρωμένη στο άρθρο 265 του ΚΠΔ, ανακριτική πράξης της "κατάσχεσης ψηφιακών πειστηρίων". Εν συνεχεία αφου προηγηθεί η θεωρητική προσέγγιση και ανάλυση των θεμελιωδών εννοιών της "ηθικής απόδειξης" και των "αποδεικτικών απαγορεύσεων" επιχειρείται η αναγωγή των αποδεικτικών απαγορεύσεων στην ανακριτική πράξη της κατάσχεσης ψηφιακών πειστηρίων. Το τέταρτο και τελευταίο κεφάλαιο του κυρίου μέρους, που φέρει τον τίτλο "Νομοθετικές Κινήσεις σε Υπερεθνικό Επίπεδο" αναλύεται σε τρεις επιμέρους υπό ενότητες. Στο αυτό παρουσιάζεται η νομοθετική προσέγγιση των ΗΠΑ, στο ζήτημα της εκτός εθνικών συνόρων πρόσβασης σε αποδείξεις, με την Cloud Act αλλά και η αντίστοιχη νομοθετική πρόταση της Ευρωπαϊκής Επιτροπής, η οποία αποτυπώνεται στην E-Evidence. Ακολούθως επιχειρείται μια συγκριτική θεώρηση των δύο νομοθετικών πονημάτων, αφού προηγουμένως προηγηθεί μια σύντομη επισκόπηση διεθνών νομολογιακών υποθέσεων που απασχόλησαν την διεθνή νομική κοινότητα γύρω από το θέμα των ψηφιακών πειστηρίων και την αξιοποίηση αυτών στην ποινική δίκη.

Τέλος, στο **τελευταίο μέρος (Συμπεράσματα)** της παρούσας που αποτελείται από τρία επιμέρους κεφάλαια, συνοψίζονται τα βασικά σημεία της μελέτης, καταγράφονται τα βασικά συμπεράσματα που εξήχθησαν από αυτή, αναφέρονται οι περιορισμοί και τα όρια της διενεργηθείσας έρευνητικής προσπάθειας και προτείνονται μελλοντικές επεκτάσεις αυτής.

Κύριο Μέρος

2. **Ψηφιακές Εγκληματολογικές Προκλήσεις**

Ο Γάλλος εγκληματολόγος Dr Edmond Locard, στις αρχές του 20ου αιώνα, διατύπωσε την ***"αρχή της ανταλλαγής"***, η οποία αποτέλεσε ορόσημο για την εξέλιξη της εγκληματολογικής επιστήμης. Πιο συγκεκριμένα, υποστήριξε ότι η επαφή ενός υποκειμένου ή αντικειμένου με ένα άλλο, έχει ως αποτέλεσμα την ανταλλαγή υλικού, όπως DNA, δακτυλικά αποτυπώματα, τρίχες, κύτταρα δέρματος, αίμα, σωματικά υγρά, ίνες ρούχων κ.α. Η εφαρμογή της σχετικής αρχής και στα ψηφιακά δεδομένα αποτελεί πλέον κοινή παραδοχή. Χαρακτηριστική ερευνητική προσπάθεια, που στηρίζεται και σε αυτήν την παραδοχή, συνιστά και η πλατφόρμα LOCARD, η οποία αποτελεί ένα πρότζεκτ που χρηματοδοτήθηκε

από το ευρωπαϊκό πρόγραμμα Horizon 2020, και αποσκοπεί στην αυτοματοποίηση της συλλογής δικαστικά παραδεκτών ψηφιακών πειστηρίων, κάθε μορφής. Στόχος είναι η αύξηση της εμπιστοσύνης στην διαχείριση και επεξεργασία των ψηφιακών δεδομένων.

Αδιαμφισβήτητα, υπάρχουν πολλές προκλήσεις και ζητήματα που περιβάλλουν τον τομέα της Ψηφιακής Εγκληματολογίας στο σύνολό του. Ενδεικτικά οι προκλήσεις αυτές θα μπορούσαν να κατηγοριοποιηθούν περαιτέρω σε (α) τεχνικές, (β) επιχειρησιακές, (γ) και νομικές προκλήσεις.

i.Τεχνικές Προκλήσεις

Κατά τη διάρκεια μιας ψηφιακής εγκληματολογικής έρευνας, συναντώνται πλείστες τεχνικές προκλήσεις. Μεταξύ άλλων τέτοιες προκλήσεις συνιστούν το **μέγεθος των ερευνώμενων δεδομένων**, η **θέση αυτών**, η τυχόν **απόκρυψη, κρυπτογράφηση ή διαγραφή τους.** Οι προκλήσεις αυτές άλλοτε οδηγούν σε αδυναμία ολοκλήρωση της διενεργούμενης έρευνας και άλλοτε σε παρεμπόδιση αυτής ή πάντως σε υπερβολική κατανάλωση πόρων και χρόνου. Αναλυτικότερα, το επίπεδο κρυπτογράφησης, το μέγεθος των δεδομένων που πρέπει να ανακτηθούν, η διαλογή των δεδομένων που μπορούν να χρησιμοποιηθούν πράγματι, ως αποδεικτικά στοιχεία, που είναι δηλαδή σχετικά και όχι νομικά αδιάφορα, ο εντοπισμός της τοποθεσίας αποθήκευσης των δεδομένων, ο οποίος δεν είναι πάντα εύκολος, ασκούν σημαντική επιρροή σε μια εγκληματολογική έρευνα. Επί παραδείγματι, οι πεπειραμένοι δράστες, όχι σπάνια χρησιμοποιούν τεχνολογίες όπως VPN, proxies και TOR , ώστε να δρουν ανώνυμα χωρίς να αφήνουν κανένα ίχνος ή ίχνος, γεγονός που περιορίζει τον όγκο των δεδομένων που ανακτώνται και αναλύονται για οποιοδήποτε πιθανό ίχνος ή αποδεικτικό στοιχείο. Όπως βέβαια προαναφέρθηκε, σοβαρή πρόκληση συνιστά και “το σκούπισμα ή η διαγραφή δεδομένων ή και η απόκρυψη δεδομένων”. Πέραν τούτων, λόγω του ρυθμού εξέλιξης της τεχνολογίας αλλά και της πληθώρας τεχνικών και τεχνολογιών που χρησιμοποιούνται επί παραδείγματι από τις συσκευές IoT, τα εγκληματολογικά εργαλεία είναι σχεδόν αναξιόπιστα όσον αφορά τους διαφορετικούς τύπους συσκευών, με αποτέλεσμα η διαδικασία ανάκτησης δεδομένων να καθίσταται άλλοτε δυσχερής και άλλοτε σχεδόν αδύνατη. Η πιο επίκαιρη δε πρόκληση, σχετίζεται με την τεχνολογία νέφους και την μετακίνηση των δεδομένων.

ii. Επιχειρησιακές / Λειτουργικές Προκλήσεις

Εκτός από τις τεχνικές προκλήσεις, οι επιχειρησιακές προκλήσεις αποτελούν επίσης σοβαρή απειλή για την ψηφιακή εγκληματολογική έρευνα. Το πρόβλημα εν προκειμένω ξεκινά από την **έλλειψη προηγούμενης εμπειρίας διαχείρισης περιστατικών**, την **έλλειψη τυποποιημένων διαδικασιών**, αρχών και προτύπων και συνακόλουθα την έλλειψη **ετοιμότητας.** Με άλλα λόγια, οι ερευνητές ψηφιακής εγκληματολογίας εξακολουθούν να μην είναι σε θέση να εντοπίσουν οποιοδήποτε περιστατικό. Στην πραγματικότητα, ακόμη κι αν καταφέρουν να εντοπίσουν ένα περιστατικό, πολλές φορές είτε αδυνατούν να ανταποκριθούν έγκαιρα σε αυτό με αποτέλεσμα να χάνονται κρίσιμα για την ποινική υπόθεση αποδεικτικά στοιχεία, είτε δεν έχουν καθόλου την ικανότητα να ανταποκριθούν. Σε αυτή την κατηγορία προκλήσεων σκόπιμο κρίνεται να συμπεριληφθούν επιπλέον η **έλλειψη κατάλληλων σύγχρονων ερευνητικών εργαλείων**, **η έλλειψη υποδομών και πολιτικών διαχείρισης πραγματικών περιστατικών συλλογής ψηφιακών πειστηρίων .** Στην ίδια κατηγορία προκλήσεων θα πρέπει να συμπεριληφθεί και η **έλλειψη ανθρώπινου δυναμικού**, πολλώ δε μάλλον κατάλληλα καταρτισμένου, εκπαιδευμένου και εφοδιασμένου με **γνώσεις ορθής χρήσης εργαλείων εγκληματολογίας ακόμα και στην περίπτωση που αυτά υπάρχουν.**

iii. Νομικές προκλήσεις

Στην συγκεκριμένη κατηγορία προκλήσεων, ως βασικότερες σκόπιμο κρίνεται να αναφερθούν η **έλλειψη ή αμφισβήτηση δικαιοδοσίας,** η **έλλειψη ειδικά νομοθετημένης και αναλυτικά ρυθμισμένης διαδικασίας και η ύπαρξη ζητημάτων ασφάλειας και απορρήτου**. Ειδικότερα, το ζήτημα δικαιοδοσίας συνιστά όλο και μεγαλύτερη πρόκληση λόγω της διασυνοριακής κίνησης των ψηφιακών πειστηρίων αλλά και των εγκληματιών. Η εμπλοκή περισσότερων εννόμων τάξεων δημιουργεί σοβαρά προβλήματα τόσο ως προς το αξιόποινο των τελεσθέντων πράξεων όσο και ως προς την εξουσία αναζήτησης αποδεικτικών στοιχείων.

3. Θεωρίες/Μοντέλα Μεθοδολογίας Ψηφιακής Εγκληματολογίας

Δεν έχει έως σήμερα κατοχυρωθεί παγκοσμίως μια κοινά αποδεκτή μεθοδολογία ψηφιακής εγκληματολογίας. Τα προτεινόμενα κατά καιρούς στην βιβλιογραφία μοντέλα ποικίλλουν. Ωστόσο, σε όλα τα μοντέλα, παρά τις υπάρχουσες παραλλαγές, συναντά κανείς κάποια κοινά βασικά βήματα και διαδικασίες [21]. Σύμφωνα με το Εθνικό Ινστιτούτο Δικαιοσύνης των Η.Π.Α. *(National Institute of Justice)*, τα ψηφιακά πειστήρια θα πρέπει να ανακτώνται, να εξετάζονται και να αναλύονται μόνο από πρόσωπα, ειδικά εκπαιδευμένα προς τον σκοπό αυτό. Η ποικιλομορφία των ψηφιακών μέσων από κοινού με την ραγδαία ανάπτυξη της τεχνολογικής επιστήμης, καθιστούν αναγκαία την δημιουργία εξειδικευμένων κεντρικών δομών που στις οποίες θα πρέπει να ανατίθεται η διενέργεια της συγκεκριμένης διαδικασία.

i. **National Institute of Standards and Technology (NIST)**

Σύμφωνα με το **National Institute of Standards and Technology (NIST)[22],** τα πιο συνήθη βήματα που εφαρμόζονται σε κάθε έρευνα είναι τα κάτωθι:
Συλλογή Δεδομένων (Data Collection), η Εξέταση (Examination), η Ανάλυση (Analysis) και η Αναφορά (Reporting)[23]

Βήμα 1ο : Συλλογή Δεδομένων (Data Collection)
Εντοπισμός/ Ταυτοποίηση (identify) - Απόκτηση (acquire) - Προστασία (protect)

Σε πρώτο στάδιο ο ερευνητής εντοπίζει τις πηγές από την χρήση των οποίων δύναται εν τέλει να οδηγηθεί σε δεδομένα και πληροφορίες. Όσο εξελίσσεται η επιστήμη και η τεχνολογία εισχωρεί όλο και περισσότερο με ποικίλους τρόπους στη καθημερινότητα, τόσο αυξάνονται και οι πηγές ψηφιακών δεδομένων. Ενδεικτικά τέτοιες πηγές αποτελούν οι σταθεροί και φορητοί υπολογιστές, δίκτυα, smartphones, smartwatches, mp3 players, iPods, ψηφιακές κάμερες και λοιπές smart συσκευές (Διαδίκτυο των πραγμάτων). Μέσω αυτών των

[21] Pollitt, M.M., *"An Ad Hoc Review of Digital Forensic Models",* 2nd International Workshop on Systematic Approaches to Digital Forensic Engineering , 2007
[22] Dr. Sudesh Rani, "*digital forensic models: a comparative analysis",* 2018
[23] Reith, M., Carr, C. and Gunsch, G., "An Examination of Digital Forensic Models", international Journal of Digital Evidence, 2002

ψηφιακών συσκευών ο ερευνητής δύναται να εξάγει πληροφορίες, αρχεία και δεδομένα. Ενώ σημαντικές πηγές δεδομένων αποτελούν και τα μέσα εξωτερικής αποθήκευσης, δηλαδή οι εξωτερικοί σκληροί δίσκοι, τα USB sticks, οι οπτικοί δίσκοι και οι κάρτες μνήμης.

Κρίσιμο για τον ερευνητή είναι να εντοπίσει και τον πάροχο Διαδικτύου που χρησιμοποιείται για την σύνδεση των ως άνω συσκευών στο διαδίκτυο αλλά και να προβεί σε καταγραφή τυχόν Τοπικού Δικτύου, ήτοι της τοπολογίας του, των δικτυακών συσκευών και των ρυθμίσεων του δρομολογητή.

Σε αυτό το πρώτο βήμα, σύμφωνα με το εφαρμοζόμενο μοντέλο, περιλαμβάνονται και ο Σχεδιασμός, η Ανάκτηση και η Επαλήθευση. Αμέσως μετά τον εντοπισμό των πιθανών πηγών από το ανακριτικό όργανο, το τελευταίο θα πρέπει μπορέσει να ανακτήσει από αυτές τα δεδομένα που χρειάζεται ώστε εν συνεχεία να τα αξιολογήσει. Ο ερευνητής σε αυτό το σημείο θα κατηγοριοποιήσει και θα διαχωρίσει τις πηγές που έχει εντοπίσει, λαμβάνοντας υπόψη την πιθανή αξία μιας πηγής, την πτητικότητα και ρευστότητα των δεδομένων αλλά και την προσπάθεια που απαιτείται για την συλλογή τους. Κάθε πηγή δεδομένων πρέπει να αντιμετωπίζεται από τον ερευνητή με βάση τα συγκεκριμένα χαρακτηριστικά της αλλά και τη κατάσταση λειτουργίας στην οποία αυτή βρίσκεται την στιγμή διενέργειας της έρευνας. Επί παραδείγματι θα πρέπει να επιφυλάσσεται διαφορετική μεταχείριση σε έναν ηλεκτρονικό υπολογιστή που εντοπίζεται απενεργοποιημένος και διαφορετική στο κάποιον που βρίσκεται σε λειτουργία. Πιο συγκεκριμένα, δεν θα πρέπει να παραγνωρίζεται ότι κρίσιμα δεδομένα ενδέχεται να είναι προσωρινά αποθηκευμένα και στην μνήμη RAM του υπολογιστή ή και στο δίκτυο, με αποτέλεσμα τυχόν επανεκκίνηση ή κλείσιμο υπολογιστή να συνεπάγεται την οριστική απώλεια τους. Έτσι ο ερευνητής θα πρέπει πάντοτε να σέβεται την σειρά πτητικότητας δεδομένων. Σύμφωνα με την σειρά πτητικότητας, στην τεχνολογία αποθήκευσης δεδομένων θα πρέπει κατά σειρά να ελέγχονται οι καταχωρητές, η μνήμη ram, τα προσωρινά συστήματα αρχείων, οι δίσκοι αποθήκευσης, οι εκτυπώσεις και εν τέλει τα offline αρχεία backup. Οι καταχωρητές, βρίσκονται στον επεξεργαστή και αποτελούν στοιχεία μνήμης περιορισμένου αποθηκευτικού όγκου αλλά και ταχύτητας πρόσβασης ανάλογη της ισχύος και επιδόσεως του επεξεργαστή, στερούνται ωστόσο ιδιαίτερης χρηστικής αξίας σε μια τέτοια έρευνα. Η προσωρινή μνήμη RAM, διαθέτει υψηλό βαθμό πτητικότητας, αφού τυχόν δεδομένα που βρίσκονται αποθηκευμένα σε αυτή χάνονται αν διακοπεί η τροφοδοσία ρεύματος. Στην μνήμη RAM ο ερευνητής ενδέχεται να εντοπίσει αποθηκευμένες πληροφορίες συνδεδεμένου χρήστη, δικτυακές συνδέσεις, κωδικούς πρόσβασης, τρέχουσες

διεργασίες, ανοικτά αρχεία, δημοσιεύσεις σε κοινωνικά δίκτυα, παλαιότερα στιγμιότυπα οθόνης κ.λπ.

Μετά την ανάκτηση των δεδομένων, κρίσιμη προκειμένου να είναι δικαστικά αξιοποιήσιμα τα ψηφιακά πειστήρια, που πρόκειται να συλλεχθούν είναι η επαλήθευση της ακεραιότητάς τους. Έτσι, ο ερευνητής θα πρέπει να πιστοποιεί ότι δεν έχει αλλοιώσει τα δεδομένα που έχει συλλέξει. Η επαλήθευση γίνεται με εργαλεία της ψηφιακής εγκληματολογίας, και συγκεκριμένα με χρήση μονόδρομης κρυπτογραφικής συνάρτησης κατακερματισμού. Η συνάρτηση κατατεμαχισμού, μετά την εισαγωγή δεδομένων επιστρέφει τιμές, οι οποίες καλούνται τιμές κατατεμαχισμού (hash values/ hashes). Τόσο η κοινώς χρησιμοποιούμενη SHA-1, όσο και άλλες κρυπτογραφικές συναρτήσεις εγγυόνται ότι για κάθε διαφορετική είσοδο δεδομένων, η έξοδος είναι μοναδική. Έτσι η συνάρτηση αυτή δέχεται ως είσοδο μια ακολουθία δεδομένων οποιουδήποτε μήκους και παράγει μια σύνοψη σταθερού πάντα μήκους, ενώ η παραμικρή αλλαγή, στην συνάρτηση εισόδου παράγει δραματικά διαφορετικό αποτέλεσμα.

Βήμα 2ο : Εξέταση (Examination)

Μετά την συλλογή ακολουθεί η εξέταση των δεδομένων, κατά την οποία τα τελευταία αξιολογούνται, προκειμένου εν συνεχεία να εξαχθούν χρήσιμες πληροφορίες από αυτά. Η εξέταση, λόγω του όγκου των δεδομένων πραγματοποιείται με εργαλεία της ψηφιακής εγκληματολογίας, όπως επί παραδείγματι με αναζήτηση με λέξεις κλειδιά μέσω των οποίων δύναται να εντοπιστεί τυχόν επαναλαμβανόμενο μοτίβο, με φιλτράρισμα, κατηγοριοποίηση και σύνδεση διαφορετικών τύπων δεδομένων.

Βήμα 3ο : Ανάλυση (Analysis)

Εν συνεχεία στο στάδιο της ανάλυσης ο ερευνητής επιχειρεί να προβεί σε εξαγωγή συμπερασμάτων στηριζόμενος στις πληροφορίες που εξέτασε στο προηγούμενο στάδιο της διαδικασίας.

Βήμα 4ο : Αναφορά (Reporting)

Σε τελικό στάδιο ακολουθεί η σύνταξη αναφοράς των αποτελεσμάτων. Ο ερευνητής ερμηνεύει τα ευρήματα που προέκυψαν στα προηγούμενα στάδια με αντικειμενικότητα και αμεροληψία και τα παραθέτει με χρήση απλής και κατανοητής γλώσσας. Ειδικότερα, η

αναφορά περιλαμβάνει στοιχεία και αξιολογήσεις για τα δεδομένα που έχει συλλέξει και επεξεργαστεί ο ερευνητής. Πρέπει δε αυτή πάντα για λόγους αξιοπιστίας να περιλαμβάνει στοιχεία όπως την ώρα και την ημερομηνία διενέργειας των παραπάνω ενεργειών, τον τόπο διενέργειας αυτών, την εφαρμοσθείσα μέθοδο και τα εργαλεία που αξιοποιήθηκαν, έτσι ώστε να είναι δυνατή η επαλήθευση τους.

ii. Computer Forensic Investigative Process

Το 1995, από τον M. M. Pollitt, προτάθηκε το μοντέλο **"Computer Forensic Investigative Process ",** ως μεθοδολογία διαχείρισης ψηφιακών πειστηρίων που θα οδηγεί στο αξιόπιστα και νομικά αποδεκτά πειστήρια. Το μοντέλο αυτό περιελάμβανε τέσσερα διακριτά στάδια. Το στάδιο της **"Απόκτησης /Ανάκτησης"** (Acquisition phase), όπου τα αποδεικτικά στοιχεία αποκτώνται με αποδεκτό και κατάλληλο τρόπο, κατόπιν έγκρισης από την αρμόδια αρχή · το στάδιο **"Αναγνώρισης"** (Identification phase), όπου όπου γίνονται οι απαραίτητες διεργασίες για να αναγνωριστούν τα ψηφιακά πειστήρια που αποκτήθηκαν και να μετατραπούν σε μορφή κατανοητή από τον άνθρωπο ·το στάδιο της **"Αξιολόγησης"** (Evaluation phase), στο οποίο προσδιορίζεται εάν τα στοιχεία που εντοπίστηκαν κατά το προηγούμενο στάδιο είναι πράγματι σχετικά με την υπόθεση που ερευνάται και εάν μπορούν να θεωρηθούν ως νόμιμα αποδεικτικά στοιχεία · τέλος το στάδιο της**"Παραδοχής"** (Admission), όπου τα αποκτηθέντα και εξαχθέντα ψηφιακά πειστήρια παρουσιάζονται στο Δικαστήριο. [24]

iii. **DFRWS Investigative Model**

Το 2001, ο Palmer, πρότεινε το μοντέλο "**DFRWS Investigative Model"**, το οποίο αποτελείται από έξι βασικά στάδια. Συγκεκριμένα, αποτελείται από το στάδιο της **Ταυτοποίησης** (Identification), της **Διαφύλαξης** (Preservation), της **Συλλογής** (Collection), **της Εξέτασης** (Examination), της **Ανάλυσης** (Analysis) και της **Παρουσίασης** (Presentation).[25] Στο πρώτο στάδιο αυτό της Ταυτοποίησης, δημιουργείται προφίλ συστήματος και διενεργείται αναγνώριση τυχόν δυσλειτουργία στο σύστημα. Ακολουθεί, το στάδιο της διαφύλαξης

[24] Xiaoyu Du, Nhien-An Le-Khac, Mark Scanlon "*Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service*", School of Computer Science,University College Dublin, 2017
[25] Dr. Sudesh Rani, *"digital forensic models: a comparative analysis",* 2018

(preservation) κατά το οποίο διασφαλίζεται η ακεραιότητα και αξιοπιστία των δεδομένων που έχουν συγκεντρωθεί στο πλαίσιο της έρευνας. Κατά το συγκεκριμένο διαδικαστικό στάδιο θα πρέπει να διενεργείται και η ιεράρχηση των δεδομένων (chain of custody). Ακολουθεί το στάδιο της συλλογής (collection), όπου τα αποδεικτικά στοιχεία συγκεντρώνονται με την αξιοποίηση κατάλληλων ανακριτικών εργαλείων. Κατά το στάδιο της εξέτασης (examination) αμέσως μετά διενεργείται ιχνηλάτηση των πειστηρίων, εφαρμόζονται τεχνικές επικύρωσης και φιλτραρίσματος προκειμένου να ανακαλυφθούν αι να εξαχθούν τυχόν κρυμμένα στοιχεία. Στο στάδιο της ανάλυσης (analysis) πραγματοποιείται εξόρυξη δεδομένων (data mining) ενώ στο τελικό στάδιο αυτό της παρουσίασης (presentation) ο ερευνητής παραδίδει τα ευρήματά του, φροντίζοντας να τα τεκμηριώσει καταλλήλως.

iv. **Abstract Digital Forensic Model (ADFM)**

Κατόπιν εξέτασης διαφόρων μοντέλων ψηφιακής εγκληματολογίας, το 2002, οι Reith, Carr, & Gunsch, πρότειναν το μοντέλο "**Abstract Digital Forensic Model (ADFM)**[26]", βασιζόμενοι στο μοντέλο DFRWS ως πηγή έμπνευσης. Το μοντέλο αυτό αποτελείται από οκτώ διακριτά στάδια. Το στάδιο της **Ταυτοποίησης** (Identification), της **Προετοιμασίας** (Preparation), της **Στρατηγικής Προσέγγισης** (Strategy Approach), της **Διατήρησης** (Preservation), της **Συλλογής** (Collection), της **Εξέτασης** (Examination), της **Ανάλυσης** (Analysis), της **Παρουσίασης** (Presentation) και της **Επιστροφής Αποδεικτικών Στοιχείων** (Returning Evidence)[27].

v. **The Integrated Digital Investigation Process Model (IDIP)**

Το 2003, το μοντέλο "**The Integrated Digital Investigation Process Model (IDIP)",** προτάθηκε από τους **Carrier** και Spafford[28]. Το συγκεκριμένο μοντέλο προτείνει μια ενοποιημένη διαδικασία αντιμετώπισης φυσικών και ψηφιακών πειστηρίων. Στο πλαίσιο του συγκεκριμένου μοντέλου διαχωρίζεται η έρευνα του ψηφιακό τόπο εγκλήματος από αυτή

[26] Khuram Mushtaque *"Digital Forensic Investigation Models, an Evolution study",* 2015
[27] Dr. Sudesh Rani, *"digital forensic models: a comparative analysis*" 2018
[28] Kohn, M.D., Eloff, M.M. and Eloff, J.H.P., "Integrated Digital Forensic Process Model Computers & Security", 2018

του φυσικού. Τα πειστήρια, τα οποία εντοπίζονται στον φυσικό του εγκλήματος τα χειρίζεται κατ' αρχήν ο ανακριτικός υπάλληλος που διενεργεί την έρευνα ως φυσικές αποδείξεις, σύμφωνα με τους κανόνες που προβλέπονται για αυτές. Κατ' εξαίρεση μόνο φυσικές και ψηφιακές αποδείξεις διαχειρίζονται με ενιαίο τρόπο εάν οι πρώτες είναι πηγές , δηλαδή υλικοί φορείς των δεύτερων. Το μοντέλο αναλυτικά περιλαμβάνει 17 επιμέρους υποστάδια .

vi. **The Enhanced Integrated Digital Investigation Process (EIDIP)**

Το 2004, τομοντέλο "**The Enhanced Integrated Digital Investigation Process (EIDIP)",**[29] [30] το οποίο αποτελεί μια βελτιωμένη εκδοχή του "Integrated Digital Investigation Process Model" (IDIP), προτάθηκε από τους Venansius Baryamureeba και Florence Tushabe. Οι εμπνευστές του επεδίωκαν να επανακαθορίσουν την διαδικασία συλλογής και εξέτασης ψηφιακών και φυσικών πειστηρίων. Το συγκεκριμένο μοντέλο αποτελείται επίσης από πέντε βασικά στάδια. Κατά το πρώτο στάδιο **"Ετοιμότητας"(Readiness Phase)**, κύριος σκοπός είναι να διασφαλιστεί ότι η διαδικασία θα πραγματοποιηθεί από άρτια εκπαιδευμένα και πλήρως εξοπλισμένα πρόσωπα (Operations Readiness phase) και σε εγκαταστάσεις / δομές ικανές να εξυπηρετήσουν τις ανάγκες της διαδικασίας (Infrastructure Readiness Phase). Το επόμενο στάδιο, αυτό της "**Ανάπτυξης" (Deployment phases),** εκτελείται στον τόπο τέλεσης της εγκληματικής πράξης και αποτελείται από πέντε υπο στάδια. Το υποστάδι του "Εντοπισμού και της Ειδοποίησης" (Detection and Notification phase), της " Ερευνας του Φυσικού περιβάλλοντος του τόπου του Εγκλήματος"(Physical Crime Scene Investigation), της έρευνας του "Ψηφιακού Περιβάλλοντος του τόπου του εγκλήματος"(Digital crime scene investigation phase), της "Επιβεβαίωσης" (Confirmation phase) και αυτό της "Υποβολής" (Submission phase). Το στάδιο που ακολουθεί είναι αυτό της **"Ανίχνευσης"** (Traceback phases). Σε αυτό το στάδιο, εντοπίζεται και διερευνάται η φυσική σκηνή του εγκλήματος προκειμένου να αναγνωριστούν οι συσκευές που πιθανώς χρησιμοποιήθηκαν για την εκτέλεση της εγκληματικής πράξης. Στο στάδιο της **"Εξουσιοδότησης"** (Authorization phase)λαμβάνεται η απαραίτητη κατα τον νόμο έγκριση από αρμόδιες δικαστικές αρχές προκειμένου να

[29] Khuram Mushtaque,"*Digital Forensic Investigation Models, an Evolution study",* 2015
[30] Baryamureeba, V. and Tushabe, F, "The Enhanced Digital Investigation Process Model", Fourth Digital Forensic Research Workshop, 2004

επιτραπεί διενέργεια περαιτέρω έρευνας και να αποκτηθεί πρόσβαση σε περισσότερες πληροφορίες. Σε επόμενο στάδιο (Dynamite phases) ερευνάται η κύρια σκηνή του εγκλήματος, συλλέγονται και αναλύονται τα αντικείμενα που βρέθηκαν στον κύριο τόπο του εγκλήματος προκειμένου να ληφθούν περαιτέρω στοιχεια για το έγκλημα Το στάδιο αυτό αποτελείται από πέντε υποστάδια. Το στάδιο διερεύνησης της φυσικής σκηνής του εγκλήματος (Physical Crime Scene Investigation phase), το στάδιο διερεύνησης της ψηφιακής σκηνής του εγκλήματος (Digital crime scene investigation phase), το στάδιο ανασυγκρότησης(Reconstruction phase), που περιλαμβάνει τη συναρμολόγηση των κομματιών ενός ψηφιακού παζλ και τον εντοπισμό των πιο πιθανών ερευνητικών υποθέσεων, το στάδιο επικοινωνίας (Communication phase), που περιλαμβάνει την παρουσίαση των τελικών ερμηνειών και συμπερασμάτων σχετικά με τα φυσικά και ψηφιακά αποδεικτικά στοιχεία που έχουν διερευνηθεί και το στάδιο της ανασκόπησης (Review phase), όπου η όλη έρευνα επανεξετάζεται και εντοπίζονται τομείς βελτίωσης[31].

vii. **Digital Forensics Investigation Model (DFIM)**

Το 2011, από τους Ademu, Imafidon και Preston, προτάθηκε το μοντέλο **"Digital Forensics Investigation Model (DFIM)"**[32]. Το μοντέλο αυτό αποτελείται από 4 στάδια με επαναλαμβανόμενες διαδικασίες. Στο πρώτο στάδιο, της **"προετοιμασίας"** πραγματοποιείται προετοιμασία, αναγνώριση, εξουσιοδότηση και επικοινωνία. Σε επόμενο στάδιο, αυτό της **"αλληλεπίδρασης"** συλλέγονται, διατήρούνται και τεκμηρίωνονται τα δεδομένα. Στο στάδιο της "**ανοικοδόμησης**" εξετάζονται και αναλύονται τα δεδομένα μέσω εκτέλεσης διερευνητικών δοκιμών. Ενώ έπεται το τέταρτο και τελευταίο στάδιο που είναι η **"παρουσίαση"**[33].

viii. Model for Hybrid Evidence Investigation

[31] Baryamureeba, V. and Tushabe, F., "The Enhanced Digital Investigation Process Model", Fourth Digital Forensic Research Workshop, 2004

[32]Mohammad Qatawneh, W. Almobaideen, "*DFIM: a new digital forensics investigation model for internet of things*", 2020

[33] Mohammad Qatawneh, Wesam Almobaideen, Mohammed Khanafseh, Ibrahim Al Qatawne, *"HDFM: a new digital forensics investigation model for internet of things",* 2019

Το 2013, οι Βλαχόπουλος, Μάγκος και Χρυσικόπουλος, πρότειναν το υβριδικό μοντέλο " Model for Hybrid Evidence Investigation"[34]. Το συγκεκριμένο μοντέλο δύναται να τύχει εφαρμογής τόσο σε περιστατικά στα οποία υπάρχουν τόσο φυσικά όσο και ψηφιακά πειστήρια, από κοινού ή διακριτά. Το μοντέλο αυτό αποτελείται από 4 βασικά στάδια και 12 υποστάδια. Το πρώτο στάδιο της **Προετοιμασίας (Preparation)**, περιλαμβάνει το υποστάδιο της **Ειδοποίησης** (Notification) ότι διαπράχθηκε ένα έγκλημα, της λήψης **Εξουσιοδότησης** (Authorization) από την αρμόδια αρχή και της **Προετοιμασίας** (Preparation) των εργαλείων και του ανθρώπινου δυναμικού που θα διεξάγει την έρευνα. Το δεύτερο στάδιο, αυτό της "Έρευνας του τόπου του εγκλήματος" (Crime scene investigation), περιλαμβάνει τα υποστάδια της **Διατήρησης** (Preservation), κατά το οποίο αρμόδιος ανακριτικός υπάλληλος φροντίζει για την ασφάλεια του τόπου έρευνας, της "**Ταυτοποίησης**" (Identification), όπου και αναγνωρίζονται τα πιθανά πειστήρια, της "**Συλλογής – Εξέτασης"** (Collection-Examination), όπου ο ερευνητής συγκεντρώνει τόσο φυσικά όσο και ψηφιακά δεδομένα που συνδέονται με την εγκληματική πράξη και της "Μεταφοράς" (Transportation) των αποδεικτικών στοιχείων. Στο τρίτο στάδιο, αυτό της "Εργαστηριακής εξέτασης" (Laboratory examination) περιλαμβάνεται η **Εξέταση** (Examination) των εξαχθέντων στοιχείων στο εργαστήριο, η **Αποθήκευση** (Storage) των πειστηρίων σε ασφαλή χώρο και η **Αναφορά** (Report) των αποτελεσμάτων της εργαστηριακής εξέτασης. Στο τέταρτο και τελευταίο στάδιο, αυτό των "**Συμπερασμάτων"** (Conclusion), περιλαμβάνεται η Ανακατασκευή (Reconstruction) της σκηνής του εγκλήματος κατά την οποία αξιολογούνται τα στοιχεία και παρουσιάζονται τα γεγονότα και **η Διάχυση** (Dissemination) κατά την οποία διενεργείται ανασκόπηση της έρευνας προκειμένου αυτή να αποτελέσει εργαλείο στην αντιμετώπιση μελλοντικά αντίστοιχων περιπτώσεων.

4. Το Ισχύον νομοθετικό καθεστώς σε Εθνικό Επίπεδο

4.1 Τα δικονομικά χαρακτηριστικά – Αρχές της Ανακριτικής Διαδικασία

Η ανακριτική διαδικασία πλαισιώνεται από κανόνες, που διέπουν τον τρόπο λειτουργίας των ανακριτικών υπαλλήλων καθώς και το προϊόν της εξαγωγικής διαδικασίας, δηλαδή τις αποδείξεις. Οι κανόνες αυτοί διαμορφώθηκαν σύμφωνα με θεσμικές αρχές, οι

[34] Konstantinos Vlachopoulos, Emmanouil Magkos, and Vassileios Chrissikopoulos, *"A model for hybrid evidence investigation",* International Journal of Digital Crime and Forensic, 2016

οποίες και προσδίδουν συγκεκριμένα χαρακτηριστικά στην ποινική διαδικασία, ως σύνολο. Βασικές αρχές που διαπνέουν την ανακριτική διαδικασία στο σύνολο της είναι αυτές της *"**αυτεπάγγελτης συγκέντρωσης αποδεικτικού υλικού**", της "**αναλογικότητας**"και ενίοτε της " **μυστικότητας**".*

Σύμφωνα με την αρχή της "**αυτεπάγγελτης συγκέντρωσης του αποδεικτικού υλικού",** τα ανακριτικά όργανα είναι επιφορτισμένα με την διενέργεια ανακριτικών πράξεων. Από μια άλλη σκοπιά τα τελευταία είναι αρμόδια για την συγκέντρωση υλικού που σχετίζεται με την υπό έρευνα αξιόποινη δράση. Δεν δεσμεύονται από τις θέσεις και διαθέσεις των εμπλεκομένων προσώπων και δρουν δίχως να αναμένουν πρωτοβουλίες των ενδιαφερομένων προσώπων. Το έργο της ανακριτικής διαδικασίας θεωρείται ότι ολοκληρώνεται όταν έχουν εξαντληθεί, μέσα από την έρευνα, όλες οι πιθανές εκδοχές σχετικά με τον εντοπισμό της αλήθειας αναφορικά με την τέλεση της πράξης. Η ανακριτική διαδικασία πάντως κινείται σε επίπεδο ενδείξεων ενοχής, δεδομένου ότι τελικά η απόδειξη της ενοχής επιφυλάσσεται για τον Δικαστή, ο οποίος είναι επιφορτισμένος με την κρίση περί αθωότητας ή ενοχής εφόσον η υπόθεση τελικα παραπεμφθεί είτε από τον Εισαγγελέα με απευθείας κλήση, είτε από το αρμόδιο δικαστικό συμβούλιο με βούλευμα, στο ακροατήριο.

Η **αρχή της αναλογικότητας**, η οποία διαπνέει το δικαιικό μας σύστημα εν γένει, αποτελεί εξίσου σημαντική παράμετρο και στην ανακριτική έρευνα. Η ενσωμάτωση αυτής στην ανακριτική διαδικασία σχετίζεται με την εφαρμογη θεμελιωδών αρχών και κανόνων που δημιουργούν ένα δίχτυ προστασίας για τις ατομικές ελευθερίες και τα δικαιώματα των εμπλεκόμενων προσώπων. Πιο συγκεκριμένα, σύμφωνα με την αρχή της αναλογικότητας, οι δράσεις που εντάσσονται στην ανακριτική δραστηριότητα πρέπει να *"αποτελούν την προσφορότερη και αποτελεσματικότερη για τον επιδιωκόμενο σκοπό ενέργεια, να λαμβάνουν χώρα μόνο στο μέτρο του αναγκαίου για την επίτευξη του σκοπού αυτού και να φροντίζουν τον σκληρό πυρήνα των ατομικών δικαιωμάτων των θιγομένων προσώπων, στο μέτρο που τέτοιες ενέργειες ξεπερνούν το αναγκαίο μέτρο, ήτοι αποτελούν την όχι λιγότερο επαχθή επιλογή"*[35].

Εν αντιθέσει με την κύρια επ' ακροατηρίω ποινική διαδικασία, η ανακριτική έρευνα και γενικότερα το στάδιο της προδικασίας διέπεται από **μυστικότητα** των ενεργειών των εμπλεκόμενων λειτουργών. Η μυστικότητα που καλύπτει την δράση των εμπλεκόμενων

[35] Χ. Σεβαστίδης, *«Κώδικας Ποινικής Δικονομίας, ερμνεία κατ' άρθρο»,* 2015

λειτουργών έχει διττό σκοπό. Από την μία εξυπηρετεί και προστατεύει την ίδια την έρευνα, διασφαλίζοντας την αποτελεσματικότητα της διαδικασίας ως σύνολο και από την άλλη προστατεύει την προσωπικότητα των εμπλεκόμενων μερών, ήτοι του κατηγορουμένου, αλλά ενίοτε και του καταγγέλλοντος – θύματος. Πιο συγκεκριμένα, τυχόν δημόσια έκθεση των ενεργειών των αρμοδίων υπαλλήλων, ενδεχομένως θα διευκόλυνε τεχνικές συγκάλυψης και θα οδηγούσε είτε σε παρεμπόδιση της δράσης τους είτε και σε καταστροφή ή αλλοίωση των πειστηρίων, πριν την επέμβαση των ανακριτικών υπαλλήλων ή πάντως θα εξέθετε τα εμπλεκόμενα πρόσωπα σε κίνδυνο. Η αρχή της μυστικότητας κάμπτεται πάντως αναφορικά με την άσκηση δικαιωμάτων του κατηγορουμένου αλλά και του παρισταμένου προς υποστήριξη της κατηγορίας, μέσα από την αναγνώριση στον καθένα από αυτούς δικαιωμάτων, που στόχο έχουν την πληροφόρησή τους αναφορικά με την πορεία των ανακριτικών ενεργειών και των αποτελεσμάτων τους

Συμφώνως προς το άρθρο 178 § 1 του ΚΠΔ, στην ανακριτική διαδικασία επιτρέπεται κατ' αρχήν η χρήση κάθε αποδεικτικού μέσου. Η δε αναφορά σε ειδικότερες κατηγορίες αποδεικτικών μέσων *(λ.χ. έγγραφα, μάρτυρες, πραγματογνωμοσύνη κ.λπ.)* έχει σαφώς ενδεικτικό και όχι αποκλειστικό χαρακτήρα, σύμφωνα με την βούληση του ιστορικού νομοθέτη.

4.2 Παραγγελία για ποινική έρευνα και κίνηση ποινικής δίωξης

Η ποινική δίωξη, ασκείται στο όνομα της Ελληνικής Πολιτείας, η οποία είναι και ο μοναδικός και αποκλειστικός φορέας εξουσίας. Κινείται δε αυτή in rem και όχι in personam, δηλαδή αναφέρεται σε συγκεκριμένη αξιόποινη πράξη και είναι αποδεσμευμένη από την απόδοση αυτής σε συγκεκριμένο πρόσωπο ως υπαίτιο.

Με την αρμοδιότητα τόσο για κίνηση της ποινικής δίωξης, όσο και για επιχείρηση και εποπτεία ερευνών σχετικά με την εξιχνίαση, προετοιμασία – συγκέντρωση αποδεικτικού υλικού μέχρι την τελική παραπομπή σε δίκη κατηγορουμένου, ή την με οποιονδήποτε άλλο προβλεπόμενο τρόπο, παύση της ποινικής δίωξης, είναι επιφορτισμένος κατά κανόνα ο Εισαγγελέας Πλημμελειοδικών κατά το άρθρο 27 παράγραφος 1 του ΚΠΔ. Κατ' εξαίρεση σύμφωνα με την ιεραρχική δομή της Εισαγγελικής Αρχής και κατά τα οριζόμενα στο άρθρο 28 παράγραφος 1 του ΚΠΔ σε εγκλήματα εξαιρετικής σημασίας το αρμόδιο Συμβούλιο

Εφετών δύναται να διατάξει τον Εισαγγελέα Εφετών να προβεί εκείνος στην άσκηση ποινικής δίωξης.

Ανακριτικές ενέργειες δύναται να διαταχθούν από τον αρμόδιο Εισαγγελικό λειτουργό τόσο πριν την κίνηση της ποινικής δίωξης, με σκοπό την αποδεικτική ενίσχυση αυτής και την εν γένει αξιοποίηση πληροφοριών αναφορικά με διάπραξη αξιόποινης πράξης, όσο και μετά από΄ αυτή. Ο αρμόδιος Εισαγγελέας δύναται να διατάσσει προκαταρκτική εξέταση ή προανάκριση[36]. Τόσο στις δύο αυτές περιπτώσεις, όπως και στην περίπτωση της ανάκρισης, η παραγγελία του Εισαγγελέα Πλημμελειοδικών καθορίζει και διαγράφει τα επιτρεπτά πλαίσια της έρευνας. Αποδέκτης της παραγγελίας του Εισαγγελέα Πλημμελειοδικών περί διενέργειας συγκεκριμένης ανακριτικής πράξης είναι κάποιος ανακριτικός υπάλληλος, από τον κύκλο των προσώπων που καθορίζονται στο άρθρο 31 ΚΠΔ με σαφή αναφορά/παραπομπή της διάταξης σε ειδικότερα νομοθετήματα.

4.3 Η αστυνομική έρευνα

Από την ανακριτική έρευνα, η οποία δύναται να επιχειρείται και από αστυνομικούς, ως ανακριτικούς υπαλλήλους, κατά τα ορισμένα στο άρθρο 31 του ΚΠΔ διακρίνεται σαφώς, και τους κανόνες που την διέπουν, η αστυνομική έρευνα, τόσο ως προς τα όρια όσο και ως προς τον σκοπό διενέργειας της. Η τελευταία εντάσσεται στο πλέγμα των διοικητικών αρμοδιοτήτων των σωμάτων ασφαλείας. Πρόκειται για έρευνα που διενεργείται κατά την κρίση κρίση του αστυνομικού υπαλλήλου, που εκτιμά ότι υπάρχει συνθήκη που αφορά προπαρασκευή ή τέλεση αξιόποινης πράξης και σύμφωνα με αυτή, χωρίς να μεσολαβεί ενέργεια εισαγγελικού λειτουργού.

Το πλαίσιο της διενεργούμενης από τους αστυνομικούς υπαλλήλους, έρευνας ενεργούντων στα πλαίσια των αστυνομικών και όχι των ανακριτικών τους αρμοδιοτήτων, σκιαγραφείται από τα άρθρα 93 και ειδικότερα 96 επ. του ΠΔ 141/1991149. Η αστυνομική έρευνα δύναται να περιλαμβάνει ακόμα και έρευνα σε κατοικία, εφόσον πάντως αυτή γίνεται με τη προηγούμενη ρητή και μη εξαναγκασμένη συναίνεση του ενοίκου της. Επιπλέον, σε αυτή υπάγονται και έρευνες σε μέσα μεταφοράς, σωματικές έρευνες, έρευνες σε ιδιωτικούς χώρους πλην της κατοικίας και σε δημόσιους, ελεύθερα προσβάσιμους σε όλους χώρους .

[36] Π. Παπανδρέου, «*Η Προκαταρκτική εξέταση»*, ΠοινΔικ 2006

Σε κάθε περίπτωση, κατά την διενέργεια των σχετικών ερευνών, θα πρέπει στο μέτρο του δυνατού να διασφαλίζεται ότι δεν προκαλείται αδικαιολόγητη ενόχληση του προσώπου που υποβάλλεται σε έρευνα ή συνδέεται με αυτή και να μην προσβάλλεται η προσωπικότητα του.

4.4 Ανακριτικές Πράξεις

i. Έρευνα

Η **έρευνα**, αποτελεί μεταξύ άλλων, νομοθετικά προβλεπόμενη στον Κώδικα Ποινικής δικονομίας **ανακριτική πράξη** και ειδικότερα ρυθμίζεται στα άρθρα 243 επ. αυτού. Με την διενέργεια της ανακριτικής αυτής πράξης, αποσκοπείται η συγκέντρωση δεδομένων κρίσιμων, είτε για τη απόδειξη διάπραξης συγκεκριμένης εγκληματικής πράξης, είτε για την αποκάλυψη και τον εντοπισμό των φερόμενων δραστών, είτε, τέλος, για τη πιστοποίηση και αποκατάσταση τυχόν προκληθείσας στον παθόντα ζημίας.

Η έρευνα, ως ανακριτική πράξη, ως μέτρο δηλαδή δικονομικού καταναγκασμού, από την φύση της, άνευ ετέρου, προσβάλλει συνταγματικά προστατευόμενα ατομικά δικαιώματα, όπως το άσυλο της κατοικίας, την αξία και την τιμή του ανθρώπου.

Κατά τα οριζόμενα στο άρθρο 253 του νέου Κώδικα Ποινικής Δικονομίας, η ανακριτική πράξη της έρευνας δύναται να διενεργηθεί, τόσο για κακούργημα όσο και για πλημμέλημα, εφόσον άρχισε οιαδήποτε ανακριτική διαδικασία. Στην προισχύσασα μορφή, πρώτού δηλαδή τροποποιηθεί με το άρθρο 8 του Ν.4637/2019 (Α΄180), η εν λόγω διάταξη, προέβλεπε ρητά την διενέργεια ανάκρισης, ως απαραίτητη προϋπόθεση για τη διεξαγωγή ερευνών. *"Πλέον, εφόσον κρίνεται σκόπιμο και μάλιστα προς την κατεύθυνση της ανεύρεσης της ουσιαστικής αλήθειας, καθίσταται δυνατή η διενέργεια ερευνών κατά τη διεξαγωγή της εν γένει ανακριτικής διαδικασίας κι έτσι ουδέν περιθώριον ερμηνευτικής ασάφειας ή κενού αφήνεται από τον Νομοθέτη"*. [37].

Ειδικότερα, στην έννοια της ανακριτικής διαδικασίας εμπίπτουν, η προκαταρκτική εξέταση, η προανάκριση και η κυρία ανάκριση. Η προκαταρκτική εξέταση διατάσσεται σύμφωνα με το άρθρο 31 παρ. 1^{α} του ΚΠΔ, από τον αρμόδιο Εισαγγελικό λειτουργό

[37] Κωνσταντίνος Χριστόπουλος, "*Η σκοπιμότητα των ερευνών και των ειδικών ανακριτικών πράξεων επι ορισμένων εγκλημάτων"*, 2021

προκειμένου ο τελευταίος εν συνεχεία να αποφασίσει εάν στην προκειμένη περίπτωση θα πρέπει να κινήσει ποινική δίωξη, ή συμπληρωματικά να διατάξει προανάκριση ή κύρια ανάκριση . Προκαταρκτική εξέταση, σύμφωνα με το άρθρο 245 του ΚΠΔ μπορεί να διαταχθεί πριν την κίνηση της ποινικής δίωξης και σε περίπτωση αυτόφωρου κακουργήματος ή πλημμελήματος αλλά και κατόπιν αυτής σύμφωνα με το άρθρο 243 του ΚΠΔ

Συνοψίζοντας, από την συνδυαστική θεώρηση των άρθρων 253 επ. του ΚΠΔ συνάγεται ότι η διενέργεια έρευνας είναι επιτρεπτή εφόσον : 1. Έχει ξεκινήσει η ανακριτική διαδικασία, ήτοι εφόσον έχει παραγγελθεί από τον αρμόδιο Εισαγγελέα η διενέργεια προκαταρκτικής εξέτασης, προανάκρισης ή κύριας ανάκρισης για κακούργημα ή πλημμέλημα, ή πάντως ενεργείται αστυνομική προανάκριση σύμφωνα με το άρθρο 245 παρ. 2 του ΚΠΔ χωρίς προηγούμενη εισαγγελική εντολή, 2. εύλογα συμπεραίνεται ότι η διενέργεια έρευνας αποτελεί πρόσφορο μέσο προς την αποκάλυψη τελεσθείσας εγκληματικής ενέργειας ή δράστη ή την αποκατάσταση προκληθείσας ζημίας.

Σε περίπτωση που η έρευνα δεν διεξάγεται από δικαστικό λειτουργό αλλά από αστυνομικό υπάλληλο, συμπράττει υποχρεωτικά πάντοτε ως δεύτερος ανακριτικός υπάλληλος δικαστικός λειτουργός. Η θεσμοθετημένη παρουσία δικαστικού λειτουργού, κατά την διενέργεια έρευνας αποσκοπεί στην διασφάλιση των ατομικών δικαιωμάτων του ερευνώμενου αλλά και στην διασφάλιση της αντικειμενικότητας των ευρημάτων και στην αποτροπή ψευδών αποτελεσμάτων, όπως επί παραδείγματι την παράνομη απόκρυψη ευρημάτων ή την ενοχοποίηση αθώου.

Αν δεν συμπράττει δικαστικός λειτουργός ή μέχρι της αφίξεώς του τα αστυνομικά όργανα προβούν σε κατ' οίκον έρευνα, αυτή είναι μη νόμιμη.[38]

Ανακριτική πράξη έρευνας συνιστά και η έρευνα που πραγματοποιείται σε ηλεκτρονικό σύστημα υπολογιστή, ενώ όπως θα αναλυθεί παρακάτω η αντιγραφή των δεδομένων που θα εντοπιστούν κατά την έρευνα συνιστά κατάσχεση.

[38] Κ. Φράγκος, «Κατ' άρθρο ερμηνεία Κώδικα Ποινικής Δικονομίας», Sakkoulas-Online.gr, 2020

ii. Άσυλο κατοικίας - Έρευνες

Η προστασία της κατοικίας σε συνταγματικό εθνικό επίπεδο θεμελιώνεται στα άρθρα 9 και 19 του Συντάγματος. Πέραν τούτου όμως, η κατοικία προστατεύεται και με διατάξεις υπερεθνικής ισχύος, ήτοι με το άρθρο 7 του ΧΘΔΑ, το άρθρο 8 παρ. 1 της ΕΣΔΑ, το άρθρο 17 παρ. 1 του ΔΣ/ΑΠΔ, το άρθρο 12 της ΟΔΔΑ και το άρθρο 6 παρ. 2 της Διακήρυξης του Ευρωπαϊκού Κοινοβουλίου. Ειδικότερα, "*παν πρόσωπο δικαιούται σε σεβασμό της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και της αλληλογραφίας του*" σύμφωνα με το άρθρο 8 της ΕΣΔΑ.

Η παραβίαση του ασύλου κατοικίας τυποποιείται και σε ποινικό επίπεδο, όπου ουσιαστικά η παραβίαση της συνεπάγεται την πλήρωση της αντικειμενικής υπόστασης των θεσμοθετημένων στα άρθρα 189, 241, 334 και 370Α παρ. 2 του ΠΚ ποινικών αδικημάτων.

Το «άσυλο κατοικίας» απαγορεύει την άνευ προηγούμενης συναίνεσης του κατόχου είσοδο και παραμονή οργάνων δημόσιας τάξης, εξοπλισμού έρευνας και παρακολούθησης ή και αστυνομικών σκύλων, στην προστατευόμενη κατοικία.[39] Πιο συγκεκριμένα, ααπαγορεύεται η επέμβαση των οργάνων επιβολής του νόμου, εκτός εάν η επέμβαση αυτή κατ' εξαίρεση ρητά επιτρέπεται από διάταξη νόμου και κρίνεται αναγκαία με βάση την αρχή της αναλογικότητας. Δηλαδή με άλλα λόγια, μόνο εφόσον η επέμβαση αυτή συνιστά μέτρο αναλογικό και απαραίτητο για την διασφάλιση της δημόσιας και εθνικής ασφάλειας, την προστασία της ανθρώπινης υγείας, των ηθικών αξιών, των ατομικών δικαιωμάτων και ελευθεριών των υποκειμένων , και μη δυνάμενο να επιτευχθεί με ηπιότερα μέσα.

Τέλος, με το άρθρο 171 παρ. 1 εδ. δ' ΚΠΔ, επιφυλάσσεται **ακυρότητα** και μάλιστα απόλυτη, για την περίπτωση παραβίασης των νομοθετικών διατάξεων που ρυθμίζουν τα δικαιώματα παρουσίας, υπεράσπισης και εκπροσώπησης κατηγορουμένου και υπόπτου.

[39] Δαγτόγλου, ΠΔ, *«Ατομικά Δικαιώματα»,* τόμος Α, εκδόσεις Αντ. Σάκκουλα, 2005

iii. Κατάσχεση

- Κατάσχεση “πραγμάτων”

Στο τρίτο κεφάλαιο του νέου ΚΠΔ (ν. 4620/2019), που φέρει τον τίτλο «ΚΑΤΑΣΧΕΣΗ» και αποτελείται από τα άρθρα 260 έως 269, είναι ενσωματωμένες όπως συμπληρώθηκαν και διαμορφώθηκαν, οι ρυθμίσεις που αφορούν τη δέσμευση περιουσιακών στοιχείων, την κατάσχεση, την παρακατάθεση, την φύλαξη πραγμάτων αλλά και την κατάσχεση πλέον ψηφιακών δεδομένων και την άρση της κατάσχεσης.

Η κατάσχεση αποτελεί επίσης μία από τις νομοθετικά προβλεπόμενες στον Κώδικα Ποινικής Δικονομίας, ανακριτικές πράξεις. Η πράξη αυτή συνίσταται στην από ορισμένο πρόσωπο, **αφαίρεση της κατοχής πραγμάτων**, τα οποία συνδέονται με συγκεκριμένη εγκληματική πράξη, ως αντικείμενα αυτής ή εργαλεία/ μέσα διάπραξης της , ή προϊόντα της. Η αφαίρεση δε αυτή συντελείται προς ευόδωση της ανακριτικής διαδικασίας και δη με σκοπό την σσυγκέντρωση και διατήρησης αποδείξεων ή και με σκοπό την διασφάλιση της επιβαλλόμενης δήμευσης ή νομοθετικά προβλεπόμενης καταστροφής αυτών.

Η κατάσχεση παραδοσιακά συνδέεται με την αφαίρεση **αντικειμένων**, δηλαδή ενσώματων πραγμάτων, συμπεριλαμβανομένων των **εγγράφων**, από την κατοχή κάποιου προσωρινά ή οριστικά, εφόσον ακολουθήσει και δήμευση. Η κατάσχεση επιβάλλεται τόσο στο αντικείμενα που αποτέλεσαν μέσα τέλεσης όσο και στο αντικείμενα που αποτελούν προϊόντα εγκληματικής πράξης, ενώ δύναται να επιβληθεί και σε κάθε άλλο αντικείμενο που αποτελεί αποδεικτικό στοιχείο για το τελεσθέν έγκλημα.

Τυχαία ευρήματα, δηλαδή αποδεικτικά στοιχεία μέσω των οποίων αποκαλύπτεται ότι τελέστηκε ή προκαλούνται υπόνοιες ότι τελέστηκε έτερη εγκληματική πράξη ή εντοπίζεται άλλος δράστης για τον οποίο ως σήμερα δεν είχε ασκηθεί ποινική δίωξη, εάν προκύψουν κατά τη διενέργεια έρευνας για άλλη συγκεκριμένη αξιόποινη πράξη μπορούν να κατασχεθούν νόμιμα και να αξιοποιηθούν από τις ανακριτικές αρχές. Η αξιοποίηση αυτώ δικαιολογείται από τον νόμιμο χαρακτήρα της διενεργηθείσας έρευνας, ο οποίος πιστοποιείται από την παρουσία ανεξάρτητου δικαστικού λειτουργού.

Προς διασφάλιση της εξυπηρέτησης των ως άνω νομοθετικά προβλεπόμενων σκοπών σύμφωνα με τα προβλεπόμενα στην διάταξη του άρθρου 149 του ΚΠΔ , τα ανακριτικά όργανα είναι επιφορτισμένα με την σύνταξη **έκθεσης κατάσχεσης**. Κατά τα οριζόμενα στην σχετική

διάταξη *"Η έκθεση πρέπει να συντάσσεται στον τόπο όπου γίνεται η πράξη ή η δήλωση που βεβαιώνεται σ' αυτήν και στον ίδιο το χρόνο της ενέργειας ή, αν αυτό είναι αδύνατο, αμέσως κατόπιν".* Πάντως παρά την νομοθετική υπαγόρευση για "άμεση" σύνταξη της σχετικής έκθεσης στον τόπο και τον χρόνο διενέργειας της κατάσχεσης, προκειμένου να πιστοποιούνται με ακρίβεια οι διενεργηθείσες πράξεις/ ενέργειες, δεν απαγγέλλεται σχετική ακυρότητα σε περίπτωση μη τήρησης της σχετικής διαδικασίας, με αποτέλεσμα η σχετική αναφορά να αποτελεί απλώς προτροπή ή θα έλεγε κανείς ακόμα και ευχολόγιο.

- Κατάσχεση ψηφιακών πειστηρίων

Με τον νέο Κώδικα Ποινικής δικονομίας εισήχθει για πρώτη φορά ειδική, ρητή, νομοθετική πρόβλεψη για μια ειδικότερη μορφή κατάσχεσης, αυτή των ψηφιακών πειστηρίων. Σύμφωνα με την αιτιολογική έκθεση του Νέου Κώδικα Ποινικής Δικονομίας, "*Με τη ρύθμιση της διάταξης αυτής, που συνιστά μια επιβεβλημένη νεωτεριστική αποτύπωση επενέργειας της σύγχρονης τεχνολογικής εξέλιξης στην ποινική δίκη,* ***παρέχεται η απαραίτητη και δικαιοκρατικά / επαρκής νομική βάση για τη διενέργεια της συγκεκριμένης ανακριτικής πράξης, αφού, ενόψει του ότι τα ψηφιακά δεδομένα είναι άϋλα****, οποιαδήποτε ρύθμιση του Κώδικα που αναφέρεται* ***σε υλικά πειστήρια και έγγραφα, τα οποία είναι διακριτά έναντι των δεδομένων, δεν καταλαμβάνει την πραγματική φύση και τις ανάγκες αυτών****, ενώ, παράλληλα, παρέχονται οι δέουσες εγγυήσεις και προϋποθέσεις για την αποτροπή τυχόν αυθαιρεσιών, προβλέποντας τη σύνταξη ειδικής έκθεσης, τη χρήση κατάλληλου εξοπλισμού κατάσχεσης, τον περιορισμό της πρόσβασης μόνο σε εξουσιοδοτημένο προσωπικό, αλλά και μέτρα κατά της τυχαίας απώλειας και διαγραφής των ψηφιακών δεδομένων*"[40]. Κατά τα ανωτέρω, η ενσωμάτωση της προκείμενης ρύθμισης στο Τρίτο Κεφάλαιο του Νέου Κώδικα Ποινικής Δικονομίας συνιστούσε επιβεβλημένη ενέργεια προκειμένου να συμπληρωθεί το υφιστάμενο έως τότε νομοθετικό κενό, ενώ παράλληλα αντανακλούσε την επίδραση της διαρκώς εξελισσόμενης τεχνολογικής επιστήμης στην ποινική προδικασία και την ποινική δίκη.

Η ύπαρξη του συγκεκριμένου νομοθετικού κενού αλλά και η ανάγκη κάλυψης του με θέσπισης νέων ειδικών νομοθετικών διατάξεων, αναντίρρητα συνάγεται από την πάγια νομολογική αξίωση του Ευρωπαϊκού Δικαστηρίου Δικαιωμάτων του Ανθρώπου, να

[40] https://www.hellenicparliament.gr/UserFiles/c8827c35-4399-4fbb-8ea6-aebdc768f4f7/11027276.pdf

ρυθμίζεται ειδικά σε νομοθετική διάταξη κάθε επέμβαση των οργάνων δημόσιας τάξης στις ατομικές ελευθερίες και τα δικαιώματα του ατόμου αλλά και από την συνταγματικάά κατοχυρωμένη αρχή της “της επιφύλαξης νόμου ή της επιφύλαξης υπέρ του νόμου". Η ύπαρξη της ίδιας ανάγκης περαιτέρω επιβεβαιώνεται και από κυρωθείσα σε εθνικό επίπεδο με το νόμο 4411/2016 Σύμβαση της Βουδαπέστης για το Κυβερνοέγκλημα, η οποία αξίωνε την ενσωμάτωση αντίστοιχων ρυθμίσεων. [41]

Πιο συγκεκριμένα, με την Σύμβαση της Βουδαπέστης, αναγνωρίστηκαν στα Κράτη - μέλη, οι δυνατότητες να προβλέψουν σε εθνική νομοθεσία: έρευνα και κατάσχεση (και απομακρυσμένη έρευνα, γνωστοποίηση στοιχείων συνδρομητών, διατήρηση, κοινοποίηση, γνωστοποίηση δεδομένων επικοινωνιών και δεδομένων κίνησης και θέσης, συλλογή και αποθήκευση άμεσα από αρχές σε πραγματικό χρόνο δεδομένα κίνησης και θέσης επικοινωνιών, συλλογή και καταγραφή άμεσα από αρχές δεδομένα επικοινωνιών . Σύμφωνα με το άρθρο 19 παρ. 3 της Σύμβασης της Βουδαπέστης για το έγκλημα στον Κυβερνοχώρο *“Κάθε Συμβαλλόμενο Μέρος θα λάβει τα νομοθετικά και άλλα μέτρα που είναι αναγκαία για να δύνανται οι αρμόδιες αρχές του να κατάσχουν ή ομοίως να εξασφαλίζουν τα δεδομένα υπολογιστή στα οποία απέκτησαν πρόσβαση σύμφωνα με τις παραγράφους 1 ή 2. Τα μέτρα αυτά περιλαμβάνουν την εξουσία: α. να κατάσχουν ή ομοίως να ασφαλίζουν ένα σύστημα υπολογιστή ή μέρος αυτού ή ένα μέσον αποθήκευσης δεδομένων υπολογιστή,β. να παράγουν και να διατηρούν ένα αντίγραφο αυτών των δεδομένων υπολογιστή,γ. να διατηρούν την ακεραιότητα των σχετικών αποθηκευμένων δεδομένων υπολογιστή,δ. να καθιστούν απρόσιτα ή να αφαιρούν αυτά τα δεδομένα υπολογιστή από το εξεταζόμενο σύστημα υπολογιστή*.”[42]

Με το άρθρο 265 ΚΠΔ, ο εθνικός νομοθέτης ικανοποίησε τις τρεις από τις τέσσερις αξιώσεις του Συμβουλίου της Ευρώπης, αφού κατέστη εφικτό στις ανακριτικές αρχές “να κατάσχουν ένα σύστημα υπολογιστή”, “να παράγουν αντίγραφο”, “να διατηρούν ακεραιότητα”. Δεν προέβη ωστόσο σε συγκεκριμένη πρόβλεψη ώστε να καθίσταται εφικτό για τις αρχές να “καταστήσουν τα δεδομένα απρόσιτα”, αποκλείοντας την πρόσβαση σε αυτά χωρίς να τα αφαιρέσουν, ενδεχομενως με κλείδωμα υπολογιστή, αρχείου ή φακέλου. Η απουσία σχετικής πρόβλεψης αν και φαινομενικά μοιάζει δευτερεύουσα, μιας και ο ίδιος

[41] Κ. Φράγκος, «Κατ' άρθρο ερμηνεία Κώδικα Ποινικής Δικονομίας», Sakkoulas-Online.gr, 2020
[42] https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-4411-2016/symvasi-tis-voydapestis-gia-egklima-ston-kyvernohoro-0

σκοπός τις περισσότερες φορές μπορεί να επιτευχθεί και με την αφαίρεση, είτε του ίδιους του δεδομένου, είτε του υπολογιστικού συστήματος ή του μέσου αποθήκευσης, στο οποίο αυτό βρίσκεται, πρέπει ωστόσο να σημειωθεί ότι δεν στερείται ουσιαστικής πρακτικής σημασίας. Κι αυτό γιατί κάποιες φορές, λόγω της ίδιας της φύσης των ψηφιακών δεδομένων αλλά και των πληροφοριακών συστημάτων, τυχόν αντιγραφή αρχείου μπορεί να οδηγήσει σε αλλοίωση ή απώλεια κρίσιμων δεδομένων π.χ. μεταδεδομένων, αφού με την ενέργεια αντιγραφής ουσιαστικά δημιουργείται ένα νέο αρχείο, με νέα μεταδεδομένα. Αλλά και απο μια τελείως διαφορετική σκοπιά, πρακτικά η δυνατότητα "αποκλεισμού πρόσβασης - με κλείδωμα" ενός λογαριασμού ή κάποιων φακέλων, είναι κρίσιμης σημασίας και για περιπτώσεις όπου τα υπό κατάσχεση δεδομένα βρίσκονται αποθηκευμένα σε πληροφοριακό σύστημα επιχείρησης. Σε μια τέτοια περίπτωση, από την μία τυχόν αντιγραφή όλων των αρχείων είναι πρακτικά ασύμφορη ή πάντως δυσχερής λόγω του μεγάλου όγκου δεδομένων αι από την άλλη η τυχόν αφαίρεση όλων των πληροφοριακών συστημάτων, αντί του περιορισμού πρόσβασης, μπορεί να προκαλέσει σημαντική βλάβη στην ερευνόμενη επιχείρηση, συνιστώντας ενδεχομένως και νόμιμη βάση διεκδίκησης αποζημίωσης στα πολιτικά δικαστήρια. Ο ίδιος ακριβώς ισχυρισμός θα μπορούσε στο πλαίσιο της αρχής της αναλογικότητας να διατυπωθεί και από κάθε ύποπτο, από την κατοχή του οποίου κατάσχεται ολόκληρο πληροφοριακό σύστημα, αντί του αποκλεισμού πρόσβασης σε συγκεκριμένα αρχεία, ως σημαντικά επαχθέστερη ενέργεια. Έχει πάντως διατυπωθεί η άποψη ότι παρά την έλλειψη ειδικής συγκεκριμένης αναφοράς, ότι *" το κλείδωμα των δεδομένων επιτόπου, χωρίς αφαίρεση τους από το σύστημα στο οποίο είναι αποθηκευμένα, είναι νοητό με βάση το επιχείρημα εκ του μείζονος το έλασσον"* δεδομένου ότι χωρεί το μείζον δηλαδή η αφαίρεση του υλικού φορέα μαζί με το σύνολο των δεδομένων που αυτό περιέχει. [43]

Πιο συγκεκριμένα, με τη διάταξη του 265 ΚΠΔ, αναγνωρίστηκε στις ανακριτικές αρχές, ρητά η δυνατότητα, να διενεργούν κατάσχεση, των ψηφιακών δεδομένων και αυτοτελώς και όχι μόνο των υλικών φορέων, στους οποίους αυτά είναι αποθηκευμένα. Η κατάσχεση ψηφιακών δεδομένων μπορεί να επιβληθεί:

*«α) Σε ένα **σύστημα υπολογιστή** στο σύνολό του ή σε μέρος αυτού και **στα δεδομένα υπολογιστή που είναι αποθηκευμένα σε αυτόν**, στα οποία έχει **φυσική πρόσβαση** εκείνος που διενεργεί την ανάκριση»*[44]

[43] Γ. Ναζίρης, *" Η κατάσχεση ψηφιακών Δεδομένων",* Ποινική Δικαιοσύνη, Τεύχος Φεβρουάριος 2020
[44] ΦΕΚ

Κάθε υπολογιστικό σύστημα περιλαμβάνει υλικό *(hardware)* και λογισμικό *(software)* μέρος. Τα βασικά στοιχεία που συνθέτουν το υλικού μέρους κάθε υπολογιστικού συστήματος είναι ο επεξεργαστής ή άλλως η κεντρική μονάδα επεξεργασίας *(Central Processing Unit - CPU)*, που εκτελεί λογικές/αριθμητικές πράξεις, η κεντρική μνήμη *(Ram)*, που επιτρέπει την καταγραφή και ανάκληση των εκτελούμενων εντολών, δευτερεύουσα - περιφερειακή μνήμη, μονάδες εισόδου και εξόδου *(input/output)* και περιφερειακές συσκευές .

Εν προκειμένω ρυθμίζεται η κατάσχεση δεδομένων, από ένα σύστημα υπολογιστή που εντοπίζεται σε φυσικό χώρο από ανακριτικό υπάλληλο κατά την διάρκεια της έρευνας, είτε μέσω κατάσχεσης του υλικού φορέα είτε μέσω κατάσχεσης των ίδιων των ψηφιακών δεδομένων. Η δυνατότητα κατάσχεσης των ίδιων των δεδομένων, χωρίς να είναι απαραίτητη και η αφαίρεση του υλικού φορέα, συνιστά μια καινοτομία του νέου κώδικα ποινικής δικονομίας, μείζονος σημασίας, δεδομένου ότι η αφαίρεση του υλικού φορέα που αποτελούσε μονόδρομο κατά το προϊσχύσαν δίκαιο, είναι αν οχι τις περισσότερες φορές περιττή πάντως κατά βάση δυσανάλογη και ανεπιεικής.

«β) *σε ένα **μέσο αποθήκευσης δεδομένων υπολογιστή**, στο οποίο υπάρχουν αποθηκευμένα δεδομένα υπολογιστή και έχει φυσική πρόσβαση εκείνος που διενεργεί την ανάκριση»*[45]*,*

Η συγκεκριμένη περίπτωση αποσκοπεί στο να καλύψει νομοθετικά την κατάσχεση ενός μέσου αποθήκευσης, ανεξάρτητου από το σύστημα υπολογιστή, όπως επί παραδείγματι σε ένα οπτικό δίσκο, ένα usb stick ή και σε έναν εξωτερικό σκληρό δίσκο αποθήκευσης.

γ) *«σε ένα **απομακρυσμένο σύστημα υπολογιστή** στο σύνολό του ή σε μέρος αυτού και **στα δεδομένα** υπολογιστή που είναι αποθηκευμένα σε αυτόν **ή σε ένα απομακρυσμένο μέσο αποθήκευσης δεδομένων υπολογιστ**ή και στα δεδομένα υπολογιστή που είναι αποθηκευμένα σε αυτό, **τα οποία είναι διασυνδεδεμένα στο σύστημα υπολογιστή, στο οποίο έχει φυσική πρόσβαση εκείνος που διενεργεί την ανάκριση.** Στην τελευταία περίπτωση, τα ψηφιακά δεδομένα που είναι αποθηκευμένα και προσβάσιμα μέσω συστήματος και υπηρεσιών νεφοϋπολογιστικής (cloud services) δεν θεωρούνται αποθηκευμένα σε απομακρυσμένο σύστημα υπολογιστή ή σε απομακρυσμένο μέσο*

[45] ΦΕΚ

αποθήκευσης δεδομένων υπολογιστή, τα οποία είναι διασυνδεδεμένα στο σύστημα υπολογιστή στο οποίο έχουν φυσική πρόσβαση οι αρχές»[46]

Με την ως άνω διάταξη επιχειρείται ρητή διάκριση ανάμεσα σε δεδομένα αποθηκευμένα σε ένα απομακρυσμένο σύστημα υπολογιστή και δεδομένα που είναι αποθηκευμένα και προσβάσιμα μέσω συστημάτων νεφουπολογιστικής. Με την παρούσα ειδικότερα *"η φυσική πρόσβαση σε ένα τοπικό σύστημα υπολογιστή που είναι διασυνδεδεμένο με ένα απομακρυσμένο σύστημα εξομοιούται με φυσική πρόσβαση στο τελευταίο, επιτρέποντας την ανάκτηση δεδομένων από αυτό σαν να επρόκειτο για δεδομένα αποθηκευμένα στο τοπικό σύστημα. Για την εφαρμογή της διάταξης είναι αδιάφορο αν τα δεδομένα ανακτώνται από ένα απομακρυσμένο ηλεκτρονικό υπολογιστή, ένα δίκτυο υπολογιστών, ένα πληροφοριακό σύστημα π.χ. μια βάση δεδομένων, ένα μέρος συστήματος π.χ. ένα λογαριασμό χρήστη …"*[47]. Αδιάφορος κατ' αρχήν είναι και ο τρόπος με τον οποία επιτυγχάνεται η διασύνδεση, είτε στις περιπτώσεις τοπικών δικτύων είτε και στις περιπτώσεις σύνδεσης τοπικού πληροφοριακού συστήματος με απομακρυσμένα μέσα αποθήκευσης. Έτσι η σύνδεση μπορεί να επιτυγχάνεται με αξιοποίηση οποιαδήποτε τεχνολογίας, όπως επί παραδείγματι με χρήση ειδικού λογισμικού απομακρυσμένης πρόσβασης λ.γ. teamviewer, anydesk κ.λπ., ή χρήση port forwarding μέσω router, ή χρήση Virtual Private Network (VPN), με ρητή εξαίρεση αυτην της τεχνολογίας νεφουπολογιστικής. Πιο συγκεκριμένα, ρητά διευκρινίζεται ότι *«τα δεδομένα που είναι προσβάσιμα μέσω υπηρεσιών νεφοϋπολογιστικής δεν θεωρούνται αποθηκευμένα σε απομακρυσμένο σύστημα υπολογιστή ή σε απομακρυσμένο μέσο αποθήκευσης»*[48]. Σταθμό δε στην αντιμετώπιση και των χειρισμό αυτών, έχει αποτελέσει η υπ' αριθμόν 613/2006 απόφαση του Συμβουλίου Πλημμελειοδικών Αθηνών, η οποία έκρινε ότι ως προς αυτά απαιτείται να ακολουθηθεί η διαδικασία που αφορά σε ανάκτηση δεδομένων επικοινωνιών, ήτοι το πρώτο εξαχθέν αντίτυπο επέχει θέση "οιονεί πρωτότυπου", αλλά έχει μειωμένη αξιοπιστία, που απαιτεί διασταύρωση και με άλλα αποδεικτικά στοιχεία

Σύμφωνα με την παράγραφο 2 του νέου άρθρου 265, η κατάσχεση συνίσταται στην α. αφαίρεση υλικού φορέα ή αντιγραφή και αφαίρεση αποθηκευμένων ψηφιακών δεδομένων και σε β. αναπαραγωγή και επαλήθευση αυθεντικότητας και ακεραιότητας, που

---

[46] ΦΕΚ
[47] Γ. Ναζίρης, *" Η κατάσχεση ψηφιακών Δεδομένων"*, Ποινική Δικαιοσύνη, Τεύχος Φεβρουάριος 2020
[48] ΦΕΚ

πραγματοποιούνται αποκλειστικά με την χρήση κατάλληλου εξοπλισμού. Ο κατάλληλος εξοπλισμός μπορεί να συνίσταται σε software ή hardware και συνδυασμό αυτών. Πάντως παρά τον φαινομενικά επιτακτικό χαρακτήρα της διάταξης, ως προς την χρήση "αποκλειστικά" κατάλληλου εξοπλισμού, για την πραγματοποίηση της κατάσχεσης, ο νομοθέτης δεν καθιερώνει ρητά σχετική ακυρότητα σε περίπτωση παραβίασης της[49]. Εξάλλου στην ίδια διάταξη δεν προκαθορίζονται ειδικά τα μέσα που είναι κατάλληλα για την διενέργεια της κατάσχεσης αλλά ο νομοθέτης αρκείται σε γενικότερη πρόβλεψη. Παραταύτα έχει διατυπωθεί θεωρητικά η άποψη ότι "***...η πλημμελής εξαγωγή δεδομένων, και ιδίως η μη τήρηση κάποιου πρωτοκόλλου για την επαλήθευση της αυθεντικότητας και της ακεραιότητας, είναι δυνατό να παίξει ουσιώδη ρόλο στο σχέση με την αποδεικτική αξιοποίηση των δεδομένων στο μεταγενέστερα στάδια της ποινικής διαδικασίας***"[50].

Στην παράγραφο 3 του άρθρου 265 του ΚΠΔ, προβλέπεται ρητά η σύνταξη "ειδικής έκθεσης", η οποία αντιπαραβάλλεται προς την γενικότερη "έκθεση κατάσχεσης" που ρυθμίζεται στο ΚΠΔ. Επομένως η έκθεση αυτή θα πρέπει να διακρίνεται από την έκθεση κατάσχεσης ενσώματων και λοιπών αντικειμένων, που δεν υπάγονται στην σχετική ρύθμιση και πρέπει κατ΄ελαχιστο να περιλαμβάνει το είδος των κατασχεθέντων ψηφιακών δεδομένων αλλά και να περιγράφει τις ενέργειες που πραγματοποιήθηκαν. Κατά τα λοιπά τυγχάνουν εφαρμογής στο αυτή και οι γενικές διατάξεις του ΚΠΔ σχετικά με τις εκθέσεις *(148 επ. ΚΠΔ),* ενώ επί συγκεκριμένων παρατυπιών επιφυλάσσεται και γι αυτή η σχετική ακυρότητα του άρθρου 153 ΚΠΔ. Είναι επομένως η έκθεση άκυρη, σε περίπτωση που λείπει ημεροχρονολογία σύνταξης, εκτός αν αυτή προκύπτει με βεβαιότητα από το όλο περιεχόμενο της έκθεσης, δεν καταγράφεται το ονοματεπώνυμο και δεν ακολουθεί η υπογραφή των προσώπων που σύμφωνα με το άρθρο 150 ΚΠΔ συνέπραξαν στην διαδικασία, ή εξετάσθηκαν, ή συνέταξαν την έκθεση.

Ζήτημα δημιουργήθηκε ως προς το χρονικό σημείο, στο οποίο θεωρείται ότι πραγματοποιήθηκε η κατάσχεση, δηλαδή ως προς το εάν αυτή συντελείται την στιγμή αφαίρεσης του υλικού φορέα ή την ή την μεταγενέστερη στιγμή ανάκτησης των δεδομένων από τον κατασχεθέντα υλικό φορέα αλλά και ως προς το κατά πόσο απαιτείται σύνταξη

[49] Αντίστοιχα "*μπορεί να θεωρηθεί οτι περιγράφει απλώς τον τρόπο της κατάσχεσης των δεδομένων, χωρίς να καθιερώνει ένα δικονομικό τύπο η τήρηση του οποίου επιβάλλεται με ποινή ακυρότητας"* - Γ. Ναζίρης, *" Η κατάσχεση ψηφιακών Δεδομένων",* Ποινική Δικαιοσύνη, Τεύχος Φεβρουάριος 2020

[50] Γ. Ναζίρης, *" Η κατάσχεση ψηφιακών Δεδομένων",* Ποινική Δικαιοσύνη, Τεύχος Φεβρουάριος 2020

διακριτής έκθεση για τις δυο διαδικασίες. Σύμφωνα με την υπ' αριθμόν 6/2021 Γνωμοδότηση του Αντεισαγγελέα του Αρείου Πάγου κ. Χαράλαμπου Βουρλιώτη, *"... τα (άυλα) ψηφιακά δεδομένα που είναι αποθηκευμένα σε ένα σύστημα ή σε ένα μέσο αποθήκευσης δεδομένων ή σε ένα απομακρυσμένο σύστημα υπολογιστή στο σύνολο του ή σε μέρος αυτού ή σε ένα απομακρυσμένο μέσο αποθήκευσης δεδομένων υπολογιστή, αποτελούν μέρος του υλικού φορέα στον οποίο εμπεριέχονται, είτε πρόκειται για σύστημα υπολογιστή είτε για μέσο αποθήκευσης, από τη φύση δε του πράγματος και κατά λογική ακολουθία, τα ψηφιακά δεδομένα κατάσχονται ταυτόχρονα με τον περιέκτη υλικό φορέα, ανεξάρτητα από το είδος και τη μορφή του, χωρίς να συντρέχει περίπτωση διακριτής κατάσχεσής τους και σύνταξης σε μεταγενέστερο χρόνο και διαφορετικό τόπο ιδιαίτερης, εκτός αυτής που αφορά στον υλικό φορέα τους, σχετικής έκθεσης, συνακόλουθα δε ουδεμία ακυρότητα της συγκεκριμένης ανακριτικής πράξης, συναπτόμενη με τη νομιμότητα των κτηθέντων, ως άνω, αποδεικτικών μέσων, υπόκειται. Η τεχνική υποστήριξη του ανωτέρω Τμήματος που παρέχεται με τη διάθεση προσωπικού ειδικών γνώσεων και κατάλληλου εξοπλισμού, για την συλλογή, εξαγωγή, ανάλυση, διατήρηση, αναπαραγωγή και επαλήθευση της αυθεντικότητας των κατασχεθέντων δεδομένων, συνιστά περίπτωση πραγματογνωμοσύνης, η οποία διέπεται από τις σχετικές δικονομικές διατάξεις, οι διαπιστώσεις δε και τα συμπεράσματα αυτής αποτελούν συνέχεια και αναπόσπαστο μέρος της οικείας, κατά κανόνα χρονικά προηγούμενης, έκθεσης κατάσχεσης του υλικού φορέα."*[51]

- Φύλαξη και σφράγιση των κατασχεθέντων πραγμάτων και ψηφιακών δεδομένων

Με την διάταξη του άρ. 268 του νέου ΚΠΔ, η οποία παραμένει ίδια σχεδόν με τα προϊσχύσαντα άρ. 266 και 267 ΚΠΔ, που ενσωματώθηκαν σ αυτή, ρυθμίζεται η φύλαξη και η τύχη και η καταστροφή των κατασχεθέντων πραγμάτων. Σύμφωνα με την ως άνω διάταξη, τα "πράγματα", αφού κατασχεθούν παραδίδονται προς φύλαξη εντός του δικαστικού μεγάρου, στον γραμματέα του δικαστηρίου, ή αν αυτό δεν είναι εφικτό σε τρίτο ικανό και αξιόπιστο πρόσωπο που ορίζεται ως μεσεγγυούχος από αυτόν που ενεργεί την ανάκριση.

[51]https://eisap.gr/%CE%B3%CE%BD%CF%89%CE%BC%CE%BF%CE%B4%CF%8C%CF%84%CE%B7%CF%83%CE%B7-6-2021/

Μάλιστα ως μεσεγγυούχος δύναται να διορισθεί και ο ίδιος ο παθών ή ο κατηγορούμενος[52] Κατ΄άρθρο πρώην 266 § 2 ΚΠΔ και ήδη 268 ΚΠΔ, το δικαστικό συμβούλιο ή ο ανακριτικός υπάλληλος δύνανται να επιβάλλουν στον μεσεγγυούχο την καταβολή εγγύησης. Ο μεσεγγυούχος για οποιαδήποτε βλάβη ή απώλεια των πραγμάτων, των οποίων η φύλαξη του έχει ανατεθεί ευθύνεται αστικά για αδικοπραξία και ποινικά κατά το 177 ΠΚ., ενώ στερείται του δικαιώματος χρήσης αυτών. Ο διορίσαντας ανακριτής ή ανακριτικός υπάλληλος και επί προανάκρισης ο εισαγγελέας, μέχρι της εισαγωγής της υπόθεσης στο ακροατήριο, δύνανται να προβούν σε αλλαγή του προσώπου του μεσεγγυούχου. Τυχόν σχετική ανακύπτουσα αμφισβήτηση επιλύεται από το συμβούλιο, κατ' άρθρο 307 εδ. β', στ'. Αφ ης στιγμής εισαχθεί η υπόθεση στο ακροατήριο, με απευθείας κλήση του Εισαγγελέα ή παραπεμπτικό βούλευμα του Δικαστικού Συμβουλίου, αρμόδιο να διατάξει την αλλαγή του μεσεγγυούχου είναι το δικαστικό συμβούλιο, το οποίο προσδιορίζεται ανάλογα με το δικαστήριο παραπομπής.

Αντίστοιχα, κατά τα προβλεπόμενα στην διάταξη του άρθρο 268 παράγραφος 1 εδ. β του ΚΠΔ, για χρήματα ή άλλα τιμαλφή μετά την κατάσχεση ακολουθεί διαδικασία κατάθεσης στο Ταμείο Παρακαταθηκών και Δανείων.

Αν υπάρχει ανάγκη είναι δυνατό ακόμη τα κατασχεθέντα πράγματα ή έγγραφα να ασφαλιστούν με επίθεση της σφραγίδας της υπηρεσίας ή με άλλο τρόπο. [53] Περαιτέρω, αν παρίστανται και το αιτηθούν, δύνανται να σφραγίσουν τα κατασχεθέντα και όσοι έχουν έννομο συμφέρον δύνανται, οπότε και η αποσφράγιση αν αυτό είναι εφικτό, διενεργείται παρουσία αυτών, αφού προηγουμένως βεβαιωθεί ότι δεν έχουν παραβιαστεί οι σφραγίδες. Ως σφραγίδες, νοούνται ενδεικτικά και όχι περιοριστικά ταινίες, μολυβδοσφραγίδες, μελανοσφραγίδες, ισπανικό κερί,, καλώδια, σπάγκος κ.λπ. Τυχόν παραβίαση σφραγίδων οδηγεί σε πλήρωση της αντικειμενικής υπόστασης του πλημμελήματος, που στοιχειοθετείται στο άρθρο 178 νέου ΠΚ.

Σύμφωνα με την υπ' αριθμ. 5/2012 Γνωμοδότηση του Εισαγγελέα του Αρείου Πάγου, *«θεωρούνται πράγματα και έχουν επ' αυτών εφαρμογή οι περί κατασχέσεως διατάξεις του ΚΠΔ τα ευπαθή πειστήρια βιολογικού υλικού (τμήματα του σώματος των θυμάτων) που χρησιμοποιούνται από τους ανακριτικούς υπαλλήλους με σκοπό την εξιχνίαση διαφόρων*

[52] ΕφΚερκ. 14/1999, *Ποιν.Χρον. ΜΘ΄σ. 1055*
[53] Μ. Μαργαρίτη, *«Ερμηνεία Κώδικα Ποινικής Δικονομίας»,* 2008

εγκληματικών πράξεων»[54]. Πιο συγκεκριμένα, τα τμήματα ευπαθών πειστηρίων βιολογικού υλικού, που συνέλεξαν ανακριτικοί υπάλληλοι στο πλαίσιο έρευνας εξιχνίασης διαφόρων κακουργημάτων, για διενέργεια εργαστηριακών εξετάσεων, όπως DNA, μετά το πέρας της εξέτασης από την αρμόδια αρχή, αποτελούν μέρος της δικογραφίας και για τη φύλαξη, τύχη ή καταστροφή τους εφαρμόζονται οι γενικές διατάξεις των άρθρων 266, 307, 310, 373 επ. του ΚΠΔ ή ειδικές, εφόσον υπάρχουν, πρόκειται για πράγματα και μπορούν να καταστραφούν .

Αντίστοιχα ειδικότερα ρυθμίζεται η φύλαξη των ψηφιακών δεδομένων στο σχέση με αυτή των "κατασχεθέντων πραγμάτων" στην παράγραφο 4 του άρθρου 256 του ΚΠΔ, σύμφωνα με την οποία *"τα ψηφιακά δεδομένα που κατάσχονται διατηρούνται αποθηκευμένα καθ' όλη τη διάρκεια της ποινικής διαδικασίας σε ένα και μόνο υλικό μέσο αποθήκευσης που περιέχεται στη δικογραφία. Ασφαλές αντίγραφο αυτού ώστε να διασφαλίζεται η δυνατότητα ανάκτησης των δεδομένων που έχουν κατασχεθεί, σε περίπτωση απώλειας ή καταστροφής, σχηματίζεται κατά την κατάσχεσή τους και διατηρείται στο γραφείο πειστηρίων του πρωτοδικείου στο οποίο υποβάλλεται η δικογραφία και το οποίο παρέχει τις κατάλληλες εγγυήσεις φυσικής ασφάλειας και πρόσβασης σε εκείνους μόνο που ασκούν καθήκοντα στην υπόθεση. Η παρούσα ισχύει αναλόγως και στα ψηφιακά δεδομένα που αφορούν στα δεδομένα επικοινωνίας που περιλαμβάνονται στη δικογραφία[55]."* Έχει διατυπωθεί η άποψη ότι τυχόν ύπαρξη περισσότερων του ενός αντιγράφων, δηλαδή περισσότερων υλικών φορέων αποθήκευσης με τον ίδιο περιεχόμενο, εντός της δικογραφίας, δεν συνεπάγεται την ακυρότητα της διαδικασίας, αλλά ενδεχομένως τίθεται θέμα αξιοπιστίας [56].

- Πρόσβαση σε κατασχεθέντα ψηφιακά δεδομένα

Στην παράγραφο 5 του άρθρου 265 του ΚΠΔ ρυθμίζεται η πρόσβαση στα κατασχεθέντα ψηφιακά πειστήρια, ως ακολούθως : *"Η πρόσβαση και η δυνατότητα αναπαραγωγής των ψηφιακών δεδομένων που κατάσχονται επιτρέπεται μόνο σε όσους*

[54]https://eisap.gr/%ce%b3%ce%bd%cf%89%ce%bc%ce%bf%ce%b4%cf%8c%cf%84%ce%b7%cf%83%ce%b7-05-2012/
[55] ΦΕΚ
[56] Γ. Ναζίρης, *" Η κατάσχεση ψηφιακών Δεδομένων"*, Ποινική Δικαιοσύνη, Τεύχος Φεβρουάριος 2020

ασκούν δικαστικά, εισαγγελικά και ανακριτικά καθήκοντα στην υπόθεση ή τους γραμματείς. Προς το σκοπό αυτό χρησιμοποιούνται τα κατάλληλα τεχνικά μέσα. Τέτοια μέσα είναι η κρυπτογράφηση και η χρήση κωδικών ασφαλείας για την πρόσβαση και αναπαραγωγή των κατασχεμένων ψηφιακών δεδομένων από το υλικό μέσο αποθήκευσης στο οποίο βρίσκονται αποθηκευμένα. Η παρούσα ισχύει αναλόγως και στα ψηφιακά δεδομένα που αφορούν στα δεδομένα επικοινωνίας που περιλαμβάνονται στη δικογραφία.[57]" Με την σχετική διάταξη φαίνεται να αποκλείεται κατ' αρχήν η πρόσβαση επί των ψηφιακών δεδομένων σε πρόσωπα πέραν των περιοριστικά προβλεπόμενων σε αυτή, δηλαδή ακόμα και στους διαδίκους. Κάτι τέτοιο θα ήταν αδιανόητο και δογματικά ασυνεπές στο μέτρο που και τα ψηφιακά πειστήρια, αποτελούν αποδεικτικό υλικό και αντικείμενο της δικογραφίας η πρόσβαση στο οποίο θα πρέπει να εξασφαλίζεται για τον ύποπτο/ κατηγορούμενο, αλλά και για τον υποστηρίζοντα την κατηγορία διάδικο σύμφωνα με τα γενικότερα άρθρα υπ' αριθμ. 100, 105, 107 και 244 του ΚΠΔ. Επομένως κατά την άποψη της γράφουσας, το νόημα της σχετικής διάταξης συνίσταται στον αποκλεισμό της "άμεσης" πρόσβασης, επί των ψηφιακών δεδομένων, ενώ το δικαίωμα πρόσβαση σε αυτά ικανοποιείται όπως και στο κάθε άλλο αντικείμενο της δικογραφίας με την λήψη αντιγράφου το οποίο θα πρέπει να εκδίδεται με επιμέλεια προσώπου που έχει "άμεση" πρόσβαση κατόπιν οικονομικής επιβάρυνσης και σχετικού αιτήματος των εμπλεκόμενων προσώπων.

4.5. Ειδικές Ανακριτικές Πράξεις

Σε συμμόρφωση της χώρας μας προς τις διεθνείς συμβατικές της δεσμεύσεις και ειδικότερα σύμφωνα το άρθρο 20 της Σύμβασης των Ηνωμένων Εθνών, για το οργανωμένο έγκλημα, η οποία υπογράφηκε τον 12/2000 στο Παλέρμο της Ιταλίας, από περισσότερα από 120 Κράτη, με το άρθρο 6 του Ν. 2928/2006 εισήχθη στον Κώδικα Ποινικής Δικονομίας, και δη στο κεφάλαιο περί ερευνών, η διάταξη του άρθρου 253Α. Σύμφωνα με την Εισηγητική Έκθεση του παραπάνω νόμου, "*οι προτεινόμενοι περιορισμοί δικαιωμάτων προβλέπονται ήδη στο ισχύον δίκαιο, αφ' ενός σε διατάξεις ειδικών ποινικών νόμων… όπως …(στη) νομοθεσία για τα ναρκωτικά, τα όπλα, τα πυρομαχικά κ.λπ., εμπορία αρχαιοτήτων, διαφθορά στο εσωτερικό της αστυνομίας και αφ' ετέρου σε διατάξεις της νομοθεσίας για την άρση του*

[57] ΦΕΚ

απορρήτου προς διακρίβωση πολλών κατηγοριών κακουργημάτων και της νομοθεσίας για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού του χαρακτήρα. Οι ισχύουσες αυτές διατάξεις … εκλογικεύθηκαν, με σκοπό να ισχύουν ενιαίες προϋποθέσεις για την εφαρμογή τους. Εξάλλου εντάχθηκαν στον ΚΠΔ, ώστε να αποκτήσουν στην συνείδηση των εφαρμοστών του δικαίου την θέση που τους αρμόζει"[58]. Εν συνεχεία μετά τις τρομοκρατικές επιθέσεις της 11ης Σεπτεμβρίου του 2001, σε βάρος των Ηνωμένων Πολιτειών Αμερικής, η Ευρωπαϊκή Ένωση, υιοθέτησε την από 22.06.2002 και υπ' αριθμόν 2002/475/ΔΕΥ απόφαση - πλαίσιο (ΕΕ L 164) για την καταπολέμηση της τρομοκρατίας. Στόχος της σχετικής ενωσιακής πρωτοβουλίας, ήταν η δια μέσου κοινών δεσμεύσεων, όσον αφορά στην οριοθέτηση της έννοιας της τρομοκρατίας και την υιοθέτηση αυστηρότερων πλαισίων ποινών, εναρμόνιση των εθνικών νομοθεσιών, για την αποτελεσματικότερη καταπολέμηση της τρομοκρατίας. Προς εκπλήρωση σχετικής υποχρέωσης της η Ελλάδα με το άρθρο 42 παράγραφος 1 του Ν. 3251/2004 τροποποίησε το άρθρο 253Α ΚΠΔ, επεκτείνοντας το πεδίο εφαρμογής του και στο άρθρο 187Α ΠΚ, δηλαδή στις τρομοκρατικές πράξεις.

Με την ψήφιση του Ν. 4620/2019 και την θέση σε ισχύ του Νέου Κώδικα Ποινικής Δικονομίας, η προβλεπόμενη στο άρθρο 253Α του παλαιού κώδικα ρύθμιση για τις "Ειδικές ανακριτικές πράξεις επί ορισμένων εγκλημάτων", αντικαταστάθηκε από το νέο άρθρο 254 ΚΠΔ. Σύμφωνα με την Εισηγητική έκθεση του Ν.4620, η παλαιά ρύθμιση του 253Α αλλά και αυτή του 253Β για τις ειδικές ανακριτικές πράξεις επί εγκλημάτων διαφθοράς *"αναμορφώθηκαν εν μέρει και συμπληρώθηκαν ώστε να αντανακλούν πληρέστερα τις αξιώσεις δικαιοκρατικότητας και δικαιότητας .. ενόψει...ιδίως του μυστικού και προληπτικού χαρακτήρα (των πράξεων αυτών).."*[59]. Καινοτομία της νέας διάταξης αποτελεί η αυτοτελής ρύθμιση της "συγκαλυμμένης έρευνας" ως ειδικής ανακριτικής πράξης, η οποία μολονότι προβλεπόταν στο 253 Β του ΚΠΔ, για τα εγκλήματα διαφθοράς, δεν διακρινόταν στο 253Α από την ανακριτική διείσδυση, η οποία διαφοροποιείται εννοιολογικά. Η προσθήκη αυτή αν και φαινομενικά "τυπική", μοιάζει να τονίζει την αναντίλεκτη αναγκαιότητα για "στενή" ερμηνευτική προσέγγιση της παρούσας διάταξης, η οποία αποκλίνει απο θεμελιώδεις αρχές της ποινικής προδικασίας, και θέτει σε "κίνδυνο" δικαιώματα και προσωπικές ελευθερίες

[58] https://www.ministryofjustice.gr/wp-content/uploads/2019/08/58bNomos_ait_ekthesi_n_3875.pdf
[59] https://www.hellenicparliament.gr/UserFiles/c8827c35-4399-4fbb-8ea6-aebdc768f4f7/11027276.pdf

τόσο του εκάστοτε "υπόπτου" όσο και ενδεχομένως τρίτα πρόσωπα τα οποία δεν σχετίζονται με τις προβλεπόμενες στο νόμο εγκληματικές δραστηριότητες.

Στον νέο Κώδικα Ποινικής Δικονομίας, απαριθμούνται περιοριστικά απο τον νομοθέτη, έξι επιτρεπτές ειδικές ανακριτικές πράξεις, οι οποίες ακολουθούνται από αυξημένα εγγυητικά μέτρα ασφαλείας. Η "νέα" [60]ανακριτική πράξη της "συγκαλυμμένης έρευνας", επιτρέπει σε ανακριτικό υπάλληλο ή "έμπιστο" ιδιώτη να διευκολύνει, ενεργώντας παθητικά και όχι ως agent provocateur την τέλεση κάποιου από τα περιοριστικά απαριθμούμενα στο νόμο εγκλήματα, τα οποία ο δράστης έχει "προαποφασίσει"(τουλάχιστον αρχή εκτέλεσης κατά το ΕΔΔΑ).Από την άλλη στην "ανακριτική διείσδυση", που συχνά συγχέεται εννοιολογικά με την "συγκαλυμμένη έρευνα", ανακριτικός υπάλληλος ή "έμπιστος" ιδιώτης, διεισδύει σε εγκληματική ή τρομοκρατική οργάνωση και αναλαμβάνει διεκπεραιωτικά καθήκοντα, με σκοπό να εξιχνιάσει την δομή της, να αποκαλύψει τα μέλη και τα εγκλήματα που έχουν τελέσει ή προαποφασίσει. Λοιπές, ειδικές ανακριτικές πράξεις που συναντώνται συχνά στην πράξη είναι η "άρση απορρήτου του περιεχομένου των επικοινωνιών ή δεδομένων θέσης ή κίνησης", σύμφωνα με την διαδικασία των άρθρων 4 και 5 του ν. 2225/1994, αλλά και η "καταγραφή δραστηριότητας ή άλλων γεγονότων εκτός οικίας". Άλλες προβλεπόμενες ειδικές ανακριτικές πράξεις είναι οι "ελεγχόμενες μεταφορές" αλλά και η "συσχέτιση συνδυασμού δεδομένων προσωπικού χαρακτήρα".

Στο άρθρο 4, του νόμου 2225/1994, σύμφωνα με την υπ' αριθμ. 2/2017 Γνωμοδότηση του Εισαγγελέα του Αρείου Πάγου, «*προσδιορίζονται συγκεκριμένα οι αξιόποινες πράξεις για τις οποίες είναι επιτρεπτή η άρση του απορρήτου, ενώ με το άρθρο 5 καθορίζεται η διαδικασία άρσης, στην παράγραφο δε 10 αυτού του άρθρου ορίζεται ότι το περιεχόμενο της ανταπόκρισης ή επικοινωνίας που έγινε γνωστό λόγω της άρσης του απορρήτου, καθώς και κάθε άλλο σχετικό με αυτή στοιχείο απαγορεύεται, και μάλιστα με ποινή ακυρότητας να αξιοποιηθεί αποδεικτικά σε άλλη ποινική, πολιτική, διοικητική και πειθαρχική δίκη για σκοπό διαφορετικό από εκείνον που είχε καθοριστεί με την διάταξη του αρμόδιου συμβουλίου*».[61]

[60] Αν και προβλεπόταν στο 253 Β του παλαιότερου ΚΠΔ, για τα εγκλήματα διαφθοράς, δεν διακρινόταν στο 253Α από την ανακριτική διείσδυση

[61] ΓνωμΕισΑΠ 2/2017, Ποινική Δικαιοσύνη, σελ 676

Προκειμένου να ενεργοποιηθεί οποιαδήποτε από τις παραπάνω περιγραφόμενες ανακριτικές πράξεις θα πρέπει να συντρέχουν σοβαρές ενδείξεις και δεν αρκούν απλές υπόνοιες πρόκειται να τελεστεί ή τελέσθηκε κάποια από τις προβλεπόμενες στην σχετική διάταξη (ή σε ειδικούς ποινικούς νόμους) "σοβαρές" αξιόποινες πράξεις, ήτοι: σύσταση ή συμμετοχή ή διεύθυνση σε "εγκληματική οργάνωση" (187 παρ.1&2), τέλεση τρομοκρατικών πράξεων, σύσταση ή συμμετοχή ή διεύθυνση σε τρομοκρατική οργάνωση (187 Α), παραχάραξη νομίσματος και άλλων μέσων πληρωμής (207 παρ. 1&2), κυκλοφορία πλαστών νομισμάτων και άλλων μέσων πληρωμής (208 παρ. 1 εδ. α'), καθ' υπέρβαση κατασκευή νομίσματος (208Α) εκτός από τις ιδιαίτερα ελαφρές περιπτώσεις, εμπορία ανθρώπων (323Α), βιασμό (336) σε βάρος ανηλίκου, κατάχρηση ανικάνου προς αντίσταση (338) σε βάρος ανηλίκου, γενετήσιες πράξεις με ανηλίκους ή ενώπιόν τους (339 παρ 1&3), κατάχρηση ανηλίκων (342 παρ.1), πορνογραφία ανηλίκων (348Α), προσέλκυση παιδιών για γενετήσιους λόγους (348Β), πορνογραφικές παραστάσεις ανηλίκων (348Γ) και ασέλγεια με ανήλικο έναντι αμοιβής (351Α), αλλά και η "εξάρθρωση" αυτών με άλλα ηπιότερα μέσα να είναι αδύνατη ή ιδιαιτέρως δυσχερής (αρχή αναγκαιότητας).

Οι "ενδείξεις ενοχής" αποτελούν μια νομική έννοια, και η συνδρομή της μπορεί να ελεγχθεί από την αιτιολογία του παραπεμπτικού βουλεύματος. Σύμφωνα με τον Θ. Δαλακούρα, πρόκειται για μία *"περίπλοκη κρίση στην οποία προβαίνει ad hoc το κατά περίπτωση αρμόδιο ανακριτικό όργανο ή δικαστήριο εν όψει συγκεκριμένης αξιόποινης πράξης και σε σχέση με ένα ή περισσότερα πρόσωπα στα οποία αποδίδεται η τέλεση της. Πρόκειται κατά κυριολεξία για μία βασιζόμενη σε συγκεκριμένα πραγματικά περιστατικά πιθανολόγηση αναφορικά με την συνδρομή των στοιχείων ποινικής υπόστασης του εγκλήματος που αποδίδεται στον κατηγορούμενο"*[62]. Σύμφωνα με την αιτιολογική έκθεση του ν.2928/2001, *"οι ενδείξεις ότι έχουν τελεστεί αξιόποινες πράξεις .... είναι σοβαρές και επομένως απλή καταγγελία, φυσικά δεν αρκεί"*. Το υψηλό, νομοθετικά απαιτούμενο μέγεθος ενδείξεων, ετέθη απο τον νομοθέτη σε συμμόρφωση προς την "αρχή της αναλογικότητας" ως επιπλέον εγγυητικό μέτρο, λόγο του ιδιαιτέρως επαχθούς χαρακτήρα των ειδικών ανακριτικών πράξεων. Τυχόν καταστρατήγηση της αρχής της αναλογικότητας ως προς την συνδρομή του εκ του νόμου απαιτούμενου βαθμού ενδείξεων ενοχής, συνιστά παραβίαση της θεμελιώδης δικονομικής αρχής της "δίκαιης δίκης", και άρα συνεπάγεται απόλυτη

[62] Δαλακούρας Θ., *"Αρχή αναλογικότητας και μέτρα δικονομικού καταναγκασμού"*, Ποινικά Χρονικά, 1993

ακυρότητα προδικασίας του άρθρου 171 παρ. 1 εδ.δ' του ΚΠΔ, που οδηγεί σε αποδεικτική απαγόρευση αξιοποίησης.

Η σωρευτική συνδρομή των παραπάνω γενικών προϋποθέσεων, *(1.προβλεπόμενη αξιόποινη πράξη, 2.σοβαρές ενδείξεις ενοχής, 3. Η με έτερο τρόπο αδυναμία ή δυσχέρεια αποκάλυψης της εγκληματικής πράξης)*, οεπιδιωκόμενος με την επικείμενη ανακριτική πράξη σκοπός και ο χρόνος που διήρκησε αυτή, θα πρέπει να μνημονεύονται ειδικά σε "ειδικά αιτιολογημένο βούλευμα" που εκδίδεται από δικαστικό συμβούλιο κατόπιν σχετικής πρότασης του αρμόδιου Εισαγγελέα. Σε εξαιρετικά επείγουσες περιπτώσεις την έρευνα μπορεί να εγκρίνει απευθείας, με έκδοση σχετικής "διάταξης" και ο εισαγγελέας ή ο ανακριτής, έχοντας ωστόσο παράλληλα εντός 3ημέρου την υποχρέωση να υποβάλλει πρόταση προς επικύρωση, της σχετικής διατάξεως. στο αρμόδιο συμβούλιο, υπό ποινή αυτοδίκαιης άρσης της ισχύος της. Σε αυτή την περίπτωση τα τυχόν ευρήματα δεν είναι αξιοποιήσιμα, εφόσον εντός ευλόγου χρονικού διαστήματος, όχι μεγαλύτερο των πέντε ημερών, δεν εκδοθεί σχετικό βούλευμα.

Κατ΄εξαίρεση, στην παράγραφο 4 του άρθρου 254 του ΚΠΔ, προβλέπεται ότι οι ανακριτικές πράξεις της άρσης απορρήτου, των ελεγχόμενων μεταφορών και της καταγραφής δραστηριότητας μπορούν να διενεργηθούν σε βάρος αμέτοχου στην τέλεση της εγκληματικής πράξης υποκειμένου, με σκοπό να ταυτοποιηθεί ο κατηγορούμενος , ή να συναχθούν άλλα στοιχεία όπως ο τόπος διαμονής ή κατοικίας αυτού, εφόσον τηρούνται οι λοιπές γενικές προϋποθέσεις που αναφέρθηκαν και υπό την πρόσθετη προϋπόθεση ότι είναι αδύνατη η αποκάλυψη αυτών με άλλο επιεικέστερο για τα υποκείμενα τρόπο. Συλλεγέντα κατά τα ανωτέρω αποδεικτικά στοιχεία τα οποία σχετίζονται με τρίτο αμέτοχο πρόσωπο επιβάλλεται να καταστρέφονται, χωρίς καθυστέρηση αμέσως μετά την πλήρωση του ανακριτικού σκοπού. Τα ως άνω αποδεικτικά στοιχεία διατηρούνται για μεγαλύτερο χρονικό διάστημα μόνο εφόσον από αυτά προκύπτει η τέλεση κακουργήματος κατά της ζωής, της σωματικής ακεραιότητας, της προσωπικής ή γενετήσιας ελευθερίας, του πολιτεύματος ή της ακεραιότητας της χώρας, από το τρίτο κατ' αρχήν φαινομενικά αμέτοχο πρόσωπο, οπότε και είναι δυνατή η περαιτέρω αξιοποίηση αυτών σε διανοιγείσα ποινική δίκη.

Τα βασικότερα κοινά χαρακτηριστικά των ειδικών ανακριτικών πράξεων, οι οποίες διενεργούνται σε βάρος υποκειμένου, κατά του οποίου δεν έχει ακόμα ασκηθεί ποινική δίωξη, είναι η άμεση συσχέτιση τους με "σοβαρές" εγκληματικές ενέργειες, ο ιδιαίτερα

επαχθής για τον ύποπτο χαρακτήρας και η μυστικότητα τους καθώς διενεργούνται πάντοτε εν αγνοία του υποκειμένου, το οποίο αφορούν.

4.6. Απόδειξη

i. Αρχή Ηθικής Απόδειξης

Διάφορες παράμετροι, όπως το περιβάλλον, ο χρόνος τέλεσης, η τοποθεσία και τρόποι τέλεσης ενός αδικήματος, το προφίλ και οι ικανότητες του εκάστοτε δράστη, επηρεάζουν τη διαδικασία διαμόρφωσης αποδεικτικών στοιχείων. Οι αρμόδιες αρχές με τις ανακριτικές πράξεις, που διενεργούν είναι υπεύθυνες για την εύρεση και συλλογή της αποδεικτικής ύλης. Η διαδικασία με την οποία αποσκοπείται ο σχηματισμός δικανικής πεποίθησης για την τέλεση ή μη της αξιόποινης πράξης και για την υπαιτιότητα του κατηγορουμένου για αυτή, αποτελεί τον ορισμό της απόδειξης.

Η δικανική κρίση, αποτελεί προϊόν ελεύθερης εκτίμησης, δεδομένου ότι διαμορφώνεται από την συνείδηση αλλά και την πείρα του εκάστοτε δικαστικού υπαλλήλου, με αποτέλεσμα να διαφοροποιείται από δικαστικό σε δικαστικό. Δεν τυγχάνει επομένως στην ποινική διαδικασία εφαρμογής το *«σύστημα νομικών αποδείξεων»*, σύμφωνα με το οποίο ο δικαστικός λειτουργός δεν είναι ελεύθερος για την αξιοποίηση και εκτίμηση των αποδεικτικών μέσων αλλά δεσμεύεται να προσδώσει σε αποδεικτικό μέσο την αξία που εκ των προτέρων ο νόμος του προσδίδει, αλλά το σύστημα της *«ελεύθερης εκτίμησης» των αποδεικτικών μέσων.*

Η *«αρχή ελεύθερης εκτίμησης των αποδεικτικών μέσων ή της ηθικής απόδειξης»* ρυθμίζεται στην πρώτη παράγραφο του άρθρου 177 του νέου ΚΠΔ, που παραμένει ίδια με την προϊσχύσασα.[63] Σύμφωνα με την αρχή αυτή, η οποία διαπνέει την ποινική αποδεικτική διαδικασία, δεν υφίσταται υποχρέωση των δικαστών να ακολουθούν «νομικούς κανόνες αποδείξεων» αλλά οι τελευταίοι αποφασίζουν σύμφωνα με την πεποίθηση τους και ακολουθώντας την φωνή της συνείδησης.

[63] 177 παρ 1. Νόμος 4620/2019 *"Οι δικαστές δεν ακολουθούν νομικούς κανόνες αποδείξεων, πρέπει όμως να αποφασίζουν κατά την πεποίθησή τους, ακολουθώντας τη φωνή της συνείδησής τους και οδηγούμενοι από την απροσωπόληπτη κρίση που προκύπτει από τις συζητήσεις και που αφορά την αλήθεια των πραγματικών περιστατικών, την αξιοπιστία των μαρτύρων και την αξία των άλλων αποδείξεων, αιτιολογώντας πάντοτε ειδικά και εμπεριστατωμένα με ποια αποδεικτικά μέσα και με ποιους συλλογισμούς σχημάτισαν τη δικανική τους κρίση"*

Πιο συγκεκριμένα, η "αρχή της ηθικής απόδειξης" δίνει στους δικαστές την δυνατότητα να αποφασίζουν κατά το δοκούν, *"σύμφωνα με την πεποίθηση τους ακολουθώντας την φωνή της συνείδησης και οδηγούμενοι από την απροσωπόληπτη κρίση που προκύπτει από την συζήτηση σχετικά με αλήθεια πραγματικών γεγονότων αξιοπιστία μαρτύρων και αξία των λοιπών αποδείξεων"*[64]. Με άλλα λόγια, ο δικαστής πλην εξαιρέσεων δεν δεσμεύεται από τους νομικούς κανόνες για την αξιοποίηση και εκτίμηση των αποδεικτικών μέσων. Επί παραδείγματι, εναπόκειται στην κρίση του να διατάξει ή όχι διενέργεια πραγματογνωμοσύνης, να λάβει ή οχι υπόψη μαρτυρικές καταθέσεις, ή τυχόν ομολογία του κατηγορουμένου, και σε τι βαθμό.

ii. Περιορισμοί στην αρχή Ηθικής Απόδειξης - Αποδεικτικές Απαγορεύσεις

(α) Νομοθετικές διατάξεις - Ιστορική προσέγγιση

Νομοθετικό φραγμό στην προσπάθεια αναζήτησης της αντικειμενικής αλήθειας αποτελούν σημαντικές εξαιρέσεις που διέπουν τον παραπάνω κανόνα της ηθικής απόδειξης. Ο δικαστικός λειτουργός προφανώς δεν δύναται να αναζητεί αποδεικτικά μέσα με οποιονδήποτε τρόπο και τίμημα, γι' αυτό και η αρχή της *«αναζήτησης της ουσιαστικής αλήθειας»* οχι σπάνια υποχωρεί ή πάντως πρέπει να υποχωρεί όταν συγκρούεται με άλλες ανώτερες απ' αυτήν αξίες.

Σύμφωνα με τις νομοθετικές προβλέψεις των άρθρων 139 ΚΠΔ και 20 Συντ, ο δικαστής οφείλει να σέβεται το τεκμήριο αθωότητας, να μην αρκείται μόνο στην διαίσθηση του και η απόφαση που εκδίδει να είναι πάντοτε επαρκώς αιτιολογημένη. Έτσι έμμεσο περιορισμό, στην "αρχή ηθικής απόδειξης", δημιουργεί και η υποχρέωση του δικαστικού λειτουργού να θεμελιώνει την κρίση του με βάση την κοινή λογική και τους κανόνες που αυτή υποδεικνύει, την κοινή πείρα και την φύση των πραγμάτων[65].

Περεταίρω, σε υπερεθνικό επίπεδο το άρθρο 8 της ΕΣΔΑ, (ΝΔ 53/1974), το οποίο έχει υπερνομοθετική ισχύ σύμφωνα και με το άρθρο 28 παρ. 1 του Συντ., ορίζει ότι *«παν*

[64] Άρθρο 177 παράγραφος 1, ΚΠΔ
[65] Αδάμ Χ. Παπαδαμάκης, *"Ποινική Δικονομίας: Η δομή της ποινικής δίκης"*, στ' έκδοση, Εκδόσεις Σάκκουλα, 2012

πρόσωπον δικαιούται εις τον σεβασμόν της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και της αλληλογραφίας του. Δεν επιτρέπεται να υπάρξη επέμβαση δημοσίας αρχής εν τη ασκήσει του δικαιώματος τούτου, εκτός εάν η επέμβαση αυτή προβλέπεται υπό του νόμου και αποτελεί μέτρον το οποίον, εις μίαν δημοκρατικήν κοινωνίαν, είναι αναγκαίον διά την εθνικήν ασφάλειαν, την δημοσίαν ασφάλειαν, την οικονομικήν ευημερίαν της χώρας, την προάσπισιν της τάξης και την πρόληψιν ποινικών παραβάσεων, την προστασίαν της υγείας ή της ηθικής, ή την προστασίαν των δικαιωμάτων και ελευθεριών άλλων[66]».

Με το άρθρο 19 παρ. 3 του Συντάγματος, όπως αυτό διαμορφώθηκε κατά την συνταγματική αναθεώρηση του 2001, καθιερώθηκε απόλυτη απαγόρευση αξιοποίησης αποδεικτικών μέσων κτηθέντων μέσω παραβίασης των συνταγματικών διατάξεων υπ' αριθμ. 9, 9Α και 19. Προβλέπεται λοιπόν συνταγματικά απόλυτη απαγόρευση της αξιοποίησης των αποδείξεων που αποκτήθηκαν αντίθετα με τα άρθρα 9, σχετικά με το άσυλο κατοικίας και προστασίας της ιδιωτικής και οικογενειακής ζωής, 9^{A} περί προστασίας προσωπικών δεδομένων και ιδιωτικού απορρήτου και 19 περί απορρήτου των επιστολών και της ελευθερίας της επικοινωνίας, του Συντάγματος. Από την ως άνω τροποποίηση του άρθρου 19 Σ, προκύπτει ευκρινώς η κατόπιν σχετικής σταθμίσεως, πρόκριση της προστασίας θεμελιωδών δικαιωμάτων, από τον συνταγματικό νομοθέτη, έναντι της άνευ όρων αποκάλυψης της αλήθειας. Η συνταγματική διάταξη του άρθρου 19 παρ. 3 Σ και η απόλυτη απαγόρευση που αυτή ενσωματώνει τυγχάνουν άμεσης εφαρμογής και συνεπάγονται τον παραμερισμό κάθε άλλης αντίθετης νομοθετικής διάταξης.[67]. Από την άλλη υποστηρίχθηκε με σημαντικά επιχειρήματα και η άποψη "*ότι, παρά την απόλυτη διατύπωσή του (άρθρου), πρόθεση του αναθεωρητικού νομοθέτη δεν ήταν να θεσπίσει μια απόλυτη απαγόρευση αξιοποίησης των παρανόμως κτηθέντων αποδεικτικών μέσων… (που)δε θα συνεκτιμούσε τις προβλεπόμενες από το ίδιο το Σύνταγμα κάμψεις του απορρήτου και θα παρέβλεπε το γεγονός ότι το άρθρο 19 παρ. 3 Συντ. δεν έχει υπέρτερο κύρος από οποιαδήποτε άλλη συνταγματική διάταξη, όπως το συνταγματικά διασφαλισμένο δικαίωμα παροχής έννομης προστασίας και δικαστικής ακρόασης...ο δικαστής θα πρέπει να σταθμίζει in concreto αν θα επιβληθούν περιορισμοί στο δικαίωμα ακρόασης ή στο δικαίωμα σεβασμού του απορρήτου*

[66] https://www.e-nomothesia.gr/kat-anthropina-dikaiomata/nomothetiko-diatagma-53-1974-phek-256a-20-9-1974.html

[67] Ελευθέριος Βενιζέλος,*"Το αναθεωρητικό κεκτημένο"*, εκδόσεις Σάκκουλα, 2002

των επικοινωνιών, κάνοντας μια στάθμιση μεταξύ των συγκρουόμενων δικαιωμάτων, με βάση τη συνταγματικά κατοχυρωμένη αρχή της αναλογικότητας"[68].

Το άρθρο 177 παράγραφος 2 του ΚΠΔ συνιστά ίσως την πιο σημαντική εξαίρεση και τον μεγαλύτερο φραγμό στην αρχή της ηθικής απόδειξης. Ιστορικά, η σχετική παράγραφος με την οποία θεσπίστηκε γενική απαγόρευση αξιοποίησης παρανόμως κτηθέντων αποδεικτικών μέσων εισήχθει, το πρώτον, με την διάταξη της παράγραφου 7του άρθρο 2 του νόμου 2408/1996[69]. Σύμφωνα με το τότε περιεχόμενο της σχετικής διάταξης, απαγορευόταν η αξιοποίηση παρανόμως κτηθέντων αποδεικτικών μέσων, εκτός εάν επρόκειτο για κακουργηματικές πράξεις, απειλούμενες με την ποινή της ισόβιας κάθειρξης οπότε και υπό την προϋπόθεση οτι μεσολαβούσε προς τούτο αιτιολογημένη παρεμπίπτουσα απόφαση του δικαστηρίου προβλεπόταν επαναφορά στον κανόνα της ηθικής απόδειξης. Η εν λόγω παράγραφος 2 τροποποιήθηκε με την παράγραφο 2 του άρθρου 10 του νόμου 3674/2008, τον Αύγουστο του 2008, οπότε και προβλέφθηκε ότι εν γένει τα *"Αποδεικτικά μέσα, που έχουν αποκτηθεί με αξιό-ποινες πράξεις ή μέσω αυτών, δεν λαμβάνονται υπόψη στην ποινική διαδικασία"*[70] εισάγοντας έτσι μία ρύθμιση που από πολλούς θεωρητικούς κρίθηκε ως άκαμπτη, ανελαστική και contra στο προϊσχύσαν και ορθότερο μοντέλο των σταθμίσεων, ενώ με τον ίδιο νόμο επήλθαν τροποποιήσεις στις διατάξεις που προστατεύουν το απόρρητο της επικοινωνίας. Με άλλα λόγια, ο ν. 3674/2008, προέβη σε μια οριζόντια διαχείριση των παρανόμως κτηθέντων στοιχείων, ανεξαρτήτως της σοβαρότητας του αδικήματος, οδηγώντας σε *"μια άκαμπτη και ανελαστική ρύθμιση"*. Όπως αναφέρεται και στην αιτιολογική έκθεση του Νέου Κώδικα Ποινικής Δικονομίας, διατηρείται όμοιο με το προισχύσαν το γράμμα του άρθρου 177 παρ. 2 ΚΠΔ, *"καθώς θεωρήθηκε από την Επιτροπή ότι η εν προκειμένω διαλαμβανόμενη αποδεικτική απαγόρευση αξιοποίησης όσων αποδεικτικών μέσων αποκτήθηκαν με αξιόποινες πράξεις ή μέσω αυτών αποτυπώνει ενεργή δικαιοκρατική αξίωση που δεν πρέπει να νοθευτεί…"*[71] .

[68]Ελισάβετ Συμεωνίδου-Καστανίδου, "*Παραβίαση απορρήτου επικοινωνιών και αποδεικτικές απαγορεύσεις στην ποινική δίκη",* Ποινική Δικαιοσύνη, τεύχος 11/2015

[69] «αποδεικτικά μέσα, που έχουν αποκτηθεί με αξιόποινες πράξεις ή μέσω αυτών, δε λαμβάνονται υπόψη για την κήρυξη της ενοχής, την επιβολή ποινής ή τη λήψη μέτρων καταναγκασμού, εκτός αν πρόκειται για κακουργήματα που απειλούνται με ποινή ισόβιας κάθειρξης και εκδοθεί για το ζήτημα αυτό ειδικά αιτιολογημένη απόφαση του δικαστηρίου. Μόνη η ποινική όμως δίωξη των υπαιτίων των πράξεων αυτών δεν εμποδίζει την πρόοδο της δίκης»

[70] https://www.e-nomothesia.gr/kat-epikoinonies-telepikoinonies-telephonia/n-3674-2008.html

[71] https://www.hellenicparliament.gr/UserFiles/c8827c35-4399-4fbb-8ea6-aebdc768f4f7/11027276.pdf

Διάσπαρτες στην νομοθεσία εντοπίζονται και περισσότερες διατάξεις, οι οποίες κατοχυρώνουν ειδικότερες αποδεικτικές αποδεικτικές εξαιρέσεις, πέραν αυτών των άρθρων 177 παρ. 2 ΚΠΔ και 19 παρ. 3 Σ., παρότι οι τελευταίες πάντως συνιστούν τον κορμό των αποδεικτικών απαγορεύσεων. Χαρακτηριστικά τέτοια παραδείγματα, αποτελούν οι διατάξεις των άρθρων 188, 206, 210, 212, 222, 223 παρ. 4 και 5, 273 παρ. 2 εδ. β', 365 του Κώδικα Ποινικής Δικονομίας. Στις παραπάνω διατάξεις ρυθμίζονται ζητήματα που αφορούν την νομιμότητα διενεργηθείσας πραγματογνωμοσύνης, την εξέταση τεχνικών συμβούλων, την απαγόρευση εξέτασης συγκεκριμένων μαρτύρων, το δικαιώματος άρνησης μαρτυρίας για τους εξ' αίματος συγγενείς του κατηγορουμένου, το δικαίωμα μη αυτοενοχοποίησης, και το δικαίωμα άρνησης του κατηγορουμένου να αναγνωστεί επί του ακροατηρίου ένορκη κατάθεση. Επιπροσθέτως, με το άρθρο 10 του Ν. 1805/1988 τροποποιήθηκε το άρθρο 577 του ΚΠΔ, με το οποίο απαγορεύεται να προηγηθεί την κατάφασης ενοχής, η ανάγνωση του ποινικού μητρώου του κατηγορουμένου.

Αντιστοίχως στον Ποινικό Κώδικα, χρονολογικά εισήχθει με το άρθρο 31 παρ. 2 του ν. 1941/1991[72], η διάταξη του άρθρου 370 Δ παρ. 2, με την οποία ποινικοποιήθηκε η αξιοποίηση αθέμιτων φωνοληψιών και απεικονίσεων, δημιουργώντας με αυτό τον τρόπο απόλυτη απαγόρευση. Εν συνεχεία, δυνάμει του άρθρου 33 παρ. 9 του ν. 2172/1993[73] καταργήθηκε η ανωτέρω διάταξη, ενώ με την παρ. 7 του ίδιου άρθρου αντικαταστάθηκε αυτή του άρθρου 370 Α[74], η οποία με τη σειρά της τροποποιήθηκε με την παρ. 8 του άρθρου 6 ν. 3090/2002[75]. εν συνεχεία με την παρ. 10 ν. 3674/2008 και τέλος με τον ν. 4619/2019.

[72] *"Η επίκληση και προσαγωγή ενώπιον οιουδήποτε ποινικού δικαστηρίου, ανακριτικής ή δημόσιας αρχής των αποτυπώσεων που παρήχθησαν κατά παράβαση της προηγούμενης παραγράφου είναι απαράδεκτη."*

[73] *"Καταργούνται οι εξής διατάξεις του Ποινικού Κώδικα...Το άρθρο 370Δ, που προστέθηκε με το άρθρο 31 του ν. 1941/1991 και αριθμήθηκε με το άρθρο 19 παρ. 4 του ν. 1968/1991."*

[74] 370Α παρ. *4 " Η πράξη της παραγράφου 3 δεν είναι άδικη αν η χρήση έγινε ενώπιον οποιουδήποτε δικαστηρίου, ανακριτικής ή άλλης δημόσιας αρχής για τη διαφύλαξη δικαιολογημένου συμφέροντος που δεν μπορούσε να διαφυλαχθει διαφορετικά και ιδίως σε ποινικό δικαστήριο για την υπεράσπιση του κατηγορουμένου και γενικά αν η χρήση έγινε για την εκπλήρωση καθήκοντος του κατηγορουμένου ή για τη διαφύλαξη έννομου ή άλλου δικαιολογημένου ουσιώδους δημοσίου συμφέροντος."*

[75] 370Α παρ. 4 "*Η πράξη της παραγράφου 3 δεν είναι άδικη, αν η χρήση έγινε ενώπιον οποιασδήποτε δικαστικής ή άλλης ανακριτικής αρχής για τη διαφύλαξη δικαιολογημένου συμφέροντος, που δεν μπορούσε να διαφυλαχθεί διαφορετικά."*

(β) Ερμηνεία του άρθρου 177 παράγραφος 2 ΚΠΔ : περί αποδεικτικών απαγορεύσεων

Σύμφωνα με την διάταξη της παραγράφου 2 του άρθρου 177 του ΚΠΔ "Αποδεικτικά μέσα, που έχουν αποκτηθεί με αξιόποινες πράξεις ή μέσω αυτών, δεν λαμβάνονται υπόψη στην ποινική διαδικασία."

- *Η έννοια της αξιόποινης πράξης*

Κατά τα προβλεπόμενα άρθρο 14 του Ποινικού Κώδικα, *"1. Έγκλημα είναι πράξη άδικη και καταλογιστή στο δράστη της, η οποία τιμωρείται από το νόμο. 2. Στις διατάξεις των ποινικών νόμων ο όρος «πράξη» περιλαμβάνει και τις παραλείψεις."*[76] Για την κατάφαση του αξιοποίνου λοιπόν απαιτείται, μια ανθρώπινη συμπεριφορά που συνίσταται σε θετική ενέργεια ή παράλειψη με την οποία πληρούται η αντικειμενική*(αρχικά άδικη) και υποκειμενική υπόσταση (αρχικά καταλογιστή)*, συγκεκριμένου ποινικού αδικήματος, ενώ δεν τυγχάνει εφαρμογής κάποιος από τους νομοθετικά προβλεπόμενους λόγους άρσης του αδίκου *(τελικά άδικη)* ή του καταλογισμού *(τελικά καταλογιστή)*.

Κατά την κρατούσα στην θεωρία άποψη, η έννοια της αξιόποινης πράξης ερμηνευόμενη τελολογικά στο πλαίσιο του άρθρου 177 παρ. 2 ΚΠΔ, θα πρέπει να θεωρηθεί οτι συμπεριλαμβάνει μόνο τις αρχικά και τελικά άδικες πράξεις[77]. Με άλλα λόγια, τυχόν συνδρομή στοιχείων που αίρουν τον καταλογισμό ή αποκλείουν το αξιόποινο, είναι εν προκειμένω νομικά αδιάφορα, δεν εξαλείφουν τον αξιόποινο χαρακτήρα της διενεργηθείσας ενέργειας και κατά συνέπεια δεν αποκλείουν την εφαρμογή του άρθρου 177 παρ. 2 ΚΠΔ .[78]

Παρά την γραμματική διατύπωση της διάταξης του άρθρου 177 παρ. 2 ΚΠΔ δεν θα πρέπει πάντως να θεωρείται ότι ο νομοθέτης επιθυμεί να υπαχθούν στην έννοια των αποδεικτικών απαγορεύσεων και να θεωρηθούν παρανόμως κτηθέντα μόνο αποδεικτικά στοιχεία που προέκυψαν κατά παράβαση των διατάξεων του Ποινικού Κώδικα, αποκλείοντας δηλαδή με άλλα λόγια την εφαρμογή της σχετικής διάταξης σε αποδεικτικά μέσα που αποκτήθηκαν με προσβολή συνταγματικών δικαιωμάτων, η οποία ενδεχομένως δεν τυποποιείται ως αξιόποινη. Προκειμένου να αποφευχθεί μια τέτοια ερμηνεία, προτάθηκε

[76] https://www.lawspot.gr/nomikes-plirofories/nomothesia/poinikos-kodikas-nomos-4619-2019
[77] Α. Τζαννετής, ΠοινΧρ. ΜΗ'/1998
[78] Α. Τζαννετής ΠοινΧρ. ΜΗ'/1998

από την θεωρία μια διασταλτική προσέγγιση της διάταξης, προκειμένου να περιλαμβάνονται σε αυτή και αποδεικτικά στοιχεία που προέκυψαν μεν από μη αξιόποινες πράξεις, οι οποίες όμως αντίκεινται σε συνταγματικά κατοχυρωμένα δικαιώματα και ελευθερίες.[79]

- *Αιτιώδης σύνδεσμος*

Προκειμένου να συντρέχει περίπτωση εφαρμογής του άρθρου 177 παρ. 2 ΚΠΔ, είναι απαραίτητο να καταφάσκεται επιπλέον αιτιώδης σύνδεσμος μεταξύ της αξιόποινης πράξης και την κτήσης των αποδεικτικών στοιχείων. Από διάφορους θεωρητικούς προκρίνεται η στενή ερμηνευτική προσέγγιση της διάταξης με την εφαρμογή συγκεκριμένων ειδικότερων κριτηρίων.

Πιο συγκεκριμένα, υποστηρίχθηκε πως με το άρθρο 177 παρ. 2 ΚΠΔ δεν θεσπίζεται αποδεικτική απαγόρευση για την αξιοποίηση των προϊόντων εγκλήματος ως αποδεικτικών μέσων έτσι επί παραδείγματι δύναται να αξιοποιηθεί χωρίς περιορισμούς το σώμα του εγκλήματος πλαστογραφίας κατά την ποινική αποδεικτική διαδικασία .

Αντίστοιχα και στις περιπτώσεις εκείνες όπου εγκληματική πράξη απέχει χρονικά από την περιέλευση του αποδεικτικού στοιχείου στις ανακριτικές αρχές, δεν θα πρέπει να θεωρείται ότι συντρέχει περίπτωση εφαρμογής του άρθρου 177 παρ. 2, με αποτέλεσμα να μην υπάγεται έτσι στην έννοια αυτού επί παραδείγματι κλοπιμαίο το οποίο εντοπίστηκε κατά την νόμιμη διενέργεια ανακριτικής πράξης έρευνας σε οικία τρίτου προσώπου[80]

- *Απώτερη Επενέργεια - "Μέσω" αξιόποινης πράξης*

Η απαγόρευση του άρθρου 177 παρ. 2 ΚΠΔ , όπως αυτή ισχύει σήμερα αλλά και κατά την προισχύουσα μορφή της, συνεπάγεται και την απόλυτη αδυναμία αξιοποίησης αποδείξεων που προέκυψαν «μέσω» τέλεσης αξιόποινων πράξεων. Με την διάταξη αυτή ουσιαστικά ενσωματώθηκε στον ΚΠΔ η θεωρία «των καρπών του απαγορευμένου δέντρου» (fruits of the poisonous tree doctrine)[81]. Σύμφωνα με την ως άνω θεωρία, η αποδεικτική απαγόρευση καταλαμβάνει και τα παράγωγα αποδεικτικά στοιχεία, δηλαδή αυτά που προέκυψαν μέσω αξιόποινης πράξης

[79] Α. Τζαννετής ΠοινΧρ. ΜΗ'/1998
[80] Α. Τζαννετής ΠοινΧρ. ΜΗ'/1998
[81] ΑΠ 1568/2004, Ποιν.Δικ

Η απουσία μιας τέτοια νομοθετικής πρόβλεψης, θα συνιστούσε κίνδυνο για όλο το οικοδόμημα των αποδεικτικών απαγορεύσεων αφού ουσιαστικά θα οδηγούσε στο παράλογο αποτέλεσμα να δύνανται να αξιοποιούνται χωρίς περιορισμούς τα εμμέσως κτηθέντα παράνομα αποδεικτικά στοιχεία. Σύμφωνα δε με την γλαφυρό σχολιασμό έγκριτου θεωρητικού αυτή η παράλειψη *"θα αποτελούσε μια κερκόπορτα, μέσω της οποίας θα καθίστατο δυνατή η ακώλυτη εισροή παράνομων αποδεικτικών στοιχείων στην ποινική διαδικασία"*[82].

- *Αξιόποινη απόκτηση από διωκτικές αρχές*

Κατά την επιβολή μέτρων δικονομικού καταναγκασμού, δύναται να αποκτηθούν παράνομα αποδεικτικά μέσα από τις ανακριτικές αρχές . Επι παραδείγματα, η σύλληψη, η επιβολή προσωρινής κράτησης, η διενέργεια πραγματογνωμοσύνη, ερευνών, κατασχέσεων και λοιπών ανακριτικών πράξεων, αποτελούν μέτρα δικονομικού καταναγκασμού, δηλαδή δικονομικές ενέργειες, που διενεργούνται από τα ανακριτικά όργανα και πλήττουν θεμελιώδη έννομα αγαθά του υποκειμένου[83]. Τα μέτρα δικονομικού καταναγκασμού και για ονομάζονται «δικονομικές πράξεις διπλής λειτουργίας» επειδή επιτελούν διπλή λειτουργία ήτοι τόσο δικονομική όσο και ουσιαστική. Από την μια, η δικονομική λειτουργία τους έγκειται στην αναζήτηση της ουσιαστικής αλήθειας και από την άλλη η ουσιαστική λειτουργία τους έγκειται στην πλήρωση της αντικειμενικής υπόστασης συγκεκριμένων αξιόποινων πράξεων, όπως επί παραδείγματι αυτής του άρθρου 334 του ΠΚ, η οποία αναμφίβολα πραγματώνεται κατά τη διεξαγωγή μιας ανακριτικής πράξης κατ' οίκον έρευνας, ο τελικά άδικος χαρακτήρας των οποίων αίρεται, υπό την προϋπόθεση ότι διεξάγονται νομότυπα, καθώς η τέλεσή τους αποτελεί περίπτωση εκ του νόμου επιβαλλόμενης κατ' άρθρο 20 του ΠΚ, ενάσκηση δικαιώματος ή εκπλήρωση καθήκοντος[84]

Η παράτυπη, κατά παράβαση των σχετικών διατάξεων διεξαγωγή πράξεων δικονομικού καταναγκασμού οδηγεί στην πλήρωση του της παραγράφου 2 του άρθρου 177 του ΚΠΔ και κατά συνέπεια συνεπάγεται συνδρομή αποδεικτικής απαγόρευσης.

[82]Α. Τζαννετής ΠοινΧρ. ΜΗ'/1998
[83]Θ. Δαλακούρας, *« Ποινική Δικονομία»,* 2003
[84]Ν. Ανδρουλάκης, «Θεμελιώδεις έννοιες της ποινικής δίκης», 2007

iii. Απόλυτη Ακυρότητα

Από την παράγραφο δυο του άρθρου 177 του ΚΠΔ προκύπτει ότι με την αξιοποίηση απαγορευμένων αποδεικτικών στοιχείων κατά την ποινική αποδεικτική διαδικασία πλήττεται το δικαίωμα υπεράσπισης του κατηγορουμένου και προκαλείται απόλυτη ακυρότητα της διαδικασίας, σύμφωνα με την περίπτωση δ΄ της παραγράφου 1 του άρθρου 171 του ΚΠΔ.

iii. Αποδεικτικές Απαγορεύσεις και Κατάσχεση Ψηφιακών Πειστηρίων

Η κατάσχεση ψηφιακών πειστηρίων, όπως προαναφέρθηκε αποτελεί μια από την ρητά πλέον θεσμοθετημένες στον Κώδικα Ποινικής Δικονομίας ανακριτικές πράξεις. Πρόκειται λοιπόν για μια πράξη δικονομικού καταναγκασμού, η οποία διενεργείται από την ανακριτικές αρχές στο πλαίσιο αναζήτησης της αλήθειας μέσω της εύρεσης κρίσιμων για την αποκάλυψη αυτής αποδεικτικών στοιχείων. Δεδομένου ότι, όπως αναλύθηκε παραπάνω η μη νομότυπη διενέργεια πράξεων δικονομικού καταναγκασμού από τις ανακριτικές αρχές συνεπάγεται την πλήρωση του 177 παρ. 2 ΚΠΔ, θα πρέπει να γίνει δεκτό ότι ψηφιακά πειστήρια που κατάσχονται, δηλαδή αφαιρούνται, αντιγράφονται και επαληθεύονται κατά παράβαση του νόμου, οδηγούν σε αποδεικτική απαγόρευση και συνακόλουθα η χρήση αυτών σε απόλυτη ακυρότητα της διαδικασίας.

Ο ίδιος ο νομοθέτης, παρότι με την νέα διάταξη του άρθρου 265 ΚΠΔ διατείνεται ότι "*παρέχονται οι δέουσες εγγυήσεις και προϋποθέσεις για την αποτροπή τυχόν αυθαιρεσιών, προβλέποντας τη σύνταξη ειδικής έκθεσης, τη χρήση κατάλληλου εξοπλισμού κατάσχεσης, τον περιορισμό της πρόσβασης μόνο σε εξουσιοδοτημένο προσωπικό, αλλά και μέτρα κατά της τυχαίας απώλειας και διαγραφής των ψηφιακών δεδομένων*"[85], δεν επέλεξε να προβλέψει ρητά "σχετική ακυρότητα", σε περίπτωση παραβίασης των κανόνων που τίθενται με την συγκεκριμένη διάταξη. Έτσι κατ' αρχήν με βάση το ισχύον νομοθετικό πλαίσιο δεν θα πρέπει επί παραδείγματι να θεωρηθεί ότι τίθεται θέμα ακυρότητας σε περίπτωση "μη χρήσης κατάλληλου εξοπλισμού". Εξάλλου στην ίδια διάταξη δεν προκαθορίζονται ειδικά τα μέσα που είναι κατάλληλα για την διενέργεια της κατάσχεσης αλλά ο νομοθέτης αρκείται σε γενικότερη πρόβλεψη.

[85] https://www.hellenicparliament.gr/UserFiles/c8827c35-4399-4fbb-8ea6-aebdc768f4f7/11027276.pdf

Παραταύτα έχει διατυπωθεί θεωρητικά η άποψη ότι *"...η πλημμελής εξαγωγή δεδομένων, και ιδίως η μη τήρηση κάποιου πρωτοκόλλου για την επαλήθευση της αυθεντικότητας και της ακεραιότητας, είναι δυνατό να παίξει ουσιώδη ρόλο στο σχέση **με** την αποδεικτική αξιοποίηση των δεδομένων στο μεταγενέστερα στάδια της ποινικής διαδικασίας"*[86].

Περαιτέρω, σε σχέση με την ειδική έκθεση, η σύνταξη της οποίας αξιώνεται από το άρθρο 265 ΚΠΔ, θα πρέπει να γίνει δεκτό ότι τυγχάνουν εφαρμογής και οι γενικές διατάξεις του ΚΠΔ σχετικά με τις εκθέσεις *(148 επ. ΚΠΔ),* με αποτέλεσμα επί συγκεκριμένων παρατυπιών να επιφυλάσσεται και γι' αυτή η σχετική ακυρότητα του άρθρου 153 ΚΠΔ. Τυχόν δε παράλειψη σύνταξης της ή ακυρότητα αυτής θα πρέπει να θεωρηθεί ότι αποτελεί περίπτωση μη νομότυπης διενέργειας πράξης δικονομικού καταναγκασμού, που συνεπάγεται αποδεικτική απαγόρευση αξιοποίησης.

5. Νομοθετικές Κινήσεις σε Υπερεθνικό Επίπεδο

5.1. Νομολογιακές Περιπτώσεις

Καθημερινά, όλο και περισσότερες έξυπνες συσκευές, οι οποίες φαίνεται, κατ' αρχήν τουλάχιστον, να αποσκοπούν στην βελτίωση του βιοτικού επιπέδου του σύγχρονου ατόμου, γίνονται "μάρτυρες" βιοτικών συμβάντων και καταστάσεων με ποινικό ενδιαφέρον, δημιουργώντας σειρά προβληματισμών. Πότε και σε ποιο βαθμό θα πρέπει να αξιοποιούνται; Αν και σε τι βαθμό πλήττεται η ιδιωτικότητα του εκάστοτε υποκειμένου των δεδομένων;

Τον **Απρίλιο του 2011**, στις ΗΠΑ, τέσσερις άντρες συνελήφθησαν και διώχθηκαν για ληστείες κατά συρροή. Ένας εκ των συλληφθέντων ομολόγησε ότι συμμετείχαν και άλλα πρόσωπα, ως απλοί συνεργοί - τσιλιαδόροι, τους οποίους ως τότε δεν έχουν καταφέρει να ταυτοποιήσουν οι αρμόδιες ανακριτικές αρχές. Ο ως άνω συλληφθείς δράστης, παρέδωσε στις αρχές το κινητό του τηλέφωνο μέσω του οποίου ανακτήθηκαν τηλεφωνικοί αριθμοί μερικών εκ των εμπλεκόμενων προσώπων. Εν συνεχεία το FBI ζήτησε και έλαβε, δεδομένα θέσης (cell- site location information - CSLI), δηλαδή δεδομένα που προκύπτουν βάση εγγύτητας της εκάστοτε

[86] Γ. Ναζίρης, " Η κατάσχεση ψηφιακών Δεδομένων", Ποινική Δικαιοσύνη, Τεύχος Φεβρουάριος 2020

τηλεφωνικής συσκευής με την κεραία, από τα οποία και εξήχθει το συμπέρασμα ότι τα συγκεκριμένα πρόσωπα που συνομιλούσαν με τον συλληφθέντα κατά τον κρίσιμο χρόνο τέλεσης της ληστείας βρισκόταν γεωγραφικά στον ίδιο χώρο με αυτόν. [87]

Τον **Δεκέμβριο του 2013**, εκδόθηκε ένταλμα προς την Microsoft, προκειμένου η τελευταία να παραχωρήσει στις ανακριτικές αρχές περιεχόμενο μηνυμάτων ηλεκτρονικής αλληλογραφίας αλλά και δεδομένα που σχετίζονται με εξωτερικά στοιχεία επικοινωνίας, στο πλαίσιο υπόθεσης ναρκωτικών. Κατά το σχετικό ένταλμα τα δεδομένα έπρεπε να τεθούν στην διάθεση των ανακριτικών αρχών εφόσον βρισκόταν "υπό την κατοχή ή τον έλεγχο" αμερικάνικης εταιρείας. Στην συγκεκριμένη περίπτωση, κάποια εξωτερικά στοιχεία επικοινωνίας ήταν αποθηκευμένα εγχώρια, ενώ το περιεχόμενο της επικοινωνίας δηλαδή των email, ήταν αποθηκευμένο σε ένα διακομιστή στο Δουβλίνο, στην Ιρλανδία. Η Microsoft παρείχε πληροφορίες για τα εξωτερικά στοιχεία επικοινωνίας, αλλά αρνήθηκε να εκπληρώσει το ένταλμα ως προς το περιεχόμενο της επικοινωνίας, υποστηρίζοντας ότι η σχετική αποκάλυψη θα συνιστούσε ανεπίτρεπτη εφαρμογή εθνικής νομοθεσίας σε υπερεθνικό έδαφος, δεδομένα ότι αυτά βρισκόταν αποθηκευμένα στο server σε αλλοδαπή χώρα . Από την άλλη η κυβέρνηση των ΗΠΑ υποστήριξε ότι ο νόμος υποχρέωνε τους παρόχους να αποκαλύπτουν τυχόν αρχεία υπό τον έλεγχό τους. Μετά από πολλές προσφυγές και αποκλίνουσες αποφάσεις από τα δικαστήρια, η υπόθεση έφτασε στο Ανώτατο Δικαστήριο.[88]

Το **2014** το Ανώτατο Δικαστήριο των Η.Π.Α. στην υπόθεση **"Riley v. California"**[89], έκρινε ότι μεταξύ άλλων, πριν την λήψη δεδομένων από κινητά, η αστυνομία θα πρέπει να έχει εξασφαλίσει σχετικό ένταλμα, για λόγους προστασίας της ιδιωτικότητας. Ασάφεια ωστόσο εξακολουθεί να υπάρχει σύμφωνα με την Pat Augustine, όσον αφορά λοιπές έξυπνες συσκευές όπως, τα "smartwatches" ή τα "fit trackers".

Το 2015, στην Πολιτεία Αρκάνσας των Η.Π.Α., ο James A. Bates, κατηγορήθηκε με ανθρωποκτονία πρώτου βαθμού, όταν εντοπίστηκε νεκρός από τις αρχές στην μπανιέρα του σπιτιού του ο Victor Collins, τον οποίο ο ίδιος ο Bates είχε προσκαλέσει την προηγούμενη μέρα. Οι αρχές παρατήρησαν μελανιές και εκδορές στο σώμα του θύματος καθώς και σημάδια που υποδείκνυαν ότι είχε γίνει απόπειρα να καθαριστεί το σημείο στο οποίο εντοπίστηκε το θύμα[90].

[87] Carpenter VS United States, No 16-402, 585 U.S., 2018
[88] United states v. Microsoft Corporation, No 17-2, 584 U.S., 2018
[89] 134 S. Ct. 2473 (2014)
[90] Holly Kathleen Hall, "*Arkansas v. Bates: Reconsidering the Limits of a Reasonable Expectation of Privacy*", 2017

Οι αρχές κατέσχεσαν μια συσκευή Amazon Echo, ως αντικείμενο ποινικής έρευνας που διεξήγαγαν σε κατοικία, όπου εντοπίστηκε νεκρό θύμα[91], υποπτευόμενοι ότι ενδεχομένως να μπορεί να τους αποκαλύψει κάποια στοιχεία για τον δράστη. Κατόπιν εκδόσεως σχετικού εντάλματος, ζητήθηκε από την Amazon να παραδώσει στις αρχές, διαθέσιμο ακουστικό υλικό της συγκεκριμένης συσκευής που τηρείται στους servers της, για το τελευταίο κρίσιμο 48ωρο με την αιτιολογία ότι βάσιμα πιστεύει πως η εταιρεία έχει στην κατοχή της αρχεία που συνδέονται με την ερευνώμενη υπόθεση ανθρωποκτονίας. Η Amazon, αρχικά συμμορφώθηκε εν μέρει παραδίδοντας τα στοιχεία του συνδρομητή και το ιστορικό αγοράς της συσκευής, αρνήθηκε όμως να παράσχει πρόσβαση σε φωνητικές εγγραφές ή απομαγνητοφωνημένες εντολές, επικαλούμενη ζητήματα ιδιωτικότητας του πελάτη - υποκειμένου και συγκεκριμένα την 4η Τροπολογία του Συντάγματος των Η.Π.Α., ενώ εν συνεχεία κατόπιν συναίνεσης του ίδιου του υποκειμένου, τις προσκόμισε στις δικαστικές αρχές. Όπως χαρακτηριστικά υπογραμμίζεται στο paper "UB Journal of Media Law & Ethics", η 4η Τροπολογία τίθεται σε ισχύ, και η επέμβαση συνεπάγεται ανεπίτρεπτη παραβίαση στην ιδιωτικότητα, εφόσον αυτή λαμβάνει χώρα εντός της προστατευόμενης "κατοικίας", *"..και παρ οτι ο τοπικός αυτός διαχωρισμός εντός/εκτός κατοικίας έδειχνε να λειτουργεί, τούτο έπαψε να ισχύει αφής στιγμής τέθηκε στην εξίωση το Διαδίκτυο και τα δεδομένα μεταφέρονται στους διακομιστές και στο νέφος. Το ζήτημα αυτό επηρεάζει ακόμα και την έκδοση ενταλμάτων, τα οποία πρέπει συγκεκριμένα να περιγράφουν τον φυσικό χώρο που πρόκειται να ερευνηθεί.[92]"* Κατά τον ***Joel Reidenberg***, διευθυντή του *"Center on Law and Information Policy"* της Νομικής Σχολής *"Fordham"* της Νέας Υόρκης, *" Σύμφωνα με την 4η τροπολογία, αν έχεις εγκαταστήσει μια συσκευή που ακούει και μεταδίδει σε τρίτα μέρη, έχεις αποχαιρετήσει τα δικαιώματα σου στην ιδιωτικότητα κατά την Νομοθεσία περί Ηλεκτρονικών Επικοινωνιών και Ιδιωτικότητας[93]".* Από την άλλη πλευρά η δικαστής **Sonia Sotomayor** στην υπόθεση United States v. Jones, έθεσε τον προβληματισμό ότι *"ίσως είναι απαραίτητο να αναθεωρήσουμε την λογική, ότι ένα υποκείμενο δεν έχει δικαιολογημένη προσδοκία ιδιωτικότητας σε πληροφορίες που εθελοντικά έχει*

[91] "Murder defendant volunteers Echo recordings Amazon fought to protect", Alex Hern, Tue 7 Mar 2017 11.11 GMThttps://www.theguardian.com/technology/2017/mar/07/murder-james-bates-defendant-echo-recordings-amazon

[92] Holly Kathleen Hall, "*Arkansas v. Bates: Reconsidering the Limits of a Reasonable Expectation of Privacy*", 2017

[93]Joel Reidenberg, director of the Center on Law and Information Policy at Fordham Law School in New York City,*"A device like the Amazon Echo is essentially a microphone transmitting data to third parties, "so reasonable privacy doesn't exist. Under the Fourth Amendment, if you have installed a device that's listening and is transmitting to a third party, then you've waived your privacy rights under the Electronic Communications Privacy Act,"*, https://www.mic.com/articles/162865/amazon-echo-privacy-is-alexa-listening-to-everything-you-say

αποκαλύψει σε τρίτα μέρη...Η προσέγγιση αυτή είναι προβληματική, στα πλαίσια της ψηφιακής εποχής, κατά την οποία οι άνθρωποι ανακαλύπτουν σημαντική ποσότητα πληροφοριών για τους εαυτούς τους σε τρίτα μέρη για την διεκπεραίωση ασήμαντων εργασιών"[94].

Το **2015** επίσης ζητήθηκε από την **Apple**, στα πλαίσια διερεύνησης ποινικής υπόθεσης τρομοκρατίας και ειδικότερα στην επίθεση **San Bernardino**, να ξεκλειδώσει μια συσκευή iPhone που ανήκε σε έναν από τους σκοπευτές. Η άρνηση της Apple να προβεί στην συγκεκριμένη ενέργεια βασίστηκε στην προστασία της ασφάλειας και ιδιωτικότητας των πελατών της, και στον κίνδυνο δημιουργίας ενός "επικίνδυνου" νομολογιακού προηγούμενου.

Το **2016,** στην δίκη για τον βιασμό και την ανθρωποκτονία της 19χρονης φοιτήτριας ιατρικής Maria Ladenburger, ως αποδεικτικό στοιχείο χρησιμοποιήθηκαν δεδομένα από την εφαρμογή "Apple Health" που βρισκόταν στο κινητό του κατηγορουμένου. Ο τελευταίος αρνήθηκε να δώσει στην αστυνομία τον κωδικό του τηλέφωνό του, ωστόσο η πρόσβαση σε αυτό ανακτήθηκε με την συνδρομή ιδιωτικής εταιρείας. Τα δεδομένα από το τηλέφωνο αποκάλυψαν τις κινήσεις του δράστη και υπέδειξαν ότι υπήρχαν δύο κορυφές έντονης δραστηριότητας, τις οποίες η εφαρμογή του καταχώρησε ως «ανάβαση σκάλας». Με συνδυασμό των δεδομένων γεωεντοπισμού και φυσικής κατάστασης του δράστη, οι αρχές συμπέραναν ότι ο κατηγορούμενος είχε σύρει το σώμα της παθούσας και εν συνεχεία ανέβηκε τις σκάλες.

Επίσης το **2016,** στην υπόθεση **C-207/16, το ΔΕΕ**, απασχόλησε η πρόσβαση των εθνικών αρχών στα δεδομένα ηλεκτρονικών επικοινωνιών, για σκοπούς διενέργειας ποινικής έρευνας, υπό το πρίσμα της υπ' αριθμόν **2002/58/ΕΚ Οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες**. Πιο συγκεκριμένα, οι Ισπανικές αρχές ζήτησαν δικαστικά να τους επιτραπεί πρόσβαση σε δεδομένα προσωπικού χαρακτήρα, που βρισκόταν στην κατοχή παρόχων υπηρεσιών ηλεκτρονικών επικοινωνιών, προκειμένου να καταστεί εφικτό να ταυτοποιήσεις τους κατόχους κινητών μέσω των καρτών SIM αυτών, οι οποίες είχαν ενργοποοιηθεί, κατά τη διάρκεια χρονικού διαστήματος δώδεκα ημερών, με τον κωδικό IMEI του κλαπέντος κινητού τηλεφώνου. Τα δεδομένα στα οποία ζητούσαν πρόσβαση ήταν οι τηλεφωνικοί αριθμοί που αντιστοιχούν στις ως άνω κάρτες SIM, τα στοιχεία ταυτοποίησης των κατόχων των εν λόγω καρτών (ονοματεπώνυμο και διεύθυνσή τους) και οχι το περιεχόμενο των επικοινωνιών που πραγματοποιήθηκαν ούτε τον

[94] Sonia Sotomayor "*It may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties…This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks", https://www.datasecuritylawjournal.com/2012/11/16/is-secrecy-a-prerequisite-for-privacy/*

εντοπισμό της θέσεώς του. Στις σκέψεις 56 και επόμενες της παρούσας απόφασης, το Δικαστήριο. εστιάζοντας στην **"αρχή της αναλογικότητας"** διαπιστώνει οτι ***"μια σοβαρή επέμβαση μπορεί να δικαιολογείται μόνον από σκοπό καταπολεμήσεως της εγκληματικότητας, η οποία πρέπει επίσης να χαρακτηρίζεται ως «σοβαρή»"***. Εν ολίγοις, προκειμένου να κριθεί κατά πόσο είναι δικαιολογημένη μια επέμβαση η οποία έρχεται σε σύγκρουση με την προστασία έτερων θεμελιωδών δικαιωμάτων κρίσιμη είναι η in concreto στάθμιση, τόσο της σοβαρότητας της επέμβασης, όσο και της σοβαρότητας του ποινικού αδικήματος χάριν του οποίου γίνεται. Ειδικότερα το Δικαστήριο κατέληξε, ότι το άρθρο 15, παράγραφος 1, της οδηγίας 2002/58, ερμηνευόμενο υπό το πρίσμα των άρθρων 7 και 8 του Χάρτη, έχει την έννοια ότι η πρόσβαση δημοσίων αρχών στα παραπάνω δεδομένα συνιστά επέμβαση στα θεμελιώδη δικαιώματα του Χάρτη που δεν έχει "σοβαρό χαρακτήρα" δεν θα πρέπει να αποτελεί εμπόδιο στην καταπολέμηση της βαριάς εγκληματικότητας, περιορίζοντας την δυνατότητα εντοπισμού, διερεύνησης, κατάφασης και καταστολής εγκληματικών πράξεων.

Το **2017**, στην πόλη Farmington, στην Πολιτεία Κονέκτικατ των Η.Π.Α., στα πλαίσια διερεύνησης ανθρωποκτονίας σε βάρος της **Ms. Sullivan**, σύμφωνα με τον Δικαστή Houran, "πιθανολογήθηκε" απο το Δικαστήριο οτι η Amazon διατηρούσε αρχεία εγγραφών από την συσκευή Echo που βρισκόταν στο σπίτι του θύματος, κατά την κρίσιμη περίοδο τέλεσης του εγκλήματος, οι οποίες ενδεχομένως να περιέχουν κρίσιμα στοιχεία. Επιπλέον στην παρούσα υπόθεση ζητήθηκε από το Δικαστήριο, να παρασχεθούν επιπλέον πληροφορίες σχετικά με τυχόν άλλες "έξυπνες" συσκευές που φαίνεται να συνδεόταν με την Echo κατά την κρίσιμη χρονική περίοδο. [95]

Το 2018, στην πόλη Σαν Χοσέ, της Πολιτείας Καλιφόρνια, των Η.Π.Α., η αστυνομία προέβη σε συλλογή δεδομένων από το "fitness tracker" που φορούσε το θύμα, ερευνώμενης ανθρωποκτονίας. Μέσω αυτών μπόρεσε να διαπιστώσει το ακριβές χρονικό σημείο του θανάτου αλλά και την ένταση που προηγήθηκε, παρακολουθώντας την καταγραφή σφυγμών. Ο κρίσιμος αυτός χρονικός προσδιορισμός σε συνδυασμό με πλάνα από κάμερες κυκλοφορίας οδήγησε την αστυνομία, στην τοποθέτηση του υπόπτου στον χώρο του εγκλήματος. Στην συλλογή των κρίσιμων δεδομένων από το FitBit, βάσει σχετικού εντάλματος, συνεισέφερε ο διευθύνων σύμβουλος της Fitbit, Mr. Jeff Bonham.

[95]https://www.independent.co.uk/life-style/gadgets-and-tech/news/amazon-echo-alexa-evidence-murder-case-a8633551.html

5.2.Cloud Act

ο Νόμος "περί Νόμιμης Χρήσης Δεδομένων στο εξωτερικό" (**Clarifying Lawful Overseas Use of Data Act** or **CLOUD Act** - HR 4943)[96] είναι ένας ομοσπονδιακός νόμος των Ηνωμένων Πολιτειών, που θεσπίστηκε το Μάρτιο του 2018. Με τον σχετικό νόμο, τροποποιήθηκε η ισχύουσα από το 1986 Νομοθεσία (Stored Communications Act - SCA) προκειμένου να επιτραπεί στις ομοσπονδιακές αρχές επιβολής του νόμου των ΗΠΑ να υποχρεώσουν τις εταιρείες τεχνολογίας που εδρεύουν στις ΗΠΑ , μέσω εντάλματος ή κλήτευσης να παρέχουν ζητούμενα δεδομένα, που είναι αποθηκευμένα σε διακομιστές ακόμα και εάν τα δεδομένα δεν είναι αποθηκευμένα στις ΗΠΑ αλλά σε ξένο κράτος. Με άλλα λόγια μέσω της σχετικής διάταξης εξουσιοδοτούνται τα αρμόδια ανακριτικά όργανα των ΗΠΑ να αιτηθούν και να λάβουν πρόσβαση σε δεδομένα, αποθηκευμένα σε τρίτη χώρα.[97]

Αξίζει να σημειωθεί ότι η παραπάνω νομοθετική διάταξη ψηφίστηκε ενόσω εκκρεμούσε στο Ανώτατο Δικαστήριο των ΗΠΑ η υπόθεση "United States vs Microsoft". Στην υπόθεση αυτή, το κύριο ζήτημα που τέθηκε ενώπιον του Ανωτάτου Δικαστηρίου ήταν εαν οι αρχές επιβολής του νόμου των ΗΠΑ δύνανται με ένταλμα να εξαναγκάσουν μια αμερικανική εταιρεία να αποκαλύψει το περιεχόμενο email που είναι αποθηκευμένο στο τρίτη χώρα. Το Υπουργείο Δικαιοσύνης (DOJ) είχε προσφύγει στο ομοσπονδιακό δικαστήριο ζητώντας έκδοση εντάλματος, προκειμένου να υποχρεωθεί η Microsoft να αποκαλύψει στις αρχές τόσο το περιεχόμενο όσο και εξωτερικά στοιχεία επικοινωνίας. Στην συγκεκριμένη περίπτωση, κάποια εξωτερικά στοιχεία επικοινωνίας ήταν αποθηκευμένα εγχώρια, ενώ το περιεχόμενο της επικοινωνίας δηλαδή των email, ήταν αποθηκευμένο σε ένα διακομιστή στο Δουβλίνο, στην Ιρλανδία. Η Microsoft παρείχε πληροφορίες για τα εξωτερικά στοιχεία επικοινωνίας, αλλά αρνήθηκε να εκπληρώσει το ένταλμα ως προς το περιεχόμενο της επικοινωνίας, υποστηρίζοντας ότι η σχετική αποκάλυψη θα συνιστούσε ανεπίτρεπτη εφαρμογή εθνικής νομοθεσίας σε υπερεθνικό έδαφος. Από την άλλη η κυβέρνηση των ΗΠΑ υποστήριξε ότι ο νόμος υποχρέωνε τους παρόχους να αποκαλύπτουν τυχόν αρχεία υπό τον έλεγχό τους. Μετά από πολλές προσφυγές και αποκλίνουσες αποφάσεις από τα δικαστήρια, η υπόθεση έφτασε στο Ανώτατο Δικαστήριο. Εν αναμονή λοιπόν της απόφασης στην υπόθεση της Microsoft, η

[96]Clarifying Lawful Overseas Use of Data (CLOUD) Act, Pub. L. No. 115-141, 132 Stat. 348 (2018) https://www.congress.gov/bill/115th-congress/house-bill/4943/text
[97] Jennifer Daskal, "*Unpacking the CLOUD Act*", 2018

"**CLOUD Act**" συμπεριλήφθηκε σε μια τροπολογία σε ένα γενικό νομοσχέδιο δαπανών και πέρασε απότομα. Ο νόμος υπογράφηκε στις 23 Μαρτίου 2018. Η υπόθεση Ηνωμένες Πολιτείες κατά της Microsoft απορρίφθηκε.

Η "**CLOUD Act**" αποτελείται από δύο βασικά μέρη. Στο «Μέρος Ι» θεσμοθετείται η υποχρέωση των παρόχων, να παρέχουν δεδομένα περιεχομένου στις αρχές επιβολής του νόμου των Η.Π.Α ανεξαρτήτως της θέσης αποθήκευσης τους. Ειδικότερα, με αυτή τροποποιήθηκε η υφιστάμενη νομοθεσία έτσι ώστε να απαιτείται πλέον οι πάροχοι να παραδίδουν δεδομένα που βρίσκονται στην κατοχή τους. Την ίδια στιγμή, ο νόμος παρέχει περιορισμένες ευκαιρίες στους παρόχους να προσφύγουν δικαστικά κατά σχετικού εντάλματος, για δεδομένα που βρίσκονται στο εξωτερικό με βάση την υπάρχουσα νομοθετική σύγκρουση. Πιο συγκεκριμένα, τόσο οι εγχώριοι όσο και ξένοι πάροχοι επιτρέπεται να αμφισβητήσουν ένα τέτοιο ένταλμα, εντός δεκατεσσάρων ημερών υπό τρεις προϋποθέσεις που πρέπει να πληρούνται σωρευτικά, δηλαδή, (1) η επικοινωνία να αφορά ξένο πρόσωπο, δηλαδή άτομο που δεν είναι πολίτης ή κάτοικος ΗΠΑ (2) η συμμόρφωση του παρόχου με το ένταλμα να δημιουργεί «ουσιαστικό κίνδυνο» παραβίασης νόμου (3) ο οποίος να έχει θεσπιστεί από ξένο Κράτος, που έχει εκτελεστική συμφωνία με τις ΗΠΑ με την οποία παρέχει στο αυτή νομοθετικά αντίστοιχη δυνατότητα να αμφισβητήσει σχετικό ένταλμα.

Το «Μέρος ΙΙ» εξουσιοδοτεί αξιωματούχους των Η.Π.Α να συνάπτουν εκτελεστικές συμβάσεις με τρίτες χώρες, δυνάμει των οποίων θα επιτρέπεται σε παρόχους να αποκαλύπτουν το αποθηκευμένο στις ΗΠΑ περιεχόμενο επικοινωνιών, σε αρχές τρίτων χωρών, χωρίς πάντως να εξαλείφει άλλους μηχανισμούς μεταφοράς δεδομένων, όπως ισχύουσες Συνθήκες αμοιβαίας δικαστικής συνδρομής (mutual legal assistance treaty - MLAT), δικαστικά αιτήματα ή άλλα ανεπίσημα αιτήματα. Τυχόν συναφθείσες συμβάσεις πρέπει να επανεξετάζονται και μπορούν να ανανεώνονται κάθε πέντε χρόνια. Για την σύναψη αυτών θα πρέπει να πληρούνται τέσσερα κριτήρια: (α) Πρώτον, το εσωτερικό εθνικό δίκαιο της εκάστοτε αλλοδαπής κυβέρνησης θα πρέπει να παρέχει «ισχυρή ουσιαστική και διαδικαστική προστασία για την ιδιωτική ζωή και τις πολιτικές ελευθερίες» · (β) δεύτερον, η αλλοδαπή κυβέρνηση πρέπει να υιοθετεί διαδικασίες για την ελαχιστοποίηση της απόκτησης, διατήρησης και διάδοσης πληροφοριών που σχετίζονται με πολίτες ή κατοίκους των ΗΠΑ · (γ) τρίτον, με την σύμβαση απαγορεύεται να προβλέπεται οποιαδήποτε υποχρέωση των παρόχων να αποκρυπτογραφούν ή όχι τα δεδομένα · (δ) τέταρτον, οι παραγγελίες για χορήγηση δεδομένων που θα δίδονται βάσει της συμφωνίας θα πρέπει να

πληρούν μια σειρά από συνθήκες, να περιλαμβάνουν προσταστευτικές δικλείδες για τα ανθρώπινα δικαιώματα των πολιτών των ΗΠΑ. Ειδικότερα, θα πρέπει οι σχετικές παραγγελίες να δίνονται μόνο στο πλαίσιο έρευνας για σοβαρό έγκλημα · να προσδιορίζουν ένα συγκεκριμένο ερευνώμενο άτομο ή πάντως άλλο συγκεκριμένο αναγνωριστικό ως στόχο · να συμμορφώνονται με το εσωτερικό δίκαιο της χώρας αυτής · να βασίζονται σε εύλογη αιτιολόγηση που υποστηρίζεται από αξιόπιστα γεγονότα και όχι απλές εικασίες · να υπόκεινται σε έλεγχο ή επίβλεψη από δικαστήριο, δικαστή, ή άλλη ανεξάρτητη αρχής· να έχουν περιορισμένη χρονική διάρκεια και συγκεκριμένα να μην διαρκούν περισσότερο από όσο είναι εύλογο και αναγκαίο · και να εκδίδονται μόνο εάν δεν υπάρχει άλλο λιγότερο δυσμενές μέσο. Τα δεδομένα πρέπει ελαχιστοποιούνται επίσης χρησιμοποιώντας διαδικασίες ελαχιστοποίησης.

Αυτό που τελικά αποτέλεσε Μέρος ΙΙ του Νόμου, στην πραγματικότητα δεν ήταν κάτι καινούργιο αλλά κάτι είχε ήδη στο παρελθόν επιδιωχθεί ενεργά από την κυβέρνηση Ομπάμα. Τεχνικές εταιρείες, αξιωματούχοι, ακαδημαϊκοί εμπειρογνώμονες και πολίτες συμμετείχαν σε μια πολυετή συζήτηση για τα ζητήματα, ενώ πολλοί εκπρόσωποι άσκησαν ενεργά πιέσεις στα μέλη του Κογκρέσου τόσο υπέρ όσο και κατά βασικών διατάξεων.[98] Άλλωστε, προγενέστερη έκδοση του νόμου CLOUD είχε προταθεί και ως αυτόνομο νομοσχέδιο[99].

Ο νόμος "**CLOUD Act"**, όπως σχεδόν κάθε νομοθετικό εγχείρημα, αποτέλεσε προϊόν συμβιβασμού κατόπιν διαπραγμάτευσης, με αποτέλεσμα, εγγενώς να είναι ατελής. Μεταξύ άλλων ελαττωμάτων και ελλείψεων, δεν ρυθμίζει το ενδεχόμενο πολυμερών συμφωνιών, αφήνοντας αναπάντητα βασικά ερωτήματα σχετικά με τη δυνατότητα και τα περιγράμματα μιας πιθανής συμφωνίας ΗΠΑ και Ευρωπαϊκής Ένωσης [100] · και παραμελεί να παρέχει ρητή προστασία σε εταιρείες που ανταποκρίνονται σε αιτήματα ξένων κυβερνήσεων για χορήγηση δεδομένων[101].

Στον αντίποδα, θα έλεγε κανείς ωστόσο ότι αντικατοπτρίζει επίσης μια προσπάθεια να ανταπόκρισης στις μεταβαλλόμενες ανάγκες της επιβολής του νόμου, δημιουργώντας νέους μηχανισμούς για την αντιμετώπιση των αναγκών αυτών

---

[98] J. Daskal and A. K. Woods, *"Cross-Border Requests: A Proposed Framework",* Just Security, 2015
[99] S.2383 (115th Cong.); H.R. 4943 (115th Cong.)
[100] J. Daskal and P. Swire, *"A Possible EU-US Agreement on Law Enforcement Access to Data?",* Lawfare, 2018
[101] Jennifer Daskal, "*Unpacking the CLOUD Act",* 2018

5.3.“E-Evidence”

Λίγο μετά την υιοθέτηση της “**CLOUD Act”**, από τις ΗΠΑ και συγκεκριμένα τον Απρίλιο του 2018, η Ευρωπαϊκή Επιτροπή πρότεινε “E-Evidence”. Πρόκειται για μια νομοθετική πρόταση, που αντικατοπτρίζει την διασυνοριακή προσέγγιση της “**CLOUD Act”**.

Πιο συγκεκριμένα, η Ευρωπαϊκή Επιτροπή αξιολογώντας τόσο το γεγονός ότι όλο και περισσότεροι δράστες αξιοποιούν την τεχνολογία κατά τον σχεδιασμό και τη διάπραξη αδικημάτων, με αποτέλεσμα και οι ανακριτικές αρχές να στηρίζονται όλο και περισσότερο σε ψηφιακά πειστήρια για τον εντοπισμό και την καταστολή αυτών, όσο και το γεγονός ότι η πρόσβαση στα ηλεκτρονικά αποδεικτικά στοιχεία μπορεί να αποδειχθεί χρονοβόρα και πολύπλοκη διαδικασία, ιδίως όταν τα δεδομένα είναι αποθηκευμένα στο εξωτερικό, πρότεινε τον Απρίλιο του 2018 νέους κανόνες, ώστε η πρόσβαση σε ψηφιακά πειστήρια να καταστεί καλύτερη και ταχύτερη για τις αρχές. Οι πάροχοι επιγραμμικών υπηρεσιών αποθηκεύουν τα δεδομένα των χρηστών σε διακομιστές, που ενδέχεται να βρίσκονται σε διαφορετικές χώρες, τόσο εντός όσο και εκτός της ΕΕ. Το γεγονός αυτό καθιστά τη συλλογή ηλεκτρονικών αποδεικτικών στοιχείων πολύ δυσκολότερη για τις δικαστικές αρχές, καθώς οι τελευταίες είναι υποχρεωμένες να ακολουθούν χρονοβόρες και πολύπλοκες διαδικασίες για την απόκτησή τους. Στατιστικά πάνω από το 50% του συνόλου των ποινικών ερευνών υποβάλλεται διασυνοριακό αίτημα πρόσβασης σε ηλεκτρονικά αποδεικτικά στοιχεία.[102] Ο βασικός στόχος των νέων κανόνων που προτείνει η Επιτροπή είναι να επιταχυνθεί η πρόσβαση σε ηλεκτρονικά αποδεικτικά στοιχεία ανεξάρτητα από το πού βρίσκονται τα δεδομένα.

Κατά την αρχική πρόταση της Επιτροπής, οι νέοι κανόνες θα παρέχουν στις δικαστικές αρχές μιας χώρας της ΕΕ την δυνατότητα να ζητούν απευθείας πρόσβαση σε ηλεκτρονικά αποδεικτικά στοιχεία από κάθε πάροχο που προσφέρει υπηρεσίες στην Ευρωπαϊκή Ένωση και είναι εγκατεστημένος ή εκπροσωπείται σε άλλο κράτος μέλος. Με αυτό τον τρόπο θα επιταχύνεται άμεση διεκπεραίωση της αίτησης πρόσβασης, καθότι δεν θα υπάρχει ανάγκη να μεσολαβούν οι αρχές του άλλου κράτους μέλους. Οι προτεινόμενοι κανόνες περιέχονται σε δύο νομοθετικές προτάσεις, έναν κανονισμό σχετικά με τις ευρωπαϊκά εντάλματα χορήγησης ηλεκτρονικών αποδεικτικών στοιχείων σε ποινικές υποθέσεις και μια οδηγία

[102] https://www.consilium.europa.eu/el/policies/e-evidence/

σχετικά με τη θέσπιση εναρμονισμένων κανόνων για τον ορισμό νόμιμων εκπροσώπων με σκοπό τη συγκέντρωση αποδεικτικών στοιχείων στο πλαίσιο ποινικών διαδικασιών

Ο κανονισμός σχετικά με εντάλματα χορήγησης ηλεκτρονικών αποδεικτικών στοιχείων θα επιτρέψει στις αρχές να έχουν πρόσβαση σε αποθηκευμένα δεδομένα, ανεξαρτήτως του πού βρίσκονται. Μέσω της σχετικής διαδικασίας θα επιτρέπεται στις δικαστικές αρχές ενός κράτους μέλους να ζητούν πρόσβαση σε ηλεκτρονικά αποδεικτικά στοιχεία απευθείας από έναν πάροχο υπηρεσιών που είναι εγκατεστημένος ή εκπροσωπείται σε άλλο κράτος μέλος. Ο πάροχος υπηρεσιών θα είναι υποχρεωμένος να αποκριθεί εντός 10 ημερών ή εντός 6 ωρών εφόσον επείγει. Με το ίδιο ένταλμα θα απαγορεύεται τη διαγραφή ηλεκτρονικών αποδεικτικών στοιχείων από τον πάροχο υπηρεσιών όσο εκκρεμεί η εκτέλεση αυτού. Οι κανόνες αυτοί θα βασίζονται στην αρχή αμοιβαίας αναγνώρισης μεταξύ των κρατών μελών και θα εφαρμόζονται μόνο σε αποθηκευμένα δεδομένα, καθώς οι προτεινόμενοι κανόνες δεν καλύπτουν τα δεδομένα από υποκλοπή τηλεπικοινωνιών σε πραγματικό χρόνο.

Η οδηγία από την άλλη θα υποχρεώνει όλους τους παρόχους υπηρεσιών που δεν είναι εγκατεστημένοι στην Ευρωπαϊκή Ένωση αλλά παρέχουν υπηρεσίες στην Ένωση να διορίζουν νόμιμο εκπρόσωπο. Ο τελευταίος θα είναι υπεύθυνος για την παραλαβή και την εκτέλεση ενταλμάτων . Στόχος είναι όλοι οι πάροχοι υπηρεσιών που λειτουργούν στην ΕΕ να έχουν τις ίδιες υποχρεώσεις όσον αφορά την πρόσβαση στα ηλεκτρονικά αποδεικτικά στοιχεία.

Τον Ιούνιο του 2019, το Συμβούλιο εξουσιοδότησε την Ευρωπαϊκή Επιτροπή να διαπραγματευτεί συμφωνία εξ ονόματος της ΕΕ με τις Ηνωμένες Πολιτείες σχετικά με τη διασυνοριακή πρόσβαση σε ηλεκτρονικά αποδεικτικά στοιχεία και να συμμετάσχει στις διαπραγματεύσεις με το Συμβούλιο της Ευρώπης για δεύτερο πρόσθετο πρωτόκολλο της σύμβασης της Βουδαπέστης για το έγκλημα στον κυβερνοχώρο.

Οι διαπραγματεύσεις με τις Ηνωμένες Πολιτείες που έχουν στόχο να διευκολυνθεί η διασυνοριακή πρόσβαση σε ηλεκτρονικά αποδεικτικά στοιχεία για τη δικαστική συνεργασία σε ποινικές υποθέσεις άρχισαν τον Σεπτέμβριο του 2019 και είναι υπό εξέλιξη.Επί του παρόντος, οι εγκατεστημένοι στις ΗΠΑ πάροχοι υπηρεσιών συνεργάζονται με τις ευρωπαϊκές αρχές επιβολής του νόμου με άμεση και εθελοντική συνεργασία ή μέσω διαδικασιών αμοιβαίας δικαστικής συνδρομής. Το δίκαιο των ΗΠΑ δεν επιτρέπει πάντοτε στους παρόχους υπηρεσιών να αποκρίνονται άμεσα στα ευρωπαϊκά αιτήματα για πρόσβαση σε ηλεκτρονικά

αποδεικτικά στοιχεία. Ενδεχόμενη συμφωνία ΕΕ-ΗΠΑ θα διευκολύνει τη συνεργασία και θα διαμορφώσει ισχυρές διασφαλίσεις για την προστασία των θεμελιωδών δικαιωμάτων.

5.4. Συγκριτική Προσέγγιση

Αναντίρρητα, η νομοθετική πρωτοβουλία των ΗΠΑ "CLOUD ACT" αντιπροσωπεύει σε διεθνές επίπεδο την έναρξη ενός εποικοδομητικού διαλόγου για θέσπιση ουσιαστικών και διαδικαστικών κανόνων, που διέπουν την πρόσβαση των αρχών επιβολής του νόμου στα ψηφιακά αποδεικτικά στοιχεία και τη μεταβαλλόμενη σχέση μεταξύ των εδαφικών ορίων και της ανάγκης ψηφιακών αποδεικτικών στοιχείων.

Από την άλλη, οι προτάσεις οδηγίας και κανονισμού "E- EVIDENCE" της Ευρωπαϊκής Ένωσης, αντιπροσωπεύουν τη συμβολή της Ευρώπης σε αυτή τη συζήτηση και έχουν αξιοσημείωτες ομοιότητες με τον νόμο CLOUD ACT.

Ενώ ο νόμος "CLOUD ACT" έχει πλέον θεσπιστεί στη νομοθεσία των ΗΠΑ, η πρόταση της Ευρωπαϊκής Επιτροπής είναι ακόμη υπό εξέταση, κατά συνέπεια υπάρχει η ευκαιρία να τροποποιηθεί το κείμενο έτσι ώστε να ενισχυθούν οι εγγυήσεις για τα ατομικά δικαιώματα και να ελαχιστοποιηθούν οι κίνδυνοι.

Οι δύο προτάσεις αν και έχουν σημαντικές διαφορές, παρουσιάζουν επίσης βασικές ομοιότητες. Και οι δύο προβλέπουν πρόσβαση σε δεδομένα και διατήρηση αυτών ανεξάρτητα από το που αποθηκεύονται. Η ομοιότητα αυτή έχει ως αποτέλεσμα, πολλές από τις κριτικές που αφορούν το "**CLOUD Act"** να ισχύουν εξίσου και για την "E-Evidence". Ειδικότερα, όπως και στο Μέρος ΙΙ του"CLOUD ACT", έτσι και στο σχέδιο κανονισμού "E-EVIDENCE" προβλέπεται ένας μηχανισμός έκδοσης εντάλματος απευθείας προς ιδιωτική εταιρεία που κατέχει αποδεικτικά στοιχεία ενδιαφέροντος, ακόμη και αν αυτή η ιδιωτική εταιρεία βρίσκεται εκτός της εδαφικής δικαιοδοσίας της χώρας που διεξάγει την έρευνα, με στόχο την παράκαμψη της διαδικασίας αμοιβαίας νομικής συνδρομής.

Πέραν των ανωτέρω και άλλες μονομερείς πρωτοβουλίες αφθονούν σε παγκόσμιο επίπεδο. Έτσι το Ηνωμένο Βασίλειο επιτρέπει πλέον την έκδοση εξωεδαφικών ενταλμάτων *(extraterritorial warrants)* ενώ η Αυστραλία θέσπισε πρόσφατα νομοθεσία που επιτρέπει την έκδοση εντάλματος παροχής τεχνικής συνδρομής *(technical assistance orders)* σε παρόχους

που βρίσκονται εκτός εδάφους της αλλά έχουν έναν ή περισσότερους τελικούς χρήστες στην Αυστραλία.[103]

Συμπεράσματα

6.1 Σύνοψη και συμπεράσματα

Σε εθνικό επίπεδο, σημαντική πρόοδος πράγματι επετεύχθει προς την κατεύθυνση της ορθής αξιοποίησης των ψηφιακών πειστηρίων με την θεσμοθέτηση της έννοιας της ψηφιακής κατάσχεσης στο άρθρο 265 του νέου κώδικα ποινικής δικονομίας. Πρόκειται για μια διάταξη που παρά τις ελλείψεις της κινείται συνολικά στην "σωστή κατεύθυνση", αφού μεταξύ άλλων για πρώτη φορά έδωσε στις αρχές την δυνατότητα να προβαίνουν σε κατάσχεση ψηφιακών δεδομένων, διακριτά από τον εκάστοτε υλικό φορέα αποθήκευσης τους, αναγνωρίζοντας ουσιαστικά τη ίδια την φύση των ψηφιακών δεδομένων. Πράγματι ο νομοθέτης φαίνεται το πρώτον σε τέτοια τουλάχιστον έκταση να επιχειρεί μέσω του συγκεκριμένου νομοθετικού εγχειρήματος να κατανοήσει πραγματικά τόσο την φύση των "ψηφιακών δεδομένων", διακρίνοντας τα σαφώς από τον υλικό τους φορέα και αντιμετωπίζοντας τα με βάση τα εγγενή τους χαρακτηριστικά · αλλά και των τεχνολογιών αποθήκευσης και μετακίνησης αυτών. Ειδικότερα, το πρώτον ο νομοθέτης κάνει λόγο για περιπτώσεις απομακρυσμένης πρόσβασης σε πληροφοριακά συστήματα αλλά και για την τεχνολογία της νεφουπολογιστικής, και αξιοποιεί ρητά έστω και αφηρημένα, μέσω μιας γενικότερης πρόβλεψης για "κατάλληλο εξοπλισμό" την τεχνολογία ως εργαλείο διενέργειας ανακριτικών πράξεων.

Η σχετική διάταξη έχει λοιπόν αναντίρρητα θετικό πρόσημο, πέραν των "ήσσονος"σημασίας ελλείψεων που αναλύθηκαν παραπάνω, ήτοι την απουσίας ρητής πρόβλεψης περί "αποκλεισμού πρόσβασης - κλειδώματος", του "χρονικού πλαισίου" διενέργειας κατάσχεσης των δεδομένων, όταν έχει προηγηθεί κατάσχεση υλικού φορέα, αλλά και της ανάγκης για σύνταξη μίας ή περισσότερων εκθέσεων στην συγκεκριμένη περίπτωση, - *που αν δεν καλυφθούν στην πράξη μέσω νομολογιακών και ερμηνευτικών*

[103] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) (Austl.), Sch. 1 § 317C (defining scope of coverage), https://www.legislation.gov.au/Details/C2018A00148

προσεγγίσεων, πάντως εύκολα μπορούν να αποτελέσουν αντικείμενο νομοθετικής τροποποίησης - . Πέραν όμως των παραπάνω ελλείψεων, κατά την άποψη της γράφουσας σημαντική έλλειψη εξακολουθεί να συνιστά και η απουσία πρόβλεψης, ειδικότερων τεχνικών διαδικασιών, αρχών, προτύπων και διαδικαστικών βημάτων/ διατυπώσεων, που να δημιουργούν ένα συγκεκριμένο πλαίσιο διενέργειας της ανακριτικής αυτής πράξης, λειτουργώντας παράλληλα και ως ένα δίχτυ ασφαλείας. Πιο συγκεκριμένα, δεδομένου ότι στην διάταξη με την οποία ρυθμίζεται η κατάσχεση ψηφιακών πειστηρίων δεν δίδεται αναλυτική διαδικασία διενέργειας αυτής - *όπως επί παραδείγματι τέτοια προκύπτει από τα διάφορα θεωρητικά μοντέλα που αναλύθηκαν στην αρχη της παρούσας* - ούτε προβλέπεται χρήση συγκεκριμένων εργαλείων και αυστηρών διαδικαστικών βημάτων, από την μία παρέχεται μια ευελιξία στα ανακριτικά όργανα, ευελιξία μάλιστα που θα μπορούσε κανείς να υποστηριξει ότι συμπλέει με την εγγενή ιδιότητα της τεχνολογίας να εξελίσσεται ραγδαία, αλλά από την άλλη αφήνεται και ένα ευρύ πεδίο δράσης των ανακριτικών οργάνων που περιορίζει την δυνατότητα ελέγχου και μπορεί να αποτελέσει πρόσφορο έδαφος για αυθαιρεσίες. Έτσι μέσα από μια τέτοια πρόβλεψη δύναται να προστατευθούν και πληρέστερα τα δικαιώματα και οι ατομικές ελευθερίες των εμπλεκόμενων προσώπων και ειδικότερα να τίθενται όρια στις ανακριτικές αρχές, αλλά και να καθίσταται εφικτή από την πλευρά της υπεράσπισης η άσκηση πραγματικού ελέγχου, που μπορεί να οδηγήσει ενδεχομένως σε επίκληση αποδεικτικών απαγορεύσεων και ακυροτήτων.

Σε υπερεθνικό επίπεδο από την άλλη, όλες αυτές οι πρωτοβουλίες επιδιώκουν πράγματι να ανταποκριθούν στην αυξανόμενη ψηφιοποίηση των πληροφοριών, στον ρόλο τρίτων παρόχων στον έλεγχο αυτών των πληροφοριών και στο γεγονός ότι οι πάροχοι και τα δεδομένα ενδιαφέροντος διατηρούνται ολοένα και περισσότερο εκτός συνόρων. Αυτές οι αλλαγές παρέχουν ευκαιρίες όσο και προκλήσεις. Κατά την ανάκτηση δεδομένων και αποδεικτικών στοιχείων σε διεθνές, υπερεθνικό επίπεδο, σαφώς διακυβεύονται κυριαρχικά συμφέροντα επιβολής και ενυπάρχουν σημαντικές προκλήσεις. Τόσο η “CLOUD ACT” των ΗΠΑ όσο και η Ευρωπαϊκή πρόταση “E - Evidence”, αποτελούν σημαντική συνεισφορά σε αυτές τις προσπάθειες – μια συνεισφορά που μπορεί και πρέπει να οικοδομηθεί μέσω της σύναψης ισχυρών διμερών συμφωνιών που προστατεύουν και προάγουν την ιδιωτική ζωή και τις πολιτικές ελευθερίες.

Στόχος τέτοιων συμφωνιών θα πρέπει να είναι η διευκόλυνση της νόμιμη και ταχείας διασυνοριακής πρόσβασης σε δεδομένα μέσω ρητά καθορισμένων διαδικασιών, που παράλληλα προστατεύουν τα υποκείμενα και προωθούν την ασφάλεια σε παγκόσμιο επίπεδο. Έτσι δεν πρέπει να λησμονείται ότι με όλες αυτές τις διασυνοριακές προτάσεις, που αποσκοπούν στην υποβοήθηση της διαδικασίας επιβολής του νόμου σε διεθνές επίπεδο, θα πρέπει να διασφαλίζονται πρωτίστως με καθιέρωση ειδικών δικλείδων ασφαλείας και τα δικαιώματα των υποκειμένων, που θα έλεγε κανείς ότι έως σήμερα αφήνονται "εκτεθειμένα" και αποτελούν το μεγαλύτερο "κενό" που διαπιστώνεται στις υφιστάμενες νομοθετικές προσπάθειες.

6.2 Όρια και περιορισμοί της έρευνας

Από την μία η ευρύτητα του ερευνώμενου αντικειμένου και από την άλλη συνεχής εξέλιξη αυτού σε εθνικό και υπερεθνικό επίπεδο, εξέλιξη που είναι σύμφυτη τόσο με την ίδια την φύση των ψηφιακών δεδομένων όσο και με την διεθνή θεώρηση του ζητήματος, κατέστησαν αδύνατη μια "εξαντλητική προσέγγιση" αυτού. Αντ΄αυτού επιχειρήθηκε μια "οριοθέτηση" βασικών εννοιών, μια "καταγραφή" υφιστάμενων προβληματισμών και προκλήσεων και τέλος μια "σκιαγράφηση" νομοθετικών κινήσεων σε εθνικό και διεθνές περιβάλλον. Αναμφίβολα κάθε κεφάλαιο της παρούσας μελέτης από μόνο του θα μπορούσε να αποτελέσει διακριτό αντικείμενο ενός ερευνητικού έργου, Κρίθηκε ωστόσο σκόπιμο να παρουσιαστεί καθένα από αυτά στην παρούσα έστω και πιο συνοπτικά χάριν πληρέστερης σύλληψης και κατανόησης του προβλήματος που επιχειρήθηκε να λυθεί.

Παράλληλα, η απουσία επισταμένης τεχνολογικής γνώσης στην γράφουσα, από μόνη της έθεσε εξ αρχής όρια στο συγκεκριμένο συγγραφικό εγχείρημα. Παρά την προσπάθεια κατανόησης βασικών τεχνολογικών εννοιών που συνδέονται άμεσα με το ερευνώμενο αντικείμενο, σε καμία περίπτωση δεν μπορεί να υποστηριχθεί ότι κατέστη εφικτή η επισταμένη προσέγγιση αυτών.

6.3 Μελλοντικές Επεκτάσεις

Δεδομένου ότι πρόκειται για ένα ερευνητικό ζήτημα, το οποίο σήμερα βρίσκεται στο διεθνές νομοθετικό "προσκήνιο", η συνεχής θεωρητική αξιολόγηση του, θα πρέπει να

συμπορεύεται με τις νέες νομοθετικές κινήσεις που βρίσκονται σε εξέλιξη αλλά και να παρακολουθεί τις συνεχείς εξελίξεις σε τεχνολογικό επίπεδο, ώστε να ασκείται εποικοδομητική κριτική. Κάθε νομοθετική προσπάθεια, τόσο σε εθνικό όσο και σε διεθνές επίπεδο αποτελεί έναν "ζωντανό οργανισμό", που δεν δύναται να παραμένει ανεπηρέαστος από τις εξελίξεις γύρω του και ως τέτοιος θα πρέπει και να αντιμετωπίζεται.

Πιο συγκεκριμένα, προτείνεται σε ευρωπαϊκό επίπεδο, η παρακολούθηση και ο σχολιασμός της εν εξελίξη νομοθετικής διαδικασίας για την κατοχύρωση της E- Evidence αλλά και η επισκόπηση τυχόν διμερών συμφωνιών που θα ανακύψουν στο πλαίσιο εφαρμογής του Μέρους ΙΙ της Cloud Act. Ενώ σε εθνικό επίπεδο προτείνεται η αξιολόγηση και ο σχολιασμός νομολογίας που αναμένεται σταδιακά να ανακύψει λόγω του νεοεφάρμοστου Κώδικα Ποινικής Δικονομίας.

ΒΙΒΛΙΟΓΡΑΦΙΑ

i. Ελληνική

- Αγγελής Εμ. Ι., «Διαδίκτυο (internet) και ποινικό δίκαιο – Έγκλημα στον κυβερνοχώρο», ΠΧρ, 2000
- Αδάμ Χ. Παπαδαμάκης, "Ποινική Δικονομία: η δομής της ποινικής δίκης", ΣΤ΄έκδοση, εκδόσεις Σάκκουλα, 2012
- Αναγνωστόπουλος Η., «Αστυνομική παγίδευση και δίκαιη δίκη», ΠΧρ, 2001
- Ανδρουλάκης Ν. , "Θεμελιώδεις έννοιες της ποινικής δίκης", Εκδ. Δίκαιο & Οικονομία Π. Ν. Σάκκουλα Αθήνα, 3η έκδοση, 2007
- Βενιζέλος Ελ., "Το αναθεωρητικό κεκτημένο", εκδόσεις Σάκκουλα, 2002
- Δαλακούρας Θ., «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη, 2019.
- Δαλακούρας Θ., «Οι ειδικές ανακριτικές πράξεις του άρθρ. 6 του Ν. 2928/2001», ΠΧρ, 2001
- Δαλακούρας Θ., "Ποινική Δικονομία Βασικές έννοιες και θεσμοί της Ποινικής Δίκης", Τόμος Β' εκδ. Αντ. Ν. Σάκκουλα Αθήνα- Κομοτηνή 2003
- Δαλακούρας Θ., "Αρχή αναλογικότητας και μέτρα δικονομικού καταναγκασμού", Ποινικά Χρονικα, 1993
- Δαλακούρας Θ., "Απαγορευμένα αποδεικτικά μέσα : δογματικές βάσεις για την θεμελίωση των αποδεικτικών απαγορεύσεων στην Ποινική Δίκη" , ΠοινΧρ ΜΣΤ/1996
- Δαλακούρας Θ., "Η αποδεικτική απαγόρευση της αξιοποιήσεως των αθέμιτων φωνοληψιών και απεικονίσεων κατ' άρθρο 370 Δ παρ. 2 ΚΠΔ", Υπερ 2/1992
- Δημητράτος Ν., "Η εξέλιξη του θεσμού των αποδεικτικών απαγορεύσεων στο ελληνικό ποινικό δικονομικό δίκαιο- συγχρόνως μια συγκριτική επισκόπηση του αντίστοιχου αμερικανικού και γερμανικού δικαιικού πλαισίου", ΠοινΧρ. ΝΑ/2001
- Δημητράτος Ν., «Περί των αποδεικτικών απαγορεύσεων στην ποινική δίκη», εκδ. Αντ., 1992
- Διονυσοπουλος Τ., «Αστυνομική διείσδυση. Συνταγματικά και δικονομικά προβλήματα μιας «νομιμοποιημένης» ανακριτικής πράξης», ΠΛογ, 2003

- Ηλιοπούλου- Στράγγα Τ. , "Χρήση παρανόμως κτηθέντων αποδεικτικών μέσων και δικαίωμα υπεράσπισης του κατηγορουμένου, Η αποδεικτική απαγόρευση του α. 19 παρ. 3 του αναθεωρημένου Συντάγματος, πρόλογος Ν. Κ. Ανδρουλάκη)", Εκδ. Αντ. Ν. Σάκκουλα Αθήνα- Κομοτηνή 2003
- Καρράς Α., «Ποινικό Δικονομικό Δίκαιο», 7η Έκδ, Νομική Βιβλιοθήκη, 2019
- Λίβου Ν., "Η δικονομική αξιολόγηση των τυχαίων ευρημάτων (εξ' αφορμής της ΑΠ 157/1998, ΠοινΧρ. ΜΗ' σελ. 781 επ.)", ΠοινΧρ. ΜΗ'/1998
- Μανωλεδάκης Ι. «Ποινικό Δίκαιο, Επιτομή Γενικού Μέρους», 7η έκδ., Σάκκουλας, 2005
- Μαργαρίτης Μ. – Μαργαρίτη Α., «Κώδικας Ποινικής Δικονομίας – Θεωρία - Νομολογία», Π.Ν. Σάκκουλας, 2020
- Μαργαρίτης Μ., "Κώδικας Ποινικής Δικονομίας, ερμηνεία κατ' άρθρο, Τόμος Α'" (άρθρα 1-304), Εκδ. Νομική βιβλιοθήκη 2010
- Μιχαηλίδου *Χ.,* "Κυβερνοέγκλημα και ηλεκτρονική απόδειξη ένας τρόπος εξακρίβωσης του ψηφιακού αποτυπώματός του. Ευρώπη με μια ματιά." – The Art of Crime, *2018*
- Μυλωνόπουλος Χ. Χρ., «Ποινικό Δίκαιο Γενικό Μέρος», Εκδόσεις Σάκκουλας, Τόμος Ι, 2007
- Ναζίρης Γ., "Η κατάσχεση ψηφιακών Δεδομένων", Ποινική Δικαιοσύνη, Τεύχος Φεβρουάριος 2020
- Νάιντος Χ. "Αποδεικτικές απαγορεύσεις στην ποινική δίκη" 2010
- Παπαδαμάκης Χ. Α., «Ανακριτική διείσδυση: όρια και υπερβάσεις», ΠοινΔικ 2010
- Παπαδαμάκης Χ. Α., «Ποινική Δικονομία – Θεωρία-Πράξη-Νομολογία», Εκδόσεις Σάκκουλα, 9η εκδ., 2019
- Παπανδρέου Π. , "Η Προκαταρκτική εξέταση", ΠοινΔικ 2006
- Σεβαστίδης Χ.," Κώδικας Ποινικής Δικονομίας," ερμηνεία κατ' άρθρο, 2015
- Σπινέλλης Λ. Δ., "Αποδεικτικές απαγορεύσεις στην ποινική δίκη", ΠοινΧρ. ΛΣΤ'/1986 σελ. 865 επ.
- Συμεωνίδου-Καστανίδου Ελ, "Παραβίαση απορρήτου επικοινωνιών και αποδεικτικές απαγορεύσεις στην ποινική δίκη", Ποινική Δικαιοσύνη, τεύχος 11/2015
- Τζαννετή Α. «Αποδεικτικές απαγορεύσεις και εναλλακτική νόμιμη κτήση αποδείξεων» ΠοινΧρ ΜΕ'/1995

- Τριαντάφυλλος Γ., "Αποδεικτικές απαγορεύσεις και αρχή της αναλογικότητας", ΠοινΧρ. ΝΖ'/2007
- Φράγκος Κ., "Κώδικας Ποινικής Δικονομίας (Ν. 4620/2019 και Ν. 4637/2019)", 2η έκδ., 2020
- Χριστόπουλος Κ, "Η ΣΚΟΠΙΜΟΤΗΤΑ ΤΩΝ ΕΡΕΥΝΩΝ ΚΑΙ ΤΩΝ ΕΙΔΙΚΩΝ ΑΝΑΚΡΙΤΙΚΩΝ ΠΡΑΞΕΩΝ ΕΠΙ ΟΡΙΣΜΕΝΩΝ ΕΓΚΛΗΜΑΤΩΝ", 2021

ii. Ξενόγλωσση

- Baryamureeba, V. and Tushabe, F., "The Enhanced Digital Investigation Process Model" In Proceedings of the Fourth Digital Forensic Research Workshop, (2004)
- Coco Celine and Dr. Galli Francesca, *"Surveillance: Ethical issues, legal limitations, efficiency",* (2012)
- Daskal Jennifer, "Unpacking the CLOUD Act", (2018)
- Daskal J. and SwireP., "A Possible EU-US Agreement on Law Enforcement Access to Data?", Lawfare (21 May 2018)
- Daskal J. and Woods A. K., "Cross-Border Requests: A Proposed Framework", Just Security (24 November 2015)
- Goodison S. E., Davis R. C., and Jackson Br. A., Digital Evidence and the U.S. Criminal Justice System, Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence, https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf
- Grabosky P., "Security in the 21st Century, Security Journal" (2007)
- Holly Kathleen Hall, "Arkansas v. Bates: Reconsidering the Limits of a Reasonable Expectation of Privacy", 2017
- Iqlezakis Ioannis, " Messenger Messages and Facebook Photographs as Means of Evidence - Heraklion Jury Trial Court ", Content Downloaded from HeinOnline, (2019)
- Khuram Mushtaque, "Digital Forensic Investigation Models, an Evolution study", (2015)
- Kohn, M.D., Eloff, M.M. and Eloff, J.H.P., "Integrated Digital Forensic Process Model Computers & Security", (2013)
- Kyriakides Eleni, The CLOUD Act, E-Evidence, and Individual Rights, 5 EUR. DATA PROT.L. REV. 99 (2019).

- Mike Mcguire, S. Dowling, “Cyber crime: A review of the evidence Research Report 75 Chapter 2: Cyber-enabled crimes -fraud and theft” (2013)
- Myeonki Kim, “THE NEED FOR A LENIENT ADMISSIBILITY STANDARD FOR DEFENSE FORENSIC EVIDENCE”, (2018)
- Ortiz -Pradillo Juan Carlos ,“*The new regulation of technology - related investigative measures in Spain”,* (2017)
- Pollitt, M.M., An Ad Hoc Review of Digital Forensic Models. In Proceedings of 2nd International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE 2007)
- Qatawneh Mohammad, Almobaideen W., “DFIM: A NEW DIGITAL FORENSICS INVESTIGATION MODEL FOR INTERNET OF THINGS”, (2020)
- Reith, M., Carr, C. and Gunsch, G., “An Examination of Digital Forensic Models. International Journal of Digital Evidence”, (2002)
- Robinson Gavin,“The European Commission's e-Evidence Proposal”, Content Downloaded from HeinOnline, (2018)
- Ryan J. Daniel, Shpantzer Gal, “Legal Aspects of Digital Forensics” The George Washington University, Washington, D. C. (2002)
- Dr. Sudesh Rani, “DIGITAL FORENSIC MODELS: A COMPARATIVE ANALYSIS”, (2018)
- The Parliamentary Office of Science and Technology , “Digital Forensics and Crime”, (2016)
- Vaciago Giuseppe and Ramalho David Silva ,*“Online searches and online surveillance: the use of trojans and other types of malware as means of obtaining evidence in criminal proceedings”*, Digital Evidence and Electronic SIgnature Law Review, 13, (2016)
- Vlachopoulos Konstantinos , Magkos Emmanouil and Chrissikopoulos Vassileios. A model for hybrid evidence investigation. International Journal of Digital Crime and Forensic (2016)
- Wahl Thomas, “ New E-Evidence Legislation: Trilogue Started – Criticism on EP Stance”, (2021)
- Xiaoyu Du, Nhien-An Le-Khac, Mark Scanlon “Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service”, School of Computer Science,University College Dublin, (2017)

- Yaacoub A. Jean-Paul , Noura N. Hassan , Salman Ola and Chehab Ali, ”DIGITAL FORENSICS VS. ANTI-DIGITAL FORENSICS: TECHNIQUES, LIMITATIONS AND RECOMMENDATIONS “American University of Beirut, Electrical and Computer Engineering Department”, (April 1, 2021)
- Yeboah-Boateng Ezer Osei and Akwa-Bonsu Elvis, “Digital Forensic Investigations: Issues of Intangibility, Complications and Inconsistencies in Cyber-Crimes”, Ghana Technology University College (GTUC), (2016)

iii. Νομολογιακές Αποφάσεις

- ΑΠ 1918/2017, ΠΟΙΝΧΡ 2019/125
- ΑΠ 305/2019, ΤΝΠ ΝΟΜΟΣ.
- ΕΦΛΑΜ 6/2021, ΤΝΠ ΝΟΜΟΣ.
- ΠΛΗΜ ΠΕΙΡΑΙΑ 109/2017, ΠΟΙΝΔ/ΝΗ 2018/308
- ΣυμβΠλημ 196/2017, ΠΟΙΝΧΡ 2019/536
- ΣυμβΠλημΑρτ 50/2015, ΠΟΙΝΔ/ΝΗ 2015/1121
- Carpenter VS United States, No 16-402, 585 U.S., 2018
- United states v. Microsoft Corporation, No 17-2, 584 U.S., 2018

iv. Υπερσύνδεσμοι Ιστοσελίδων

(*τελευταία επίσκεψη σε όλες τις ιστοσελίδες πραγματοποιήθηκε την 10.01.2022)*

- https://ec.europa.eu/home-affairs/what-we-do/cybercrime/e-evidence_el
- https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690522/EPRS_BRI(2021)690522_EN.pdf
- https://www.consilium.europa.eu/el/policies/e-evidence/
- https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en
- https://www.consilium.europa.eu/el/policies/e-evidence/
- https://ec.europa.eu/home-affairs/what-we-do/cybercrime/e-evidence_el

- https://www.hellenicparliament.gr/UserFiles/c8827c35-4399-4fbb-8ea6-aebdc768f4f7/11027276.pdf
- https://www.consilium.europa.eu/el/policies/e-evidence/
- https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-4411-2016/symvasi-tis-voydapestis-gia-egklima-ston-kyvernohoro-0
- http://www.et.gr/idocsnph/search/pdfViewerForm.html?args=5C7QrtC22wFqnM3eAbJzrXdtvSoClrL8PT2mlaPXRibtIl9LGdkF53UIxsx942CdyqxSQYNuqAGCF0IfB9HI6qSYtMQEkEHLwnFqmgJSA5WIsluVnRwO1oKqSe4BlOTSpEWYhszF8P8UqWb_zFijGMqgncuOLN9VfqAr3uaqTfxgCPfk1b8I49-ZpbxDzxW
- https://eisap.gr/%CE%B3%CE%BD%CF%89%CE%BC%CE%BF%CE%B4%CF%8C%CF%84%CE%B7%CF%83%CE%B7-6-2021/
- https://www.legislation.gov.au/Details/C2018A00148
- https://eisap.gr/%ce%b3%ce%bd%cf%89%ce%bc%ce%bf%ce%b4%cf%8c%cf%84%ce%b7%cf%83%ce%b7-05-2012/
- https://www.ministryofjustice.gr/wp-content/uploads/2019/08/58bNomos_ait_ekthesi_n_3875.pdf
- https://www.e-nomothesia.gr/kat-anthropina-dikaiomata/nomothetiko-diatagma-53-1974-phek-256a-20-9-1974.html
- https://www.e-nomothesia.gr/kat-epikoinonies-telepikoinonies-telephonia/n-3674-2008.html
- https://www.lawspot.gr/nomikes-plirofories/nomothesia/poinikos-kodikas-nomos-4619-2019
- https://www.theguardian.com/technology/2017/mar/07/murder-james-bates-defendant-echo-recordings-amazon
- https://www.mic.com/articles/162865/amazon-echo-privacy-is-alexa-listening-to-everything-you-say

- https://www.datasecuritylawjournal.com/2012/11/16/is-secrecy-a-prerequisite-for-privacy/
- https://www.independent.co.uk/life-style/gadgets-and-tech/news/amazon-echo-alexa-evidence-murder-case-a8633551.html
- Clarifying Lawful Overseas Use of Data (CLOUD) Act, Pub. L. No. 115-141, 132 Stat. 348 (2018) https://www.congress.gov/bill/115th-congress/house-bill/4943/text,

Κυρώσεις για λογοκλοπή

Η λογοκλοπή είναι ένα πολύ σοβαρό παράπτωμα. Με απόφαση με το άρθ. 7.2 του Κανονισμού «σε περιπτώσεις λογοκλοπής ή παράλειψης αναφοράς στη μεταπτυχιακή Διπλωματική Εργασία, η ελάχιστη κύρωση, μετά από απόφαση της ΕΔΕ, είναι η υποχρέωση του φοιτητή να επιλέξει άλλον επιβλέποντα καθηγητή με διαφορετικό θέμα Διπλωματικής και να επαναλάβει το τρίτο εξάμηνο με ανάλογες πρόσθετες οικονομικές υποχρεώσεις, ενώ μέγιστη κύρωση μπορεί να είναι η οριστική διαγραφή του από το Πρόγραμμα. Εάν έχει ήδη αποφοιτήσει, ανακαλείται το Μεταπτυχιακό Δίπλωμα Ειδίκευσης και προωθείται το θέμα στο Δικαστικό Γραφείο του Πανεπιστημίου για την έναρξη των ανάλογων νομικών διαδικασιών».