ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»

Ακαδημαϊκό έτος 2022-2023

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της ΧΡΥΣΟΥΛΑΣ ΑΝΤΩΝΙΑΔΟΥ (Α.Μ.: ΜΔΙ 2104)

«Έξυπνες συσκευές και ψηφιακή εγκληματολογική έρευνα (smartphone | smart devices | smart home | IoT & Cloud Forensics) »

Επιβλέπουσα:

Ευαγγελία (Λίλιαν) Μήτρου, Καθηγήτρια Πανεπιστημίου Αιγαίου, Δικηγόρος

Πειραιάς, 2023

ΑΦΙΕΡΩΣΗ

Αφιερωμένη στην αγαπημένη μου οικογένεια που με στηρίζει σταθερά σε κάθε μου βήμα και στα ανίψια μου Αριάδνη, Νεφέλη & Θησέα, την παντοτινή πηγή έμπνευσης & δύναμης μου…

Ακόμα, στον σύντροφο μου, Λάμπρο, που στάθηκε δίπλα μου σε όλη αυτή την διαδρομή στηρίζοντας με, με κάθε τρόπο.

ΕΥΧΑΡΙΣΤΙΕΣ

Φτάνοντας σχεδόν στο τέλος της διαδρομής ως μεταπτυχιακή φοιτήτρια του ΜΠΣ «***Δίκαιο και Τεχνολογίες Πληροφορικής & Επικοινωνιών***» του τμήματος Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς, νιώθω την ανάγκη να ευχαριστήσω από καρδιάς, πρώτα απ' όλους τον Διευθυντή του προγράμματος και καθηγητή μας κ. Γκρίτζαλη Στέφανο για την τόσο ζεστή και φοιτητοκεντρική του προσέγγιση και ευαισθησία σε κάθε ζήτημα που μας απασχολούσε αλλά και το ζωηρό ερευνητικό του ενδιαφέρον που 'παρέσερνε' ακόμα και τους μη τεχνολογικά μυημένους (όπως εγώ) νομικούς στην ανακάλυψη νέων οριζόντων ενδιαφέροντος, με τρόπο τόσο απλό και εύληπτο.

Επίσης, στην επιβλέπουσα καθηγήτρια μου κα. Μήτρου Λίλιαν που μου εμπιστεύτηκε ένα τόσο ενδιαφέρον θέμα, για το πλούσιο ερευνητικό υλικό που μου υπέδειξε, τις τόσο στοχευμένες διαλέξεις καθ' όλη τη διάρκεια του προγράμματος αλλά και την υποστήριξη και κατανόηση της όταν αυτό το πόνημα φάνταζε ακόμα ακατόρθωτο.

Τέλος, ένα μεγάλο ευχαριστώ σε όλους τους διδάσκοντες/σες καθηγητές/τριες μας αλλά και προσκεκλημένους ομιλητές/τριες για τις ενδιαφέρουσες συζητήσεις, τα γνωστικά ερεθίσματα και το παράδειγμα τους.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Περιεχόμενα

ΠΕΡΙΛΗΨΗ

Η Ψηφιακή εγκληματολογία ακολουθώντας την εξέλιξη του Κυβερνοεγκλήματος αλλά και την ψηφιακή διάσταση κάθε εγκλήματος, καλείται να επαναδιαπραγματευτεί τις εγκληματολογικές θεωρίες και να αναζητήσει καινούριες επιστημονικές σκέψεις για την πρόληψη και την αντιμετώπιση του εγκλήματος στο ψηφιακό περιβάλλον, στο διαδίκτυο και γενικότερα σε συνάρτηση με τις νέες τεχνολογίες στην Κοινωνία της Πληροφορίας. Το παρόν πόνημα εκκινεί με όσο το δυνατόν πληρέστερη προσέγγιση της επιστήμης της ψηφιακής εγκληματολογίας, των αρχών, των χαρακτηριστικών, της οριοθέτησης της, του αντικειμένου διερεύνησης της που είναι τα ψηφιακά δεδομένα/πειστήρια, των διαδικασιών που την διέπουν, του νομικού της πλαισίου αλλά και του ρόλου που διαδραματίζουν τα μεταδεδομένα σε αυτή.

Στην συνέχεια επιχειρείται μια ερμηνευτική προσέγγιση του Διαδικτύου των Πραγμάτων (ΔτΠ) μέσω σύντομης ιστορικής αναδρομής και παραδειγμάτων, των ιδιαίτερων χαρακτηριστικών αυτού του οικοσυστήματος αλλά και των νέων προκλήσεων και νέων ευκαιριών που φέρνει για την ψηφιακή εγκληματολογία.

Ακολουθεί, η απαραίτητη -κατά την γράφουσα-ανάλυση του φαινομένου της νεφοϋπολογιστικής λόγω της εξάρτησης του με το ΔτΠ, οι προκλήσεις στον τομέα της ψηφιακής εγκληματολογίας στο νέφος και οι νομοθετικές προσπάθειες διασυνοριακής πρόσβασης στα ψηφιακά αποδεικτικά στοιχεία που είναι αποθηκευμένα σε αυτό, σε ευρωπαϊκό και διεθνές επίπεδο (πρόταση Κανονισμού e-Evidence & Cloud Act).

Στα επόμενα κεφάλαια επιχειρείται χαρτογράφηση του έξυπνου σπιτιού, των έξυπνων συσκευών (συμπεριλαμβανομένων και των φερόμενων συσκευών), των έξυπνων κινητών μέσα από παραδείγματα, εφαρμογές, ιδιαίτερα χαρακτηριστικά και τις προκλήσεις της ψηφιακής έρευνας σε καθένα από αυτά αλλά και τα 'ανοιχτά ζητήματα' που παραμένουν στα περιβάλλοντα αυτά.

Τέλος, αναδεικνύονται νέα εγκληματολογικά μοντέλα αξιοποίησης ψηφιακών αποδείξεων μέσα από 'ανοιχτές πηγές' και 'κοινωνικά δίκτυα' και με ποιο τρόπο μπορούν αυτά να είναι παραδεκτά ενώπιον του δικαστηρίου ενώ ταυτόχρονα

τονίζεται η ανάγκη αφομοίωσης της προστασίας της ιδιωτικής ζωής και των προσωπικών δεδομένων κατά την διεξαγωγή εγκληματολογικών ερευνών και ευαισθητοποίησης γύρω από ζητήματα ηθικής που ανανοηματοδοτούν τις ψηφιακές έρευνες.

Λέξεις-Κλειδιά: Ψηφιακή Εγκληματολογία, Έξυπνες συσκευές, Έξυπνο σπίτι, Έξυπνα κινητά, Εγκληματολογία έξυπνων κινητών, Διαδίκτυο των Πραγμάτων και Εγκληματολογική έρευνα, Νεφοϋπολογιστική και εγκληματολογική έρευνα

ABSTRACT

Digital criminology, following the evolution of cybercrime and the digital dimension of every crime, is called upon to renegotiate criminological theories and to seek new scientific ideas for the prevention and treatment of crime in the digital environment, on the Internet and in general in connection with new technologies in the Information Society. This paper starts with as complete an approach as possible to the science of digital forensics, its principles, characteristics, delimitation, the object of its investigation, which is digital data/resources, the processes governing it, its legal framework and the role played by metadata in it.

In the following, an interpretative approach to the Internet of Things (IoT) is attempted through a brief historical review and examples, the specific characteristics of this ecosystem and the new challenges and new opportunities it brings for digital forensics.

This is followed by the necessary - in the author's opinion - analysis of the cloud phenomenon due to its dependence on the IoT, the challenges in the field of digital forensics in the cloud and the legislative efforts of cross-border access to digital evidence stored in it, at European and international level (proposed e-Evidence & Cloud Act Regulation).

The following chapters attempt to map the smart home, smart devices (including wearable devices), smart mobiles through examples, applications, specific features and challenges of digital investigation in each of them and the 'open issues' that remain in these environments.

Finally, new forensic models for the exploitation of digital evidence through 'open sources' and 'social networks' are highlighted and how these can be admissible in court while stresses the need to assimilate privacy and personal data protection when conducting forensic investigations and to raise awareness of ethical issues that reinvigorate digital investigations.

Keywords: Digital Forensics, Smart devices, Smart Home, Smartphones, Smartphone Forensics, IoT and IoT forensics, Cloud Forensics.

ΕΙΣΑΓΩΓΗ

Η εκθετική αύξηση της χρήσης πληροφοριακών συστημάτων και εν γένει των σύγχρονων τεχνολογιών απ᾽ολους μας, στην σύγχρονη καθημερινότητα, δεν δύναται σε καμία περίπτωση να αφήσει ανεπηρέαστη την «εγκληματική εφευρετικότητα».[1] Νέες μορφές εγκληματικών συμπεριφορών αλλά και παραδοσιακά εγκλήματα τελούμενα πλέον με την χρήση νέων τεχνολογιών απασχολούν ολοένα και περισσότερο τις δικαστικές και ανακριτικές αρχές.

Η νομική επιστήμη φαίνεται να ακολουθεί ασθμαίνοντας, προσπαθώντας να προλάβει τις εξελίξεις, ενώ η ανάγκη για πρόληψη, διερεύνηση και καταστολή της νέας 'βελτιωμένης' και 'διεθνοποιημένης' εγκληματικότητας, έχει πλέον καταστήσει επιβεβλημένη την αξιοποίηση των ίδιων τεχνολογικών μέσων και από τις αρμόδιες διωκτικές αρχές.

Καθώς τα παραδοσιακά εγκληματολογικά εργαλεία θεωρούνται πλέον παρωχημένα, η ψηφιακή εγκληματολογία, ως κλάδος της επιστήμης των υπολογιστών και δη της ασφάλειας αυτών, αποτελεί πλέον από τους βασικότερους πυλώνες του οπλοστασίου των αρμόδιων αρχών, η πλήρης αξιοποίηση του ωστόσο απαιτεί συνεχή παρακολούθηση των τεχνολογικών εξελίξεων και ανάπτυξη αντίστοιχων 'αντανακλαστικών' και δεξιοτήτων.

Στο πρώτο κεφάλαιο της παρούσας διπλωματικής, αποσαφηνίζεται το αντικείμενο της ψηφιακής εγκληματολογίας, ο εντοπισμός δηλαδή και η εξέταση ψηφιακών δεδομένων/πειστηρίων για την εξακρίβωση αξιόποινων συμπεριφορών με τρόπο νομικά παραδεκτό και με προορισμό (τις περισσότερες φορές) την δικαστηριακή αξιοποίηση, δίνονται με συντομία οι φάσεις από τις οποίες διήλθε η επιστήμη αυτή για πληρέστερη κατανόηση και του κοινωνικού πλαισίου αλλά και των εκάστοτε διερευνητικών απαιτήσεων μέσα στο πέρασμα του χρόνου ενώ παράλληλα παρατίθενται οι κατηγοριοποιήσεις/εξειδικεύσεις της ψηφιακής εγκληματολογίας (με γνώμονα το υπό διερεύνηση κάθε φορά αντικείμενο).

Στο δεύτερο κεφάλαιο, αναλύονται οι βασικές αρχές που διέπουν την ψηφιακή εγκληματολογία, η τυποποίηση των διαδικασιών χειρισμού των ψηφιακών δεδομένων και οι αυστηρές απαιτήσεις που πρέπει να πληρούνται ώστε να θεωρούνται αξιοποιήσιμα.

Εν συνεχεία, στο επόμενο κεφάλαιο γίνεται ανάλυση του αντικειμένου της ψηφιακής εγκληματολογίας, ήτοι των ψηφιακών αποδεικτικών στοιχείων, των ιδιαίτερων χαρακτηριστικών τους, των κατηγοριών τους, των απαιτήσεων χειρισμού τους ανάλογα με την φύση και τις ιδιότητες τους και της βαρύνουσας σημασίας που έχει η αποτύπωση των ενεργειών του ερευνητή (αλυσίδα φύλαξης).

Έπειτα, στο τέταρτο κεφάλαιο, αναδεικνύεται η σημασία των μεταδεδομένων στην ψηφιακή έρευνα καθώς είναι αυτά που αποκαλύπτουν με τρόπο πιο διεισδυτικό πληροφορίες για τους υπόπτους αλλά και πιο αντικειμενικό και αδιάβλητο συγκριτικά με μεθόδους στις οποίες μεσολαβεί ο ανθρώπινος παράγοντας (π.χ. διενέργεια

[1] Ματάμη, Ε. (2022). Ψηφιακά πειστήρια και αποδεικτικές απαγορεύσεις στην ποινική δίκη σε εθνικό και υπερεθνικό επίπεδο.

πραγματογνωμοσύνης κτλ.) ενώ παράλληλα εξετάζεται η νομική θεώρηση τους σε εθνικό-υπερεθνικό και διεθνές επίπεδο.

Στο πέμπτο κεφάλαιο, επιχειρείται εισαγωγή στον κόσμο του Διαδικτύου των Πραγμάτων, του δικτύου επικοινωνίας δηλαδή πλήθους συσκευών, οικιακών συσκευών, καθώς και κάθε αντικειμένου που ενσωματώνει ηλεκτρονικά μέσα, αισθητήρες, λογισμικό, και συνδεσιμότητα σε δίκτυο που επιτρέπει την σύνδεση και ανταλλαγή δεδομένων καθώς και πως αξιοποιείται το οικοσύστημα αυτό στο πλαίσιο της ψηφιακής διερεύνησης με ό,τι περιορισμούς (τεχνικούς, νομικούς κτλ.) μπορεί να συνεπάγεται.

Αντιστοίχως στο αμέσως επόμενο κεφάλαιο, επιχειρείται η εννοιολογική προσέγγιση του cloud computing, του μοντέλου δηλαδή υπολογιστών που περιλαμβάνει διακομιστές, δίκτυα, αποθηκευτικούς χώρους, εφαρμογές και εργαλεία ανάπτυξης κατ' απαίτηση και αποκεντρωμένα, σε επιχειρήσεις και όχι μόνο, καθώς και πως αυτό το μοντέλο αξιοποιείται από κακόβολους χρήστες για την διάπραξη εγκληματικών ενεργειών αλλά και το πλήθος προκλήσεων που θέτει το εικονικό αυτό περιβάλλον στην διεξαγωγή εγκληματολογικών ερευνών.

Σε παρόμοια λογική, στα επόμενα κεφάλαια δίνονται οι ορισμοί και παραδείγματα του έξυπνου σπιτιού, έξυπνων συσκευών και φερόμενων συσκευών, του αποδεικτικού πλούτου που αυτά μπορεί να περιέχουν, την συνδρομή τους στα πλαίσια των ψηφιακών ερευνών, των εμποδίων που καλούνται να υπερπηδήσουν ενώ σε διακριτό κεφάλαιο επιχειρείται ανάλυση της εγκληματολογίας σε έξυπνα τηλέφωνα, των ερευνητικών μοντέλων για την μέγιστη δυνατή αξιοποίηση των δεδομένων που αυτά παράγουν με γνώμονα όμως και σεβόμενα την διαφύλαξη των προσωπικών δεδομένων και ελευθεριών των εμπλεκομένων.

Κλείνοντας, στα κεφάλαια εννέα και δέκα αντίστοιχα, υπογραμμίζεται η δημιουργία και η σημασία ενός νέου εγκληματολογικού μοντέλου μέσα από την αξιοποίηση αποδεικτικών πηγών από τα μέσα κοινωνικής δικτύωσης καθώς και η ανάγκη διατήρησης και ευαισθητοποίησης σε ζητήματα ιδιωτικότητας όλων των παραγόντων που εμπλέκονται και παρεμβαίνουν στην ιδιωτική σφαίρα των ατόμων, με τέτοιο τρόπο όπως κατά την διεξαγωγή εγκληματολογικών ερευνών.

1. ΨΗΦΙΑΚΗ ΕΓΚΛΗΜΑΤΟΛΟΓΙΑ

-Τι πραγματεύεται η ψηφιακή εγκληματολογία/ψηφιακή δικανική

Αν αναλογιστεί κανείς ότι διανύουμε από τις εντονότερες φάσεις ανάπτυξης τεχνολογιών πληροφορικής και επικοινωνιών, τις οποίες συναντούμε σε κάθε πτυχή της καθημερινότητας, εύκολα θα αντιληφθεί ότι η «παραδοσιακή» εγκληματολογική έρευνα με τις τεχνικές και τις μεθόδους της δεν είναι πλέον επαρκής.

Η εγκληματολογία (forensics/forensic science)[2] ή Δικανική[3] ασχολείται με την ανακάλυψη, ανάλυση και νομική τεκμηρίωση των αποδείξεων, που συνδέουν μια αξιόποινη πράξη με ένα πρόσωπο ή σύνολο προσώπων με αποδεικτικά στοιχεία.

Με την μεταφορά ωστόσο του κύριου όγκου της σοβαρής εγκληματικότητας στο Διαδίκτυο[4] και την ψηφιοποίηση των αξιόποινων συμπεριφορών, η μετεξέλιξη από το μοντέλο της συμβατικής εγκληματολογικής έρευνας σε αυτό της **ψηφιακής**, κρίνεται παραπάνω από αναγκαία.

Έτσι, η ψηφιακή εγκληματολογία (Digital Forensics) είναι η επιστήμη που ασχολείται με την ανάκτηση, την συλλογή, διατήρηση, ανάλυση και παρουσίαση ψηφιακών αποδείξεων κατά τρόπο νομικά αποδεκτό.

Είναι καλό να διευκρινιστεί εξαρχής ότι αν και συνδέεται στενά με το ηλεκτρονικό έγκλημα (computer crime)[5] ή/και το **Κυβερνοέγκλημα** (cyber crime)[6], (όπως hacking, cracking, malware infection κτλ.) δεν περιορίζεται αποκλειστικά σε αυτά, καθώς αφορά ψηφιακά δεδομένα- ίχνη οπουδήποτε δύνανται αυτά να

---

[2] Ο όρος «forensics» προέρχεται ετυμολογικά από τον λατινικό όρο «forum» δηλαδή αγορά/δημόσιος χώρος συνάθροισης υπό την έννοια ότι τα ευρήματα της προορίζονται να παρουσιαστούν ενώπιον κοινού/δικαστηρίου.

[3] Ο όρος δικανική επιστήμη αναφέρεται στην εφαρμογή επιστημονικών μεθόδων για την αρωγή νομικών διαδικασιών.

[4] Δαγκλής Ν., Δαλακούρας Θ., Δανιήλ Γ., Κιούπης Δ., Ναζίρης Γ., Νούσκαλης Γ.,Παπαθανασίου Α., Νάιντος Χ., Γκύζης Δ., Καργόπουλος Α.-Ι., Κάτος Β., Κουδελή Μ., Μοροζίνης Ι.,Σαββίδης (2023) Ηλεκτρονικό Έγκλημα (Ουσιαστικές και δικονομικές όψεις) ΝΒ σελ 351

[5] Εγκλήματα που τελούνται με την χρήση Ηλεκτρονικού Υπολογιστή (Η/Υ)

[6] Εγκλήματα που τελούνται μέσω του Διαδικτύου

ανευρεθούν (πχ σε ψηφιακές συσκευές ή άλλα ψηφιακά μέσα αποθήκευσης) και κατά την τέλεση και εξακρίβωση κοινών εγκλημάτων.

1.1. Σύντομο ιστορικό της ψηφιακής εγκληματολογίας

Για να κατανοήσουμε καλύτερα την διαδρομή που έχει διανύσει μέχρι και σήμερα η επιστήμη της ψηφιακής εγκληματολογίας με ό,τι αυτό μπορεί να συνεπάγεται από άποψη - τεχνικών και μη - προκλήσεων, αρκεί να ανατρέξουμε στις επιμέρους χρονικές φάσεις από τις οποίες έχει διέλθει:

Έτσι κατά την διάρκεια του πρώτου σταδίου, την δεκαετία **70'-90'** οι επαγγελματίες της ψηφιακής εγκληματολογίας συνεργάζονταν με τις διωκτικές και ανακριτικές αρχές **μόνο** κατά περίπτωση (ad hoc) καθώς η ανάγκη διενέργειας τέτοιου είδους εγκληματολογικής έρευνας ήταν μάλλον περιορισμένη, αφού η χωρητικότητα των δίσκων των υπολογιστών εκείνης της εποχής ήταν μικρή, με αποτέλεσμα οι χρήστες να αποθηκεύουν λιγότερο και να εκτυπώνουν περισσότερο.

Το δεύτερο στάδιο, **1999-2007,** χαρακτηρίζεται και ως η «χρυσή εποχή» της ψηφιακής εγκληματολογικής έρευνας διότι πολλοί προμηθευτές άρχισαν να αναπτύσσουν ειδικά εγκληματολογικά εργαλεία που απαιτούσαν σχετικά περιορισμένη εκπαίδευση και επέτρεπαν την ανάκτηση διαγραμμένων αρχείων, βασική ανάλυση αρχείων και ανάλυση μηνυμάτων ηλεκτρονικού ταχυδρομείου.[7] Πρόκειται επίσης για την περίοδο που γεννήθηκαν νέοι κλάδοι, όπως η εγκληματολογία δικτύου (network forensics) και η εγκληματολογία μνήμης (memory forensics) -όπως θα αναλυθεί και παρακάτω μεταξύ άλλων- για να απαντήσει σε προκλήσεις όπως: απόκτηση δεδομένων που επιτρέπουν την κατανόηση των συμβάντων του δικτύου και απόκτηση δεδομένων μνήμης που θα μας επέτρεπαν να παρακάμψουμε τους ελέγχους ασφαλείας των υπολογιστών. Η ραγδαία ανάπτυξη της σε αυτή την χρονική φάση επέφερε και την επαγγελματοποίηση της με αποτέλεσμα την αποδοχή στην χρήση συγκεκριμένων εργαλείων και διαδικασιών για την διεξαγωγή ψηφιακών ερευνών από την κοινότητα των εμπειρογνωμόνων.

Το τρίτο στάδιο, που χρονολογείται μεταξύ **2007-2010** θέτει και τις βάσεις για την ακόμα μεγαλύτερη εξειδίκευση της ψηφιακής έρευνας, όπως την γνωρίζουμε σήμερα, ανάλογα με το είδος και τον τύπο του μέσου που κάθε φορά εξετάζεται.

1.2. Κατηγορίες της ψηφιακής εγκληματολογίας

Όπως συμβαίνει με την εγκληματολογική επιστήμη γενικότερα, έτσι και η ψηφιακή εγκληματολογία χωρίζεται σε διάφορους επιμέρους κλάδους, ανάλογα με τις ψηφιακές συσκευές που εμπλέκονται: **εγκληματολογία υπολογιστών**

[7] Nieto, A., Rios, R., Lopez, J., Ren, W., Wang, L., Choo, K. K. R., & Xhafa, F. (2019). Privacy-aware digital forensics.

(computer forensics), **εγκληματολογία μνήμης** (memory forensics), **εγκληματολογία κινητών συσκευών** (mobile device forensics), **εγκληματολογία βάσεων δεδομένων** (database forensics), **εγκληματολογική ανάλυση δεδομένων** (forensic data analysis) και φυσικά η **εγκληματολογία δικτύων** αυτή καθαυτή (network forensics).[8]

1.3. Εγκληματολογία Υπολογιστών

Το είδος αυτό μπορεί να το συναντήσουμε και ως εγκληματολογία με βάση τον κεντρικό υπολογιστή (host-based forensics), θεωρείται από τους πρώτους τομείς της ψηφιακής εγκληματολογίας και ασχολείται με την απόκτηση και ανάλυση δεδομένων που βρίσκονται σε μεμονωμένους υπολογιστές, συνήθως ηλεκτρονικούς υπολογιστές, φορητούς υπολογιστές, διακομιστές, σταθμούς εργασίας κτλ.[9]. Τα δεδομένα βρίσκονται κατά κύριο λόγο στον σκληρό δίσκο σε μη πτητική κατάσταση και στην μνήμη. Περαιτέρω, αποδεικτικά στοιχεία ανευρίσκονται και σε μέρη όπως στην αποθήκευση υλικολογισμικού (λ.χ. κεντρική πλακέτα ή κάρτες γραφικών) ή ακόμα και με την μορφή μέσων αποθήκευσης που παραμένουν σε μια υποδοχή μονάδας δίσκου (DVD ή/και κάρτες SD πχ). Ακόμα και η κατάσταση του υλικού του υπολογιστή και των εξαρτημάτων του, μπορεί να αποτελέσει αποδεικτικό στοιχείο όπως για παράδειγμα ένα keylogger που έχει συνδεθεί μεταξύ του πληκτρολογίου και των βυσμάτων USB της κεντρικής πλακέτας (ή των κεντρικών πλακετών).

1.4. Εγκληματολογία της Μνήμης

Η εγκληματολογία μνήμης ασχολείται με την εγκληματολογική ανάλυση του περιεχομένου της μνήμης ενός υπολογιστή[10]. Είναι η μόνη μέθοδος έρευνας που παραμένει αξιοποιήσιμη, όταν οι 'ύποπτοι' δεν εγγράφουν δεδομένα στη μη πτητική μνήμη του συστήματος κατά τη διάρκεια μιας επίθεσης. Επιπλέον, η μέθοδος αυτή επιτρέπει την ανάλυση πιο πτητικών στοιχείων, δηλαδή

[8] ENISA, Introduction to Network Forensics Handbook, final version 1.0, Jan 2019 p.10
[9] ENISA, Introduction to Network Forensics Handbook, final version 1.0, Jan 2019 p.12
[10] ENISA, Introduction to Network Forensics Handbook, final version 1.0, Jan 2019 p.12

περιεχομένου μνήμης RAM[11] που θα χανόταν μετά από επανεκκίνηση ή απενεργοποίηση του συστήματος, όπως η κατάσταση του πυρήνα του λειτουργικού συστήματος ή των διεργασιών στο σύστημα. Ως εκ τούτου, η εγκληματολογία μνήμης συμπληρώνει την εγκληματολογία με βάση τον υπολογιστή καθώς και την εγκληματολογία δικτύου, όταν επιτρέπει την ανάκτηση των κλειδιών κρυπτογράφησης του σκληρού δίσκου ή των κλειδιών των συνδέσεων δικτύου. Μπορεί επιπλέον να βοηθήσει στην ανακάλυψη εάν οι δικτυακές διεπαφές έχουν τεθεί σε κατάσταση αδέσμευτης λειτουργίας για την καταγραφή της δικτυακής κίνησης (traffic data), ή μπορεί να βρει ίχνη συνδέσεων δικτύου που χρησιμοποιήθηκαν προηγουμένως σε τμήματα της μνήμης που έχουν απελευθερωθεί αλλά δεν έχουν ακόμη αντικατασταθεί.

1.5. Εγκληματολογία Κινητών Τηλεφώνων

Η εγκληματολογία κινητών συσκευών είναι ένας κλάδος της ψηφιακής εγκληματολογίας που σχετίζεται με την ανάκτηση ψηφιακών αποδεικτικών στοιχείων ή δεδομένων από μια κινητή συσκευή υπό εγκληματολογικά ορθές συνθήκες. Ο όρος "κινητή συσκευή" σημαίνει συνήθως κινητά τηλέφωνα, αλλά μπορεί επίσης να αφορά ταμπλέτες, φορητούς υπολογιστές, φορητές συσκευές και άλλες συσκευές που μπορούν να μεταφερθούν - οι οποίες διαθέτουν μνήμη και ασύρματη σύνδεση δικτύου(-ων).[12]

Ενδεικτικά, κάποιες από τις προκλήσεις που καλείται να λύσει το εν λόγω είδος είναι:

- *Η δυσκολία διαχωρισμού συσκευής από το δίκτυο.*

Οι περισσότερες κινητές συσκευές διαθέτουν όχι μόνο Wi-Fi αλλά και GSM [13](για ασύρματη σύνδεση), Near Field Communication (NFC), συνδεσιμότητα με

[11] Η μνήμη τυχαίας προσπέλασης (*RAM, Random Access Memory*) είναι όρος που χρησιμοποιούμε για ηλεκτρονικές διατάξεις προσωρινής αποθήκευσης ψηφιακών δεδομένων (μνήμης υπολογιστή), οι οποίες επιτρέπουν πρόσβαση στα αποθηκευμένα δεδομένα στον ίδιο χρόνο οπουδήποτε και αν βρίσκονται αυτά, δηλαδή με «τυχαία πρόσβαση».
https://el.wikipedia.org/wiki/%CE%9C%CE%BD%CE%AE%CE%BC%CE%B7_%CF%84%CF%85%CF%87%CE%B1%CE%AF%CE%B1%CF%82_%CF%80%CF%81%CE%BF%CF%83%CF%80%CE%AD%CE%BB%CE%B1%CF%83%CE%B7%CF%82

[12] ENISA, Introduction to Network Forensics Handbook, final version 1.0, Jan 2019 p.12

[13] Global System for Mobile Communication

υπέρυθρες. Επιπλέον, οι κινητές συσκευές έχουν την δυνατότητα να επανασυνδέονται δυναμικά μέσω ενός διαφορετικού δικτύου όταν η κύρια σύνδεση δικτύου αποτυγχάνει.

- *Η απενεργοποίηση μιας πηγής ενέργειας στις κινητές συσκευές μπορεί να είναι δυσχερής.*

Για παράδειγμα, οι μπαταρίες μπορεί να μην αφαιρούνται ή η συσκευή μπορεί να διαθέτει ηλιακό πάνελ, γεγονός που έρχεται σε αντίθεση με τις συνήθεις εγκληματολογικές διαδικασίες.

- *Η πλήρης κρυπτογράφηση της συσκευής καθιστά την απόκτηση δεδομένων δύσκολη, αν όχι αδύνατη.*
- *Μπορεί να μην υπάρχει τυπικό υλικό διασύνδεσης, όπως πχ πληκτρολόγιο ή οθόνη.*
- *Οι μορφές δεδομένων των εφαρμογών μπορεί να είναι άγνωστες (ιδιόκτητες) αλλά και να αλλάζουν συνεχώς.*

Για τους παραπάνω λόγους υπάρχει μεγάλη ποικιλία εργαλείων για την εξαγωγή αποδεικτικών στοιχείων από κινητές συσκευές, δεδομένου ότι κανένα εργαλείο ή μέθοδος δεν μπορεί να αποκτήσει όλα τα αποδεικτικά στοιχεία απ' όλους τους τύπους συσκευών.

1.6. Εγκληματολογία Δικτύων[14]

Η εγκληματολογία δικτύου ασχολείται με την παρακολούθηση και ανάλυση της κίνησης του δικτύου υπολογιστών, τόσο σε τοπικό όσο και σε διαδικτυακό/WAN[15] επίπεδο με σκοπό την συλλογή πληροφοριών, την συλλογή πειστηρίων ή και την ανίχνευση εισβολών.

Παρατηρούμε, ότι η εγκληματολογία υπολογιστών με την αντίστοιχη των δικτύων αλληλοσυμπληρώνονται. Οι «ύποπτοι» μπορεί να κρύβονται τόσο καλά

[14] ENISA, Introduction to Network Forensics Handbook, final version 1.0, Jan 2019 p.12

[15] WAN, συντ. του όρου Wide *Area Network.* Είναι ένα σύνολο υπολογιστών που εκτείνονται σε μια ευρεία γεωγραφική περιοχή ή εναλλακτικά πολλά LAN's (Local Area Networks) μαζί που δημιουργούν ένα δίκτυο επικοινωνίας μεταξύ τους. https://el.wikipedia.org/wiki/%CE%94%CE%AF%CE%BA%CF%84%CF%85%CE%BF_%CE%B5%CF%85%CF%81%CE%B5%CE%AF%CE%B1%CF%82_%CF%80%CE%B5%CF%81%CE%B9%CE%BF%CF%87%CE%AE%CF%82

ώστε να είναι σχεδόν αόρατοι στις περισσότερες έρευνες. Ωστόσο αν χρειαστεί να επικοινωνήσουν, τα πακέτα αυτά (δεδομένων), θα φανούν στο διαδίκτυο. Παρόλα αυτά, η εγκληματολογία δικτύου δεν μας απαντά στο τι συνέβη με τα δεδομένα αυτά (ποιες διεργασίες έστειλαν/έλαβαν τα δεδομένα αυτά, τι έκαναν με αυτά κτλ.).

2. ΑΡΧΕΣ ΠΟΥ ΔΙΕΠΟΥΝ ΤΗΝ ΨΗΦΙΑΚΗ ΕΓΚΛΗΜΑΤΟΛΟΓΙΑ

Αν και δεν υφίσταται μια ενιαία μεθοδολογία για την διεξαγωγή ψηφιακών ερευνών με αυστηρώς ομοιόμορφη εφαρμογή σε όλες τις περιπτώσεις, η κρατούσα φαίνεται να συμπυκνώνεται και να οριοθετείται κατά τον Davidoff [16], στις αρχές **OSCAR.**

Το ακρωνύμιο OSCAR σημαίνει:

- **O**btain information: Δηλαδή απόκτηση πληροφοριών, όπως ημερομηνία και ώρα που ανακαλύφθηκε το περιστατικό, τα εμπλεκόμενα πρόσωπα και συστήματα, τι συνέβη αρχικά, ποιες ενέργειες έγιναν ακολούθως, ποιος είναι ο υπεύθυνος κτλ. Οι στόχοι της διερεύνησης θα πρέπει να καθοριστούν, να καταγραφούν και να ιεραρχηθούν, καθώς πάντα θα υπάρχουν περιορισμοί πόρων για την διερεύνηση.
- **S**trategize: Αυτό αφορά την στρατηγική και τον προγραμματισμό της έρευνας. Η απόκτηση θα πρέπει να ιεραρχηθεί ανάλογα με την αστάθεια των πηγών, την πιθανή αξία τους για την έρευνα και την προσπάθεια που απαιτείται για την απόκτηση τους. Αυτός ο κατάλογος προτεραιοτήτων θα πρέπει να αποτελεί σημείο εκκίνησης για την κατανομή των πόρων και του προσωπικού για την διεξαγωγή των σχετικών εργασιών (απόκτηση πληροφοριών και αποδεικτικών στοιχείων).
- **C**ollect evidence: Με βάση το παραπάνω σχέδιο, συλλέγονται αποδεικτικά στοιχεία από κάθε αναγνωρισμένη πηγή. Πρέπει να ληφθούν υπόψη ωστόσο τρία σημεία:

[16] Davidoff, S., & Ham, J. (2012). Network forensics: tracking hackers through cyberspace (Vol. 2014). Upper Saddle River: Prentice hall.

1. *Τεκμηρίωση*: Το αρχείο καταγραφής **(audit trail)** πρέπει να καταγράφεται και να φυλάσσεται με ασφάλεια σύμφωνα με τις ίδιες κατευθυντήριες γραμμές όπως και τα ίδια τα αποδεικτικά στοιχεία (όπως θα αναλυθεί παρακάτω).
2. *Καταγραφή των ίδιων των αποδεικτικών στοιχείων*: Αυτό αφορά το μέρος όπου καταγράφονται τα πακέτα (δεδομένων), αντιγράφονται τα αρχεία καταγραφής, αποτυπώνονται οι σκληροί δίσκοι των συστημάτων κτλ.
3. *Αποθήκευση/Μεταφορά*: Πρόκειται για την διατήρηση της αλυσίδας φύλαξης/επιμέλειας, δηλαδή την παρουσίαση της κατάσχεσης, της φύλαξης, του ελέγχου, της μεταφοράς, της ανάλυσης, και της διάθεσης των αποδεικτικών στοιχείων (εδώ ψηφιακών/ηλεκτρονικών).

- **A**nalyze: Κατά την διάρκεια της ανάλυσης, ο ερευνητής ανακτά αποδεικτικό υλικό χρησιμοποιώντας διάφορες μεθοδολογίες και εργαλεία. Ο ερευνητής εγκληματολογίας Brian Carrier περιέγραψε μια «διαισθητική διαδικασία» κατά την οποία εντοπίζονται πρώτα τα προφανή αποδεικτικά στοιχεία και εν συνεχεία «διεξάγονται εξαντλητικές έρευνες για την συμπλήρωση των κενών» Carrier 2006[17].
  Να σημειωθεί βέβαια ότι η μέθοδος που θα επιλεγεί για την ανάλυση εξαρτάται από την υπόθεση και τα συλλεχθέντα στοιχεία. Είναι πιθανό να χρειαστούν αρκετές επαναλήψεις εξέτασης και ανάλυσης για να υποστηριχθεί μια θεωρία.
- **R**eport: Πρόκειται για την μετάδοση των αποτελεσμάτων των ερευνών στο κοινό για το οποίο προορίζεται (πελάτης, δικαστήριο κτλ.) και πρέπει να είναι κατανοητό από μη τεχνικά άτομα, και τεκμηριωμένο.

Ομοίως, οι Jones et al[18] εντοπίζουν τους πέντε βασικούς πυλώνες που αποτελούν βάση για την διαχείριση των ηλεκτρονικών αποδεικτικών στοιχείων.

[17] ENISA, Introduction to Network Forensics Handbook, final version 1.0, Jan 2019 p.13
[18] Watson, D. L., & Jones, A. (2013). Digital forensics processing and procedures: Meeting the requirements of ISO 17020, ISO 17025, ISO 27001 and best practice requirements. Newnes.

- *Ακεραιότητα δεδομένων*: Κανένα μέτρο που λαμβάνεται δεν πρέπει να αλλάζει τις ηλεκτρονικές συσκευές ή τα μέσα, τα οποία μπορεί στη συνέχεια να χρησιμοποιηθούν στο δικαστήριο.
- *'Διαδρομή 'ελέγχου*: Θα πρέπει να δημιουργείται και να διατηρείται μια διαδρομή ελέγχου ή άλλο αρχείο όλων των ενεργειών που πραγματοποιούνται κατά το χειρισμό ηλεκτρονικών αποδεικτικών στοιχείων, υπό την έννοια ότι ένα ανεξάρτητο τρίτο μέρος θα πρέπει να μπορεί να εξετάσει τις εν λόγω ενέργειες και να επιτύχει το ίδιο αποτέλεσμα.
- *Υποστήριξη από 'ειδικούς'*: Εάν υποτεθεί ότι στα πλαίσια διεξαγωγής μιας έρευνας, ενδέχεται να ανευρεθούν ψηφιακά/ηλεκτρονικά αποδεικτικά στοιχεία, τότε ο επικεφαλής της έρευνας θα πρέπει έγκαιρα να ενημερώσει εξειδικευμένους συμβούλους.
- *Κατάλληλη κατάρτιση*: Οι πρώτοι ανταποκριτές (first incident responders)[19] θα πρέπει να είναι κατάλληλα εκπαιδευμένοι ώστε να αναζητήσουν και να κατασχέσουν τα ψηφιακά αποδεικτικά στοιχεία σε περίπτωση που δεν υπάρχουν διαθέσιμοι εμπειρογνώμονες στον τόπο του συμβάντος.
- *Νομιμότητα*: Το πρόσωπο και η υπηρεσία που είναι επιφορτισμένα με την υπόθεση είναι υπεύθυνα για την τήρηση του νόμου, των εγκληματολογικών και δικονομικών αρχών και των προαναφερόμενων αρχών. Αυτό ισχύει τόσο για την **πρόσβαση** όσο και για την **κατοχή** των ψηφιακών αποδεικτικών στοιχείων.

Οι αρχές αυτές υιοθετήθηκαν στο πλαίσιο του έργου της Ευρωπαϊκής Ένωσης και του Συμβουλίου της Ευρώπης για την ανάπτυξη ενός οδηγού «κατάσχεσης ηλεκτρονικών αποδεικτικών στοιχείων». Και αυτό διότι, όπως θα δούμε αναλυτικά παρακάτω, ενώ οι νόμοι σχετικά με το παραδεκτό των αποδεικτικών στοιχείων διαφέρουν από χώρα σε χώρα, η χρήση αυτών των αρχών είναι εξαιρετικά σημαντική καθώς είναι κοινές διεθνώς.

3. ΤΑ ΨΗΦΙΑΚΑ ΔΕΔΟΜΕΝΑ/ΑΠΟΔΕΙΚΤΙΚΑ ΣΤΟΙΧΕΙΑ

3.1. Ορισμός

Κατά τον ισχύοντα Ποινικό Κώδικα (Π.Κ)[20] και στα πλαίσια συμμόρφωσης της χώρας μας ουσιαστικά με τις επιταγές της *Σύμβασης για το έγκλημα στον Κυβερνοχώρο* (άλλως *Σύμβαση της Βουδαπέστης*, 2001) και τεχνικά μέσα από τις διατάξεις του εφαρμοστικού της Ν

[19] Το άτομο που θα επιληφθεί να κάνει την πρώτη εκτίμηση περιστατικού ή/και θα βρεθεί πρώτο στην σκηνή του εγκλήματος/συμβάντος.
[20] **Ν 4619/2019** (ΦΕΚ Α 95/11.06.2019)

4411/2016[21], ορίζει στο άρθρο **13** περ. **θ'** ότι «***Ψηφιακά δεδομένα είναι η παρουσίαση γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη προς επεξεργασία από πληροφοριακό σύστημα, συμπεριλαμβανομένου προγράμματος που παρέχει τη δυνατότητα στο πληροφοριακό σύστημα να εκτελέσει μια λειτουργία***».

Από τον παραπάνω ορισμό διαμορφώνεται μια εικόνα για τα αποδιδόμενα χαρακτηριστικά τόσο από άποψη νομική όσο και τεχνολογική, τα οποία με την σειρά τους είναι στοιχεία που θα καθορίσουν τον τρόπο με τον οποίο γίνεται η επιστημονική και τεχνική προσέγγιση τους, στο περιβάλλον της ανακριτικής έρευνας με σκοπό την άντληση και την αξιοποίηση τους στην ποινική δίκη.[22]

3.2. Κατηγορίες ψηφιακών δεδομένων

Τα ψηφιακά αυτά δεδομένα ή ψηφιακά πειστήρια ανάλογα με το είδος τους μπορούν να αξιολογηθούν και να κατηγοριοποιηθούν σε:

- **(ηλεκτρονικά) ακατέργαστα δεδομένα (raw data)**: πρόκειται για πρωτότυπες ηλεκτρονικές μορφές που μπορούν να αποθηκευτούν σε μέσο που μπορεί να φιλοξενήσει και να αποθηκεύσει ηλεκτρονικά δεδομένα, χωρίς όμως από αυτά να μπορεί να εξαχθεί αξιοποιήσιμο ψηφιακό δεδομένο.
- **δεδομένα υπολογιστή (computer evidence)**: δεδομένα τα οποία αντλούνται από τον ηλεκτρονικό υπολογιστή και αφορούν λειτουργίες και λογισμικό που εκτελούνται σε αυτόν (λχ αν υποστηρίζει λογισμικό για αρχεία κειμένου ή εικόνας/ήχου).
- **δεδομένα Διαδικτύου (internet data):** είναι τα δεδομένα που αφορούν την περιήγηση στο διαδίκτυο και την χρήση των σχετικών προσφερόμενων εφαρμογών. Τα διαδικτυακά δεδομένα, ως αποδεικτικά στοιχεία μπορούν να χωριστούν σε αυτά που **είναι διαθέσιμα στο κοινό** *(π.χ. δημοσιεύσεις φόρουμ, όπου το φόρουμ δεν απαιτεί σύνδεση για προβολή)* και σε εκείνα που είναι **ιδιωτικά** (*π.χ. πληροφορίες λογαριασμού Facebook)*. Μπορεί να υπάρχουν περιθώρια για την **απόκτηση και των δύο** (*π.χ. καταγράφοντας το κείμενο μιας ανάρτησης φόρουμ και κατόπιν ζητώντας τα στοιχεία λογαριασμού του χρήστη που έκανε την ανάρτηση από τον κάτοχο του φόρουμ).*[23]

---

[21] **Ν 4411/2016** (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*».

[22] Παπαδόπουλος, Θ. (2020). Η Ανακριτική Διερεύνηση Ηλεκτρονικών Εγκλημάτων. Όρια και έκταση εφαρμογής της εγχώριας και διεθνούς πρακτικής υπό το φως των εγγυήσεων προστασίας των ατομικών δικαιωμάτων και της νομολογίας του ΕΔΔΑ.

[23] Παπαδόπουλος, Θ. (2020). Η Ανακριτική Διερεύνηση Ηλεκτρονικών Εγκλημάτων. Όρια και έκταση εφαρμογής της εγχώριας και διεθνούς πρακτικής υπό το φως των εγγυήσεων προστασίας των ατομικών δικαιωμάτων και της νομολογίας του ΕΔΔΑ.

- **μεταδεδομένα (metadata):** πρόκειται για πληροφορίες που ενσωματώνει το εκάστοτε πρόγραμμα στα αρχεία που αυτό παράγει. Είναι κυρίως πληροφορίες που περιγράφουν χωροχρονικά την εκάστοτε πληροφορία όπως πχ πληροφορίες σχετικά με την δημιουργία, τη προσπέλαση, τη τροποποίηση, την διαγραφή, την ανάκτηση, την εκτύπωση, την μεταφορά, την μετακίνηση σε άλλη θέση καθώς και το μέγεθος ενός αρχείου. Η προστιθέμενη αξία αυτού του είδους πληροφορίας έγκειται στο ότι συνδράμει στην εξαγωγή πορισμάτων όπως μοτίβο διαχείρισης ενός αρχείου *(δηλαδή συχνότητα επισκεψιμότητας του αλλά και προσπάθεια αλλοίωσης του/εξαφάνισης ιχνών).*
- **δεδομένα κίνησης (traffic data):** αναφέρονται στα δεδομένα, που υποβάλλονται σε επεξεργασία για τους σκοπούς της διαβίβασης μίας επικοινωνίας σε δίκτυο ηλεκτρονικών επικοινωνιών ή της χρέωσής της. Στα δεδομένα κίνησης μπορεί να περιλαμβάνονται, μεταξύ άλλων, **ο αριθμός**, **η διεύθυνση**, η **ταυτότητα της σύνδεσης** ή **του τερματικού εξοπλισμού** του συνδρομητή ή/και χρήστη, οι **κωδικοί πρόσβασης**, τα **δεδομένα θέσης**, η **ημερομηνία και ώρα έναρξης/λήξης** και η **διάρκεια της επικοινωνίας**, ο **όγκος των διαβιβασθέντων δεδομένων**, πληροφορίες σχετικά με το **πρωτόκολλο**, τη **μορφοποίηση**, τη **δρομολόγηση της επικοινωνίας** καθώς και **το δίκτυο** από το οποίο προέρχεται ή στο οποίο καταλήγει η επικοινωνία αυτή.
- **δεδομένα θέσης (location data):** δηλαδή δεδομένα, που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών και που υποδεικνύουν τη **γεωγραφική θέση** του τερματικού εξοπλισμού του χρήστη μίας διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών.
- **δεδομένα συνδρομητή (subscriber data):** είναι στοιχεία σχετικά με την ταυτότητα του κατόχου ή του χρήστη της υπηρεσίας τηλεπικοινωνιών και αφορούν το όνομα, επώνυμο, διεύθυνση του προσώπου, αλλά και σε άλλα στοιχεία ταυτοποίησης του.
- **δεδομένα περιεχομένου συνομιλιών (content data):** τα οποία αναφέρονται στο περιεχόμενο της επικοινωνίας, είτε πρόκειται για **γραπτό** (ηλεκτρονικό ταχυδρομείο, μηνύματα), είτε **προφορικό**.[24]

3.3. Φύση ψηφιακών δεδομένων/πειστηρίων

Τα ψηφιακά πειστήρια είναι τα δεδομένα εκείνα λοιπόν, τα ευρήματα ψηφιακής μορφής που εντοπίζονται, εξάγονται και ερμηνεύονται, όπως θα αναλυθεί εκτενώς παρακάτω, κατά την ψηφιακή εγκληματολογική έρευνα και σύμφωνα με επιστημονικά αποδεκτές μεθόδους, προκειμένου να είναι αξιοποιήσιμα σε δικονομική διαδικασία.[25] Αν και τα ψηφιακά πειστήρια ήταν κατεξοχήν

[24] Βλ. Ν 2225/1994, ΦΕΚ Α 121/20.07.1994, ΠΔ 47/2005, ΦΕΚ Α 64/10.03.2005

[25] Κάτος Β. (2023) Ψηφιακά Πειστήρια, Ηλεκτρονικό Έγκλημα (Ουσιαστικές και δικονομικές όψεις),ΝΒ σελ. 400

συνυφασμένα με το ηλεκτρονικό έγκλημα, πλέον η παρουσία τους είναι καθολική-ακόμα και στα πιο «παραδοσιακά» εγκλήματα *(πχ εντοπισμός υπόπτου από το στίγμα του κινητού του τηλεφώνου ή την δραστηριότητα του στο διαδίκτυο).*

Εύλογα συμπεραίνουμε λοιπόν, ότι ο ψηφιακός κόσμος δεν είναι μια ρεπλίκα της πραγματικότητας, είναι ένας άλλος κόσμος όπου τα (ψηφιακά) μας ίχνη είναι πολύ περισσότερα συγκριτικά με τα 'φυσικά'. Αυτό οφείλεται αφενός στις φορητές ψηφιακές συσκευές που αδιαλείπτως προσπαθούν να βελτιώνουν και να εμπλουτίζουν την εμπειρία του χρήστη παράγοντας πλήθος δεδομένων, αφετέρου δε στον ίδιο το χρήστη και ειδικότερα στον τύπο που χρησιμοποιεί τα μέσα κοινωνικής δικτύωσης και συνειδητά δημοσιοποιεί (συνεχώς) προσωπικά του δεδομένα.

Το γεγονός ότι τα ψηφιακά πειστήρια είναι δεδομένα σε **ψηφιακή** και **άυλη** μορφή τα καθιστά εξαιρετικά **εύθραυστα**, λόγω της **ευμεταβλητότητας τους** καθώς και εξαιτίας του τρόπου που αποθηκεύονται και επεξεργάζονται *{πχ η προκαθορισμένη (από τον κατασκευαστή) μικρή διάρκεια ζωής ενός σκληρού δίσκου στο οποίο είναι αποθηκευμένα ψηφιακά δεδομένα και ο οποίος με μαθηματική σχεδόν ακρίβεια, κάποια στιγμή θα 'αστοχήσει', θα 'εξαντληθεί' με αποτέλεσμα την απώλεια της αποθηκευμένης σε αυτό πληροφορίας}.* Δεν μπορούμε να παραβλέψουμε ωστόσο και την από πρόθεση διαγραφή ή καταστροφή αρχείων από τον χρήστη.

Στον αντίποδα της ευμεταβλητότητας, παρατηρούμε ότι τα ψηφιακά δεδομένα, μπορούν να είναι ταυτόχρονα και **ανθεκτικά**, καθώς μια ολική καταστροφή ψηφιακών δεδομένων απαιτεί συστηματική προσπάθεια, ενώ τα πληροφοριακά συστήματα διαθέτουν μηχανισμούς διασφάλισης της **ακεραιότητας** μέσω πλεονάσματος (redundancy) και ανοχής σε σφάλματα (fault tolerance).[26] Ασφαλώς η ανάκτηση μετά από συνειδητή απόπειρα καταστροφής δεδομένων είναι ενδεχομένως χρονοβόρα και με σημαντικά υψηλό κόστος, αλλά δεν είναι αδύνατη, ενώ από τεχνικής και νομικής πλευράς είναι δυνατό σε ορισμένες περιπτώσεις να στοιχειοθετηθεί η πρόθεση και δόλος εάν αποδειχθεί ο τρόπος

[26] Κάτος Β. (2023) Ψηφιακά Πειστήρια, Ηλεκτρονικό Έγκλημα (Ουσιαστικές και δικονομικές όψεις),ΝΒ σελ.401

της απόπειρας καταστροφής. Είναι λοιπόν εμφανές ότι βασική πρόκληση για τα ψηφιακά πειστήρια είναι η **διασφάλιση της ακεραιότητας**, ώστε να είναι νομικά παραδεκτά και αξιοποιήσιμα.

3.4. Κατευθυντήριες οδηγίες διαχείρισης ψηφιακών δεδομένων

Λόγω της ιδιαίτερης φύσης αλλά και της βαρύνουσας σημασίας των ψηφιακών δεδομένων στην αποδεικτική διαδικασία, έχουν διατυπωθεί συγκεκριμένες πρακτικές και κατευθυντήριες για την ορθή διαχείριση τους τόσο κατά το στάδιο αναγνώρισης και διαλογής όσο και κατά την συλλογή και διατήρηση τους.

Πρόκειται για το Διεθνές Πρότυπο ISO/IEC 27037:2012 *«Αναγνώριση, Διαλογή, Συλλογή & Διατήρηση Ψηφιακών Τεκμηρίων»*[27] καθώς και τον οδηγό ορθής πρακτικής για τις ψηφιακές αποδείξεις που δημοσιεύτηκε στο Ηνωμένο Βασίλειο, τον Μάρτιο του 2012 από το **A**ssociation of **C**hief **P**olice **O**fficers **(ACPO).**[28] Τα εγχειρίδια αυτά παρέχουν οδηγίες, κατευθυντήριες γραμμές και υποστήριξη σε άτομα και οργανισμούς για τον χειρισμό κάθε είδους ψηφιακού τεκμηρίου.

Σύμφωνα με το Διεθνές Πρότυπο ISO/IEC 27037:2012, οι πιο κάτω βασικές αρχές πρέπει να διέπουν τον χειρισμό των ψηφιακών τεκμηρίων:

-**Συνάφεια,** δηλαδή πρέπει το υλικό που αποκτήθηκε να είναι σχετικό με την υπό διεξαγωγή έρευνα, να περιέχει δηλαδή πληροφορίες που να ενισχύουν την διεξαγόμενη έρευνα.

- **Αξιοπιστία,** ότι όλες οι διαδικασίες που χρησιμοποιούνται στο χειρισμό τεκμηρίων πρέπει να είναι **ελέγξιμες** και **επαναλαμβανόμενες (δυνατότητα αναπαραγωγής τους)** και **δικαιολογημένες**.

[27] https://www.iso.org/standard/44381.html
[28] Williams, J. (2012). Acpo good practice guide for digital evidence. Metropolitan Police Service, Association of chief police officers, GB, 1556-6013.

- **Επάρκεια**, υπό την έννοια ότι έχει συγκεντρωθεί αρκετό υλικό για να μπορεί να διεξαχθεί μια ολοκληρωμένη έρευνα.

3.4.1. Στάδια χειρισμού ψηφιακών τεκμηρίων

Α) **Αναγνώριση (Identification)**

Το πρώτο στάδιο χειρισμού ψηφιακών τεκμηρίων είναι το στάδιο της αναγνώρισης πιθανών ψηφιακών τεκμηρίων τα οποία μπορούν να φανούν χρήσιμα στην διεξαγόμενη έρευνα *(προανάκριση, προκαταρτική, κύρια ανάκριση κτλ.)* και τα οποία θα έχουν αποδεικτική αξία σε μια ποινική διαδικασία. Πριν την διεξαγωγή της έρευνας πρέπει να διασφαλιστεί ότι αυτή διεξάγεται **νόμιμα**, βάσει συγκεκριμένης νομικής βάσης για την διεξαγωγή της (άρθρ. 245 παρ. 2 ΚΠΔ)[29]. Στο στάδιο αυτό δίνεται προτεραιότητα στην εξασφάλιση ψηφιακών δεδομένων τα οποία χαρακτηρίζονται από μια αστάθεια και μεταβλητότητα (πτητικά δεδομένα/volatile)[30], ούτως ώστε να ελαχιστοποιηθεί η 'επέμβαση' σε αυτά και να αξιοποιηθούν επαρκώς κατά την έρευνα. Αν ανιχνευθούν τότε και στο μέτρο που είναι αυτό εφικτό, διενεργείται «***εν λειτουργία διερεύνηση***» ή αλλιώς ***"live forensics"***. Για τα μη ευμετάβλητα ωστόσο (non-volatile)[31] αλλά και για την συλλογή στοιχείων από μηχάνημα που βρίσκεται εκτός λειτουργίας, για τα στοιχεία που πρόκειται να αποσταλούν για περαιτέρω εργαστηριακή ανάλυση

[29] Ν 4620/2019, Κώδικας Ποινικής Δικονομίας (ΦΕΚ Τεύχος Α' 96/11.06.2019)

[30] ***Ευμετάβλητα (Volatile)*** είναι τα στοιχεία που μπορεί να 'εξαφανιστούν' με την διακοπή της τροφοδοσίας της πηγής όπου είναι αποθηκευμένα, όπως τα στοιχεία που υπάρχουν στους διάφορους καταχωρητές, στην Cache, στην RAM, η κατάσταση του δικτύου και οι διεργασίες που εκτελούνται εκείνη την στιγμή. Προτεραιότητα δίνεται στο να καταγραφεί και να στοιχειοθετηθεί οτιδήποτε αποτελεί ευμετάβλητο στοιχείο.

[31] Είνα τα στοιχεία που μπορούμε να ανακτήσουμε και αργότερα κατά την ανάλυση, προτιμούμε όμως να αποκτηθούν κατά την εν λειτουργία διερεύνηση καθώς η διαδικασία ανάκτησής τους γίνεται πολύ πιο σύνθετη στην περίπτωση της εκτός λειτουργίας διερεύνησης.

αλλά και την δημιουργία ακριβών αντιγράφων, συνηθίζεται η «*εκτός λειτουργίας διερεύνηση*» ή *'post mortem forensics'*.

Β) **Συλλογή (Collection)**

Πριν την έναρξη της συλλογής των τεκμηρίων είναι αναγκαία η τήρηση πρακτικών για την διεξαγόμενη έρευνα που θα περιλαμβάνει όλες τις λεπτομέρειες για την διεξαγωγή της. Θα πρέπει να γίνεται φωτογράφηση, βιντεοσκόπηση καθώς και σχεδιαγράφηση της σκηνής η οποία θα περιλαμβάνει απαραίτητα την τοποθεσία εντοπισμού της κάθε συσκευής, τον τύπο της, έτσι ώστε να είμαστε σε θέση αργότερα να μεταφέρουμε ή να ανακατασκευάσουμε τα δεδομένα της σκηνής.[32] Όταν η σκηνή της έρευνας έχει εξασφαλιστεί και υπάρχει νομική βάση *(σύμφωνα με τα οριζόμενα στις σχετικές διατάξεις του Κώδικα Ποινικής Δικονομίας για την έρευνα και κατάσχεση)* για κατάσχεση τεκμηρίων τα οποία έχουν επιβεβαιωθεί, τότε μπορεί να αρχίσει η συλλογή και η κατάσχεση τους. Πρέπει να ληφθεί υπόψη να αναζητηθούν -μεταξύ άλλων- τυχόν κωδικοί πρόσβασης σε συσκευές καθώς και PIN κινητών τηλεφώνων από τους κατόχους καθώς επίσης και τυχόν φορτιστές, καλώδια και εγχειρίδια χρήσης τους, ενώ USB Drives κινητά τηλέφωνα, σκληροί δίσκοι και άλλα παρόμοια αντικείμενα εξετάζονται με την χρήση διάφορων εργαλείων και τεχνικών με αυτό να γίνεται συχνότερα σε εξειδικευμένα εργαστήρια.[33]

Γ) **Απόκτηση (Acquisition)**

Το επόμενο στάδιο περιλαμβάνει την απόκτηση των ψηφιακών δεδομένων από την συσκευή στην οποία εντοπίστηκαν και έχει κατασχεθεί για ανάλυση και εξέταση είτε σε εξειδικευμένο εργαστήριο είτε επί τόπου σύμφωνα με τις διακρίσεις που αναλύθηκαν παραπάνω. Ένα καίριο στοιχείο του σταδίου αυτού είναι να προληφθεί και να αποφευχθεί οποιαδήποτε μόλυνση των δεδομένων,

[32] Mukasey, M. B., Sedgwick, J. L., & Hagy, D. W. (2008). Electronic crime scene investigation: A guide for first responders. *NCJ*, *219941*.
https://www.ncjrs.gov/pdffiles1/nij/219941.pdf

[33] Παπαθανασίου Α.Χ, (2023) Κυβερνοέγκλημα, Ψηφιακή Εγκληματολογία και Κατάσχεση Ψηφιακών Δεδομένων, Ηλεκτρονικό Έγκλημα (Ουσιαστικές και δικονομικές όψεις),ΝΒ σελ.273

δηλαδή με άλλα λόγια πρέπει να αποτραπούν οποιεσδήποτε παρεμβάσεις σε αυτά και ως εκ τούτου είναι αναγκαία η δημιουργία αντιγράφου των δεδομένων, **πριν την ανάλυση τους**, πάνω στο οποίο θα εργαστεί ο αναλυτής αφήνοντας έτσι τα πρωτότυπα δεδομένα ανέπαφα.

Δ) **Διατήρηση (Preservation)**

Κατόπιν των παραπάνω σταδίων χειρισμού των ψηφιακών τεκμηρίων, σημαντική είναι και η παράμετρος της διατήρησης τους, κάτι που θα υποβοηθήσει την διεξαγόμενη έρευνα και επίσης θα συμβάλει στην συντήρηση τους σε καλή κατάσταση μέχρι που αυτά θα χρειαστεί να παρουσιαστούν ως πειστήρια σε μια ενδεχόμενη ποινική διαδικασία (π.χ.στο δικαστήριο). Η διαδικασία αυτή της διατήρησης των ψηφιακών δεδομένων καθώς και συσκευών που περιέχουν τέτοια δεδομένα περιλαμβάνει την προστασία τους από επεμβάσεις σε αυτά καθώς και την καταστροφή τους, ενώ η διαδικασία αυτή πρέπει να ξεκινά και να διατηρείται σε όλη την διαχείριση τους. Όλα τα κατασχεθέντα ψηφιακά τεκμήρια πρέπει να προστατευτούν από τυχόν απώλεια τους, αλλοίωση ή καταστροφή τους, πάντα με γνώμονα ότι το πιο σημαντικό στην διαδικασία αυτή είναι η εξασφάλιση της **ακεραιότητας** και **αυθεντικότητας** των πιθανών ψηφιακών τεκμηρίων καθώς και της αλυσίδας φύλαξης/επιμέλειας τους.

3.4.2. Η αλυσίδα φύλαξης/επιμέλειας (Chain of Custody-CoC)

Η τεχνική επιτροπή ***(TC) ISO/PC 308***[34] *(που δημιουργήθηκε το 2016)* έχει εργαστεί για την τυποποίηση της λεγόμενης αλυσίδας φύλαξης (CoC). Πρόκειται για έναν όρο που εφαρμόζεται σε πλείστες περιπτώσεις πέρα από τη διαχείριση ψηφιακών αποδεικτικών στοιχείων. Σύμφωνα με τα λόγια της TC ISO/PC 308, «*η αλυσίδα φύλαξης είναι μια διαδοχή ευθυνών για διαδικασίες καθώς ένα προϊόν κινείται σε κάθε βήμα της αλυσίδας 'εφοδιασμού'. Κάθε εμπλεκόμενος στον εφοδιασμό πρέπει να εφαρμόζει και να τεκμηριώνει ένα σύνολο μέτρων προκειμένου να λειτουργήσει*

[34] https://www.iso.org/committee/6266669.html

η αλυσίδα επιτήρησης» Ο στόχος είναι να εξασφαλιστεί η **ιχνηλασιμότητα** και η **ακεραιότητα** του προϊόντος, το οποίο στο πλαίσιο της ψηφιακής εγκληματολογίας είναι τα ψηφιακά αποδεικτικά στοιχεία. Εάν τεθεί υπό αμφισβήτηση η ακεραιότητα και η αυθεντικότητα των ψηφιακών αποδεικτικών στοιχείων, τότε ολόκληρη η ψηφιακή έρευνα τίθεται εν αμφιβόλω ή ακόμα χειρότερα δύναται να ακυρωθεί.[35] Η ζωτικής σημασίας αλυσίδα φύλαξης των ψηφιακών δεδομένων είναι απαραίτητη για την επαλήθευση της αυθεντικότητας και της ακεραιότητας των κατασχεμένων δεδομένων, σύμφωνα και με τα διεθνή πρότυπα, «θωρακίζεται» δε νομικά στο δικαιικό μας σύστημα, μέσω της **'ειδικής έκθεσης'** του άρθρου **265 ΚΠΔ παρ. 3**[36]. Αυτό επιτυγχάνεται καθιστώντας υποχρεωτική την καταγραφή των κατασχεμένων ψηφιακών δεδομένων, του οργάνου που τα κατάσχεσε και είχε τον έλεγχο τους, του τρόπου, του τόπου και του χρόνου που αποκτηθήκαν τα δεδομένα αυτά που θα χρησιμοποιηθούν ως αποδεικτικά στοιχεία.

Από τα παραπάνω, γίνεται κατανοητό ότι η ειδική αυτή έκθεση της παρ.3, ουσιαστικά αντικαθιστά τη διενέργεια πραγματογνωμοσύνης που ακολουθούσε στην πράξη, με την οποία εξετάζονταν οι κατασχεμένοι υλικοί φορείς και αποτυπώνονταν τα περιεχόμενά τους. Καταλείπεται ωστόσο χώρος ώστε η τυχόν πραγματογνωμοσύνη στους υλικούς φορείς ή και στα περιεχόμενα αυτών, να μπορεί να απαντήσει εμπεριστατωμένα διάφορα ειδικότερα ερωτήματα τεχνικής κυρίως φύσης (λ.χ. εάν υπήρξε αλλοίωση των metadata των ψηφιακών δεδομένων κ.λπ.)[37][38]

3.5 Η ψηφιακή έρευνα & η κατάσχεση των ψηφιακών δεδομένων

[35]Nieto, A., Rios, R., Lopez, J., Ren, W., Wang, L., Choo, K. K. R., & Xhafa, F. (2019). Privacy-aware digital forensics

[36] «Η κατάσχεση που διενεργείται κατά τις παρ. 1 και 2, βεβαιώνεται με **ειδική έκθεση**, η οποία αναφέρει ειδικώς τις ενέργειες της παρ. 2 που πραγματοποιεί εκείνος που διεξάγει την ανάκριση»

[37] Καργόπουλος Α.Ι, 2023 'Τα ψηφιακά δεδομένα στο ισχύον δικονομικό πλαίσιο: Δικαιικοί άξονες & προβληματισμοί', Ηλεκτρονικό Έγκλημα (Ουσιαστικές και δικονομικές όψεις), ΝΒ

[38] Βλ. **αντιφατική** ερμηνεία της υπ'αριθμ **6/2021** Γνωμοδότηση της Εισαγγελίας του Αρείου Πάγου (Α.Π), σύμφωνα με την οποία η κατάσχεση των υλικών φορέων συνεπάγεται και κατάσχεση των ψηφιακών δεδομένων που είναι αποθηκευμένα σε αυτά.

Η έρευνα για τα αποδεικτικά μέσα ψηφιακής μορφής, ελλείψει ειδικότερων διατάξεων, διεξάγεται υπό τους όρους των άρθρων **253** και **254** παρ. 1 στοιχ.δ' **ΚΠΔ**, από το συνδυασμό των οποίων προκύπτει ότι:

Για την διενέργεια έρευνας προς αναζήτηση ψηφιακών δεδομένων ή απλής ακόμα πρόσβασης, στο σύνολο ή σε μέρος ενός πληροφοριακού συστήματος και στα ψηφιακά δεδομένα που είναι τυχόν αποθηκευμένα σε αυτό, αλλά και σε ένα μεμονωμένο μέσο αποθήκευσης των σχετικών δεδομένων, απαιτείται:

- να διεξάγεται ανακριτική διαδικασία για κακούργημα ή πλημμέλημα (άρθρ.253 ΚΠΔ)
- το υπό έρευνα, αρχικό πληροφοριακό σύστημα (δηλαδή το υλικό του, hardware) ή το πληροφοριακό σύστημα, στο οποίο επεκτείνεται η έρευνα ή το μεμονωμένο μέσο αποθήκευσης να βρίσκονται στο έδαφος της Ελλάδας.[39]
- να μπορεί βασίμως να υποτεθεί ότι η βεβαίωση του εγκλήματος, η αποκάλυψη ή η σύλληψη των δραστών ή τέλος η βεβαίωση ή η αποκατάσταση της ζημίας που προκλήθηκε, είναι δυνατόν να πραγματοποιηθεί ή να διευκολυνθεί μόνο με αυτήν (άρθρ. 253 ΚΠΔ).
- να τηρηθούν οι εγγυήσεις και οι διαδικασίες των άρθρων 4 και 5 του Ν 2225/1994 σε συνδυασμό με τις αντίστοιχες του άρθρου 254 παρ. 2-5 ΚΠΔ (άρθρ. 254 παρ. 1στοιχ. δ', 2 ΚΠΔ).

Υπό την ερμηνεία αυτή των ισχυουσών διατάξεων του ΚΠΔ καλύπτονται εμμέσως όλες οι απορρέουσες υποχρεώσεις της Σύμβαση της Βουδαπέστης που τίθενται για την πρόσβαση και έρευνα (άρθρο 19 παρ. 1, 2) καθώς και οι όροι και οι εγγυήσεις υπό τις οποίες πρέπει αυτές να διενεργούνται (άρθρο 14, 15).

[39] Σύμφωνα με αρχή του διεθνούς δικαίου κανένα κράτος δεν επιτρέπεται να διενεργεί αυθαίρετα πράξεις (κρατικής) εξουσίας σε ξένη επικράτεια. Το γεγονός ότι το διεθνές ποινικό δίκαιο 'stricto sensu' επιτρέπει την εφαρμογή των ποινικών νόμων μιας χώρας σε πραγματικά περιστατικά που για οποιοδήποτε προβλεπόμενο λόγο. *(ιθαγένεια δράστη ή θύματος κ.λπ.)* συνδέονται με την έννομη τάξη-της δεν συνεπάγεται ότι παρέχει στο αλλοδαπό κρατικό όργανο την αρμοδιότητα ή το δικαίωμα να ενεργεί πράξεις κυριαρχίας *(Acts of State)* σε έδαφος ξένου κράτους καθόσον θίγεται η εθνική κυριαρχία του τελευταίου. Τέτοια προσβολή συνιστά και η διενέργεια ανακριτικών πράξεων όπως σύλληψη, έρευνα, κατάσχεση, παρακολούθηση, έρευνα σε κατοικία κ.λπ. εκτός αν έχει συναινέσει ad hoc το κυρίαρχο κράτος ή αν υπάρχει ειδικός κανόνας του διεθνούς δικαίου που το επιτρέπει *(Μυλωνόπουλος Χ. (2021), Διεθνές & Ευρωπαϊκό Ποινικό Δίκαιο, Νομική Βιβλιοθήκη, σελ. 64-65)*.

Στη βάση αυτή θεμελιώνεται πρωταρχικά και το «δικαίωμα» των ανακριτικών Αρχών να αποκτούν πρόσβαση και να αντιγράφουν (κατάσχουν) ψηφιακά δεδομένα, που είναι αποθηκευμένα σε ένα πληροφοριακό σύστημα ή σε ένα μεμονωμένο μέσο αποθήκευσης άλλως τελείται, <u>αν υπάρχει και γνώση του ενδεχομένου έλλειψης δικαιώματος και συντρέχουν και τα λοιπά στοιχεία της υπόστασής της</u>, καταρχήν αξιόποινη πράξη (άρθρο 370Β παρ. 1 εδ. α' ΠΚ), με συνέπεια κάθε αποδεικτικό μέσο, που αποκτήθηκε με αυτή ή μέσω αυτής, να μην μπορεί να ληφθεί υπόψη στην ποινική διαδικασία (άρθρο 177 παρ. 2 ΚΠΔ).[40]

Παραμένοντας στο δικονομικό πεδίο ερευνών, κύρια πρακτική εφαρμογή έχει η διάταξη του άρθρου **265 ΚΠΔ** σχετικά με την **κατάσχεση ψηφιακών δεδομένων**, που αποτελεί νομοθετικό εργαλείο εφαρμογής προβλέψεων της Σύμβασης της Βουδαπέστης. Ειδικότερα στην παράγραφο **1** [41]προσδιορίζονται τα ψηφιακά δεδομένα που μπορούν να κατασχεθούν. Έτσι, κατάσχεση μπορεί να επιβληθεί στα δεδομένα που είναι αποθηκευμένα σε έναν υπολογιστή, στα οποία έχει όμως φυσική πρόσβαση εκείνος που διενεργεί την ανάκριση, σε ένα μέσο αποθήκευσης δεδομένων υπολογιστή στο οποίο υπάρχουν αποθηκευμένα δεδομένα υπολογιστή και έχει πάλι φυσική πρόσβαση εκείνος που διενεργεί την ανάκριση, σε ένα απομακρυσμένο σύστημα υπολογιστή, σε ένα απομακρυσμένο μέσο αποθήκευσης δεδομένων υπολογιστή, στα οποία έχει φυσική πρόσβαση εκείνος που διενεργεί την ανάκριση. Ωστόσο τα ψηφιακά δεδομένα που είναι αποθηκευμένα και προσβάσιμα μέσω συστήματος και υπηρεσιών

[40] Γκύζης Δ, (2023) Αντεισαγγελέας Εφετών 'Ψηφιακή ανακριτική πράξη' Ηλεκτρονικό Έγκλημα (Ουσιαστικές και δικονομικές όψεις), ΝΒ σελ.374

[41] *«Η κατάσχεση ψηφιακών δεδομένων μπορεί να επιβληθεί: **α)** Σε ένα σύστημα υπολογιστή στο σύνολό του ή σε μέρος αυτού και στα δεδομένα υπολογιστή που είναι αποθηκευμένα σε αυτόν, στα οποία έχει φυσική πρόσβαση εκείνος που διενεργεί την ανάκριση, **β)** σε ένα μέσο αποθήκευσης δεδομένων υπολογιστή στο οποίο υπάρχουν αποθηκευμένα δεδομένα υπολογιστή και έχει φυσική πρόσβαση εκείνος που διενεργεί την ανάκριση, **γ)** σε ένα απομακρυσμένο σύστημα υπολογιστή στο σύνολό του ή σε μέρος αυτού και στα δεδομένα υπολογιστή που είναι αποθηκευμένα σε αυτόν ή σε ένα απομακρυσμένο μέσο αποθήκευσης δεδομένων υπολογιστή και στα δεδομένα υπολογιστή που είναι αποθηκευμένα σε αυτό, τα οποία είναι διασυνδεδεμένα στο σύστημα υπολογιστή στο οποίο έχει φυσική πρόσβαση εκείνος που διενεργεί την ανάκριση. Στην τελευταία περίπτωση, τα ψηφιακά δεδομένα που είναι αποθηκευμένα και προσβάσιμα μέσω συστήματος και υπηρεσιών νεφοϋπολογιστικής (Cloud Services) δεν θεωρούνται αποθηκευμένα σε απομακρυσμένο σύστημα υπολογιστή ή σε απομακρυσμένο μέσο αποθήκευσης δεδομένων υπολογιστή τα οποία είναι διασυνδεδεμένα στο σύστημα υπολογιστή στο οποίο έχουν φυσική πρόσβαση οι αρχές.*

νεφοϋπολογιστικής (Cloud Services) δεν θεωρούνται αποθηκευμένα σε απομακρυσμένο σύστημα υπολογιστή ή σε απομακρυσμένο μέσο αποθήκευσης δεδομένων υπολογιστή.

Εδώ αξίζει να σημειωθούν οι κάτωθι επισημάνσεις:

- Για τις αξιόποινες πράξεις που συνδέονται με τα ψηφιακά δεδομένα, που είναι αποθηκευμένα σε υπηρεσία νεφοϋπολογιστικής ανακύπτει ζήτημα διεθνούς δικαιοδοσίας των ελληνικών δικαστηρίων. Όπως τονίζεται στην αιτιολογική έκθεση του ισχύοντα ΠΚ η επέκταση της αρχής της εδαφικότητας στα εγκλήματα μέσω διαδικτύου ή άλλου μέσου επικοινωνίας κρίθηκε αδικαιολόγητη. Αν οι πράξεις τελούνται μέσω διαδικτύου και στρέφονται εναντίον ημεδαπού, διώκονται ωστόσο με τις προϋποθέσεις των άρθρων 6, 7 και σε κάθε περίπτωση του άρθρου 8 ΠΚ.
- Ειδικότερα για τα μηνύματα του ηλεκτρονικού ταχυδρομείου με την υπ'αριθ.1/2017 απόφαση ΟλΑΠ (πολιτική) κρίθηκε ότι εμπίπτουν και αυτά στο απόρρητο των ανταποκρίσεων, προστατεύονται όμως κατά την παρ. 1 του άρθρου 19 Συντάγματος **μόνο κατά το στάδιο της επικοινωνίας**. Μετά την ολοκλήρωσή της, ηλεκτρονικά μηνύματα που διατηρεί ο αποστολέας ή ο παραλήπτης τους σε τυπωμένη μορφή ή στον υπολογιστή του, χωρίς χρήση κωδικού πρόσβασης, δεν εμπίπτουν στο προστατευτικό πεδίο του άρθρου 19 παρ. 1 Συντ., αλλά σε εκείνο των διατάξεων **9** και **9Α** του Συντ.[42]

Ακόμη στην παράγραφο **2** του άρθρου **265 ΚΠΔ**[43] προσδιορίζεται ο τρόπος που γίνεται η κατάσχεση των ψηφιακών δεδομένων και ειδικότερα αποσαφηνίζεται

---

[42] Τσόγκας Λ.Σ, (2021)Αντεισαγγελέας Εφετών Θράκης «ΨΗΦΙΑΚΗ ΕΠΟΧΗ ΚΑΙ ΔΙΚΑΙΟΣΥΝΗ ΣΥΓΧΡΟΝΕΣ ΜΟΡΦΕΣ ΕΓΚΛΗΜΑΤΙΚΟΤΗΤΑΣ - ΔΙΕΘΝΗΣ ΣΥΝΕΡΓΑΣΙΑ-ΣΥΓΧΡΟΝΑ ΜΕΣΑ» https://ende.gr/%CF%88%CE%B7%CF%86%CE%B9%CE%B1%CE%BA%CE%B7-%CE%B5%CF%80%CE%BF%CF%87%CE%B7-%CE%BA%CE%B1%CE%B9-%CE%B4%CE%B9%CE%BA%CE%B1%CE%B9%CE%BF%CF%83%CF%85%CE%BD%CE%B7-%CF%83%CF%85%CE%B3%CF%87%CF%81%CE%BF%CE%BD/

[43] *'Η κατά τα ανωτέρω κατάσχεση πραγματοποιείται αποκλειστικά με τη χρήση κατάλληλου εξοπλισμού που επιτρέπει σε εκείνον που τη διεξάγει:*
***α)** Την αφαίρεση και την κατάσχεση του υλικού φορέα των υπό στοιχείων αγ' της παρ. 1, στο οποίο βρίσκονται αποθηκευμένα τα δεδομένα και/ή*
***β)** την αντιγραφή και την αφαίρεση των αποθηκευμένων ψηφιακών δεδομένων των υπό στοιχείων αγ' της παρ. 1 σε μέσο αποθήκευσης δεδομένων και*

ότι η κατάσχεση πραγματοποιείται αποκλειστικά με τη χρήση κατάλληλου εξοπλισμού αλλά και τι ακριβώς επιτρέπεται να λάβει χώρα κατά τη διάρκειά της. Συγκεκριμένα επιτρέπεται σε εκείνον που τη διεξάγει, η αφαίρεση και η κατάσχεση του υλικού φορέα, η αντιγραφή, η αφαίρεση των αποθηκευμένων ψηφιακών δεδομένων σε μέσο αποθήκευσης δεδομένων καθώς και η αναπαραγωγή και η επαλήθευση της αυθεντικότητας και της ακεραιότητας των κατασχεθέντων δεδομένων. Είναι φανερό ότι εισάγεται τρόπον τινά, επιτακτικός κανόνας, σύμφωνα με τον οποίο κατάσχεση ψηφιακών δεδομένων χωρεί **αποκλειστικά** με τη χρήση κατάλληλου εξοπλισμού, ο οποίος επιτρέπει τις ενέργειες που περιγράφονται στη διάταξη. Είναι σαφές ότι αναγνωρίζεται εδώ η ιδιαίτερη φύση των ψηφιακών δεδομένων, που δεν επιτρέπει την απλή «απομάκρυνσή» τους κατά τρόπο που προσιδιάζει στην αφαίρεση ενσώματων αντικειμένων από την κατοχή ορισμένου προσώπου. Ο κατάλληλος εξοπλισμός θα μπορούσε να συνίσταται σε συσκευές και/ή λογισμικό αντιγραφής, κατά περίπτωση. Εγείρεται έτσι ζήτημα σε σχέση με το νόημα του όρου «αποκλειστικά», ιδίως ενόψει της απουσίας προκαθορισμένων μέσων που θα μπορούσαν να χρησιμοποιηθούν για την κατάσχεση ψηφιακών δεδομένων.

Συναφής παρατήρηση, θα μπορούσε να γίνει και σε σχέση με την αξιοποίηση κατάλληλα εκπαιδευμένου προσωπικού για την εξαγωγή των δεδομένων. Μολονότι η ύπαρξη τέτοιου προσωπικού είναι σε κάποιον βαθμό αυτονόητη, ή θα έπρεπε να είναι, δεν προκύπτει με βάση το γράμμα του νόμου ότι η κατάσχεση ψηφιακών δεδομένων θα είναι παράτυπη επί απουσίας τέτοιου προσωπικού. Επομένως, η διάταξη της παραγράφου 2 του άρθρου 265 ΚΠΔ μπορεί να θεωρηθεί ότι περιγράφει απλώς τον τρόπο της κατάσχεσης των δεδομένων, χωρίς να καθιερώνει έναν δικονομικό τύπο η τήρηση του οποίου επιβάλλεται επί ποινής ακυρότητας. Τούτου λεχθέντος, η πλημμελής εξαγωγή δεδομένων, και ιδίως η μη τήρηση κάποιου πρωτοκόλλου για την επαλήθευση της αυθεντικότητας και της ακεραιότητάς τους, είναι δυνατό να παίξει ουσιώδη ρόλο σε σχέση με την

γ) *την αναπαραγωγή και την επαλήθευση της αυθεντικότητας και της ακεραιότητας των κατασχεθέντων δεδομένων'*

αποδεικτική αξιοποίηση των δεδομένων σε μεταγενέστερα στάδια της ποινικής διαδικασίας.[44]

Η παράγραφος **3** σχετικά με την σύνταξη της ειδικής έκθεσης αναλύθηκε εκτενώς παραπάνω, στο σχετικό εδάφιο με την αλυσίδα φύλαξης/επιμέλειας. Περαιτέρω στις παραγράφους **4**[45] **& 5**[46] του υπό εξέταση άρθρου προσδιορίζεται ο τρόπος και ο χρόνος διατήρησης των ψηφιακών δεδομένων, ενώ τέλος στην παράγραφο **6**[47] ορίζεται ότι απαγορεύεται η δημιουργία και η διατήρηση αντιγράφων των ψηφιακών δεδομένων για οποιονδήποτε άλλον λόγο, εκτός αν ο αρμόδιος εισαγγελέας ή ανακριτής ή συμβούλιο ή το δικαστήριο κρίνουν ότι τα κατασχεμένα ψηφιακά δεδομένα είναι αναγκαίο να περιληφθούν σε άλλη δικογραφία.

4. Η ΣΗΜΑΣΙΑ ΤΩΝ ΜΕΤΑΔΕΔΟΜΕΝΩΝ ΣΤΗΝ ΨΗΦΙΑΚΗ ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΗ ΕΡΕΥΝΑ ΚΑΙ ΤΟ ΑΠΟΡΡΗΤΟ ΑΥΤΩΝ

Ήδη έχει επιχειρηθεί μια πρώτη εννοιολογική οριοθέτηση και κατηγοριοποίηση των μεταδεδομένων, καθώς αποτελούν -μεταξύ άλλων- και αυτά αντικείμενο

[44]Ναζίρης Γ. (2023) Η κατάσχεση των ψηφιακών δεδομένων», Ηλεκτρονικό Έγκλημα (Ουσιαστικές και δικονομικές όψεις), ΝΒ σελ.501

[45]*' 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.'*

[46] *'Η πρόσβαση και η δυνατότητα αναπαραγωγής των ψηφιακών δεδομένων που κατάσχονται επιτρέπεται μόνο σε όσους ασκούν δικαστικά, εισαγγελικά και ανακριτικά καθήκοντα στην υπόθεση ή τους γραμματείς. Προς το σκοπό αυτό χρησιμοποιούνται τα κατάλληλα τεχνικά μέσα. Τέτοια μέσα είναι η κρυπτογράφηση και η χρήση κωδικών ασφαλείας για την πρόσβαση και αναπαραγωγή των κατασχεμένων ψηφιακών δεδομένων από το υλικό μέσο αποθήκευσης στο οποίο βρίσκονται αποθηκευμένα. Η παρούσα ισχύει αναλόγως και στα ψηφιακά δεδομένα που αφορούν στα δεδομένα επικοινωνίας που περιλαμβάνονται στη δικογραφία'*

[47] *'Απαγορεύεται η δημιουργία και η διατήρηση αντιγράφων των ψηφιακών δεδομένων για οποιονδήποτε άλλον λόγο εκτός αν ο αρμόδιος εισαγγελέας ή ανακριτής ή συμβούλιο ή το δικαστήριο κρίνουν ότι τα κατασχεμένα ψηφιακά δεδομένα είναι αναγκαίο να περιληφθούν σε άλλη δικογραφία. Η παρούσα ισχύει αναλόγως και στα ψηφιακά δεδομένα που αφορούν στα δεδομένα επικοινωνίας που περιλαμβάνονται στη δικογραφία'*

ενδιαφέροντος στα πλαίσια μιας ψηφιακής εγκληματολογικής έρευνας υπό την έννοια ότι αποτελούν και τα ίδια, ψηφιακά αποδεικτικά στοιχεία (βαρύνουσας σημασίας όπως θα αναδειχθεί παρακάτω).

Αναλυτικότερα, τα μεταδεδομένα αποτελούν δεδομένα, που εξηγούν/περιγράφουν άλλα δεδομένα, καθώς αποτυπώνουν μια δομημένη περιγραφή των βασικών χαρακτηριστικών ενός πληροφοριακού πόρου, με αποτέλεσμα να καθιστούν ευκολότερη την ανάκτηση, την επεξεργασία και τη διαχείριση της πληροφορίας. Κατά μία έννοια έπονται των αρχικών/βασικών δεδομένων και για το λόγο αυτό, άλλωστε, τους έχει προσδοθεί το πρόθεμα «μετά».[48] Συναφώς με τα προεκτεθέντα, τα μεταδεδομένα επικοινωνίας αποτελούν δεδομένα, που παράγονται ως αποτέλεσμα της μετάδοσης μιας επικοινωνίας και αποκαλύπτουν πληθώρα στοιχείων για το επικοινωνιακό γεγονός, όπως το γεωγραφικό πλάτος και μήκος, υψόμετρο του τερματικού σταθμού του αποστολέα ή του παραλήπτη, οποιαδήποτε πληροφορία ονομασίας, αρίθμησης ή διεύθυνσης των επικοινωνούντων μερών, τον όγκο, την αρχή, το τέλος ή τη διάρκεια της επικοινωνίας, με αποτέλεσμα να αποτελούν τρόπον τινά τα «συμφραζόμενα» αυτής, σε αντίθεση με το περιεχόμενό της. Ως εκ τούτου, τα μεταδεδομένα αποτελούν ένα πλούσιο πληροφοριακό πλούτο, καθώς αποκαλύπτουν προσωπικές πληροφορίες σχετικά με τα εμπλεκόμενα πρόσωπα (τα επικοινωνούντα μέρη), τον χρόνο, την συχνότητα και την διάρκεια της μεταξύ τους επικοινωνίας, το είδος αυτής *(π.χ. τηλεφωνική κλήση, μήνυμα, email)*, το χρησιμοποιούμενο μέσο *(πχ. σταθερή τηλεφωνία, smartphone, tablet)*, την τοποθεσία αυτών, αφήνοντας έτσι πίσω πληθώρα (ψηφιακών) ιχνών για διερεύνηση.

Με την ταχεία εξέλιξη της τεχνολογίας σε εκθετικό βαθμό, την ψηφιοποίηση της επικοινωνίας και την καθολική χρήση των κοινωνικών δικτύων έχουν επικρατήσει παγκοσμίως τα φορητά μέσα επικοινωνίας, έχοντας ως επακόλουθο τη συσσώρευση όλων των επικοινωνιών μας σε μία μοναδική συσκευή, η οποία μάλιστα βρίσκεται διαρκώς πάνω μας, παρέχοντάς μας παράλληλα άμεση

[48] Landau, S. (2020, October). Categorizing uses of communications metadata: Systematizing knowledge and presenting a path for privacy. In *New Security Paradigms Workshop 2020* (pp. 1-19).

πρόσβαση στο Διαδίκτυο.[49] Τα αναλυτικά ίχνη των μεταδεδομένων επικοινωνίας, που παράγει η αδιάκοπη αυτή χρήση των φορητών έξυπνων συσκευών επικοινωνίας διευκολύνει αφενός τη συλλογή πρωτοφανούς πληθώρας δεδομένων και δημιουργίας συσχετισμών αυτών, προς αξιοποίηση στο πλαίσιο μιας εγκληματολογικής έρευνας, αφετέρου κλυδωνίζει ουσιώδη (ατομικά) δικαιώματα και ελευθερίες, όπως το απόρρητο της επικοινωνίας, την ιδιωτικότητα και την προστασία προσωπικών δεδομένων. Αξίζει να επισημανθεί εδώ ότι, οι τεχνολογικές εξελίξεις κι η καθολική χρήση των έξυπνων μέσων επικοινωνίας έχουν αλλάξει τη φύση των δεδομένων, που μπορούν να συλλεχθούν, διαμορφώνοντας νέες κατηγορίες μεταδεδομένων, όπως δεδομένα γεω-εντοπισμού, βιομετρικά δεδομένα, δεδομένα αναγνώρισης προσώπου και δακτυλικών αποτυπωμάτων, με αποτέλεσμα να μπορούν να αποκαλύψουν ζωτικές πληροφορίες για τα υποκείμενα των δεδομένων αυτών.[50] Η ένταση της διεισδυτικότητας των πληροφοριών αυτών για κάθε πτυχή της καθημερινότητας των ατόμων, με τρόπο αποκαλυπτικό μέχρι και για τις κοινωνικές, πολιτικές και θρησκευτικές πεποιθήσεις των ατόμων, συμβάλλει στην εξόρυξη μοτίβων, στην χαρτογράφηση συμπεριφοράς των ατόμων και στην σκιαγράφηση του **ψηφιακού προφίλ** του που αντανακλά το βιοπορτρέτο του.

Παρατηρούμε επίσης ότι ενώ το περιεχόμενο της επικοινωνίας δεν μπορεί να είναι δομημένο, ενιαίο ή ομοιόμορφο αφού διακρίνεται από τον υποκειμενισμό (των μερών) , τα μεταδομένα αυτού, τα οποία παράγονται με αυτοματοποιημένο τρόπο, μπορούν να επεξεργαστούν εύκολα και γρήγορα με τρόπο αντικειμενικά παραδεκτό, σχεδόν με μαθηματική ακρίβεια. Αυτό αδιαμφισβήτητα εξυπηρετεί την ταχύτητα αξιοποίησης τους ως αποδεικτικό υλικό αλλά και την οικονομία του χρόνου, της έρευνας αλλά και του κόστους αυτής *(καθώς το περιεχόμενο συνήθως είναι κρυπτογραφημένο και απαιτεί άλλες μεθόδους και εργαλεία για την αποκρυπτογράφηση του).* Καθώς δεν μεσολαβεί ο ανθρώπινος παράγοντας για την ανάλυση τους *(πχ στη περίπτωση του περιεχομένου της επικοινωνίας*

[49] Wicker, S. B. (2013). Cellular convergence and the death of privacy. Oxford University Press, USA.
[50] Bernal, P. (2016). Data gathering, surveillance and human rights: recasting the debate. Journal of Cyber Policy, 1(2), 243-264.

αξιοποιούνται οι επιστημονικές γνώσεις ειδικού πραγματογνώμονα, ψυχολόγου κτλ.) διασφαλίζεται περισσότερο η εγκυρότητα και η αξιοπιστία τους.

Η πληθώρα στοιχείων που προσφέρουν τα μεταδεδομένα, συνδράμουν αποφασιστικά στην πιο ολοκληρωμένη ανακατασκευή του εγκλήματος, στην πιθανή και ταχύτερη ανεύρεση και άλλων συμμέτοχων και δημιουργία προφίλ των υπόπτων και των ιδιαίτερων χαρακτηριστικών τους για πιο εξατομικευμένη προσέγγιση, στην αιτιώδη συνάφεια μεταξύ του αξιόποινου αποτελέσματος και της σχετικής συμπεριφοράς ή παράλειψής των υπόπτων. Επιπλέον, η ανωτέρω αιτιώδης συνάφεια «ιδρύεται» και με την χρονική αλληλουχία και την χρονοσήμανση, που επιτυγχάνεται μέσω των μεταδεδομένων.

Είναι κατανοητό ότι το οπλοστάσιο της ψηφιακής εγκληματολογικής διερεύνησης, ενισχύεται σημαντικά και πολυπλεύρως από πλούσιες και διαφορετικές πηγές δεδομένων, ωστόσο για να είναι εν τέλει αξιοποιήσιμα πρέπει να τελούν υπό συγκεκριμένες δικονομικές εγγυήσεις και με γνώμονα τα ατομικά δικαιώματα και θεμελιώδεις ελευθερίες των υποκειμένων.

Κατοχύρωση απορρήτου επικοινωνίας σε διεθνές-ευρωπαϊκό και εθνικό επίπεδο-Το ζήτημα των μεταδεδομένων .

4.1. Στο διεθνές πεδίο

Σύμφωνα με το άρθρο **8** της Ευρωπαϊκής Σύμβασης Δικαιωμάτων του Ανθρώπου (1950):

1. *Παν πρόσωπον δικαιούται εις τον σεβασμόν της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και της αλληλογραφίας του.*
2. *Δεν επιτρέπεται να υπάρξη επέμβασις δημοσίας αρχής εν τη ασκήσει του δικαιώματος τούτου, εκτός εάν η επέμβασις αύτη προβλέπεται υπό του νόμου και αποτελεί μέτρον το οποίον, εις μίαν δημοκρατικήν κοινωνίαν, είναι αναγκαίον δια την εθνικήν ασφάλειαν, την δημοσίαν ασφάλειαν, την οικονομικήν ευημερίαν της χώρας, την προάσπισιν της τάξεως και την πρόληψιν*

ποινικών παραβάσεων, την προστασίαν της υγείας ή της ηθικής, ή την προστασίαν των δικαιωμάτων και ελευθεριών άλλων.

Είναι φανερό ότι κατά τον χρόνο που δημιουργήθηκε και τέθηκε σε εφαρμογή το νομοθέτημα αυτό, δεν είχε διαφανεί ακόμα η ανάγκη ειδικότερης προστασίας των μεταδεδομένων.

4.2. Στο ευρωπαϊκό πεδίο

Η ρητή αναφορά και η μετάβαση από τον όρο αλληλογραφία στον όρο, επικοινωνία, επέρχεται με τον Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (ΧΘΔΕΕ) του 2000 και το άρθρο **7** το οποίο κατοχυρώνει με την σειρά του τον σεβασμό της ιδιωτικής και οικογενειακής ζωής. Η πληρέστερη προστασία της Ιδιωτικότητας στον τομέα των ηλεκτρονικών επικοινωνιών επέρχεται με την Οδηγία **2002/58/ΕΚ**[51] , γνωστή και ως e-Privacy Directive[52], η οποία καθιέρωσε το δικαίωμα στην ιδιωτική ζωή στον τομέα των ηλεκτρονικών επικοινωνιών, συμπεριλαμβάνοντας τόσο το περιεχόμενο όσο και κάθε άλλο δεδομένο στην έννοια του απορρήτου με τρόπο πανηγυρικό ήδη εκ προοιμίου, ανεξαρτήτως του εάν αφορούν άμεσα την επικοινωνία ή αν καταγράφονται αυτόματα κατά τη χρήση του τηλεπικοινωνιακού δικτύου. Πιο συγκεκριμένα, απαγόρευσε την ακρόαση, υποκλοπή, αποθήκευση ή άλλο είδος παρακολούθησης ή επιτήρησης των επικοινωνιών και των συναφών δεδομένων κίνησης από πρόσωπα πλην των χρηστών, υπό την επιφύλαξη του **άρθρο 15** παράγραφος **1,** δηλαδή επιτρέποντας ουσιαστικά στα κράτη τη λήψη μέτρων διατήρησης των δεδομένων αυτών (κίνησης και θέσης) για περιορισμένο χρονικό διάστημα εφόσον αυτά αποτελούν αναγκαίο, κατάλληλο και ανάλογο μέτρο σε

[51] Ενσωματώθηκε στην ελληνική έννομη τάξη με τον **Ν 3471/2006 (ΦΕΚ Α 133/28.06.2006)** «*Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (Ενσωμάτωση της Οδηγίας 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Ιουλίου 2002 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών»*.

[52] Στην χώρα μας ενσωματώθηκε με τον **Ν 3471/2006** (ΦΕΚ Α 133/28.06.2006) «*Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (Ενσωμάτωση της Οδηγίας 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Ιουλίου 2002 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών»*.

μια δημοκρατική κοινωνία. Ωστόσο, αρκετά 'ανοικτό' έμεινε το πεδίο της διατήρησης των δεδομένων, προβλέποντας την έννοια της *τεχνικής αποθήκευσης*, η οποία είναι αναγκαία για τη διαβίβαση επικοινωνίας. Στο αρ.15 της οδηγίας αυτής προβλέφθηκε η δυνατότητα των κρατών μελών να λαμβάνουν νομοθετικά μέτρα που θα προβλέπουν τη φύλαξη δεδομένων για ορισμένο χρονικό διάστημα για σκοπούς διαφύλαξης της **εθνικής ασφάλειας, της εθνικής άμυνας, της δημόσιας ασφάλειας, και για την πρόληψη, διερεύνηση, διαπίστωση και δίωξη ποινικών αδικημάτων** ή της άνευ αδείας χρησιμοποίησης του συστήματος ηλεκτρονικών επικοινωνιών, εφόσον ο περιορισμός αυτός τελεί υπό όρους αναλογικότητας σε μια δημοκρατική κοινωνία.

Το νομοθετικό αυτό 'τοπίο' σεβασμού της Ιδιωτικότητας και προστασίας της εμπιστευτικότητας όλου του φάσματος της επικοινωνίας φαίνεται να υποχωρεί το 2006 στον απόηχο των τρομοκρατικών επιθέσεων στη Μαδρίτη το 2004 και στο Λονδίνο το 2005, με τις ευρωπαϊκές κυβερνήσεις να αποφασίζουν την ενίσχυση των μηχανισμών εποπτείας των τηλεπικοινωνιών, συμπεριλαμβανομένης και της διατήρησης των μεταδεδομένων επικοινωνίας, προκειμένου να καταπολεμήσουν αποτελεσματικότερα την τρομοκρατία και το οργανωμένο έγκλημα.[53] Αυτό οδήγησε στην υιοθέτηση της Οδηγίας **2006/24/ΕΚ**[54] ***(Data Retention Directive)*** για τη διατήρηση δεδομένων, που παράγονται ή υποβάλλονται σε επεξεργασία κατά την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών.

Η Οδηγία υπήρξε ιδιαιτέρως παρεμβατική καθώς τροποποιώντας την Οδηγία **2002/58/ΕΚ,** προβλέφθηκε η υποχρεωτική προληπτική διατήρηση κι επεξεργασία των μεταδεδομένων επικοινωνίας όλων ανεξαιρέτως των χρηστών (άρθρο 3) και η μη διαγραφή τους από τους Παρόχους για χρονικό διάστημα από έξι μήνες έως δυο χρόνια (άρθρα 6 και 12) με σκοπό τη **διερεύνηση, διαπίστωση και δίωξη σοβαρών ποινικών αδικημάτων,** αφού κρίθηκε ότι η διατήρηση δεδομένων έχει

[53] Μπαντή-Μαρκούτη, Β. (2015), ό.π., σελ. 3

[54] **ΟΔΗΓΙΑ 2006/24/ΕΚ** ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 15ης Μαρτίου 2006 για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών και για την τροποποίηση της Οδηγίας 2002/58/ΕΚ

αποδειχθεί ότι αποτελεί αναγκαίο και αποτελεσματικό εργαλείο στα χέρια των υπηρεσιών επιβολής του νόμου, ιδίως σε σοβαρές υποθέσεις όπως το οργανωμένο έγκλημα και η τρομοκρατία (Αιτ. σκ. 9). Σύμφωνα μάλιστα με ρητή πρόβλεψη της Οδηγίας (άρθρο 1 παρ. 2 και 5 παρ. 2.), ορίστηκε ότι η υποχρέωση διατήρησης αφορά **αποκλειστικά και μόνο** στα **μεταδεδομένα επικοινωνίας.** Ο διαχωρισμός αυτός «εξωτερικών δεδομένων» επικοινωνίας και περιεχομένου της, ορθώς επικρίθηκε ως προσχηματικός. Εξαιτίας του αυστηρού γενικοπροληπτικού χαρακτήρα της διατήρησης μεταδεδομένων χωρίς διακρίσεις και ανάλογες σταθμίσεις, η Οδηγία κρίθηκε ανίσχυρη από το Δικαστήριο της Ευρωπαϊκής Ένωσης, δυνάμει της απόφασης Digital Rights Ireland, επαναφέροντας έτσι σε ισχύ το προηγούμενο νομοθετικό καθεστώς. Αξίζει να σημειωθεί εδώ, ότι η πλέον ακυρωθείσα Οδηγία είχε ενσωματωθεί στην ελληνική δικαιοταξία με τον Νόμο **3917/2011**[55]**,** ο οποίος είναι ακόμα εν ισχύ και εφαρμόζεται παρά την ακύρωση της, εφόσον δεν έχει υπάρξει σχετικός τροποποιητικός νόμος.

Στο ρευστό αυτό και κατακερματισμένο νομικό τοπίο, προτάθηκε το 2017 το νομοθετικό εργαλείο του Κανονισμού αυτή τη φορά, για τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες και την κατάργηση της οδηγίας 2002/58/ΕΚ (κανονισμός για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες) ή άλλως **e-Privacy Regulation,** ενώ στις 10-02-2021 ανακοινώθηκε η συμφωνία επ' αυτού, χωρίς ωστόσο ακόμα να έχει ψηφισθεί. Στο προταθέν σχέδιο Κανονισμού απαλείφεται ουσιαστικά η διάκριση μεταξύ περιεχομένου και δεδομένων κίνησης και θέσης, κυριαρχεί ο όρος **μεταδεδομένα** *(αντί του όρου δεδομένα κίνησης/θέσης)* ή δεδομένα ηλεκτρονικών επικοινωνιών, τα οποία <u>εν συνόλω συγκαταλέγονται και προστατεύονται από το απόρρητο της επικοινωνίας</u>. Είναι σημαντικό ότι ως προστατευόμενη επικοινωνία ορίζεται και αυτή που λαμβάνει χώρα μεταξύ διασυνδεδεμένων συσκευών όσο και μεταξύ μηχανών, υποδεικνύοντας ότι το διαδίκτυο των πραγμάτων (Internet of Things) δεν

[55] ΝΟΜΟΣ 3917 (ΦΕΚ 22/21.02.2011) «Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις»

εξαιρείται από αυτή. Η ρύθμιση αυτή είναι εξαιρετικά ουσιώδης καθώς ο αριθμός των συνδεδεμένων με το διαδίκτυο συσκευών παρουσιάζει αλματώδη αύξηση, ενώ παράγει πλήθος μεταδεδομένων, τα οποία σχετίζονται, ταυτοποιούν και αποκαλύπτουν πλήθος σημαντικών πληροφοριών για τους χρήστες τους. Καθίσταται σαφές λοιπόν ότι με τον εν λόγω Κανονισμό επιλύονται πολλά προβλήματα του παρελθόντος, ιδιαίτερα σχετικά με την εμμονή μέρους της ελληνικής νομολογίας[56] να πρεσβεύει την παρωχημένη θέση, σύμφωνα με την οποία τα μεταδεδομένα επικοινωνίας δεν υπάγονται στην προστασία του απορρήτου, αφού αυτό δήθεν προστατεύει μόνο το περιεχόμενο αυτής ή αν παύει το απόρρητο μετά το πέρας της επικοινωνίας. Στην πράξη δηλαδή, οι εισαγγελικοί λειτουργοί ενεργούν διακρίνοντας τα συνοδά («εξωτερικά») στοιχεία μιας επικοινωνίας («δεδομένα κίνησης και θέσης») από το περιεχόμενο αυτό καθαυτό, και κατά συνέπεια νομίμως ζητούνται από τους Παρόχους τα δεδομένα κίνησης, που συνοδεύουν την επικοινωνία με την συνήθη οδό της εισαγγελικής ή ανακριτικής παραγγελίας χωρίς να ακολουθηθεί η διαδικασία άρσης του απορρήτου. Η εμπιστευτικότητα των ψηφιακών δεδομένων έχει αναχθεί και θα ενισχυθεί έτι περισσότερο, όπως είδαμε παραπάνω, σε αυτοτελή έναντι του απορρήτου των επικοινωνιών ελευθερία, με αποτέλεσμα να προστατεύεται αυτοτελώς τόσο η ροή όσο και η διατήρησή τους είτε περιέχουν επικοινωνία με την στενή έννοια του όρου είτε όχι.[57]

‘Έτσι, η λογική της παραδοσιακής διάκρισης της ταχυδρομικής επικοινωνίας μεταξύ περιεχομένου και διεύθυνσης επί του φακέλου αλληλογραφίας, και η πεποίθηση ότι τα μεταδεδομένα επικοινωνίας διαφοροποιούνται από το περιεχόμενο αυτής ως προς το βαθμό προστασίας του απορρήτου, κρίνεται ως αναχρονιστική.

56

Βλ. ΓνμδΕισΑΠ 9/2009, 12/2009 και 9/2011, ΤΝΠ ΔΣΑ, αλλά και σε αποφάσεις του Αρείου Πάγου όπως η ΑΠ689/2014, ΤΝΠ ΔΣΑ

[57] Γκύζης Δ. (2023) Αντεισαγγελέας Εφετών, ‘Ψηφιακή ανακριτική πράξη’ Ηλεκτρονικό Έγκλημα (Ουσιαστικές και δικονομικές όψεις), NB σελ. 358

4.3. Σε εθνικό επίπεδο

Στην εθνική έννομη τάξη, το απόρρητο της επικοινωνίας κατοχυρώνεται στο **άρθρο 19 του Συντάγματος**, το οποίο ορίζει ότι «1. *Το απόρρητο των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο είναι* ***απόλυτα απαραβίαστο****. Νόμος ορίζει τις εγγυήσεις υπό τις οποίες η δικαστική αρχή* ***δεν*** *δεσμεύεται από το απόρρητο για λόγους εθνικής ασφάλειας ή για διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων.* ***2.*** *Νόμος ορίζει τα σχετικά με τη συγκρότηση, τη λειτουργία και τις αρμοδιότητες ανεξάρτητης αρχής που διασφαλίζει το απόρρητο της παραγράφου 1.* ***3.*** *Απαγορεύεται η χρήση αποδεικτικών μέσων που έχουν αποκτηθεί κατά παράβαση του άρθρου αυτού και των άρθρων 9 και 9Α».*

Νόμιμη ρωγμή στο «απόλυτα απαραβίαστο» του απορρήτου των επιστολών και της ελεύθερης επικοινωνίας αποτελεί η άρση μόνο υπό τις προϋποθέσεις, που ορίζει το δεύτερο εδάφιο της ανωτέρω συνταγματικής διάταξης, δηλαδή **μόνο για λόγους εθνικής ασφάλειας ή για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων**, τα οποία ορίζονται περιοριστικά στον εκτελεστικό του συγκεκριμένου άρθρου νόμο **2225/1994**[58], σε συνδυασμό με τις ταχθείσες εγγυήσεις της διαδικασίας άρσης του απορρήτου. Να σημειωθεί ότι προαπαιτούμενο για την ολοκλήρωση της διαδικασίας της άρσης του απορρήτου είναι η διενέργεια μιας ανακριτικής πράξης, ήτοι η έκδοση διάταξης άρσης του απορρήτου από το αρμόδιο δικαστικό συμβούλιο, ώστε να μη θίγεται η ιδιωτική ζωή και η προσωπικότητα του ατόμου, παρά μόνο στο μέτρο και για όσο χρονικό διάστημα είναι απολύτως αναγκαίο. Σε αυτό συμβάλλει, η ανεξάρτητη αρχή {εν προκειμένω η Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών (ΑΔΑΕ)} η οποία είναι ουσιαστικά επιφορτισμένη με την εποπτεία της τήρησης της απαιτούμενης

[58] Ν.2225/1994 (ΦΕΚ 121/20.07.1994) όπως συμπληρώθηκε από τον **Ν 5002/2022** *(ΦΕΚ Α' 228/09-12-2022)* «*Διαδικασία άρσης του απορρήτου των επικοινωνιών, κυβερνοασφάλεια και προστασία προσωπικών δεδομένων πολιτών*»**.**

διαδικασίας από τα δικαστικά συμβούλια και τους Παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών.[59]

5. ΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ (Internet Of Things) & ΨΗΦΙΑΚΗ ΕΓΚΛΗΜΑΤΟΛΟΓΙΑ ΣΕ ΠΕΡΙΒΑΛΛΟΝ IoT (IoT Forensics)

5.1 Ορισμός, σύντομο ιστορικό, κατηγορίες, ενδεικτικές εφαρμογές

Το «Διαδίκτυο των Πραγμάτων» ή άλλως «Internet Of Things»[60] είναι το μονοπάτι για τον 'έξυπνο κόσμο', από τις εκρηκτικότερες τεχνολογίες του 21ου αιώνα, οι οποίες αξιοποιώντας την πληροφορική και την τεχνολογία έχουν ως στόχο την διευκόλυνση και την βελτίωση της εμπειρίας του εκάστοτε τελικού χρήστη. Συγκεκριμένα, αποτελεί το δίκτυο επικοινωνίας πληθώρας συσκευών, οικιακών συσκευών, αυτοκινήτων καθώς και **κάθε αντικειμένου** που ενσωματώνει ηλεκτρονικά μέσα, λογισμικό, αισθητήρες και συνδεσιμότητα σε δίκτυο ώστε να επιτρέπεται η σύνδεση και η ανταλλαγή δεδομένων.[61] Η 'ευφυία' τους εντοπίζεται στο γεγονός ότι αυτές οι συσκευές δικτύου έχουν την ικανότητα να αντιλαμβάνονται και να συλλέγουν δεδομένα από τον κόσμο, τροφοδοτώντας εν συνεχεία το Διαδίκτυο (με τα συλλεχθέντα δεδομένα) όπου μπορούν να υποβληθούν σε επεξεργασία και να αναπτυχθούν για διάφορους σκοπούς.

[59] Μαρκόπουλος, Ν. (2018) 08-05-2018 «Η συνταγματική προστασία των εξωτερικών στοιχείων της επικοινωνίας», Πρακτικά Ημερίδας της Αρχής Διασφάλισης Απορρήτου Επικοινωνιών με θέμα Απόρρητο Επικοινωνιών – Σύγχρονες Προκλήσεις. Αθήνα,Α.Δ.Α.Ε., σελ. 65

[60] Άλλες τεχνικές ονομασίες του όρου που έχουν αναπτυχθεί κατά καιρούς, είναι **ubiquitous computing** (πανταχού παρούσα υπολογιστική χρήση), **tangible media** (απτά μέσα), **wearable computing** (φερόμενη υπολογιστική χρήση), **augmented reality** (επαυξημένη πραγματικότητα), **locative media** (τοπικά μέσα**), near-field communications** (επικοινωνία κοντινού πεδίου), **body-area networking** (δικτύωση με περιοχή σώματος), **proactive computing** (προληπτική υπολογιστική χρήση), **autonomic computing** (αυτόνομη υπολογιστική χρήση), **embodied virtuality** (ενσωματωμένη εικονικότητα)
Βλ. 'M. Scott Boone, Ubiquitous Computing, Virtual Worlds, and the Displacement of Property Right, 4 Journal of Law & Policy for the Information Society 2008, σ. 91 επ'

[61] Stergiou, C., Psannis, K. E., Kim, B. G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. Future Generation Computer Systems, 78, 964-975.

Ουσιαστικά, «κοινά αντικείμενα», όπως πχ φωτιστικά, τηλεοράσεις, ζυγαριά και πολλά άλλα, τα οποία διαθέτουν δυνατότητα συνδέσεως στο Διαδίκτυο, μετουσιώνονται σε ευφυή και γίνονται μέρος ενός δικτύου πραγμάτων. Κατ' αυτό τον τρόπο λειτουργεί ως **προέκταση του Διαδικτύου**, το οποίο επιτρέπει την επικοινωνία **μεταξύ ανθρώπων, διαδικασιών και πραγμάτων.**[62]

Ο νομικός ορισμός δε, ανευρίσκεται και στη νέα σχετική νομοθεσία, **Ν. 4961/2022**[63] περί *'αναδυόμενων τεχνολογιών πληροφορικής και επικοινωνιών'* και συγκεκριμένα στο άρθρο **31 παρ. 5** κατά το οποίο το **Διαδίκτυο των Πραγμάτων** είναι «*κάθε τεχνολογία η οποία: **α)** επιτρέπει σε συσκευές ή ομάδα διασυνδεδεμένων ή σχετιζόμενων συσκευών, μέσω της σύνδεσής τους με το διαδίκτυο, να εκτελούν, βάσει προγράμματος, αυτόματη επεξεργασία ψηφιακών δεδομένων, συμπεριλαμβανομένης της τεχνολογίας εκείνης που αφορά στη διασύνδεση φυσικών πραγμάτων, ιδίως συσκευών, οχημάτων και κτιρίων, με ηλεκτρονικά εξαρτήματα, λογισμικό, αισθητήρες (sensors), ελεγκτές ενεργοποίησης (actuators), ραδιοζεύξεις και σύνδεση δικτύου και **β)** επιτρέπει τη συλλογή και ανταλλαγή ψηφιακών δεδομένων, προκειμένου να προσφέρουν ποικίλες υπηρεσίες στους χρήστες, με ή χωρίς την ανθρώπινη συμμετοχή.*»

Σύμφωνα με την έκθεση δε της **Cisco για το 2016,** για την κατάσταση του IoT μέχρι το έτος **2030**, αναμένεται ότι πάνω από 500 δισεκατομμύρια θα συνδεθούν μέσω του Διαδικτύου, γεγονός που δείχνει ότι ο ανθρώπινος πληθυσμός έχει ήδη ξεπεραστεί από τον αριθμό των διασυνδεδεμένων συσκευών IoT.[64]

Η σύλληψη της ιδέας του 'Διαδικτύου των πραγμάτων' έγινε αρχικά το 1982, όταν ένα τροποποιημένο μηχάνημα αυτόματης πώλησης Coca-Cola στο Πανεπιστήμιο Carnegie Mellon έγινε η πρώτη συνδεδεμένη στο ARPANET συσκευή, η οποία ανέφερε το απόθεμά της και τη θερμοκρασία των φρεσκογεμισμένων ποτών

[62] Mattern, F., & Floerkemeier, C. (2010). *From the Internet of Computers to the Internet of Things* (pp. 242-259). Springer Berlin Heidelberg.

[63] Ν.4961/2022 " *Αναδυόμενες τεχνολογίες πληροφορικής και επικοινωνιών, ενίσχυση της ψηφιακής διακυβέρνησης και άλλες διατάξεις*» ΦΕΚ Α 146/27.7.2022

[64] Lutta, P., Sedky, M., Hassan, M., Jayawickrama, U., & Bastaki, B. B. (2021). The complexity of internet of things forensics: A state-of-the-art review. Forensic Science International: Digital Investigation, 38, 301210.

της,[65] ενώ η φράση 'Διαδίκτυο των Πραγμάτων' και η ιδέα προέκυψαν αρχικά σε μια ομιλία που δόθηκε από τον Peter T. Lewis τον Σεπτέμβριο του 1985 στην Ουάσιγκτον, DC, στο 15ο Ετήσιο Νομοθετικό Σαββατοκύριακο του Ιδρύματος Μαύρων Κογκρέσου[66] Σύμφωνα λοιπόν με τον Lewis, το Διαδίκτυο των Πραγμάτων, είναι «*η ενοποίηση ανθρώπων, διαδικασιών και τεχνολογίας με συνδεόμενες συσκευές και αισθητήρες για να καταστεί* ***δυνατή η απομακρυσμένη παρακολούθηση****, η κατάσταση, η τροποποίηση και η αξιολόγηση τάσεων τέτοιων πραγμάτων*». Λίγο καιρό αργότερα, το 1999, ο Kevin Ashton της Procter & Gamble, και μετέπειτα του MIT επινόησε τη φράση "Internet of Things"[67] ενώ αυτή καθιερώθηκε όταν η Gartner πρόσθεσε το IoT στη λίστα με τις νέες αναδυόμενες τεχνολογίες το **2011**, αποκτώντας έκτοτε παγκόσμια δυναμική.

Οι βασικές κατηγορίες του Διαδικτύου των Πραγμάτων είναι το **IIoT** (Industrial Internet Of Things) και το **CIoT** (Consumer Internet Of Things), δηλαδή το Βιομηχανικό και το Καταναλωτικό Διαδίκτυο των Πραγμάτων αντίστοιχα.[68] Το Βιομηχανικό Διαδίκτυο των Πραγμάτων (IIoT), αξιοποιεί την μηχανική μάθηση και την τεχνολογία μεγάλων δεδομένων για να επεξεργάζεται τα δεδομένα των αισθητήρων, σε συνδυασμό με τις τεχνολογίες αυτοματισμού, αυξάνοντας έτσι την αποτελεσματικότητα και την παραγωγικότητα μιας επιχείρησης. Από την άλλη το Καταναλωτικό Διαδίκτυο των Πραγμάτων CIoT, απευθύνεται σε μεμονωμένα άτομα ή μικρές ομάδες ατόμων, προσφέροντας σε αυτούς άνεση, ασφάλεια, ποιότητα, ευκολία και αποτελεσματικότητα στην καθημερινότητα τους.

Ενδεικτικά, από τις βασικότερες εφαρμογές του IoT, αποτελούν: ***α)*** αισθητήρες αναφορικά με δεδομένα υγείας που καταμετρούν δεδομένα του σώματος και είναι δημοφιλείς σε χρήστες που επιθυμούν να ελέγχουν τα δεδομένα αναφορικά με τις συνήθειές τους και τον τρόπο ζωής τους**. Β)** συσκευές που φοράει ο χρήστης (φερόμενες συσκευές) αντικαθιστώντας υπάρχοντα αντικείμενα, όπως ρολόγια και γυαλιά **γ)** συσκευές οικιακού αυτοματισμού που χρησιμοποιούνται για την

[65] https://www.ibm.com/blog/little-known-story-first-iot-device/
[66] CHETAN SHARMA, *«CORRECTING THE IOT HISTORY», 2016*
http://www.chetansharma.com/correcting-the-iot-history
[67] Ζιώγου, Α. (2023). Τεχνητή νοημοσύνη στο Διαδίκτυο των Πραγμάτων.
[68] https://www.cloudcredential.org/blog/knowledge-byte-the-different-types-of-iot/

αυτοματοποίηση εργασιών στο σπίτι ή για τον εξ αποστάσεως έλεγχο του οικιακού περιβάλλοντος.[69] Επίσης σχετικές εφαρμογές που αυτοματοποιούν και βελτιώνουν εργασίες σε πολλούς άλλους τομείς όπως στην υγειονομική περίθαλψη (πχ ιατρικοί αισθητήρες οι οποίοι συλλέγουν αυτόματα μετρήσεις υγείας, όπως οξυγόνο, γλυκόζη, καρδιακούς παλμούς, αρτηριακή πίεση, θερμοκρασία αλλά και αισθητήρες που εμφυτεύονται **μέσα στο σώμα**, όταν η υγεία των ασθενών πρέπει να παρακολουθείται συνεχώς).

Στην βιομηχανία , στις εφοδιαστικές αλυσίδες, στις μεταφορές, στον στρατό {Internet of Military Things (IoMT) ή το Internet of Battlefield Things (IoBT)}[70], στις έξυπνες πόλεις, είναι μόνο μερικά παραδείγματα όπου το Διαδίκτυο των Πραγμάτων ανθεί.

5.2 Εγκληματολογία σε περιβάλλον IoT (Internet Forensics)

Η εγκληματολογική έρευνα στο 'Διαδίκτυο των Πραγμάτων', είναι μια από τις υποκατηγορίες, όψεις της ψηφιακής εγκληματολογικής έρευνας, που εστιάζει στο οικοσύστημα του Διαδικτύου των Πραγμάτων (ΔτΠ) για την εξεύρεση ψηφιακού αποδεικτικού υλικού για σκοπούς εξιχνίασης εγκλημάτων, συσχέτισης ψηφιακών 'αποτυπωμάτων' με φυσικά πρόσωπα και απόδοσης ευθυνών (cyber attribution) με τρόπο σύννομο και παραδεκτό. Η βασικότερη ίσως διαφορά με την ψηφιακή εγκληματολογία *(της οποίας αποτελεί και εξειδίκευση)* εντοπίζεται στην **πηγή των ψηφιακών δεδομένων**, καθώς στο IoT είναι ευρύτατη και από πολυάριθμες και διαφορετικές πηγές. Είναι προφανές ότι οι νέες αυτές πηγές των δεδομένων, επεκτείνουν τρόπον τινά τα όρια μιας σκηνής εγκλήματος, αφού πλέον καταγράφονται συμβάντα (αυτόματα τις περισσότερες φορές μέσω των αισθητήρων, ενεργοποιητών των 'έξυπνων συσκευών' κτλ.) από το φυσικό περιβάλλον που δεν καταγραφόταν προηγουμένως ή ακόμα και αν καταγραφόταν ήταν πολύ πιο εύκολο να αλλοιωθούν σκοπίμως από τον δράστη. Η δυσκολία αλλοίωσης έγκειται, όπως θα αναλυθεί και παρακάτω, στον

[69] Φερενίκη Παναγοπούλου-Κουτνατζή, ΔiΜΕΕ, 3/2014, σελ. 346 - 358

[70] Kott, A., Swami, A., & West, B. J. (2016). The internet of battle things. Computer, 49(12), 70-75.

αποκεντρωμένο χαρακτήρα των συσκευών αυτών και την έντονη εξάρτηση τους από την νεφοϋπολογιστική *(Cloud Computing)* .

Πέρα από το πλούσιο αποδεικτικό υλικό, λόγω της ποικιλίας και της ποσότητας των δεδομένων που παράγουν τέτοιου είδους συσκευές υπό την έννοια, ότι περιλαμβάνονται σε αυτές πληθώρα μεταδεδομένων ή λοιπών δεδομένων που περιγράφουν και συγκεκριμενοποιούν τις ψηφιακές αποδείξεις, είναι εξαιρετικά σημαντικό να υπογραμμισθεί ότι είναι και πιο εύκολα διαχειρίσιμες, τόσο ως προς την αναζήτηση, το φιλτράρισμα όσο και ως προς την μεταξύ τους συσχέτιση. Κατ' αυτό τον τρόπο, τα αποδεικτικά στοιχεία που προσφέρει το IoT είναι πολύ πιο αξιόπιστα συγκριτικά με παραδοσιακές πηγές (λχ μάρτυρες).[71]

5.3 Κατηγοριοποίηση του IoT forensics με γνώμονα την πηγή δεδομένων| Πολυεπίπεδη Πηγή Δεδομένων

Σύμφωνα με τους συγγραφείς (Zawoad and Hasan), η εγκληματολογία του IoT απαρτίζεται από τρία ψηφιακά εγκληματολογικά επίπεδα:[72]

1. Εγκληματολογία σε επίπεδο «έξυπνης» συσκευής (device level forensics): Η εγκληματολογία σε αυτό το επίπεδο περιλαμβάνει την συλλογή δεδομένων από την **τοπική μνήμη των συσκευών** του Διαδικτύου των πραγμάτων, όπως γραφικά, ήχο, βίντεο κ.α. με χαρακτηριστικότερα παραδείγματα τα βίντεο και τα γραφικά από μια κάμερα CCTV *(Closed Circuit TV/Κλειστό Κύκλωμα Τηλεόρασης)* ή ήχους από το Amazon Echo.

2. Εγκληματολογία σε επίπεδο Δικτύου (network forensics): Σε αυτό το επίπεδο **εξάγονται** και **αναλύονται** τα **αρχεία καταγραφής δικτύου**. Συγκεκριμένα, περιλαμβάνονται όλα τα είδη δικτύων που οι έξυπνες συσκευές χρησιμοποιούν

[71] Lutta, P., Sedky, M., Hassan, M., Jayawickrama, U., & Bastaki, B. B. (2021). The complexity of internet of things forensics: A state-of-the-art review. *Forensic Science International: Digital Investigation*, *38*, 301210.

[72] Alabdulsalam, S., Schaefer, K., Kechadi, T., & Le-Khac, N. A. (2018). Internet of things forensics–challenges and a case study. In Advances in Digital Forensics XIV: 14th IFIP WG 11.9 International Conference, New Delhi, India, January 3-5, 2018, Revised Selected Papers 14 (pp. 35-48). Springer International Publishing.

για την αποστολή και λήψη δεδομένων. Στις περισσότερες περιπτώσεις είναι οικιακά δίκτυα, βιομηχανικά δίκτυα, LAN,[73] WAN[74], MAN[75].

Για παράδειγμα, εάν συμβεί ένα περιστατικό (ασφαλείας συνήθως) στις συσκευές IoT, όλα τα αρχεία καταγραφής που αφορούν την ροή της κυκλοφορίας (traffic data), θα μπορούσαν να είναι πιθανά αποδεικτικά στοιχεία, όπως τα firewalls ή τα αρχεία καταγραφής IDS (Intrusion Detection System).

3. Εγκληματολογία σε επίπεδο νεφοϋπολογιστικής (cloud forensics):

Στο τρίτο αυτό και τελευταίο επίπεδο, περιλαμβάνεται η **ανάλυση των δεδομένων** που **δημιουργούνται** και **αποθηκεύονται** από συσκευές IoT στις υπηρεσίες Cloud. Οι υπηρεσίες νεφοϋπολογιστικής διαδραματίζουν κομβικό ρόλο στις λειτουργίες του Διαδικτύου των πραγμάτων και αυτό διότι οι συσκευές IoT έχουν χαμηλή χωρητικότητα αποθήκευσης και υπολογιστικής ικανότητας με αποτέλεσμα να εξαρτώνται σε μεγάλο βαθμό από το Cloud[76], **είτε ως βάση του δικτύου είτε ως συμπλήρωμα**. Τα οφέλη που προσφέρουν οι υπηρεσίες Cloud είναι η ευκολία, η μεγάλη χωρητικότητα, η επεκτασιμότητα και προσβασιμότητα κατ' απαίτηση, όταν και όποτε χρειάζεται.

Οι προκλήσεις της ψηφιακής εγκληματολογίας σε περιβάλλον Cloud, είναι πολλές και θα αναλυθούν εκτενέστερα και σε επόμενο κεφάλαιο, αξίζει ωστόσο να σημειωθεί-έστω και επιγραμματικά εδώ- ότι οι κυριότερες από αυτές εστιάζονται στην **ανωνυμία** που αυτό (το νέφος) παρέχει στους χρήστες με αποτέλεσμα την **αδυναμία ταυτοποίησης** δραστών, στην **τοποθεσία των αποθηκευμένων δεδομένων,** και στην **έλλειψη ασφάλειας** αυτών.

5.4 Προκλήσεις της ψηφιακής εγκληματολογίας στο Διαδίκτυο των πραγμάτων

Η ποικιλομορφία των δεδομένων, ο πολυεπίπεδος χαρακτήρας και τα λοιπά ιδιαίτερα χαρακτηριστικά του οικοσυστήματος του Διαδικτύου των πραγμάτων, πυροδοτούν πλήθος προκλήσεων για την σύννομη διεξαγωγή της

[73] Τοπικό δίκτυο υπολογιστών (Local Area Network) Πηγή:Wikipedia.org
[74] Δίκτυο Ευρείας Περιοχής (Wide Area Network) Πηγή:Wikipedia.org
[75] Metropolitan Area Networks Πηγή: Wikipedia.org
[76] Lutta, P., Sedky, M., Hassan, M., Jayawickrama, U., & Bastaki, B. B. (2021). The complexity of internet of things forensics: A state-of-the-art review. *Forensic Science International: Digital Investigation*, *38*, 301210.

εγκληματολογίας σε αυτό. Μια απόπειρα συστηματοποίησης των προκλήσεων αυτών, μπορεί να συνδράμει στην καλύτερη θέαση των προβληματικών σημείων και πιθανών λύσεων για την αντιμετώπιση τους. Έτσι οι προκλήσεις με τις οποίες έρχονται αντιμέτωποι οι ψηφιακοί ερευνητές αλλά και η επιστημονική κοινότητα, συνοψίζονται σε **τεχνικές**, **λειτουργικές**, **νομικές** και **ερευνητικές**.[77]

5.4.1 Τεχνικές Προκλήσεις

Κατά την διάρκεια μιας εγκληματολογικής έρευνας διασταυρώνονται διαφορετικοί τύποι τεχνικών προκλήσεων, που απαιτούν την αντιμετώπιση τόσο κρυπτογραφημένων όσο και μη κρυπτογραφημένων δεδομένων.
Στους διαφορετικούς αυτούς τύπους περιλαμβάνονται το **μέγεθο**ς των δεδομένων, η **θέση** τους, η **απόκρυψη ή διαγραφή** αυτών, τα **εργαλεία** και οι **τεχνικές** που στρέφονται κατά της εγκληματολογικής έρευνας και η **ασυμβατότητα εγκληματολογικών εργαλείων**, που μπορούν να οδηγήσουν σε παρεμπόδιση της έρευνας ή υπερβολική κατανάλωση πόρων και χρόνου.

- *Κρυπτογραφικές προκλήσεις:* Το επίπεδο κρυπτογράφησης διαδραματίζει ουσιαστικό ρόλο στην πορεία μιας ψηφιακής έρευνας. Στην πράξη οι δράστες κυβερνοεγκλημάτων, χρησιμοποιούν την κρυπτογράφηση για να διατηρήσουν το απόρρητο των δεδομένων τους και να αποφύγουν μια πιθανή σύλληψη, καθιστώντας πολλές φορές σχεδόν αδύνατη την αποκρυπτογράφηση από τους σχετικούς εγκληματολόγους.

- *Μέγεθος δεδομένων:* Μια ακόμη τεχνική πρόκληση σχετίζεται με το μέγεθος των δεδομένων (μικρά, μεσαία, μεγάλα δεδομένα-Big Data)[78] που πρέπει να ανακτηθούν πέρα από τον όγκο, την φύση και τον τύπο τους. Εδώ συγκαταλέγεται επίσης, η αναζήτηση του ποια δεδομένα μπορούν να

[77]. Yaacoub, J. P. A., Noura, H. N., Salman, O., & Chehab, A. (2022). Advanced digital forensics and anti-digital forensics for IoT systems: Techniques, limitations and recommendations. *Internet of Things*, *19*, 100544.

[78] Cardenas, A. A., Manadhata, P. K., & Rajan, S. P. (2013). Big data analytics for security. *IEEE Security & Privacy*, *11*(6), 74-76.

χρησιμοποιηθούν ως αποδεικτικά στοιχεία, προσδιορίζοντας ουσιαστικά ποια είναι συναφή με την έρευνα και ποια δεν εξυπηρετούν κανένα σκοπό. Ως εκ τούτου, οι δράστες του Κυβερνοχώρου μεθοδευμένα «καλύπτουν» τα ψηφιακά τους ίχνη, αφήνοντας πίσω δεδομένα που δεν εξυπηρετούν κανένα σκοπό, ώστε να χάνεται πολύτιμος χρόνος από τους ερευνητές.

- *Τοποθεσία δεδομένων:* Ο εντοπισμός της τοποθεσίας των δυνητικών αποδεικτικών στοιχείων, είναι έργο εξαιρετικά δυσχερές, καθώς δεν είναι πάντα εφικτό να γνωρίζουμε που είναι αποθηκευμένα ή που βρίσκονται τα δεδομένα. Σε αυτό άλλωστε συμβάλλει και το γεγονός ότι οι χάκερς χρησιμοποιούν VPN[79], proxies[80] και TOR[81] για να επιτίθενται ανώνυμα χωρίς να αφήνουν ίχνη, περιορίζοντας έτσι σημαντικά το ερευνητικό πεδίο των αποδεικτικών στοιχείων από μέρους των εγκληματολόγων.

- *Απόκρυψη δεδομένων:* Η απόκρυψη δεδομένων είναι μια ακόμα δημοφιλής τεχνική των δραστών η οποία βασίζεται στην **στεγανογραφία** ενώ μια ακόμα μέθοδος που χρησιμοποιούν βασίζεται σε απόκρυψη των δεδομένων τους σε RAM, έτσι ώστε μόλις απενεργοποιηθεί η τροφοδοσία, της συσκευής τα δεδομένα να χαθούν ολοσχερώς χωρίς δυνατότητα ανάκτησης από τους εγκληματολόγους.[82]

- *Εργαλεία κατά της εγκληματολογίας ή Αντίστροφη Ψηφιακή Εγκληματολογία (**Anti-Forensics**):* Πρόκειται για οποιαδήποτε προσπάθεια υπονομεύει την διαθεσιμότητα ή χρησιμότητα των αποδεικτικών στοιχείων στην εγκληματολογική διαδικασία από μέρους

[79] **Virtual Private Network** (εικονικό ιδιωτικό δίκτυο)
[80] **Proxy Server**: Διακομιστής Μεσολάβησης, βασικό εργαλείο ανωνυμίας κατά την περιήγηση στο Διαδίκτυο, λειτουργώντας ως ενδιάμεσος μεταξύ της συσκευής ενός χρήστη και του διακομιστή ενός ιστοτόπου ή εφαρμογής που επισκέπτεται ο εκάστοτε χρήστης. Πηγή: Texnologia.net https://texnologia.net/
[81] **T**he **O**nion **R**outer: λογισμικό απόκρυψης της τοποθεσίας ενός χρήστη ή/και της διαδικτυακής του κίνησης. (Wikipedia.org) https://en.wikipedia.org/wiki/Tor_(network)
[82] Yaacoub, J. P. A., Noura, H. N., Salman, O., & Chehab, A. (2022). Advanced digital forensics and anti-digital forensics for IoT systems: Techniques, limitations and recommendations. *Internet of Things*, *19*, 100544.

των δραστών και βασίζεται κατά κύριο λόγο στην ανάπτυξη εργαλείων και διαδικασιών που στοχεύουν στην καταστροφή ή απόκρυψη πειστηρίων, στην εξάλειψη των πηγών των πειστηρίων και την παραποίηση αυτών προκειμένου να παραπλανηθεί ο ψηφιακός ερευνητής.[83]

- *Ασυμβατότητα των παραδοσιακών εγκληματολογικών εργαλείων:* Καθώς οι διάφορες έξυπνες συσκευές εμφανίζουν διαφορές στα λειτουργικά τους συστήματα, στα πρότυπα επικοινωνίας τους,[84] και εν γένει στις τεχνολογίες που χρησιμοποιούν, τα παραδοσιακά εγκληματολογικά εργαλεία, καθίστανται αναποτελεσματικά στην αντιμετώπιση διαφορετικών τύπων συσκευών, καθιστώντας έτσι οποιαδήποτε διαδικασία ανάκτησης δεδομένων από αυτά, ιδιαιτέρως δύσκολη και χρονοβόρα έως και αδύνατη.

- *Αποθήκευση δεδομένων στο Cloud:* Εξαιτίας της άμεσης εξάρτησης των συσκευών IoT από το Cloud, τα δεδομένα μετακινούνται και ανατίθενται ουσιαστικά στην ευχέρεια και δικαιοδοσία τρίτων (των Παρόχων υπηρεσιών νεφοϋπολογιστικής), ενώ είναι δυνατό να μεταφερθούν και σε διαφορετικές χώρες με ό,τι αυτό μπορεί να συνεπάγεται για την νομική τους μεταχείριση (*καθώς διαφορετικές χώρες επιβάλλουν και διαφορετικούς κανονισμούς ως προς τις υποχρεώσεις των Παρόχων σε ένα πιθανό ένταλμα για έρευνα, απόδοση των αποθηκευμένων σε αυτόν, δεδομένων, διαφορετική προσέγγιση επί του αξιοποίνου μιας πράξης κτλ.*) περιπλέκοντας σημαντικά την εγκληματολογική έρευνα.

[83] Αναστασίου, Ι. (2019). Ψηφιακή εγκληματολογία και ανάλυση σε κινητές συσκευές (Doctoral dissertation, University of Piraeus (Greece)).

[84] Alabdulsalam, S., Schaefer, K., Kechadi, T., & Le-Khac, N. A. (2018). Internet of things forensics–challenges and a case study. In *Advances in Digital Forensics XIV: 14th IFIP WG 11.9 International Conference, New Delhi, India, January 3-5, 2018, Revised Selected Papers 14* (pp. 35-48). Springer International Publishing.

5.4.2 Λειτουργικές Προκλήσεις

Πέρα από τις τεχνικές προκλήσεις, οι επιχειρησιακές προκλήσεις αποτελούν μια ακόμη «απειλή» για την ομαλή διεξαγωγή μιας ψηφιακής εγκληματολογικής έρευνας. Αυτό οφείλεται κυρίως στην **έλλειψη διαχείρισης περιστατικών**, στην **έλλειψη τυποποιημένων διαδικασιών** και στην **έλλειψη «ετοιμότητας»** της εγκληματολογίας.

- *Έλλειψη διαχείρισης περιστατικών*[85]*:* Η έλλειψη διαχείρισης περιστατικών συνίσταται κυρίως στην **έλλειψη εντοπισμού**, **ανταπόκρισης** και **πρόληψης** των περιστατικών. Με άλλα λόγια οι ερευνητές της ψηφιακής εγκληματολογίας δεν είναι πάντα σε θέση να εντοπίσουν οποιοδήποτε περιστατικό ή ακόμα και αν καταφέρουν να το εντοπίσουν, πολλές φορές καθίσταται αδύνατο να ανταποκριθούν έγκαιρα σε αυτό ή δεν έχουν καθόλου την δυνατότητα να ανταποκριθούν. Σε αυτό προστίθεται και η έλλειψη **προληπτικών εγκληματολογικών εργαλείων,** τα οποία μπορεί να προλάβαιναν τα περιστατικά εν τη γενέσει τους.

- *Έλλειψη τυποποιημένων διαδικασιών:* Λόγω της έλλειψης συγκεκριμένης ή/και ομοιόμορφης μεθοδολογίας τόσο των διαδικασιών όσο και των πολιτικών της ψηφιακής δικανικής, οι ερευνητές αντιμετωπίζουν δυσκολίες σχετικά με τον 'ενδεδειγμένο' τρόπο αντίδρασης τους σε κάθε περιστατικό.

- *Έλλειψη ετοιμότητας της εγκληματολογίας:* Είναι προφανές ότι η έλλειψη διαχείρισης περιστατικών και διαδικασιών, μοιραία οδηγούν και στην δυσκολία να προβλεφθεί ή και να εφαρμοστεί στην πράξη **«προληπτική»** εγκληματολογία έτσι ώστε να αντιμετωπίζεται έγκαιρα κάθε ψηφιακή σκηνή εγκλήματος και να ανακτώνται όσο το δυνατόν περισσότερα ψηφιακά αποδεικτικά στοιχεία.

[85] Yaacoub, J. P. A., Noura, H. N., Salman, O., & Chehab, A. (2022). Advanced digital forensics and anti-digital forensics for IoT systems: Techniques, limitations and recommendations. *Internet of Things*, *19*, 100544.

5.4.3 Νομικές Προκλήσεις

Ίσως το πιο ακανθώδες και προβληματικό πεδίο κατά την διεξαγωγή μια ψηφιακής εγκληματολογικής έρευνας και δη σε ένα (ακόμα τουλάχιστον) σχεδόν αχαρτογράφητο και πολύπλοκο περιβάλλον, όπως αυτό του Διαδικτύου των Πραγμάτων, αποτελεί η νομική όψη αντιμετώπισης περιστατικών.

- Αυτό οφείλεται κατά βάση στο **κατακερματισμένο νομικό πλαίσιο** διεξαγωγής ανακριτικών ερευνών, που δεν επιτρέπει την ομοιόμορφη και κοινή αντιμετώπιση των σχετικών εγκλημάτων του Κυβερνοχώρου και όχι μόνο, μεταξύ των κρατών με αποτέλεσμα κάθε ερευνητική διαδικασία να καθίσταται δυσκίνητη και χρονοβόρα.

- Κομβικής σημασίας είναι και το ζήτημα της **πολυδικαιοδοσίας** των δεδομένων, ιδιαιτέρως λόγω της εξάρτησης από τις υπηρεσίες νεφοϋπολογιστικής, που όπως ήδη έχει υπογραμμισθεί, τα παραγόμενα δεδομένα από μια έξυπνη συσκευή δύναται να επεξεργάζονται σε άλλη χώρα, και να αποθηκεύονται σε διαφορετική χώρα.

- Οι σημαντικότερες ίσως νομικές προκλήσεις εστιάζονται στην κατάρριψη οποιασδήποτε έννοιας **ιδιωτικότητας** των χρηστών των έξυπνων συσκευών, καθώς αυτοί φαίνεται να βρίσκονται <u>υπό αέναη</u>, <u>μη ελεγχόμενη</u> και <u>άγνωστη επιτήρηση</u> τόσο από την κρατική σφαίρα όσο και από ιδιώτες (Παρόχους cloud) [86] καθώς δεν υπάρχει επαρκής και διαφανής ενημέρωση για την καταγραφή των δεδομένων των χρηστών από τις συσκευές ΔτΠ.

  Τα σύνολα δεδομένων δε, είναι τις περισσότερες φορές ευαίσθητα (καρδιακοί παλμοί, θερμοκρασία σώματος κτλ.) ενώ και η **ιδιοκτησία** των

[86] Παναγοπούλου-Κουτνατζή, Φ. (2014). Διαδίκτυο των πραγμάτων (Internet of Things-IoT): Αποικισμός της καθημερινής ζωής ή νέα τεχνολογική πρόκληση. ΔiΜΕΕ, 3/2014, 346-358.

παραγόμενων δεδομένων κρίνεται δυσδιάκριτη (*πχ στην περίπτωση ενός 'έξυπνου αυτοκινήτου' τα δεδομένα που παράγονται από αυτό θεωρούνται κατά την ισχύουσα θεωρία ότι ανήκουν στην εταιρία που παρήγαγε το αυτοκίνητο αυτό*). Έτσι, παρόλο που ο καταναλωτής έχει την κυριότητα του αυτοκινήτου, τα δεδομένα που συγκεντρώνονται μέσω του οχήματος, δεν του αποδίδονται απευθείας, εν αντιθέσει με τα δικαιώματα στην πρόσβαση, στη χρήση και την καταστροφή των δεδομένων.[87]

- Ιδιαίτερο προβληματισμό εγείρουν και τα κενά **ασφαλείας** των συσκευών του οικοσυστήματος του ΔτΠ, καθώς εφόσον πρόκειται για μια καταναλωτική τεχνολογία, δίνεται έμφαση πρωτίστως στην **μείωση του κόστους** και του **μεγέθους τους**, την **μεγαλύτερη αυτονομία** τους και συνακόλουθα **χρηστικότητα** τους, <u>όχι όμως και στην ασφάλεια τους</u>.

5.4.4 Ερευνητικές Προκλήσεις

Σε ερευνητικό επίπεδο, πολλά είναι τα 'ανοικτά ζητήματα' που ακόμα αναζητούν λύσεις σε αυτό το ταχέως εξελισσόμενο κλάδο της ψηφιακής εγκληματολογικής έρευνας, με τα κυριότερα να αποτελούν την έλλειψη εξειδικευμένης τεχνογνωσίας τόσο από τους ερευνητές εγκληματολόγους όσο και από τα λοιπά εμπλεκόμενα μέρη όπως διωκτικές αρχές και δικαστές. Η έλλειψη μεθοδολογίας και 'επιστημονικοποίησης' της ψηφιακής έρευνας σε συνδυασμό με την έλλειψη τυποποίησης σύγχρονων εγκληματολογικών εργαλείων που θα ανταποκρίνονται στις υπάρχουσες ανάγκες και συνακόλουθα η έλλειψη σχετικών δεξιοτήτων από μέρους των εμπλεκομένων, είναι ζητήματα που χρήζουν προτεραιοποίησης αλλά και ενίσχυσης από αρμόδιους φορείς , ώστε να μην φαλκιδεύεται η αξιοπιστία της ψηφιακής εγκληματολογικής έρευνας και η συνεισφορά της.

[87] Μιχαηλάκη, Α. (2021). Δίκαιο και δεοντολογία στις εφαρμογές της επαυξημένης πραγματικότητας: τεχνολογικές προεκτάσεις και προβληματισμοί (Doctoral dissertation, Ιόνιο Πανεπιστήμιο. Σχολή Επιστήμης της Πληροφορίας και Πληροφορικής. Τμήμα Αρχειονομίας, Βιβλιοθηκονομίας και Μουσειολογίας).

5.5 Προτεινόμενες εγκληματολογικές διαδικασίες/μεθοδολογίες σε περιβάλλον ΔτΠ

Έχουν διατυπωθεί και προταθεί κατά καιρούς διάφορες μεθοδολογίες για την διεξαγωγή εγκληματολογικής έρευνας στο απαιτητικό οικοσύστημα του Διαδικτύου των Πραγμάτων, οι περισσότερες από τις οποίες φαίνονται να είναι επαρκείς σε κάποιο βαθμό αλλά όχι τόσο ολοκληρωμένες και σίγουρα όχι τόσο εμπειρικά δοκιμασμένες ώστε να είναι αξιόπιστες. Ενδεικτικά ως ακολούθως:

5.5.1 Next Big Thing

Το προταθέν αυτό μοντέλο αναπτύχθηκε από τους **Oriwoh et al,**[88] οι οποίοι προτείνουν ένα διαδικαστικό μοντέλο που εδράζεται περισσότερο στις προκλήσεις που εντοπίζονται κυρίως κατά την φάση της αναγνώρισης κατά την διεξαγωγή μιας ψηφιακής έρευνας σε περιβάλλον IoT. Σχεδιάστηκε για να συνδράμει στον προσδιορισμό πιθανών πηγών αποδεικτικών στοιχείων. Υπογραμμίζει την ανάγκη διάκρισης σε τρεις (3) ζώνες, όπου η **πρώτη ζώνη** αποτελείται από τον εμπλεκόμενο και φερόμενο δράστη, η **δεύτερη ζώνη** καλύπτει όλες τις πιθανές συσκευές εντός του δικτύου (δρομολογητές, firewalls, συστήματα ανίχνευσης εισβολής-IDS,κτλ.) ενώ η **τρίτη ζώνη** καλύπτει τις συσκευές και υπηρεσίες εκτός του δικτύου (διακομιστές ιστού, cloud κτλ).[89]

Βάσει αυτού του μοντέλου λαμβάνεται υπόψη ότι τυχόν αποδεικτικά στοιχεία που είναι αποθηκευμένα στις συσκευές θα μπορούσαν εύκολα να χαθούν, παραβιαστούν ή και να καταστραφούν. Με γνώμονα αυτό, άλλα στοιχεία εντός του οικοσυστήματος IoT που σχετίζονται με αποδεικτικά στοιχεία πρέπει να εντοπίζονται έγκαιρα από τον ερευνητή. Η διαδικασία αυτή φαίνεται να είναι επωφελής για το στάδιο της ταυτοποίησης, ωστόσο χωλαίνει στο ότι θεωρεί δεδομένο ότι ο ερευνητής θα έχει άμεση πρόσβαση σε όλες τις συσκευές και στους διακομιστές του Νέφους.

[88] Oriwoh, E., Jazani, D., Epiphaniou, G., & Sant, P. (2013, October). Internet of things forensics: Challenges and approaches. In 9th IEEE International Conference on Collaborative computing: networking, Applications and Worksharing (pp. 608-615). IEEE.

[89] Lutta, P., Sedky, M., Hassan, M., Jayawickrama, U., & Bastaki, B. B. (2021). The complexity of internet of things forensics: A state-of-the-art review. *Forensic Science International: Digital Investigation*, *38*, 301210.

5.5.2 Standard Operational Procedures (SOPs)[90]

Στην ίδια λογική του Next Big Thing κινήθηκαν και οι **Perumal et al,**[91] επικεντρώνοντας την προσπάθεια τους στην προσέγγιση του 'από πάνω προς τα κάτω', μέσω καθορισμένων τυποποιημένων λειτουργικών διαδικασιών. Η ιδέα των ζωνών 1-2-3 παραμένει και εδώ με την διαφορά ότι δίνεται έμφαση στην εξεύρεση λύσης σχετικά με την διατήρηση των 'ασταθών' δεδομένων μέσω της αυτοματοποίησης των εν λόγω διαδικασιών, η οποία αν και βοηθητική σαν λύση δεν έχει ακόμα δοκιμαστεί στην πράξη για να αξιολογηθεί κατά πόσο είναι εφικτή.

5.5.3 Last on Scene (LoS)

Ο εν λόγω αλγόριθμος εκκινεί και πάλι από το μοντέλο Next Big Thing και προτάθηκε από τους **Harbawi and Varol,**[92] μετατοπίζοντας το κέντρο βάρους της έρευνας τους στην θέση των αποδεικτικών στοιχείων με τέτοιο τρόπο ώστε η πρώτη συσκευή που θα διερευνηθεί να είναι αυτή που εμφανίστηκε και τελευταία στην σκηνή του εγκλήματος. Σύμφωνα με τους συντάκτες του μοντέλου αυτού, εξοικονομείται χρόνος και πόροι από τους εγκληματολόγους, καθώς αναζητούνται μόνο δεδομένα ενδιαφέροντος, τα οποία αν βρεθούν στην πρώτη ζώνη, η διαδικασία ολοκληρώνεται και συντάσσεται η σχετική αναφορά. Οι εγκληματολόγοι δηλαδή δεν χρειάζεται να «περάσουν» από όλα τις ζώνες αναζητώντας πιθανά αποδεικτικά στοιχεία. Ωστόσο, ο αλγόριθμος αυτός είναι ένα θεωρητικό εγχείρημα που μένει να δοκιμαστεί στην πράξη. Κάτι πολύ σημαντικό που αξίζει να επισημανθεί εδώ είναι ότι η νομική πτυχή δεν έχει ληφθεί υπόψη σε αυτό το μοντέλο, διακυβεύοντας έτσι το 'παραδεκτό' του ενώπιον του δικαστηρίου.

---

[90] Lutta, P., Sedky, M., Hassan, M., Jayawickrama, U., & Bastaki, B. B. (2021). The complexity of internet of things forensics: A state-of-the-art review. *Forensic Science International: Digital Investigation*, *38*, 301210.

[91] Perumal, S., Norwawi, N. M., & Raman, V. (2015, October). Internet of Things (IoT) digital forensic investigation model: Top-down forensic approach methodology. In *2015 Fifth International Conference on Digital Information Processing and Communications (ICDIPC)* (pp. 19-23). IEEE.

[92] Harbawi, M., & Varol, A. (2017, April). An improved digital evidence acquisition model for the Internet of Things forensic I: A theoretical framework. In 2017 5th International Symposium on Digital Forensic and Security (ISDFS) (pp. 1-6). IEEE.

6. CLOUD COMPUTING & ΨΗΦΙΑΚΗ ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΗ ΕΡΕΥΝΑ ΣΕ ΠΕΡΙΒΑΛΛΟΝ ΝΕΦΟΫΠΟΛΟΓΙΣΤΙΚΗΣ (CLOUD FORENSICS)

Λόγω της άμεσης και στενής εξάρτησης του ΔτΠ από τις υπηρεσίες νεφοϋπολογιστικής και συνακόλουθα της εγκληματολογικής έρευνας σε αυτό, μια σύντομη και ξεχωριστή επισκόπηση του φαινομένου του cloud computing, των χαρακτηριστικών του αλλά και των ιδιαιτεροτήτων που παρουσιάζει μια αντίστοιχη εγκληματολογική έρευνα σε αυτό, καθίσταται περισσότερο από αναγκαία, για μια -όσο το δυνατόν- πιο ολιστική και πιο ξεκάθαρη προσέγγιση της προβληματικής αυτής.

6.1 Ορισμός του Cloud Computing

Αν και δεν έχει αποκρυσταλλωθεί ένας κοινά αποδεκτός από όλους ορισμός για το λεγόμενο 'υπολογιστικό νέφος', αποτελεί ουσιαστικά μια τεχνολογία που χρησιμοποιεί το διαδίκτυο μεταξύ απομακρυσμένων διακομιστών[93] για την συντήρηση δεδομένων και εφαρμογών. Σύμφωνα δε με το **Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας** (*National Institute of Standards and Technology- NIST):*

"το cloud computing είναι ένα μοντέλο το οποίο παρέχει τη δυνατότητα ευχερούς, βασισμένης στη ζήτηση διαδικτυακής πρόσβασης σε ένα διαμοιραζόμενο χώρο (π.χ. δίκτυα, διακομιστές, αποθήκευση, εφαρμογές και υπηρεσίες) και το οποίο μπορεί να ***παρασχεθεί*** *και να* ***αποδεσμευτεί*** *ταχέως με ελάχιστη διαχειριστική προσπάθεια ή αλληλεπίδραση με τον πάροχο της υπηρεσίας".* [94]

Στην Οδηγία για την Κυβερνοασφάλεια (2016/1148 ΕΚ) ανευρίσκεται επίσης παρόμοια εννοιολογική προσέγγιση για την υπηρεσία της νεφοϋπολογιστικής,

[93] Ονομάζονται εναλλακτικά και **'εξυπηρετητές'** ή **server(s)** στα αγγλικά είναι υλικό ή / και λογισμικό που αναλαμβάνει την παροχή διάφορων υπηρεσιών, «εξυπηρετώντας» αιτήσεις άλλων προγραμμάτων, που μπορούν να τρέχουν στον ίδιο υπολογιστή ή σε σύνδεση μέσω δικτύου https://el.wikipedia.org/wiki/%CE%95%CE%BE%CF%85%CF%80%CE%B7%CF%81%CE%B5%CF%84%CE%B7%CF%84%CE%AE%CF%82

[94] Βλ. The NIST Definition of Cloud Computing, NIST Special Publication 800-145, 2011, σελ. 2. Διαθέσιμο στο: http://csrc.nist.gov/publications/PubsSPs.html#800-145

κάνοντας λόγο για την «*ψηφιακή υπηρεσία που επιτρέπει την πρόσβαση σε* ***κλιμακοθετήσιμο*** *και ελαστικό σύνολο* ***κοινόχρηστων*** *υπολογιστικών πόρων*».[9596]

6.2 Τεχνικά Χαρακτηριστικά του Υπολογιστικού Νέφους

Ήδη από τον ορισμό έχουν εντοπιστεί σημαντικά χαρακτηριστικά αυτού του μοντέλου/τεχνολογικού εργαλείου, όπως το κοινόχρηστο αυτού, η εύκολη παροχή του αλλά κ αποδέσμευση από αυτό και η «κλιμακούμενη» φύση του, υπό την έννοια ότι ο εκάστοτε χρήστης *(που κυμαίνεται από ένα φυσικό πρόσωπο, μέχρι δημόσιες διοικήσεις κρατών αλλά και κολοσσιαίους οργανισμούς)* μπορεί να επιλέξει μέρος από το παρεχόμενο πακέτο υπηρεσιών, να προσθέσει στην συνέχεια και άλλες ιδιότητες κτλ. Η «**αφαιρετικότητα/abstraction**» αυτή διατρέχει το σύνολο των υπηρεσιών του νέφους επιτρέποντας επί της ουσίας, στους χρήστες να εστιάζουν στις επιθυμητές κάθε φορά λειτουργίες, χωρίς να υποχρεούνται να διαχειρίζονται τις υποδομές πάνω στις οποίες στηρίζονται οι λειτουργίες αυτές.[97] Οι υπηρεσίες του Cloud δε, παρέχονται από διαφορετικούς διακομιστές, διάσπαρτους ανά τον κόσμο, οι οποίοι μπορεί να ανήκουν και σε διαφορετικούς παρόχους, οι οποίοι δημιουργούν ένα «πλέγμα επικοινωνίας» μεταξύ τους.

Η κεντρικότερη ίσως ιδέα πάνω στην οποία βασίζεται το Cloud είναι η **εικονοποίηση/εικονικότητα** (virtualization), χρησιμοποιώντας εικονικό υλικό (virtual hardware) ώστε ο φυσικός διακομιστής να μπορεί να προβαίνει στην διάθεση **εικονικών διακομιστών {virtual machine(s)}** που διαμοιράζονται τους διαθέσιμους φυσικούς πόρους.[98] Χάρη σε αυτή την εικονικότητα η οποία

[95] Οδηγία (ΕΕ) **2016/1148** του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 6ης Ιουλίου 2016 σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση

[96] Κουσουνή-Πανταζοπούλου Α. (2022) 'Cloud Computing & νομικά ζητήματα' NB, σελ.83

[97] Κουσουνή-Πανταζοπούλου Α. (2022) 'Cloud Computing & νομικά ζητήματα' NB σελ.144

[98] ΠΑΠΑΔΟΠΟΥΛΟΣ Μ./ ΕΥΓΕΝΙΔΗΣ Π., Νεφοϋπολογιστική (Cloud Computing) και προστασία προσωπικών δεδομένων, ΔιΜΕΕ 2016, σελ. 182 επ

εξασφαλίζει τεράστια ευελιξία, εξοικονόμηση κόστους, πόρων και υποδομής, οι εφαρμογές και τα δεδομένα που χρησιμοποιούν οι χρήστες του Cloud **δεν διατηρούνται/αποθηκεύονται τοπικά** στον υπολογιστή του χρήστη. Ζητήματα έτσι που άπτονται της λειτουργίας, της αξιοπιστίας και της (ασφαλούς) διατήρησης των δεδομένων των χρηστών εναπόκεινται στην **ευθύνη** του εκάστοτε **Παρόχου νέφους** (Cloud Service Provider-CSP).[99]

Άλλα επιμέρους χαρακτηριστικά του cloud computing, είναι ότι οι υπηρεσίες του προσφέρονται **κατ' απαίτηση** του πελάτη (on demand & self service) με **αναλογική** κάθε φορά **χρέωση.** Επιπλέον, η **διάθεση των πόρων** των υπηρεσιών νεφοϋπολογιστικής *(resource pooling)* γίνεται **ανεξάρτητα από την εντοπιότητα** τόσο του χρήστη όσο και των ίδιων των πόρων ενώ οι **αποϋλοποίηση** αυτών, υπό την έννοια ότι ο χρήστης δεν γνωρίζει πως «εκπληρώνεται» η εκάστοτε εντολή του στο εικονικό αυτό περιβάλλον, ούτε από πού προέρχεται η αιτηθείσα εφαρμογή ή υπηρεσία, κάνει το περιβάλλον του cloud, άμεσο, γρήγορο και ευέλικτο μεν, αόρατο δε.

Τέλος, εγγενές χαρακτηριστικό του Cloud είναι η **πολυμισθωτική** του φύση καθώς επιτρέπει την ταυτόχρονη χρήση από πληθώρα χρηστών χωρίς να είναι πάντοτε ευκρινής η διαχωριστική γραμμή μεταξύ των δεδομένων του ενός από των υπολοίπων. Αναλυτικότερα, διαφορετικοί πελάτες/χρήστες του Cloud, μοιράζονται τους ίδιους φυσικούς πόρους και ο Πάροχος ουσιαστικά είναι υπεύθυνος για την αποτελεσματική διαχείριση αυτής της κοινής χρήσης *(μέσω πολιτικών πρόσβασης, ελέγχου πρόσβασης σε δεδομένα κτλ.)*. Επιπλέον, οι απαιτήσεις προστασίας για κάθε χρήστη/μισθωτή, μπορεί να είναι διαφορετικές, καθιστώντας έτσι το Νέφος, ένα ενιαίο σημείο συμβιβασμού.[100] Κάθε μισθωτής έτσι αναπτύσσει διαφορετικές σχέσεις εμπιστοσύνης με τον Πάροχο ή με τους άλλους χρήστες/μισθωτές ενώ κάποιοι από αυτούς δεν αποκλείεται να είναι οι

[99] Κουσουνή-Πανταζοπούλου Α. (2022) 'Cloud Computing & νομικά ζητήματα' ΝΒ σελ. 5
[100] Marangos, N., Rizomiliotis, P., & Mitrou, L. (2012, December). Digital forensics in the cloud computing era. In *2012 IEEE Globecom Workshops* (pp. 775-780). IEEE.

ίδιοι κακόβολοι επιτιθέμενοι, γεγονός που εγείρει σύνθετα ζητήματα διαχείρισης της εμπιστοσύνης.[101]

6.3 Μορφές Δομής του Cloud Computing

Καθώς η παροχή της νεφοϋπολογιστικής υπηρεσίας καλείται να καλύψει πλείστες και διαφορετικές ανάγκες πληθώρας ατόμων και οργανισμών/εταιριών, έχει αναπτύξει διαφορετικές μορφές 'προσφοράς' αυτής της υπηρεσίας, πάντα βασιζόμενη στην λογική **επαναχρησιμοποίησης** των πόρων της, από το οποίο προκύπτει και το δεύτερο συνθετικό του κάθε μορφότυπου **(as a Service)**. Το τι εντάσσεται στην **σφαίρα ευθύνης** καθενός από τα εμπλεκόμενα μέρη **διαφέρει** ανάλογα με το είδος της παρεχόμενης υπηρεσίας.[102] Ομοίως, ο **βαθμός αναγνώρισης** ενός στοιχείου ως απόδειξης στο οικοσύστημα του Cloud -υπό τους όρους της ψηφιακής εγκληματολογίας- **εξαρτάται από το μοντέλο** των υπηρεσιών του Cloud.[103]

Τα μοντέλα αυτά διακρίνονται ως εξής:

- ***Software as a Service (SaaS)***: Στην περίπτωση αυτή αντικείμενο της παρεχόμενης υπηρεσίας είναι μια **εφαρμογή, ένα λογισμικό**. Πρακτικά δηλαδή οι χρήστες, δύνανται να χρησιμοποιούν τις εφαρμογές που είναι εγκατεστημένες στο κεντρικό δίκτυο διακομιστών του Παρόχου και οι οποίες διατίθενται μέσω του 'νέφους' ως υπηρεσία χωρίς να χρειάζεται να τις εγκαταστήσουν και οι ίδιοι στους υπολογιστές τους,[104] με χαρακτηριστικότερα παραδείγματα αυτά των Google Drive, Dropbox, Facebook, ηλεκτρονικό ταχυδρομείο κα. Εύλογα συμπεραίνουμε εδώ, ότι ο τελικός χρήστης δεν μπορεί να 'επέμβει' επί της εφαρμογής καθ'

[101] Marangos, N., Rizomiliotis, P., & Mitrou, L. (2012, December). Digital forensics in the cloud computing era. In *2012 IEEE Globecom Workshops* (pp. 775-780). IEEE
[102] Κουσουνή-Πανταζοπούλου Α. (2022) Cloud Computing & νομικά ζητήματα, ΝΒ σελ. 10
[103] Καντζάβελου Ι.- Κάτος Β. (2021) «Ψηφιακή Δικανική» **Κεφ 16** στο συλλογικό τόμο "Ασφάλεια Πληροφοριών & Συστημάτων στον Κυβερνοχώρο", Σωκράτης Κάτσικας, Στέφανος Γκρίτζαλης, και Κωνσταντίνος Λαμπρινουδάκης (Επιστημονική Επιμέλεια), Εκδόσεις Νέων Τεχνολογιών σελ.128
[104] Κουσουνή-Πανταζοπούλου Α. (2022) Cloud Computing & νομικά ζητήματα ΝΒ σελ. 11

οποιονδήποτε τρόπο (μόνο μικρές παραμετροποιήσεις) ούτε έχει τον έλεγχο αυτής, καθιστώντας έτσι την οποιαδήποτε εγκληματολογική έρευνα σε τέτοιο περιβάλλον εξαιρετικά πολύπλοκη και αποκλειστικά εξαρτώμενη από την διαμεσολάβηση του Παρόχου.

- ***Platform as a Service (PaaS):*** Στο συγκεκριμένο μοντέλο, η παρεχόμενη υπηρεσία είναι η πλατφόρμα νέφους. Ο χρήστης έχει δηλαδή την δυνατότητα να 'τρέξει' δικές του εφαρμογές χρησιμοποιώντας όμως την υποδομή και τα εργαλεία του Παρόχου.[105] Χαρακτηριστικά παραδείγματα αποτελούν τα Windows Azure Platform της Microsoft και Google App Engine, που απευθύνεται σε παραγωγούς λογισμικών κατά βάση. Ο έλεγχος σε αυτό το περιβάλλον καθώς και τα αντίστοιχα μέτρα ασφαλείας συμπροσδιορίζονται τόσο από τον Πάροχο όσο και από τον ίδιο τον χρήστη. Το έργο του εγκληματολόγου εδώ είναι μεν ευχερέστερο συγκριτικά με το προηγούμενο μοντέλο αλλά και πάλι δύσκολο καθώς καλείται να αντλήσει αποδεικτικό υλικό από αρχεία καταγραφής εξειδικευμένων εφαρμογών και υπό την προϋπόθεση ότι έχουν δημιουργηθεί από μηχανισμούς των χρηστών.[106]

- ***Infrastructure as a Service (IaaS):*** Στο είδος αυτό μοντέλου που είναι και το θεμέλιο και των υπολοίπων, προσφέρεται σαν υπηρεσία στον χρήστη ουσιαστικά η δομή του νέφους ήτοι λειτουργίες επεξεργασίας, αποθήκευσης, δικτύου, υπολογιστικοί πόροι ώστε ο χρήστης να είναι σε θέση να 'τρέξει' οποιασδήποτε μορφής λογισμικό *(λειτουργικά συστήματα ή προγράμματα).*[107] Χαρακτηριστικότερο παράδειγμα είναι το Application Programming Interfaces (API, Διεπαφές Προγραμματισμού Εφαρμογών) ενώ απευθύνεται σε επιχειρήσεις που έχουν την δυνατότητα να

[105]Κουσουνή-Πανταζοπούλου Α. (2022) Cloud Computing & νομικά ζητήματα, ΝΒ σελ. 13
[106] Καντζάβελου Ι- Κάτος Β (2021) «Ψηφιακή Δικανική» **Κεφ 16** στο συλλογικό τόμο "Ασφάλεια Πληροφοριών & Συστημάτων στον Κυβερνοχώρο", Σωκράτης Κάτσικας, Στέφανος Γκρίτζαλης, και Κωνσταντίνος Λαμπρινουδάκης (Επιστημονική Επιμέλεια), Εκδόσεις Νέων Τεχνολογιών
[107] European Commission, Information Society and Media, ό.π, σελ. 9, GAUL B./KOEHLER, L.M., Mitarbeiterdaten in der Computer Cloud: Datenschutzrechtliche Grenzen des Outsourcing, BB 2011, σελ. 2229

αξιοποιήσουν την ολότητα αυτού του μοντέλου. Εφόσον το **κέντρο βάρους της ευθύνης** και των **μέτρων ασφαλείας** των εφαρμογών μετατοπίζεται εν προκειμένω στον χρήστη, διαμορφώνεται μια ευνοϊκότερη κατάσταση για τους σκοπούς διεξαγωγής μιας εγκληματολογικής έρευνας. Και αυτό διότι, εφόσον ο χρήστης έχει τον έλεγχο των εικονικών μηχανών και των εγκατεστημένων λειτουργικών συστημάτων και εφαρμογών, συνήθως εγκαθιστά και αρχεία καταγραφής της δραστηριότητας αυτών, απ' όπου δυνητικά θα μπορούσε να αξιοποιήσει στοιχεία ο ερευνητής της ψηφιακής εγκληματολογίας.[108]
Από τα παραπάνω συνάγεται ότι υπάρχει **ποικιλία επιπέδων ελέγχου** και **ευθύνης** βάση του μοντέλου παροχής υπηρεσιών.[109]

6.4 Εγκληματολογικές προκλήσεις στο Cloud και τεχνικές λύσεις

Η ψηφιακή διάσταση όλων των εγκλημάτων *(γνήσιων και μη γνήσιων Κυβερνοεγκλημάτων)*[110] και η απαίτηση για διασυνοριακή πρόσβαση σε αποδεικτικά μέσα, ειδικά όταν αυτά συναντώνται σε περιβάλλοντα νεφοϋπολογιστικής-με όλες τις ιδιαιτερότητες που αυτά έχουν από άποψη μορφολογίας-πυροδοτεί πλήθος προκλήσεων για την ψηφιακή εγκληματολογική έρευνα σε αυτά.
Αρχικά, η **δυναμική συμπεριφορά** των δεδομένων στο Cloud, η **αστάθεια** και η **ασάφεια** της τοποθεσίας που κάθε φορά αυτά βρίσκονται καθώς και η **ετερογένεια** των χρησιμοποιούμενων πόρων υλικού και λογισμικού από τους χρήστες και τα προβλήματα της μεταξύ τους δια λειτουργικότητας *(π.χ. ένας πελάτης Νέφους δύναται να εγγραφεί σε ένα IaaS από το χ πάροχο, να το συνδυάσει*

[108] Καντζάβελου Ι- Κάτος Β.(2021) «Ψηφιακή Δικανική» **Κεφ 16** στο συλλογικό τόμο "Ασφάλεια Πληροφοριών & Συστημάτων στον Κυβερνοχώρο", Σωκράτης Κάτσικας, Στέφανος Γκρίτζαλης, και Κωνσταντίνος Λαμπρινουδάκης (Επιστημονική Επιμέλεια), Εκδόσεις Νέων Τεχνολογιών, 2021 σελ.129
[109] Marangos, N., Rizomiliotis, P., & Mitrou, L. (2012, December). Digital forensics in the cloud computing era. In *2012 IEEE Globecom Workshops* (pp. 775-780). IEEE.
[110] Φαρμακίδης Ε. (2021), Ευρωπαϊκή Εντολή Υποβολής και Ευρωπαϊκή Εντολή Διατήρησης στοιχείων - Η προσαρμογή των θεσμών δικαστικής συνεργασίας σε ποινικές υποθέσεις στην ψηφιακή εποχή, ΠοινΔικ, 1/2021, σελ. 28 - 43

με ένα PaaS από τον y πάροχο και να χρησιμοποιήσει και τμήματα SaaS από τον z πάροχο)[111] δυσχεραίνει την εγκληματολογική έρευνα, οι ερευνητές της οποίας πρέπει να απευθύνονται κάθε φορά σε πολλές και διαφορετικές δικαιοδοσίες κρατών για να αποκτήσουν πρόσβαση σε αυτά, μέσω νομικών διαδικασιών αμοιβαίας δικαστικής συνεργασίας. Η αστάθεια των μεταφερόμενων δεδομένων στο Cloud επιβεβαιώνεται και από το γεγονός ότι αυτά αποτελούν πρακτικά ένα **στιγμιότυπο του χρόνου αποστολής τους στο νέφος** που εύκολα μπορεί να διαφοροποιηθεί, διαγραφεί, αλλοιωθεί από τον χρήστη, κάτι που φέρει 'πλήγμα' και στην απαίτηση της αλυσίδας φύλαξης η οποία επιτάσσει την 'συνέχεια', 'ακρίβεια' και ομοιότητα' των κατασχεμένων δεδομένων και των αντιγράφων τους.[112] 'Άλλος σημαντικός παράγοντας που δυσχεραίνει επίσης την 'αλυσίδα φύλαξης' είναι ότι η μεταφορά δεδομένων σε μια χώρα που δεν έχει προβλέψει νομικό προστατευτικό πλαίσιο για τα προσωπικά δεδομένα ούτε θέτει σχετικές απαιτήσεις, δεν επιτρέπει αντίστοιχα την συνέχιση της απαιτούμενης αυτής αλυσίδας, ενώ παράλληλα σημαντικό να σημειωθεί ότι και η **κρυπτογράφηση** των δεδομένων πριν την είσοδο στο νέφος, ως **μέτρο ασφαλείας** από μέρους πολλών Παρόχων, αποτελεί σημείο ισορροπίας μεταξύ της **ιδιωτικότητας** των χρηστών αλλά και της επιτυχούς διεξαγωγής μιας έρευνας, καθώς την καθιστά σχεδόν αδύνατη τις περισσότερες φορές.[113]

Από τις προτεινόμενες τεχνικές λύσεις των θεμάτων που ανακύπτουν στην εγκληματολογική έρευνα λόγω του νέφους, φαίνεται αρκετά αξιοποιήσιμη εκείνη που προκρίνει την **διατήρηση ενός αρχείου καταγραφής** της δραστηριότητας των χρηστών στο Cloud, **τοπικά και σύγχρονα** ώστε να μπορεί αυτή να ελέγχεται χωρίς να απαιτείται η διαμεσολάβηση του Παρόχου

[111] Marangos, N., Rizomiliotis, P., & Mitrou, L. (2012, December). Digital forensics in the cloud computing era. In *2012 IEEE Globecom Workshops* (pp. 775-780). IEEE.

[112] Taylor, M., Haggerty, J., Gresty, D., & Hegarty, R. (2010). Digital evidence in cloud computing systems. Computer law & security review, 26(3), 304-308.

[113] Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials*, *22*(2), 1191-1221.

νεφοϋπολογιστικής.[114] Η πρακτική αυτή ωστόσο φαίνεται πως δεν καλύπτει την καταγραφή του δικτύου, των μεταδεδομένων αρχείων, της χρήσης διεργασιών και πολλών άλλων στοιχείων, τα οποία είναι σημαντικά για την εγκληματολογική έρευνα-ειδικά σε περιβάλλοντα IaaS και PaaS.

Αναλυτικότερα, η **ακριβής χρονοσήμανση** των αρχείων καταγραφής, αποτελεί από τα βασικότερα στοιχεία στην εγκληματολογία του Νέφους και ταυτόχρονα από τις μεγαλύτερες προκλήσεις σε αυτό. Και αυτό διότι τα αρχεία καταγραφής αποτελούν το σημείο εκκίνησης της έρευνας όπως τα δακτυλικά αποτυπώματα αποτελούν το σημείο εκκίνησης της έρευνας για τους παραδοσιακούς εγκληματολόγους (φυσικών) σκηνών εγκλήματος.[115]Τα αρχεία καταγραφής αποτελούν το εργαλείο μέσα από το οποίο ο ερευνητής δύναται να ανακατασκευάσει χρονικά την αλληλουχία των γεγονότων που οδήγησαν στο εκάστοτε περιστατικό που διερευνάται. Η **αξιοπιστία της έρευνας** εξαρτάται λοιπόν από την **εμπιστευτικότητα** και την **ακεραιότητα** των αρχείων καταγραφής.[116] Τα τεχνικά χαρακτηριστικά των διαφόρων δομών Νέφους, συμπαρασύρουν και τον τρόπο λειτουργίας και διαχείρισης των αρχείων καταγραφής(πχ διαφορετικά δικαιώματα πρόσβασης σε κάθε μοντέλο 'παράγουν' και διαφορετικά αρχεία καταγραφής των δραστηριοτήτων σε αυτά).[117] Έτσι, η χωρική διάσταση στο Νέφος (αποκεντρωμένος χαρακτήρας) είναι στενά συνδεδεμένη και με την χρονική διάσταση (η χρονοσήμανση σε ένα VM μπορεί να τροποποιηθεί είτε από τον Πάροχο, είτε από τον χρήστη, για αυτό και απαιτείται εξωγενής ρύθμιση από τρίτη αξιόπιστη πηγή) ενώ και ο συγχρονισμός του χρόνου αποτελεί κρίσιμο παράγοντα τόσο για τον εντοπισμό όσο και για την διατήρηση των αποδεικτικών στοιχείων ειδικά αν ληφθεί υπόψη

[114] Simou, S., Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2014). Cloud forensics solutions: A review. In *Advanced Information Systems Engineering Workshops: CAiSE 2014 International Workshops, Thessaloniki, Greece, June 16-20, 2014. Proceedings 26* (pp. 299-309). Springer International Publishing.

[115] Marangos, N., Rizomiliotis, P., & Mitrou, L. (2012, December). Digital forensics in the cloud computing era. In *2012 IEEE Globecom Workshops* (pp. 775-780). IEEE

[116] Marangos, N., Rizomiliotis, P., & Mitrou, L. (2012, December). Digital forensics in the cloud computing era. In *2012 IEEE Globecom Workshops* (pp. 775-780). IEEE

[117] Marangos, N., Rizomiliotis, P., & Mitrou, L. (2012, December). Digital forensics in the cloud computing era. In *2012 IEEE Globecom Workshops* (pp. 775-780). IEEE

ότι συνήθως ο διακομιστής Νέφους και ο πελάτης Νέφους βρίσκονται σε διαφορετικές ώρες.[118]

Σχετικά με τα **ευμετάβλητα δεδομένα** τα οποία είναι και πιο επιρρεπή να χαθούν κατά την απενεργοποίηση του υπολογιστή, προτάθηκε η 'ζωντανή εγκληματολογία-live forensics' όπως είδαμε και παραπάνω, η οποία ναι μεν εξασφαλίζει ότι τα πτητικά δεδομένα δεν θα χαθούν ωστόσο 'φορτώνει' τους ερευνητές με πολλαπλάσιο όγκο δεδομένων καθιστώντας την έρευνα πιο δυσκίνητη.[119] Ως απάντηση στο χρονοβόρο της υπόθεσης στην περίπτωση αυτή, κομβικής σημασίας θα ήταν να επένδυαν οι Πάροχοι στην **προσφορά μόνιμης συσκευής αποθήκευσης** των δεδομένων του πελάτη, **με συχνό συγχρονισμό** αυτής με το cloud ή ακόμα και να ενσωμάτωναν στους εικονικούς διακομιστές τους έναν τέτοιο μηχανισμό συγχρονισμού. Στα πλεονεκτήματα βέβαια του Νέφους ως προς την διαχείριση των ευμετάβλητων δεδομένων, συγκαταλέγεται η δυνατότητα που έχει ένας ερευνητής να αντιγράψει μια ολόκληρη εικονική μηχανή (VM) ενώ αυτή βρίσκεται σε λειτουργία χωρίς να απαιτείται να διακόψει την λειτουργία της. Με αυτό τον τρόπο, παρέχονται στον ερευνητή όλα τα τρέχοντα πτητικά δεδομένα.[120] Μια κατεύθυνση λοιπόν δεσμίδας λύσεων θα ήταν η μικρότερη δυνατή εμπλοκή των Παρόχων ή και η ανάληψη πρωτοβουλιών από αυτούς για μεγαλύτερη προστασία των δεδομένων των χρηστών σύμφωνα με τις παραπάνω μεθόδους. Πέρα όμως από την μείωση της εξάρτησης της πορείας -ουσιαστικά- μιας έρευνας από έναν τρίτο, τον Πάροχο, σημαντικό θα ήταν να διασφαλιστεί η όσο το δυνατόν μεγαλύτερη **διαφάνεια** των πρακτικών του αλλά και η μεγαλύτερη **νομική του δέσμευση.**

[118] Marangos, N., Rizomiliotis, P., & Mitrou, L. (2012, December). Digital forensics in the cloud computing era. In *2012 IEEE Globecom Workshops* (pp. 775-780). IEEE

[119] Simou, S., Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2014). Cloud forensics solutions: A review. In *Advanced Information Systems Engineering Workshops: CAiSE 2014 International Workshops, Thessaloniki, Greece, June 16-20, 2014. Proceedings 26* (pp. 299-309). Springer International Publishing.

[120]Marangos, N., Rizomiliotis, P., & Mitrou, L. (2012, December). Digital forensics in the cloud computing era. In *2012 IEEE Globecom Workshops* (pp. 775-780). IEEE

Αυτό θα μπορούσε να επιτευχθεί μέσω μιας μορφής audit σε περιβάλλον cloud, υπό την έννοια ότι :

- το νέφος καταγράφει τις ενέργειές του σε ένα αρχείο καταγραφής που είναι εμφανές ότι έχει παραβιαστεί.
- οι χρήστες μπορούν να ελέγξουν το αρχείο καταγραφής και να ελέγξουν για σφάλματα και τελικά μπορούν να χρησιμοποιήσουν το αρχείο καταγραφής για να κατασκευάσουν αποδείξεις για το εν λόγω σφάλμα.
- όταν ένας ελεγκτής ανιχνεύσει το σφάλμα μπορεί να αποκτήσει πρόσβαση στο αποδεικτικό υλικό για το σφάλμα αυτό, το οποίο θα μπορεί να επαληθευτεί και από τρίτο ανεξάρτητο μέρος (πλαίσιο τύπου Trust Cloud).[121]

Πολλές από τις νομικές προκλήσεις θα μπορούσαν να ξεπεραστούν με την συνδρομή και την διεύρυνση των σκοπών των ήδη υφιστάμενων **SLAs** (Service Level Agreements) τα οποία αποτελούν ψηφιακά συμβόλαια τα οποία συνάπτουν οι χρήστες με τον Πάροχο με το πάτημα ενός κουμπιού επί της ουσίας και χωρίς δυνατότητα διαπραγμάτευσης φυσικά. Θα πρέπει λοιπόν τέτοιου είδους δεσμευτικές συμφωνίες να θέσουν στο επίκεντρο την **εμπιστευτικότητα και ακεραιότητα των δεδομένων των πελατών τους**, τις **πολιτικές προστασίας της ιδιωτικότητας αυτών** *(σε περιπτώσεις κατάσχεσης του φυσικού υλικού, τα δεδομένα χρηστών του Νέφους που δεν εμπλέκονται με το υπό διερεύνηση περιστατικό, ενδέχεται να αποκαλυφθούν σε τρίτα μέρη)*[122] και **ζητήματα ασφαλείας** σε ένα τέτοιο κατανεμημένο περιβάλλον πολυμισθωτικής φύσης. Να διαθέτουν επίσης μηχανισμούς ελέγχου της ανωνυμίας των χρηστών, αλλά και ασφαλιστικές δικλείδες για την απαιτούμενη συνδρομή τους στις εγκληματολογικές έρευνες που θα εξασφαλίζει και την **ακεραιότητα της διαδικασίας**.[123]

[121]Haeberlen, A. (2010). A case for the accountable cloud. *ACM SIGOPS Operating Systems Review*, *44*(2), 52-57.

[122] Marangos, N., Rizomiliotis, P., & Mitrou, L. (2012, December). Digital forensics in the cloud computing era. In *2012 IEEE Globecom Workshops* (pp. 775-780). IEEE

[123] Marangos, N., Rizomiliotis, P., & Mitrou, L. (2012, December). Digital forensics in the cloud computing era. In *2012 IEEE Globecom Workshops* (pp. 775-780). IEEE

Όσον αφορά ζητήματα ακεραιότητας και σταθερότητας του συλλεχθέντος αποδεικτικού υλικού από το Cloud, προτάθηκε η δημιουργία μοναδικής ψηφιακής υπογραφής αλλά και η δυνατότητα ελέγχου αυτής[124] ενώ σχετικά με την χρονοσήμανση των αποθηκευμένων στο Cloud δεδομένων, λόγω των διαφορετικών χωρών στα οποία επεξεργάζονται και αποθηκεύονται, προτείνεται η υιοθέτηση ενός προτύπου ώρας ώστε να διευκολύνεται η ανακατασκευή του εγκλήματος.

Τέλος, από τα σημαντικότερα ίσως βήματα προς την επίλυση των σχετικών προβλημάτων κατά την ψηφιακή έρευνα, είναι η στελέχωση των Παρόχων με εξειδικευμένο προσωπικό που θα συνδράμει ενεργά στις προσπάθειες των ερευνητών της ψηφιακής εγκληματολογίας, και θα κατέχει τις κατάλληλες δεξιότητες[125] αλλά και η ανάπτυξη εξειδικευμένων εργαλείων προσαρμοσμένων στις απαιτήσεις της ψηφιακής έρευνας αλλά και στα διαφορετικά μοντέλα υπηρεσίας Νέφους[126] καθώς και η ενίσχυση των Παρόχων προς την κατεύθυνση δημιουργίας μοντέλου τύπου Cloud Forensics as a Service.[127]

6.5 Η νομοθετική προσέγγιση των ΗΠΑ| CLOUD ACT

Η ανάγκη για ένα ισχυρό αλλά και ταυτόχρονα ευέλικτο και αποτελεσματικό νομικό πλαίσιο που θα επιτρέπει την διασυνοριακή πρόσβαση σε αποδείξεις και δη σε αποδείξεις που ανευρίσκονται σε περιβάλλοντα νεφοϋπολογιστικής είναι επιτακτική. Την ανάγκη αυτή προσπάθησε να καλύψει νομοθετικά, η Αμερική, με την θέσπιση της '**US Clarifying Lawful Overseas Use of Data'** εφεξής **Cloud Act 2018**, η οποία προβλέπει την δυνατότητα των διωκτικών αρχών να έχουν

[124] Hegarty, R., Merabti, M., Shi, Q., & Askwith, B. (2009, June). Forensic analysis of distributed data in a service oriented computing platform. In *proceedings of the 10th Annual Postgraduate Symposium on The Convergence of Telecommunications, Networking & Broadcasting, PG Net*.

[125] Simou, S., Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2014). Cloud forensics solutions: A review. In *Advanced Information Systems Engineering Workshops: CAiSE 2014 International Workshops, Thessaloniki, Greece, June 16-20, 2014. Proceedings 26* (pp. 299-309). Springer International Publishing.

[126] Marangos, N., Rizomiliotis, P., & Mitrou, L. (2012, December). Digital forensics in the cloud computing era. In *2012 IEEE Globecom Workshops* (pp. 775-780). IEEE

[127] Janarthanan, T., Bagheri, M., & Zargari, S. (2021). IoT forensics: An overview of the current issues and challenges. *Digital Forensic Investigation of Internet of Things (IoT) Devices*, 223-254.

πρόσβαση κατά την διερεύνηση ποινικών υποθέσεων σε κάθε είδους δεδομένα που είναι αποθηκευμένα σε υπηρεσίες Cloud εκτός του εδάφους των ΗΠΑ.[128]
Αφορμή για την έκδοση του νομοθετήματος αυτού, που ψηφίστηκε από το Κογκρέσο, στάθηκε η πενταετής δικαστική αντιδικία της Αμερικανικής Κυβέρνησης με την εταιρία Microsoft. Ως Πάροχος υπηρεσιών νέφους-CSP, η τελευταία είχε αρνηθεί να συμμορφωθεί σε ένταλμα του FBI που εκδόθηκε το 2013, βασιζόμενο στην τότε ισχύουσα νομοθεσία *(Stored Communications Act – SCA 1986).* Σε εκτέλεση του συγκεκριμένου εντάλματος, το FBI ζητούσε από τη Microsoft να παραδώσει στην αστυνομία τα μηνύματα ηλεκτρονικού ταχυδρομείου καταζητούμενου Αμερικάνου εμπόρου ναρκωτικών, τα οποία ήταν αποθηκευμένα εκτός αμερικανικού εδάφους και συγκεκριμένα σε διακομιστές της Microsoft στην Ιρλανδία.[129] Καθώς, εν προκειμένω, δεν είχε εξωεδαφική εφαρμογή η τότε εσωτερική νομοθεσία (SCA 1986), το επίδικο ένταλμα ακυρώθηκε από το εφετείο.
Ούτως ή άλλως, από διαδικαστική άποψη, η κοινοποίηση του εντάλματος από το FBI <u>απευθείας</u> προς την προσφεύγουσα εταιρία, χωρίς την εμπλοκή και την κοινοποίηση σε Europol δεν ευσταθούσε, καθώς η Microsoft, διατηρούσε αποθηκευμένα προσωπικά δεδομένα σε ευρωπαϊκό έδαφος και έπρεπε η Europol να διαβιβάσει το αίτημα στις αντίστοιχες ιρλανδικές αρχές.[130] Υπό το κλίμα έντονής πολιτικής πίεσης και ζυμώσεων των διωκτικών αρχών, και ενώ η υπόθεση εκκρεμούσε ακόμα στο Ανώτατο Δικαστήριο των ΗΠΑ, ψηφίστηκε ο νέος νόμος **Cloud Act 2018**, ο οποίος υποχρεώνει τις αμερικανικές εταιρίες που παρέχουν υπηρεσίες αποθήκευσης δεδομένων στο νέφος να συμμορφώνονται με αιτήματα παροχής στοιχείων εκ μέρους αστυνομικών και διωκτικών αρχών.

Ευλόγως, το νομοθέτημα αυτό προκάλεσε τις αντιδράσεις των ευρωπαϊκών χωρών, καθώς υποχρεώνει πρακτικά τις αμερικανικές εταιρίες νέφους αλλά και παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών να συμμορφώνονται με

[128] Κουσουνή-Πανταζοπούλου Α. (2022) 'Cloud Computing & νομικά ζητήματα' NB, σελ. 193
[129] Κανέλλος Λ, (2020)'The GDPR Handbook' Για DPOs, Επιχειρήσεις & Οργανισμούς, NB σελ.287
[130] Σύμφωνα με τις επιταγές της **Σύμβασης Αμοιβαίας Δικαστικής Συνδρομής μεταξύ ΕΕ – ΗΠΑ** & Συμφωνίας ανταλλαγής δεδομένων μεταξύ διωκτικών αρχών (**EU-US «Umbrella Agreement**») του 2016 (**Οδηγία 2016/680**)

αιτήματα που αφορούν τα περιεχόμενα ή μεταδεδομένα ενσύρματων ή ηλεκτρονικών επικοινωνιών ή οποιαδήποτε άλλα στοιχεία έχουν στην κατοχή ή υπό τον έλεγχο τους, ανεξάρτητα αν τα στοιχεία αυτά βρίσκονται εντός ή εκτός ΗΠΑ[131], πράγμα που ενέχει κινδύνους για αθέμιτη αποκάλυψη προσωπικών δεδομένων Ευρωπαίων πολιτών κατά παράβαση του GDPR.[132] Με τον εν λόγω νόμο δε, προβλέπεται και η δυνατότητα σύναψης **διμερών συμφωνιών,** μεταξύ των ΗΠΑ και τρίτων χωρών σχετικά με την διασφάλιση ταχείας, αμοιβαίας διαδικασίας πρόσβασης σε ηλεκτρονικές πληροφορίες που διατηρούνται από παρόχους στο εξωτερικό. Μέχρι στιγμής, υπό το καθεστώς Cloud Act έχει συνάψει συμφωνία, το Ηνωμένο Βασίλειο τον Ιούλιο του 2020.[133]

6.6 Η πρόταση κανονισμού της Ευρωπαϊκής Ένωσης | E-evidence

Λίγο μετά την υιοθέτηση της Cloud Act των ΗΠΑ, η Ευρωπαϊκή Επιτροπή προτείνει τον Απρίλιο του 2018, την θεσμοθέτηση ενός κοινού Ευρωπαϊκού πλαισίου για την πρόσβαση στα ηλεκτρονικά αποδεικτικά στοιχεία **(e-evidence**), με σκοπό την αποτελεσματικότερη καταπολέμηση του εγκλήματος.[134]

Είναι αλήθεια ότι η Ευρωπαϊκή Επιτροπή αξιολόγησε 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 και να εξαρτώνται όλο και παραπάνω στις ψηφιακές αποδείξεις για τον εντοπισμό και την καταστολή αυτών, όσο και ότι η πρόσβαση στα ηλεκτρονικά αποδεικτικά στοιχεία αποτελεί μια εξαιρετικά χρονοβόρα και πολύπλοκη διαδικασία, -ειδικά όταν τα δεδομένα είναι αποθηκευμένα στο εξωτερικό-για αυτό και πρότεινε ένα πλαίσιο νομικών κανόνων που θα διασφαλίζουν την

---

[131] Κουσουνή-Πανταζοπούλου Α. (2022) 'Cloud Computing & νομικά ζητήματα' NB, σελ. 194

[132] Κανέλλος Λ. (2020) 'The GDPR Handbook' Για DPOs, Επιχειρήσεις & Οργανισμούς, NB 2020 σελ.300

Ορθώς όμως τόσο το άρθρο 6 παρ. 3 του Κανονισμού όσο και το άρθρο 48 επιτάσσουν συμμόρφωση με ευρωπαϊκό νομοθέτημα ή διεθνές αντίστοιχα.

[133] *Agreement of 3 October 2019 between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime»*

[134] Ζουμπουλάκης Κ. (2019)«Η πρόσβαση των αρχών στα ηλεκτρονικά αποδεικτικά στοιχεία: Τι συμβαίνει με τα προσωπικά μας δεδομένα;» Homo Digitalis, https://www.homodigitalis.gr/posts/3928

ταχύτερη και αποτελεσματικότερη πρόσβαση των αρχών στα ψηφιακά αποδεικτικά μέσα.[135] Το ενδιαφέρον άλλωστε του νομοθέτη φαντάζει αναμενόμενο, αν αναλογιστεί κανείς πως το **85%** των ποινικών ερευνών περιλαμβάνει πλέον την χρήση ψηφιακών δεδομένων.[136] 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. Κατά αυτόν τον τρόπο, θα επιταχύνεται η άμεση διεκπεραίωση της αίτησης πρόσβασης, καθότι δεν θα υπάρχει ανάγκη να μεσολαβούν οι αρχές του άλλου κράτους μέλους.

Το προταθέν πλαίσιο περιέχει έναν **κανονισμό** σχετικά με τα ευρωπαϊκά εντάλματα χορήγησης ηλεκτρονικών αποδεικτικών στοιχείων σε ποινικές υποθέσεις και μια **οδηγία** σχετικά με τη θέσπιση εναρμονισμένων κανόνων για τον ορισμό **νόμιμων εκπροσώπων** με σκοπό τη συγκέντρωση αποδεικτικών στοιχείων στο πλαίσιο ποινικών διαδικασιών. Συγκεκριμένα ο κανονισμός σχετικά με την **εντολή υποβολής**[137] και την **εντολή διατήρησης**[138] ηλεκτρονικών αποδεικτικών στοιχείων θα επιτρέψει στις αρχές να έχουν πρόσβαση σε αποθηκευμένα δεδομένα, **ανεξαρτήτως** του πού βρίσκονται τα δεδομένα αυτά. Η **εντολή υποβολής** θα επιτρέπει στις δικαστικές αρχές κράτους μέλους να αιτούνται την πρόσβαση σε ηλεκτρονικά αποδεικτικά στοιχεία **απευθείας** από 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 για επείγουσες περιπτώσεις. Η **εντολή διατήρησης** από την άλλη, θα απαγορεύει τη διαγραφή ηλεκτρονικών αποδεικτικών στοιχείων από τον Πάροχο υπηρεσιών όσο διαρκεί η επεξεργασία της εντολής υποβολής, χρονικά δηλαδή θα προπορεύεται του αιτήματος υποβολής. Είναι σημαντικό να υπογραμμισθεί ότι οι κανόνες αυτοί θα βασίζονται στις υφιστάμενες αρχές

[135] Ματάμη, Ε. (2022). Ψηφιακά πειστήρια και αποδεικτικές απαγορεύσεις στην ποινική δίκη σε εθνικό και υπερεθνικό επίπεδο.
[136] https://www.consilium.europa.eu/el/policies/e-evidence/
[137] **Η Ευρωπαϊκή Εντολή Υποβολής (ΕΕΥ) στοιχείων**
[138] **Η Ευρωπαϊκή Εντολή Διατήρησης (ΕΕΔ) στοιχείων**

αμοιβαίας αναγνώρισης μεταξύ των κρατών μελών. Θα εφαρμόζονται **μόνον σε αποθηκευμένα δεδομένα**, καθώς οι προτεινόμενοι κανόνες δεν καλύπτουν τα δεδομένα από υποκλοπή τηλεπικοινωνιών σε πραγματικό χρόνο.[139]

Όσον αφορά την **Οδηγία** για τους **νόμιμους εκπροσώπους**, αυτή θα υποχρεώνει όλους τους Παρόχους υπηρεσιών που δεν είναι εγκατεστημένοι στην Ευρωπαϊκή Ένωση αλλά παρέχουν υπηρεσίες στην Ένωση να διορίζουν **νόμιμο εκπρόσωπο**. Ο εκπρόσωπος θα είναι υπεύθυνος για την παραλαβή αποφάσεων και εντολών, τη συμμόρφωση προς αυτές και την εκτέλεσή τους. Στόχος είναι όλοι οι Πάροχοι υπηρεσιών που λειτουργούν στην ΕΕ να έχουν τις ίδιες υποχρεώσεις όσον αφορά την πρόσβαση στα ηλεκτρονικά αποδεικτικά στοιχεία. Η τελευταία εξέλιξη στην νομοθετική αυτή πρωτοβουλία είναι ότι στις 25 Ιανουαρίου 2023, το Συμβούλιο επιβεβαίωσε τη συμφωνία του με το Ευρωπαϊκό Κοινοβούλιο επί των δύο αυτών νομοθετικών προτάσεων.

6.6.1. Προβληματισμοί σχετικά με το προτεινόμενο πλαίσιο | E-evidence

Παρόλο που το προτεινόμενο νομικό πλαίσιο κινείται προς την σωστή κατεύθυνση 'αφουγκραζόμενο' την επιτακτική ανάγκη αμεσότερης και αποτελεσματικότερης πρόσβασης των αρχών στα ψηφιακά αποδεικτικά μέσα - όταν εμπλέκονται περισσότερες δικαιοδοσίες- εγείρονται ωστόσο προβληματισμοί σχετικά με την αποτελεσματική προστασία θεμελιωδών δικαιωμάτων υπό το πλαίσιο αυτό.

- ***Σχετικά με την νομική βάση.***

Η βασικότερη ίσως επιφύλαξη είναι αυτή που σχετίζεται με την νομική θεμελίωση του προτεινόμενου νομοθετήματος. Βασίζεται στο άρθρο **82** της **ΣΛΕΕ** σχετικά με την **δικαστική συνεργασία των κρατών σε ποινικές υποθέσεις** και ενώ αυτό προβλέπει-μεταξύ άλλων- την διαμεσολάβηση των αρχών του Κράτους

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

Εκτέλεσης *(του κράτους δηλαδή που λαμβάνει την εντολή να υποβάλει ή να διατηρήσει τα αποδεικτικά στοιχεία)* με τον προτεινόμενο Κανονισμό προβλέπεται 'παράκαμψη' των αρχών αυτών. Πρακτικά, στο όνομα της επιτάχυνσης της ερευνητικής διαδικασίας, το Κράτος Έκδοσης απευθύνεται στον εκάστοτε Πάροχο νέφους ή/και ηλεκτρονικών επικοινωνιών **άμεσα,** χωρίς την εμπλοκή και την γνώση των αρχών του Κράτους Εκτέλεσης, που μέχρι πρότινος λειτουργούσαν ως 'φίλτρο νομιμότητας' και εγγυητές των θεμελιωδών δικαιωμάτων των ατόμων υπό διερεύνηση και όχι μόνο. [140] Ο Πάροχος επιφορτίζεται έτσι με ένα ρόλο λήψης αποφάσεων επί θεμελιωδών δικαιωμάτων και δη κάτω υπό στενές χρονικές προθεσμίες.

- ***Αναφορικά με την διάκριση δεδομένων.***

Οι τέσσερις κατηγορίες που προτείνει ο Κανονισμός *(δεδομένα συνδρομητή-δεδομένα πρόσβασης-δεδομένα συναλλαγών- δεδομένα περιεχομένου)* και την ανάλογη νομική θωράκιση αυτών με γνώμονα την ένταση της κρατικής διείσδυσης σε αυτά, φαίνεται να μην ακολουθεί ανάλογες κατηγοριοποιήσεις που ανευρίσκονται σε αντίστοιχα νομοθετήματα μέχρι στιγμής. Για παράδειγμα, τα 'μεταδεδομένα' των ηλεκτρονικών επικοινωνιών περιλαμβάνονται τόσο στην κατηγορία 'δεδομένων πρόσβασης' όσο και στην κατηγορία 'δεδομένων συναλλαγών' με την προϋπόθεση όμως ότι δεν αποτελούν 'δεδομένα πρόσβασης'. Το αποτέλεσμα είναι να επικρατεί εννοιολογική σύγχυση και μη ευθυγράμμιση με τις έως τώρα κρατούσες κατηγορίες 'ενισχύοντας' την ανασφάλεια του δικαίου . Εδώ αξίζει να αναφέρουμε επίσης, ότι σύμφωνα με τον προτεινόμενο Κανονισμό τα δεδομένα θα πρέπει να παρέχονται στις δημόσιες αρχές του κράτους έκδοσης <u>ανεξάρτητα αν είναι κρυπτογραφημένα ή όχι</u>, το οποίο εύλογα γεννά απορία σχετικά με την δυνατότητα αποκρυπτογράφησης αυτών, και εν τέλει την αποτελεσματική και ταχεία αξιοποίηση τους στις ποινικές δίκες.

[140] Φαρμακίδης Ε (2021), Ευρωπαϊκή Εντολή Υποβολής και Ευρωπαϊκή Εντολή Διατήρησης στοιχείων - Η προσαρμογή των θεσμών δικαστικής συνεργασίας σε ποινικές υποθέσεις στην ψηφιακή εποχή, ΠοινΔικ, 1/2021, σελ. 28 - 43

- ***Όσον αφορά τις διαβιβάσεις σε τρίτες χώρες.***

Η κατάργηση των κριτηρίων της τοποθεσίας που προβλέπει το σχέδιο κανονισμού συμπαρασύρει και τις διαβιβάσεις δεδομένων προς τρίτες χώρες. Και ενώ εντός της Ευρωπαϊκής Ένωσης έχει επιτευχθεί ένα υψηλό επίπεδο προστασίας των προσωπικών δεδομένων, της ιδιωτικότητας και άλλων θεμελιωδών δικαιωμάτων και ελευθεριών των πολιτών[141] , με αποτέλεσμα οι διαβιβάσεις εντός της Ένωσης να θεωρούνται ομοιόμορφα προστατευμένες, είναι αμφίβολο αν η διαβίβαση τέτοιων δεδομένων προς τρίτες χώρες που δεν έχουν επαρκείς νομικές δικλείδες ασφαλείας, μπορεί να εγγυηθεί το ίδιο.

- ***Σχετικά με την μη εφαρμογή του 'διττού αξιοποίνου'***

Η μη τήρηση της αρχής του διττού αξιοποίνου συνεπάγεται ουσιαστικά ότι ο Πάροχος, που έχει την έδρα του ή τον εκπρόσωπό του στο Κράτος Εκτέλεσης, να εξαναγκάζεται πρακτικά από το Κράτος Έκδοσης να συμβάλει στην τιμώρηση μιας συμπεριφοράς, η οποία μπορεί να λαμβάνει χώρα στην επικράτεια του Κράτους Εκτέλεσης ελευθέρως και ατιμωρητί. Με άλλα λόγια, βάσει της ρύθμισης αυτής, το Κράτος Εκτέλεσης, στο οποίο έχει την έδρα του ή εκπροσωπείται ο Πάροχος υπηρεσιών, είναι υποχρεωμένο για μια πράξη, που δεν είναι αξιόποινη κατά το εθνικό του δίκαιο, να ανέχεται την επιβολή επαχθών δικονομικών μέτρων κατά των πολιτών του, μέτρα, τα οποία δεν θα νομιμοποιούταν να λάβει το ίδιο, αν η ίδια ακριβώς συμπεριφορά είχε επιδειχθεί εντός της επικράτειάς του.[142]

- ***Σχετικά με την επάρκεια της δικαστικής προστασίας***

Φαίνεται να είναι προβληματικό το γεγονός ότι οι αποδέκτες των εντολών, προστατεύονται και μπορούν να αντιταχθούν μόνο στην περίπτωση της ευρωπαϊκής εντολής υποβολής στοιχείων και όχι επί της εντολής διατήρησης

[141] Βλ. **τον Γενικό Κανονισμό Προστασίας Δεδομένων, την Αστυνομική Οδηγία, Οδηγία για την Προστασία των Προσωπικών Δεδομένων στις Ηλεκτρονικές Επικοινωνίες και την αναμενόμενη αντικατάσταση της από Κανονισμό**.

[142] Φαρμακίδης Ε. (2021), Ευρωπαϊκή Εντολή Υποβολής και Ευρωπαϊκή Εντολή Διατήρησης στοιχείων - Η προσαρμογή των θεσμών δικαστικής συνεργασίας σε ποινικές υποθέσεις στην ψηφιακή εποχή, ΠοινΔικ, 1/2021, σελ. 28 - 43

στοιχείων, με το σκεπτικό ότι στην δεύτερη δεν προκύπτει ουσιαστικά γνωστοποίηση άρα και προσβολή προσωπικών στοιχείων που θα έχρηζαν έννομης προστασίας. Ωστόσο, φαίνεται να έχει παραβλεφθεί το παράδειγμα σύμφωνα με το οποίο ο Πάροχος είχε εκ του νόμου υποχρέωση να διαγράψει ή να περιορίσει την επεξεργασία των δεδομένων για τα οποία όμως είχε εκδοθεί τέτοιου είδους εντολή. Από τα παραπάνω συνάγεται ότι είναι εξαιρετικά σημαντικό να συστηματοποιηθούν και να αξιολογηθούν σε βάθος τα προβληματικά σημεία έτσι ώστε δοθούν λύσεις ή/και εναλλακτικές πριν τον αποκρυστάλλωση του νομοθετήματος.

7. ΄ΕΞΥΠΝΟ ΣΠΙΤΙ | ΈΞΥΠΝΕΣ ΣΥΣΚΕΥΕΣ | ΦΕΡΟΜΕΝΕΣ ΣΥΣΚΕΥΕΣ (SMART HOME | SMART DEVICES | WEARABLES) & ΨΗΦΙΑΚΗ ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΗ ΕΡΕΥΝΑ

7.1 ΄Έξυπνο σπίτι-Εφαρμογές-Οφέλη-Προκλήσεις ασφάλειας & ιδιωτικότητας

Από τις πιο διαδεδομένες και πρακτικές εφαρμογές του Διαδικτύου των Πραγμάτων (ΔτΠ) αποτελούν τα έξυπνα σπίτια. Σε ένα έξυπνο σπίτι, η πλειονότητα των συσκευών όπως φώτα, κλειδαριές, ψυγεία, καφετιέρες, συστήματα θέρμανσης/ψύξης συλλέγουν πληροφορίες από τον φυσικό κόσμο *(συνήθως μέσω αισθητήρων, ενεργοποιητών και τεχνολογιών όπως* ***RFID***[143]*)* συνδέονται και ελέγχονται από μια κεντρική συσκευή μέσω Wi-Fi, Bluetooth κτλ. Επιτρέπει δηλαδή στους ανθρώπους να ελέγχουν και να παρακολουθούν αντικείμενα από απόσταση, -μέσω του έξυπνου κινητού τους για παράδειγμα-, και να εκτελούν προσωπικές εργασίες πιο εύκολα, γρήγορα και

[143] Πρόκειται για συντομογραφία του **"*Radio Frequency Identification*"**, τα οποία πρακτικά είναι μικρά ηλεκτρονικά κυκλώματα, συχνά στο μέγεθος ενός κόκκου ρυζιού, τα οποία φέρουν κάποιου είδους ψηφιακή πληροφορία, και χρησιμοποιούνται για την σχετικού τύπου αναγνώριση. Δηλαδή, ένα συγκεκριμένο κύκλωμα επικοινωνεί με κάποιον δέκτη και δίνει πληροφορίες για ένα συγκεκριμένο αντικείμενο ή μια συγκεκριμένη ενέργεια.
Μιχαηλάκη, Α. (2021). *Δίκαιο και δεοντολογία στις εφαρμογές της επαυξημένης πραγματικότητας: τεχνολογικές προεκτάσεις και προβληματισμοί* (Doctoral dissertation, Ιόνιο Πανεπιστήμιο. Σχολή Επιστήμης της Πληροφορίας και Πληροφορικής. Τμήμα Αρχειονομίας, Βιβλιοθηκονομίας και Μουσειολογίας).

αποτελεσματικά.[144] Επιπλέον προσφέρει πολλά οφέλη στον ιδιοκτήτη του σπιτιού, συμπεριλαμβανομένης της εξοικονόμησης ενέργειας, εξοικονόμησης χρημάτων, 'διασυνδεδεμένης και πιο προσωποποιημένης ψυχαγωγίας' και αύξηση της ασφάλειας.

Χαρακτηριστικό παράδειγμα αποτελεί το σύστημα 'έξυπνου φωτισμού' που αποτελεί συνήθως αναπόσπαστο τμήμα ενός έξυπνου σπιτιού και ένας πολύ καλός τρόπος ελέγχου της ατμόσφαιρας του. Τέτοια συστήματα επιτρέπουν τον εύκολο έλεγχο μέσω απλών φωνητικών εντολών ή εφαρμογών στα κινητά. Προγραμματίζονται έτσι ώστε να ανάβουν να ή να σβήνουν, όταν οι χρήστες μπαίνουν ή βγαίνουν από το δωμάτιο αντίστοιχα, ώστε η σπατάλη ενέργειας να μην αποτελεί ανησυχία πλέον για αυτούς. Ο οικιακός αυτοματισμός έτσι, συμβάλλει και στην όσο το δυνατόν μεγαλύτερη ασφάλεια στο σπίτι. Με την εγκατάσταση έξυπνων καμερών, οι χρήστες μπορούν να παρακολουθούν το σπίτι τους από οπουδήποτε και οποτεδήποτε και να λαμβάνουν ειδοποιήσεις ασφαλείας στο κινητό τους. Οι έξυπνες κλειδαριές θυρών επίσης, ελαχιστοποιούν τον κίνδυνο να κλειδωθούν οι χρήστες έξω από το σπίτι, καθώς μπορούν να ασφαλίσουν και να κλειδώσουν την πόρτα από οπουδήποτε με σύνδεση στο διαδίκτυο.[145] Η παραγωγή 'έξυπνου καφέ' όπου μπορεί κάποιος να ετοιμάσει το ρόφημα του μέσω του τηλεφώνου του[146] ή τα ψυγεία που επιτρέπουν στον χρήση να ελέγξει απομακρυσμένα τι χρειάζεται από το σούπερ-μάρκετ[147] αποτελούν ακόμα μερικά παραδείγματα της καθημερινότητας των ατόμων σε ένα έξυπνο σπίτι.[148]

Ευλόγως συμπεραίνουμε ότι, ο ψηφιακός μετασχηματισμός των σπιτιών τα κατέστησε κατά κάποιον τρόπο σε 'παγκοσμιοποιημένα σπίτια', αφού η πρόσβαση είναι εύκολη από οπουδήποτε κυριολεκτικά, τα οφέλη για τους

---

[144] Janarthanan, T., Bagheri, M., & Zargari, S. (2021). IoT forensics: An overview of the current issues and challenges. *Digital Forensic Investigation of Internet of Things (IoT) Devices*, 223-254.

[145] Janarthanan, T., Bagheri, M., & Zargari, S. (2021). IoT forensics: An overview of the current issues and challenges. *Digital Forensic Investigation of Internet of Things (IoT) Devices*, 223-254.

[146] «Smarter Coffee», https://firebox.com/Smarter-Coffee/p6991

[147] «Family Hub Refrigerator, https://www.samsung.com/us/explore/family-hub-refrigerator/overview/

[148] Μιχαηλάκη, Α. (2021). *Δίκαιο και δεοντολογία στις εφαρμογές της επαυξημένης πραγματικότητας: τεχνολογικές προεκτάσεις και προβληματισμοί* (Doctoral dissertation, Ιόνιο Πανεπιστήμιο. Σχολή Επιστήμης της Πληροφορίας και Πληροφορικής. Τμήμα Αρχειονομίας, Βιβλιοθηκονομίας και Μουσειολογίας).

χρήστες είναι όντως τεράστια, ωστόσο η αναδιαμόρφωση των σπιτιών σε έξυπνους κόμβους τα καθιστά παράλληλα περισσότερο 'ανασφαλή' και λιγότερο 'ιδιωτικά' καθώς τα άτομα εκτίθενται σε αυξανόμενες απειλές από τον έξω κόσμο.[149] Μια σύντομη επισκόπηση της περιπτωσιολογίας ευπαθειών των έξυπνων συσκευών θα συνδράμει στην εναργέστερη κατανόηση του μεγέθους και του βαθμού των προκλήσεων που αυτά θέτουν στους χρήστες τους και κατ' επέκταση στους ερευνητές όταν καλούνται να τις αντιμετωπίσουν. Αξίζει να υπογραμμισθεί το παράδειγμα της 'έξυπνης' ηλεκτρικής σκούπας της LG, η οποία μπορεί να καθαρίσει μόνη της το δωμάτιο χάρη στους αισθητήρες που διαθέτει που της επιτρέπουν να ανιχνεύσει το μέγεθος και το σχήμα του χώρου και στη συνέχεια να το καθαρίσει. Ωστόσο, μια ομάδα ερευνητών ανακάλυψε μια ευπάθεια στην διαδικασία σύνδεσης σε μια πύλη της LG, η οποία τους επέτρεψε να πάρουν τον έλεγχο της ηλεκτρικής σκούπας και κατά συνέπεια να τους δώσει πρόσβαση σε βίντεο ζωντανής ροής (live streaming) από το εσωτερικό του σπιτιού!![150] Ανάλογο παράδειγμα αστοχίας και 'εκμετάλλευσης' ευπαθειών της 'ευφυΐας' των συσκευών αυτών, αποτελεί η 'έξυπνη' τοστιέρα η οποία σύμφωνα με το ιστορικό του περιστατικού φαίνεται να ενεργοποιήθηκε κατά την διάρκεια της νύχτας μόνη της προκαλώντας πυρκαγιά στο νοικοκυριό. [151]

Το 2014 καταγράφεται, η πρώτη ίσως κυβερνοεπίθεση που εκμεταλλεύτηκε τα τρωτά σημεία του συσκευών του ΔτΠ αποδεικνύοντας ότι και αυτές μπορούν να γίνουν θύματα εισβολέων hackers και όχι μόνο υπολογιστές και κινητά όπως μέχρι εσχάτως πιστεύαμε. Η αμερικανική εταιρία Κυβερνοασφάλειας Proofpoint, ανακάλυψε τότε ένα ψυγείο, το οποίο έστελνε στο διαδίκτυο ανεπιθύμητα και κακόβουλα ηλεκτρονικά μηνύματα (spam). Στην επιθετική αυτή διαδικτυακή «καμπάνια», που ενορχήστρωσαν οι εισβολείς (hackers), το ψυγείο συμμετείχε ανάμεσα σε πάνω από 100.000 άλλες συσκευές που απαρτίζαν το συγκεκριμένο

[149] Caviglione, L., Wendzel, S., Vrhovec, S., & Mileva, A. (2022). Security and Privacy Issues of Home Globalization. *IEEE Security & Privacy*, *20*(1), 10-11.

[150] Popken, B. (2017). Hacked Home Devices Can Spy On You-NBC News, OCT 26 2017, 2017. https://www.nbcnews.com/tech/security/hacked-home-devices-can-spy-you-n814671

[151] Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials*, *22*(2), 1191-1221.

κακόβουλο δίκτυο (botnet). Η επίθεση είχε ως στόχο ηλεκτρονικούς υπολογιστές, δρομολογητές, «έξυπνες» τηλεοράσεις ενώ το φοβερό της υπόθεσης είναι ότι τουλάχιστον το 25% αυτών των κακόβουλων μηνυμάτων δεν 'πέρασε' καθόλου μέσα από τους παραδοσιακούς διαύλους *(υπολογιστές ή/και 'έξυπνα τηλέφωνα')* αλλά εγκαταστάθηκε και διοχετεύτηκε μέσω άλλων 'έξυπνων οικιακών συσκευών'. Προφανώς και οι ιδιοκτήτες αυτών των συσκευών δεν γνώριζαν ότι οι συσκευές τους ήταν μέρος του κακόβουλου δικτύου και είχαν «αξιοποιηθεί» από αυτό για την αποστολή των ανεπιθύμητων μηνυμάτων σε άλλους χρήστες και επιχειρήσεις – στόχους. Καμία συσκευή που είχαν παραβιάσει οι εισβολείς (hackers) δεν απέστειλε περισσότερα από δέκα τέτοια μηνύματα, ώστε να μην είναι εύκολα ανιχνεύσιμη και άρα πιο δύσκολα να μπορεί να κατασταλεί η κυβερνοεπίθεση αυτή.[152]

Ενώ προχωρώντας, αξίζει να αναφερθεί ότι το 2016 καταγράφεται η δεύτερη μεγαλύτερη επίθεση τύπου *Κατανεμημένης Άρνησης Υπηρεσιών* (*Distributed Denial of Service - DDoS*) που έγινε ποτέ και είχε ως στόχο το Dyn, έναν πάροχο DNS. Με χρήση του κακόβουλου λογισμικού Mirai, δημιουργήθηκε ένα botnet από IoT συσκευές *(έξυπνες τηλεοράσεις, διαδικτυακούς εκτυπωτές κ.λπ.)* που παραβιάστηκαν και καταλήφθηκαν από τους επιτιθέμενους. Λόγω της σπουδαιότητας των υπηρεσιών του παρόχου, επηρεάστηκε η λειτουργία σε πολλές πλατφόρμες μεγάλων κολοσσών του ψηφιακού κόσμου, όπως Amazon, Visa, Twitter, AirBnB, Netflix, Github, μεταξύ άλλων.[153]

Από τα παραπάνω γίνεται αντιληπτό ότι οι επιπτώσεις των επιθέσεων στο οικοσύστημα του IoT είναι **μεγάλης κλίμακας** και ακολουθούν την 'λογική' ενός ντόμινο ως προς τον τρόπο επηρεασμού των έξυπνων συσκευών μεταξύ τους με αντίκτυπο φυσικά στον άνθρωπο και στον φυσικό κόσμο. Αυτό οφείλεται κυρίως στο γεγονός ότι η υποδομή αυτών των διασυνδεδεμένων συσκευών βασίζεται

[152]Μιχαηλάκη, Α. (2021). *Δίκαιο και δεοντολογία στις εφαρμογές της επαυξημένης πραγματικότητας: τεχνολογικές προεκτάσεις και προβληματισμοί* (Doctoral dissertation, Ιόνιο Πανεπιστήμιο. Σχολή Επιστήμης της Πληροφορίας και Πληροφορικής. Τμήμα Αρχειονομίας, Βιβλιοθηκονομίας και Μουσειολογίας).

[153]Καντζάβελου Ι.-Κάτος Β. (2021) «Ψηφιακή Δικανική» **Κεφ 16** στο συλλογικό τόμο "Ασφάλεια Πληροφοριών & Συστημάτων στον Κυβερνοχώρο", Σωκράτης Κάτσικας, Στέφανος Γκρίτζαλης, και Κωνσταντίνος Λαμπρινουδάκης (Επιστημονική Επιμέλεια), Εκδόσεις Νέων Τεχνολογιών, σελ.132

στην τεχνολογία ***Machine-to Machine (M2M)*** στην οποία ο μεγάλος αριθμός τερματικών και άλλων συσκευών αυξάνει το μέγεθος του στόχου μιας επίθεσης, εκθέτοντας τον έτσι σε υψηλότερο κίνδυνο.[154] Ο τύπος επίθεσης παίζει επίσης ουσιώδη ρόλο καθώς ενώ το μοντέλο παροχής της υπηρεσίας είναι **client-server,** οι κλασικές επιθέσεις μετασχηματίζονται επηρεάζοντας άμεσα τον φυσικό κόσμο απειλώντας την **ιδιωτικότητα** των ατόμων *(στο παράδειγμα της 'έξυπνης' σκούπας)* ακόμα και την **ανθρώπινη ζωή** όμως.

Όπως έχει λεχθεί και αναλυθεί σε προηγούμενο κεφάλαιο, οι συσκευές του ΔτΠ αποτελούν καταναλωτικές τεχνολογίες που δεν σχεδιάζονται με γνώμονα την ασφάλεια αυτών και κατ' επέκταση και των χρηστών τους, αλλά το κύριο μέλημα των κατασκευαστών τους αποτελεί η **ελαχιστοποίηση του κόστους** και του **μεγέθους των συσκευών** με στόχο την μεγαλύτερη χρηστικότητα και αυτονομία τους. Για αυτό τον λόγο φέρουν εγγενώς πολλά **τρωτά σημεία** και **ευπάθειες** που εκμεταλλεύονται οι δράστες εγκλημάτων του κυβερνοχώρου. Οι προκλήσεις για την ψηφιακή εγκληματολογία σε ένα τέτοιο περιβάλλον διακινδύνευσης είναι ποικίλες και εντοπίζονται σε κάθε στάδιο της εγκληματολογικής έρευνας.

Έτσι κατά την **ταυτοποίηση**, η οποία περιλαμβάνει καθήκοντα εντοπισμού και διαχείρισης πιθανών αποδεικτικών στοιχείων, ο ερευνητής είναι αντιμέτωπος με πλήθος συσκευών, η χωρική οριοθέτηση των οποίων δεν είναι πάντα εφικτή. Πράγματι, η φυσική εξέταση της σκηνής εγκλήματος δεν είναι πλέον επαρκής [155]για να καλύψει την έρευνα ή να ικανοποιήσει τους σκοπούς της κλασικής κατάσχεσης καθώς πχ κάποια 'έξυπνη συσκευή' ενδέχεται να βρίσκεται μεν στον υπό διερεύνηση χώρο αλλά όχι οι λοιπές έξυπνες συσκευές με τις οποίες αυτή επικοινωνεί ή το 'έξυπνο τηλέφωνο' μέσω του οποίου ελέγχεται. Ο αριθμός των συσκευών επίσης μπορεί να είναι μεγάλος και ίσως όχι τόσο προφανής τις περισσότερες φορές *(βλ. έξυπνη καφετιέρα, ψυγείο κτλ.)* Η μικρή αποθηκευτική

[154] Καντζάβελου Ι- Κάτος Β (2021) «Ψηφιακή Δικανική» **Κεφ 16** στο συλλογικό τόμο "Ασφάλεια Πληροφοριών & Συστημάτων στον Κυβερνοχώρο", Σωκράτης Κάτσικας, Στέφανος Γκρίτζαλης, και Κωνσταντίνος Λαμπρινουδάκης (Επιστημονική Επιμέλεια), Εκδόσεις Νέων Τεχνολογιών,σελ.132

[155] Diaz Linares, I., Pardo, A., Patch, E., Dehghantanha, A., & Choo, K. K. R. (2022). IoT Privacy, Security and Forensics Challenges: An Unmanned Aerial Vehicle (UAV) Case Study. *Handbook of Big Data Analytics and Forensics*, 7-39.

και υπολογιστική ισχύς των συσκευών αυτών από την άλλη, η εξάρτηση τους από το νέφος εξ 'αυτού του λόγου, αλλά και το εύρος της έρευνας χάρη στα δίκτυα 5G-, Z-Wave[156],ZigBee[157] περιπλέκει ακόμα περισσότερο την εγκληματολογική έρευνα -ήδη από το στάδιο της ταυτοποίησης-.

Προχωρώντας στο στάδιο της **απόκτησης** και της **διατήρησης** αποδεικτικών στοιχείων σε περιβάλλον IoT, η δυσκολία που εντοπίζεται εδώ για τους ερευνητές αφορά την **ετερογένεια** των συσκευών, την διαφορετική αρχιτεκτονική και **τεχνικές προδιαγραφές** που αυτά έχουν, τα διαφορετικά πρωτόκολλά επικοινωνίας που χρησιμοποιούν, γεγονός που απαιτεί εξοικείωση του εγκληματολόγου σε διαφορετικά πρότυπα κάθε φορά αλλά και εξειδικευμένα εγκληματολογικά εργαλεία προσαρμοσμένα στους διαφορετικούς τύπους συσκευών. Όσο για την διατήρηση, η πλειονότητα των αποθηκευμένων δεδομένων είναι κατά βάση πτητικά με μικρή περίοδο επιβίωσης για αυτό συνήθως προκρίνεται η επιλογή διενέργειας 'ζωντανής εγκληματολογικής έρευνας' η οποία ωστόσο εμπεριέχει ένα βαθμό αλλοίωσης των δεδομένων, γεγονός που επιδρά αρνητικά στην ακεραιότητα αυτών.[158] Επίσης, καθώς το περιβάλλον του ΔτΠ προϋποθέτει αλληλεπίδραση σε πραγματικό χρόνο και αυτονομία μεταξύ των διαφόρων κόμβων, η δυσκολία ανακατασκευής του εγκλήματος καθίσταται ακόμα μεγαλύτερη και εν συνεπεία ο υπολογισμός του εύρους της ζημίας.[159]

Η φάση της **ανάλυσης** επικεντρώνεται στην εξέταση και ανάλυση των δεδομένων που συλλέγονται για την ανεύρεση αποδεικτικών στοιχείων με την χρήση κατάλληλων εγκληματολογικών εργαλείων. Ωστόσο, επί του παρόντος

[156] Το Z-Wave είναι ένα πρωτόκολλο ασύρματης επικοινωνίας που χρησιμοποιείται κυρίως για αυτοματισμούς κατοικιών και εμπορικών κτιρίων. https://en.wikipedia.org/wiki/Z-Wave
[157] Το Zigbee είναι ένα πρωτόκολλο που χρησιμοποιείται για ασύρματη επικοινωνία μεταξύ συσκευών. https://en.wikipedia.org/wiki/Zigbee
[158] Diaz Linares, I., Pardo, A., Patch, E., Dehghantanha, A., & Choo, K. K. R. (2022). IoT Privacy, Security and Forensics Challenges: An Unmanned Aerial Vehicle (UAV) Case Study. *Handbook of Big Data Analytics and Forensics*, 7-39.
[159] Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials*, *22*(2), 1191-1221.

υπάρχει έλλειψη ενιαίων προτύπων για τις συσκευές ΔτΠ ενώ παράλληλα η απουσία ενοποίησης με πρωτόκολλα δεδομένων, πλατφόρμες και συνδέσμους προκαλούν αναποτελεσματικότητα και σύγχυση ως προς την διαχείριση των στοιχείων. Τα παραδοσιακά εγκληματολογικά εργαλεία θεωρούνται πεπερασμένα και πολλοί από τους τύπους δεδομένων των συσκευών IoT ενδέχεται να είναι για αυτά μη αναγνώσιμοι.[160]

Προφανώς και τα ελλείματα των προηγούμενων σταδίων αντανακλώνται και στο τελευταίο στάδιο της εγκληματολογικής έρευνας, αυτό της **παρουσίασης** των αποδεικτικών στοιχείων ενώπιον του δικαστηρίου. Μέχρι να αναπτυχθεί μια πιο αποτελεσματική διαδικασία για την διερεύνηση περιστατικών που σχετίζονται με το IoT, οι δράστες θα συνεχίζουν να επωφελούνται από την έλλειψη αξιόπιστων και ακριβών αποδεικτικών στοιχείων σε βάρος τους.

7.2. 'Έξυπνες συσκευές, Φερόμενες συσκευές και ψηφιακή εγκληματολογική έρευνα

7.2.1 Εφαρμογές, Οφέλη, Τεχνικές Προκλήσεις

Η επανάσταση της τεχνολογίας του IoT που επιτρέπει σε μικρές συσκευές να λειτουργούν ως 'έξυπνα' αντικείμενα[161] με στόχο την διευκόλυνση, την αυτοματοποίηση και εξατομικευμένη εμπειρία στην καθημερινότητα των χρηστών, διασχίζει κάθε πτυχή της ανθρώπινης έκφανσης και δεν σταματά στα όρια του οικιακού αυτοματισμού προφανώς. Στον τομέα της ένδυσης για παράδειγμα, αξεσουάρ και ρούχα δύνανται να κάνουν όλο και περισσότερα από τον αρχικό στόχο παραγωγής τους, δηλαδή απλά την κάλυψη της ανάγκης για ένδυση. Όλο και περισσότερες εταιρίες επιδίδονται και επικεντρώνονται στην παραγωγή 'έξυπνων ρούχων' τα οποία φέρουν ενσωματωμένους αισθητήρες τελευταίας τεχνολογίας και έχουν την δυνατότητα να προστατεύσουν την

[160] Diaz Linares, I., Pardo, A., Patch, E., Dehghantanha, A., & Choo, K. K. R. (2022). IoT Privacy, Security and Forensics Challenges: An Unmanned Aerial Vehicle (UAV) Case Study. *Handbook of Big Data Analytics and Forensics*, 7-39

[161] Alabdulsalam, S., Schaefer, K., Kechadi, T., & Le-Khac, N. A. (2018). Internet of things forensics–challenges and a case study. In *Advances in Digital Forensics XIV: 14th IFIP WG 11.9 International Conference, New Delhi, India, January 3-5, 2018, Revised Selected Papers 14* (pp. 35-48). Springer International Publishing.

ανθρώπινη υγεία και ζωή.[162] Για παράδειγμα το 'MIMO' φορμάκι για τα βρέφη που αποτελεί ένα από τα πιο φιλόδοξα προϊόντα στον τομέα της υγείας, είναι σχεδιασμένο να προειδοποιεί για τον κίνδυνο αιφνίδιου θανάτου του μωρού[163] ή ο αθλητικός στηθόδεσμος που μπορεί να προειδοποιήσει για καρκίνο του μαστού[164]. Παραμένοντας στον τομέα της υγείας, η Google έχει ήδη γνωστοποιήσει ότι βρίσκεται σε διαδικασία ανάπτυξης 'έξυπνων φακών επαφής' οι οποίοι θα μπορούν να μετρούν το επίπεδο του σακχάρου στα δάκρυα των διαβητικών[165]. Είναι αντιληπτό ότι οι διαστάσεις που λαμβάνουν αυτές οι τεχνολογίες και τα πιθανά οφέλη για τον άνθρωπο από το ΔτΠ είναι σημαντικά και αναμένονται να γίνουν όλο και σημαντικότερα.

Η κοινωνία όμως της πληροφορίας και τεχνολογίας δεν παύει να αποτελεί μια κοινωνία διακινδύνευσης,[166] που πέρα από τα οφέλη μπορεί να φτάσει να απειλήσει ακόμα και την ανθρώπινη ζωή. Συγκεκριμένα, τον Ιανουάριο του 2017, ο FDA[167] προειδοποίησε ότι ορισμένοι βηματοδότες, οι οποίοι ουσιαστικά είναι ένα σύστημα που στέλνει ηλεκτρικά ερεθίσματα στην καρδιά για να ρυθμίσει τον καρδιακό παλμό, είναι ευάλωτοι σε 'πειρατεία'.[168] Αυτό πρακτικά σημαίνει ότι όποιος χρησιμοποιούσε τον ευάλωτο βηματοδότη εκείνη την χρονική στιγμή θα μπορούσε να έρθει αντιμέτωπος με τον θάνατο, εφόσον η ζωή του/της γινόταν

---

[162] Μιχαηλάκη, Α. (2021). *Δίκαιο και δεοντολογία στις εφαρμογές της επαυξημένης πραγματικότητας: τεχνολογικές προεκτάσεις και προβληματισμοί* (Doctoral dissertation, Ιόνιο Πανεπιστήμιο. Σχολή Επιστήμης της Πληροφορίας και Πληροφορικής. Τμήμα Αρχειονομίας, Βιβλιοθηκονομίας και Μουσειολογίας).

[163] Danny Chrichton, «With Mimo, MIT Alums Are Disrupting the Baby Nursery, Onesie at a Time» https://techcrunch.com/2015/01/27/withmimo-mit-alums-are-disrupting-the-baby-nursery-onesie-at-a-time, σε Hillary Brill και Scott Jones

[164] «Αυτό είναι το έξυπνο σουτιέν της Microsoft!» (2013) https://www.inewsgr.com/61/afto-einai-to-exypno-soutien-tis-Microsoft.htm

[165] Keum, D. H., Kim, S. K., Koo, J., Lee, G. H., Jeon, C., Mok, J. W., ... & Hahn, S. K. (2020). Wireless smart contact lens for diabetic diagnosis and therapy. *Science advances*, *6*(17), eaba3252.

[166] Beck, U. (2015). Κοινωνία της διακινδύνευσης: Καθ'οδόν προς μία άλλη νεωτερικότητα (μτφρ.: Οικονόμου Η.). *Αθήνα: Πεδίο*.

[167] Food and Drug Administration, ανήκει στο υπουργείο υγείας των Ηνωμένων Πολιτειών και είναι υπεύθυνος για την έγκριση τροφίμων και φαρμάκων. https://ti-einai.gr/fda/

[168] FDA (2017), Safety Communications - Cybersecurity Vulnerabilities Identified in St. Jude Medicals Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication, 2017

αντικείμενο ενός χάκερ που θα μπορούσε να πάρει τον έλεγχο του βηματοδότη. Περαιτέρω, στην βιομηχανία της γυμναστικής, οι πιο κοινά διαδεδομένες «έξυπνες» συσκευές είναι αυτές που μπορούν να φορεθούν (wearables). Οι συσκευές αυτές περιέχουν αισθητήρες που παρακολουθούν τον καρδιακό παλμό, τα βήματα ή τις συνήθειες κατά τη διάρκεια του ύπνου. Τα «έξυπνα» ρολόγια επίσης συγκεντρώνουν παρόμοια δεδομένα και με τη βοήθεια των τεχνολογιών WiFi και GPS, μπορεί ο χρήστης να ανακαλύψει τι απόσταση διένυσε και πού, πόσα βήματα πραγματοποίησε ή πόσα σκαλοπάτια ανέβηκε. Η πληροφορία που μεταφέρεται μέσω των διαδικτυακών συνδέσεων καταχωρείται με τέτοιο τρόπο, ώστε ο χρήστης να μπορεί να τη διατηρήσει ή να τη διαμοιραστεί.[169]
Αναντίρρητα, η διείσδυση αυτών των συσκευών στην ιδιωτική σφαίρα, η συλλογή ευαίσθητων -κατά βάση- πληροφοριών, η δημιουργία προφίλ του χρήστη μέσω των συνηθειών του, τα καθιστά ουσιαστικά όχι 'φερόμενα' αλλά 'ενσωματώσιμα' λόγω των δυνατοτήτων τους να αφουγκράζονται τον χρήστη σε τέτοιο βαθμό και να επικοινωνούν μεταξύ τους αλλά και με το περιβάλλον.

7.2.2 Μελέτη περίπτωσης εγκληματολογικής διερεύνησης σε 'έξυπνο' ρολόι

Η προσέγγιση για την απόκτηση και ανάλυση συσκευών IoT εξακολουθούν να είναι επικεντρωμένες στην συσκευή (device level).

Ένα έξυπνο ρολόι χρησιμοποιείται ως επί το πλείστον όπως ένα έξυπνο τηλέφωνο, έχοντας παρόμοιες λειτουργίες ενώ η συνδεσιμότητα του στο διαδίκτυο αποτελεί πύλη για την συλλογή αποδεικτικού υλικού. Έχει την δυνατότητα να λειτουργεί με άλλες συσκευές αλλά και ανεξάρτητα. Πολλά από τα δεδομένα που καταγράφει ένα smartwatch, όπως τα δεδομένα προπόνησης, εκκινούν χειροκίνητα από τον χρήστη ενώ άλλα δεδομένα όπως καρδιακοί παλμοί, βήματα κτλ. καταγράφονται **αυτόματα**, ενώ πολύ σημαντικό για την εγκληματολογική έρευνα είναι ότι όλα τα δεδομένα συνοδεύονται από

[169] Μιχαηλάκη, Α. (2021). *Δίκαιο και δεοντολογία στις εφαρμογές της επαυξημένης πραγματικότητας: τεχνολογικές προεκτάσεις και προβληματισμοί* (Doctoral dissertation, Ιόνιο Πανεπιστήμιο. Σχολή Επιστήμης της Πληροφορίας και Πληροφορικής. Τμήμα Αρχειονομίας, Βιβλιοθηκονομίας και Μουσειολογίας).

χρονοσφραγίδες. Σε διάδραση του έξυπνου ρολογιού με το έξυπνο τηλέφωνο, από την μελέτη περίπτωσης που διεξήχθη σε έξυπνο ρολόι γνωστής μάρκας[170], εντοπίστηκε ότι τα δεδομένα γεωεντοπισμού (GPS) δεν βρέθηκαν ποτέ στο έξυπνο ρολόι αλλά μόνο στο έξυπνο τηλέφωνο με το οποίο συνδεόταν. Το ρολόι ωστόσο όχι μόνο παράγει δεδομένα αλλά και αποθηκεύει -για αυτό άλλωστε διερευνάται ως ξεχωριστή συσκευή- για να γίνει όμως αυτό πρέπει πρώτα να έχει αντιστοιχηθεί με το έξυπνο κινητό και να έχει πιστοποιηθεί στο ίδιο δίκτυο Wi-Fi, με αποτέλεσμα να είναι προφανείς οι δυσκολίες και οι προϋποθέσεις με τις οποίες έρχεται αντιμέτωπος ο ερευνητής προκειμένου να διεξάγει την έρευνα του *(να είναι και τα δυο στην κατοχή του, να διεξάγει 'ζωντανή' έρευνα κτλ.).* Τοπικά στο ρολόι αποθηκεύονται και ανευρίσκονται ωστόσο *(ακόμα και μετά την απενεργοποίηση του έξυπνου κινητού)* i-messages, μηνύματα κειμένου τα οποία μπορούν να γραφτούν και να διαβαστούν από το ρολόι **απευθείας ,** όχι όμως να αποσταλούν *(χρειάζεται η ενεργοποίηση του έξυπνου κινητού)*, αλλά και εικόνες δύνανται να είναι τοπικά αποθηκευμένες.

Είναι προφανές λοιπόν, πόσο δαιδαλώδης και εργώδης είναι η διαδικασία της ψηφιακής εγκληματολογικής έρευνας σε ένα τέτοιο οικοσύστημα λαμβάνοντας κιόλας υπόψη τους παρόντες περιορισμούς (τυποποιημένων διαδικασιών και εργαλείων αλλά και αξιολόγηση αυτών).

8. ΈΞΥΠΝΑ ΚΙΝΗΤΑ (SMARTPHONES) ΚΑΙ ΨΗΦΙΑΚΗ ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΗ ΕΡΕΥΝΑ (SMARTPHONE FORENSICS)

Η-σχεδόν-καθολική χρήση 'έξυπνων' τηλεφώνων, η ραγδαία αύξηση και καταναλωτικοποίηση τους και οι τεράστιες δυνατότητες που αυτά προσφέρουν στους χρήστες, είναι αναμφισβήτητα.

[170] Alabdulsalam, S., Schaefer, K., Kechadi, T., & Le-Khac, N. A. (2018). Internet of things forensics–challenges and a case study. In *Advances in Digital Forensics XIV: 14th IFIP WG 11.9 International Conference, New Delhi, India, January 3-5, 2018, Revised Selected Papers 14* (pp. 35-48). Springer International Publishing.

Το γεγονός ότι τα έξυπνα κινητά δεν περιορίζονται μόνο στις παραδοσιακές λειτουργίες όπως φωνητικές κλήσεις και μηνύματα κειμένου αλλά προσφέρουν μια ποικιλία δυνατοτήτων όπως υπηρεσίες παγκοσμίου συστήματος εντοπισμού θέσης (GPS), υπηρεσίες ηλεκτρονικού ταχυδρομείου, εγγραφή βίντεο, περιήγηση στο διαδίκτυο και ποικίλες εφαρμογές[171], σε συνδυασμό με το μικρό και εργονομικό τους μέγεθος, τα καθιστά τόσο δημοφιλή μεταξύ των λοιπών έξυπνων συσκευών σε βαθμό να αποτελούν 'προέκταση' του χεριού μας και να διατρέχουν όλες τις καθημερινές μας δραστηριότητες. Για αυτό τον λόγο αποτελούν και τεράστιο αποθετήριο προσωπικών δεδομένων των χρηστών που παράγεται και αποθηκεύεται σε αυτά, δεδομένα που μπορούν να αξιοποιηθούν στο πλαίσιο μιας ψηφιακής εγκληματολογικής έρευνας για σκοπούς πρόληψης ανίχνευσης ή και απόδειξης παραβάσεων και αξιόποινων συμπεριφορών. Ακόμα και όταν το έξυπνο κινητό δεν χρησιμοποιείται ενεργά από τον χρήστη, παράγει προσωπικές πληροφορίες για αυτόν, όπως ίχνη θέσης, καταγραφές ημερομηνίας- ώρας ενεργοποίησης ή τερματισμού λειτουργίας του smartphone.
Η εγκληματολογική έρευνα στα 'έξυπνα' κινητά αποτελεί υποκατηγορία της ψηφιακής εγκληματολογίας, ένα σχετικά νέο αναδυόμενο εγκληματολογικό μοντέλο *(που ερευνάται και αναπτύσσεται την τελευταία δεκαετία)* και παρόλο που φέρει κοινά χαρακτηριστικά με την εγκληματολογία υπολογιστών, αποτελεί ξεχωριστό και διακριτό κλάδο.

8.1 Πηγές αποδεικτικών στοιχείων στα έξυπνα κινητά

Προκειμένου να συσχετιστούν τα δεδομένα των smartphone με τους τύπους αποδεικτικών στοιχείων, ακολουθείται συνήθως μια ανάλυση προσανατολισμένη στα δεδομένα. Η ανάλυση αξιοποιεί την κατηγοριοποίηση των δεδομένων smartphone ως εξής:

[171] Tsavli, M., Efraimidis, P. S., Katos, V., & Mitrou, L. (2015). Reengineering the user: privacy concerns about personal data on smartphones. *Information & Computer Security*, *23*(4), 394-405.

- ***Δεδομένα μηνυμάτων,*** πρόκειται για το περιεχόμενο και τα μεταδεδομένα των μηνυμάτων, (πχ αποστολέας, χρόνος παράδοσης κτλ.) από υπηρεσίες μηνυμάτων (λχ SMS και ηλεκτρονικό ταχυδρομείο)[172]
- ***Δεδομένα συσκευής,*** δηλαδή δεδομένα που βρίσκονται στα αποθηκευτικά μέσα της συσκευής και δεν σχετίζονται με καμία εφαρμογή όπως αρχεία πολυμέσων, αναγνωριστικά λογισμικού και υλικού μεταξύ άλλων)
- ***Δεδομένα (U)SIM κάρτας*** όπως η διεθνής ταυτότητα συνδρομητή κινητής τηλεφωνίας (IMSI) που ταυτοποιεί τον συνδρομητή στο δίκτυο
- ***Ιστορικό καταγραφής χρήστη,*** όπως ιστορικό περιήγησης στο διαδίκτυο ή αρχείο κλήσεων
- ***Δεδομένα εγκατεστημένων εφαρμογών,*** ήτοι προσωρινά ή μόνιμα δεδομένα που χρησιμοποιούνται για τους λειτουργικούς σκοπούς των εφαρμογών του κινητού
- ***Δεδομένα αισθητήρων,*** που παράγονται από τους αισθητήρες που βρίσκονται στις περισσότερες συσκευές {όπως μικρόφωνο, κάμερα, GPS, **αισθητήρες κίνησης** (γυροσκόπιο, επιταχυνσιόμετρο) ή **αισθητήρες περιβάλλοντος** (φως, θερμοκρασία, εγγύτητα, μαγνητόμετρο κτλ.)
- ***Δεδομένα 'εισόδου' του χρήστη,*** που πρακτικά αποτελεί την ενεργή διάδραση του χρήστη με το κινητό του όπως πληκτρολογήσεις,

τα οποία επεξεργάζονται εν κινήσει ή αποθηκεύονται σε μια κρυφή μνήμη πληκτρολογίου για λόγους απόδοσης.[173]

[172] Mylonas, A., Meletiadis, V., Tsoumas, B., Mitrou, L., & Gritzalis, D. (2012). Smartphone forensics: A proactive investigation scheme for evidence acquisition. In *Information Security and Privacy Research: 27th IFIP TC 11 Information Security and Privacy Conference, SEC 2012, Heraklion, Crete, Greece, June 4-6, 2012. Proceedings 27* (pp. 249-260). Springer Berlin Heidelberg.

[173] Mylonas, A., Meletiadis, V., Tsoumas, B., Mitrou, L., & Gritzalis, D. (2012). Smartphone forensics: A proactive investigation scheme for evidence acquisition. In *Information Security and Privacy Research: 27th IFIP TC 11 Information Security and Privacy Conference, SEC 2012, Heraklion, Crete, Greece, June 4-6, 2012. Proceedings 27* (pp. 249-260). Springer Berlin Heidelberg.

8.2 Προληπτική Εγκληματολογία

Καθώς η συμπεριφορά των δεδομένων και δυνητικών αποδεικτικών στοιχείων είναι δυναμική και χρονικά ευαίσθητη και ασταθής *(ιδιαιτέρως των δεδομένων από αισθητήρες)*, σε συνδυασμό με την ποικιλομορφία των πηγών και τις δυνατότητες που αυτή μπορεί να προσφέρει στην στοιχειοθέτηση προφίλ του δράστη αλλά και ανακατασκευής της σκηνής εγκλήματος, μεγάλο μέρος της βιβλιογραφίας και των ακαδημαϊκών ερευνών στρέφεται προς την **προληπτική εγκληματολογία**. Η προληπτική εγκληματολογία **(Proactive Digital Forensics- ProDF)**[174] και η εγκληματολογική ετοιμότητα που αυτή πρεσβεύει, είναι ένα οργανωτικό πλαίσιο για την ανάπτυξη διαδικασιών που αποσκοπούν στην μεγιστοποίηση της ικανότητας ενός περιβάλλοντος να συλλέγει αξιόπιστο αποδεικτικό υλικό ελαχιστοποιώντας ταυτόχρονα το κόστος της ψηφιακής εγκληματολογικής έρευνας. Ενσωματώνει τεχνικές για ζωντανή εγκληματολογία (live forensics) έτσι ώστε να εγγυάται την αξιοποίηση και των πιο ευμετάβλητων δεδομένων (όπως είναι και τα περισσότερα από τα smartphones). Σύμφωνα με αυτό το προτεινόμενο σχήμα προληπτικής έρευνας, πραγματοποιείται **ad hoc** απόκτηση αποδεικτικών στοιχείων από smartphone(s) και μόνο για την διερεύνηση ιδιαιτέρως σοβαρών εγκλημάτων *(παρόμοιας βαρύτητας με εκείνα που απαιτούνται για την άρση του απορρήτου).* Οι δρώντες σε αυτό το σχήμα είναι τρεις: **α)** το υποκείμενο που διεξάγει την προληπτική εγκληματολογική έρευνα μέσω smartphone ή αλλιώς **ο ερευνητής β)** μια **Ανεξάρτητη αρχή** που θα λειτουργεί ως θεσμικό αντίβαρο και εγγυητής των δικαιωμάτων των διερευνώμενων προσώπων **γ)** το υποκείμενο της έρευνας, ήτοι ο '**ύποπτος**'.[175] Τον ουσιαστικότερο ρόλο διαδραματίζει η ανεξάρτητη αρχή ως 'εξισοροπιστής' που θα **ελέγχει** την συλλογή αποδεικτικού υλικού από το λογισμικό που θα έχει εγκατασταθεί στο έξυπνο κινητό του υπόπτου, θα **ελέγχει** το χρονικό διάστημα αποθήκευσης των σχετικών αποδεικτικών στοιχείων έτσι ώστε να είναι **σύννομο** με σχετικά κανονιστικά πλαίσια και θα **εγκρίνει** τα αιτήματα των ερευνητών για προληπτική έρευνα κατά ατόμων. Με αυτή την αρχιτεκτονική διασφαλίζεται <u>ότι δεν θα συσσωρεύονται εξουσίες στο πρόσωπο του ερευνητή</u> που θα μπορούσαν να οδηγήσουν σε κατάχρηση και φαλκίδευση της όλης διαδικασίας ενώ επιπλέον τα δυνητικά αποδεικτικά στοιχεία θα προστατεύονται με τον ενδεδειγμένο τρόπο και υπό τους όρους της εμπιστευτικότητας, ακεραιότητας και εν γένει εγκληματολογικής ορθότητας. Σχετικά με τον ρόλο του ερευνητή, αυτός είναι να συλλέξει επαρκή αποδεικτικά στοιχεία και κατάλληλα για χρήση στο δικαστήριο ενώ τα αιτήματα του για προληπτική εγκληματολογική έρευνα **θα πρέπει να περιορίζονται** όταν οι υπόλοιπες πηγές αποδεικτικών στοιχείων έχουν 'αποτύχει' να δώσουν ακριβή στοιχεία ή δεν υφίστανται άλλες πηγές και σε κάθε περίπτωση όταν το υπό διερεύνηση έγκλημα είναι ιδιαιτέρως σοβαρό όπως υπογραμμίσθηκε και παραπάνω.

---

[174] Grobler, C., Louwrens, C., Von Solms, S.: A Multi -component View of Digital Forensics. In: Aleksy, M., Ghernaouti-Helie, S., Quirchmayr, G. International Conference on Avail ability Reliability and Security (ARES '10), 2010 p. 647-652

[175] Mylonas, A., Meletiadis, V., Tsoumas, B., Mitrou, L., & Gritzalis, D. (2012). Smartphone forensics: A proactive investigation scheme for evidence acquisition. In *Information Security and Privacy Research: 27th IFIP TC 11 Information Security and Privacy Conference, SEC 2012, Heraklion, Crete, Greece, June 4-6, 2012. Proceedings 27* (pp. 249-260). Springer Berlin Heidelberg.

Καθώς οι πληροφορίες που μπορεί να συλλεχθούν από ένα έξυπνο κινητό, μπορούν να είναι τρομερά αποκαλυπτικές για το άτομο *(και ευαίσθητες όπως βιομετρικά δεδομένα μεταξύ άλλων)* σε συνδυασμό με τις πληροφορίες που παράγονται συνεχώς και -εν αγνοία του- πολλές φορές, όπως αυτές από τους αισθητήρες του κινητού δημιουργούν ένα βαθμό επιτήρησης του ατόμου που προσιδιάζει τον βαθμό επιτήρησης ενός κρατούμενου στην φυλακή,[176] ή ενός «κατασκόπου» στην τσέπη του χρήστη.[177]

Για αυτό πρέπει να επιτευχθεί η 'χρυσή τομή' ανάμεσα στην ιδιωτικότητα και την προστασία των προσωπικών δεδομένων και της πληροφοριακής αυτοδιάθεσης των ατόμων ώστε να μην διακυβεύονται από καταχρηστικές παρεμβάσεις των αρχών αλλά ταυτόχρονα να μπορεί να μην μένει αναξιοποίητο ένα τέτοιο 'οπλοστάσιο' αποδεικτικού πλούτου για τις διωκτικές αρχές.[178]

8.2.1. Προληπτική εγκληματολογική ανάλυση αισθητήρων smartphones & λογισμικό 'Themis'

Στην ίδια λογική εγκληματολογικής ετοιμότητας με το παραπάνω προταθέν σχήμα, κινείται και το ερευνητικό (ακόμα) λογισμικό '**Themis'**[179] για την συλλογή αποδεικτικού υλικού από τους αισθητήρες των έξυπνων κινητών τηλεφώνων. Με την εκθετική αύξηση των smartphones, επήλθε και η αντίστοιχη αύξηση και χρήση αισθητήρων *(υλικού που μετρά το περιβάλλον του χρήστη)* και το οποίο όπως ήδη έχει τονιστεί προσφέρει πλούσιο υλικό για το πλαίσιο μέσα στο οποίο κινείται ο χρήστης.

Ωστόσο τα δεδομένα αυτά είναι **ευμετάβλητα** και σε συνδυασμό με την **ετερογένεια** των πλατφορμών smartphones και την εξειδίκευση που απαιτεί αυτή η ετερογένεια σε **εργαλεία** αλλά *(πχ ειδικό λογισμικό, καλώδια δεδομένων ή τροφοδοσίας ανά κάθε τύπο συσκευής smartphone)* και η αντίστοιχη **τεχνογνωσία** που πρέπει να επιδεικνύει κάθε φορά ο ερευνητής για να υποστηρίξει την έρευνα, ανέδειξε την ανάγκη δημιουργίας ενός λογισμικού που θα είναι **διαπλατφορμικό** και θα επιχειρεί **απομακρυσμένη** και **ad hoc** συλλογή αποδείξεων από τους αισθητήρες των smartphone **<u>εν τη γενέσει τους</u>**. Και αυτό διότι μεταγενέστερη εργαστηριακή ανάλυση για αυτή την κατηγορία δεδομένων δεν είναι εφικτή *(μόνο τα δεδομένα GPS μπορούν να συλλεχθούν σε post mortem ανάλυση)*. Το λογισμικό

---

[176] Davis, D. (2014) "Your mobile phone is watching YOU", *Mail Online*, 12-01-2014. Διαθέσιμο στο https://www.dailymail.co.uk/news/article-2537828/Your-mobile-phone-watching-YOU-writes-DAVID-DAVIS-Campaigning-former-Shadow-Home-Secretarys-phone-log-reveals-insidious-tracking-move.html

[177] Green, N., & Smith, S. (2004). 'A Spy in your Pocket'? The Regulation of Mobile Data in the UK. *Surveillance and Society*.

[178] **Από τα χαρακτηριστικότερα και πιο πρόσφατα παραδείγματα της ελληνικής νομολογίας περί αποδεικτικής θεμελίωσης μέσω smartphone, αποτελεί η περίπτωση κατά την οποία ο κατηγορούμενος κηρύχθηκε ένοχος για ανθρωποκτονία με δόλο (σε ήρεμη ψυχική κατάσταση) από το ΜΟΔ στην Αθήνα, λαμβανομένων υπόψη δεδομένων από το κινητό του τηλέφωνο, από το οποίο προέκυψε ότι -παρά τον αρχικό του ισχυρισμό-, βρισκόταν στον ίδιο όροφο με την παθούσα την ώρα του θανάτου της τελευταίας. Η εικοσάχρονη παθούσα είχε στραγγαλιστεί εντός της οικίας της τον Μάιο του 2021 και αρχικώς υπήρχαν υπόνοιες ότι η πράξη είχε τελεστεί από ληστές**. Γιάννης Ναζίρης «Η κατάσχεση των ψηφιακών δεδομένων» Ηλεκτρονικό Έγκλημα (Ουσιαστικές και δικονομικές όψεις) ΝΒ,2023 σελ.456

[179] Mylonas, A., Meletiadis, V., Mitrou, L., & Gritzalis, D. (2013). Smartphone sensor data as digital evidence. *Computers & Security*, *38*, 51-75.

αυτό θα χρησιμοποιεί ασύρματο κανάλι μέσω ενδεδειγμένου πρωτοκόλλου που θα εγγυάται την συμμόρφωση με τα νομοθετικά και κανονιστικά πλαίσια **προστασίας δεδομένων και απορρήτου.** Για την εγκατάσταση αυτού του λογισμικού προϋποτίθεται προεγκατάσταση σε μια ειδική ROM στο πλαίσιο ασφάλειας μιας κρίσιμης υποδομής πχ, και με την συνεργασία του εκάστοτε παρόχου smartphone ή την μεταγενέστερή εγκατάσταση στο πλαίσιο διερεύνησης υπόπτου υπό όρους 'κοινωνικής μηχανικής' για την αποδοχή του μεν, υπό πολύ αυστηρές διαδικαστικές προϋποθέσεις δε, λόγω της έντονης διείσδυσης στην ιδιωτική σφαίρα του ατόμου. Άλλωστε, οι νόμοι που εξουσιοδοτούν το κράτος να παρεμβαίνει στην ιδιωτική, επικοινωνιακή και πληροφοριακή αυτοδιάθεση πρέπει να είναι **προσβάσιμοι** και **προβλέψιμοι**, σε ένα κράτος δικαίου.[180]

Στο πλαίσιο ευρύτερης γνώσης και ευαισθητοποίησης των χρηστών αλλά και όλων των εμπλεκομένων στην παραγωγή εφαρμογών τεχνολογιών πληροφορικής και επικοινωνιών, γύρω από το νομοθετικό πλαίσιο και τον σεβασμό των προσωπικών δεδομένων, της ιδιωτικότητας και του απορρήτου των επικοινωνιών, καλό είναι να επανεξεταστεί και να αναδιαμορφωθεί ο **αδειοδοτικός μηχανισμός** που χρησιμοποιείται για την εγκατάσταση εφαρμογών στα κινητά μας τηλέφωνα. Ειδικά σε μελέτες που έγιναν σε λογισμικό Android[181], παρατηρήθηκε ότι δεν υφίσταται καμία διαφάνεια τόσο ως προς τις συνεχώς αυξανόμενες αιτήσεις αδειών για χρήση αισθητήρων κτλ. πριν την εγκατάσταση μιας εφαρμογής όσο και ως προς την τύχη των παρεχόμενων δεδομένων μέσα από την υποτιθέμενη συγκατάθεση των χρηστών. Αμφισβητείται η νομιμότητα των αδειών αυτών καθώς συχνά ομαδοποιούνται άσχετα μεταξύ τους δεδομένα (που δεν χρειάζονται για την λειτουργία της αιτούμενης εφαρμογής πχ), δεν υπάρχει ουσιαστικός έλεγχος της 'πρόσβασης' της εφαρμογής καθώς οι χρήστες δεν έχουν την δυνατότητα επιλογής (η άδεια έχει την μορφή όλα ή τίποτα) με ένα κλικ. Η προστασία της ιδιωτικότητας κλυδωνίζεται καθώς δεν υπάρχει **ούτε ενημέρωση του χρήστη** όπως θα έπρεπε να είναι, ούτε τηρείται η **αρχή του περιορισμού του σκοπού** και **απαγόρευση ασύμβατων, δευτερευουσών χρήσεων,** ούτε τηρείται **η αρχή της αναλογικότητας,** ή **χρονικός περιορισμός** των συλλεχθέντων δεδομένων**.**

Πέρα από την ανάγκη αναδιαμόρφωσης των αδειών και μεγαλύτερης διαφάνειας αυτών, υπάρχει ανάγκη ανάπτυξης τεχνικών δεξιοτήτων, ειδικότερων γνώσεων γύρω από τις ιδιαιτερότητες της εγκληματολογίας των έξυπνων κινητών, της εγκληματολογικής ετοιμότητας και της αυτοματοποίησης. Με την αιγίδα του ευρωπαϊκού ερευνητικού προγράμματος Horizon 2020, δημιουργήθηκε το πλάνο εργασίας **FORMOBILE**[182] που αποσκοπεί στον προσδιορισμό ενός νέου προγράμματος σπουδών για την εκπαίδευση πάνω στην εγκληματολογία των κινητών για τα όργανα επιβολής του νόμου και τις διωκτικές

[180] Mylonas, A., Meletiadis, V., Mitrou, L., & Gritzalis, D. (2013). Smartphone sensor data as digital evidence. *Computers & Security*, *38*, 51-75.

[181] Tsavli, M., Efraimidis, P. S., Katos, V., & Mitrou, L. (2015). Reengineering the user: privacy concerns about personal data on smartphones. *Information & Computer Security*, *23*(4), 394-405.

[182]Paullet, K., Pinchot, J., & Mishra, S. (2017). IMPLEMENTING A SUCCESSFUL TRAIN-THE-TRAINER PROGRAM IN MOBILE FORENSICS AND SECURITY. *Issues in Information Systems*, *18*(1).

αρχές, αναδεικνύοντας έμπρακτα την ανάγκη διεπιστημονικής κατάρτισης και εξειδίκευσης στον κλάδο αυτό.[183]

9. ΠΛΗΡΟΦΟΡΙΕΣ ΑΠΟ ΑΝΟΙΚΤΕΣ ΠΗΓΕΣ (OPEN-SOURCE INTELLIGENCE) & SOCIAL MEDIA EVIDENCE

Ένα νέο σύνορο στην ψηφιακή εγκληματολογία και σημαντική προσθήκη στην εργαλειοθήκη του ερευνητή ψηφιακών πειστηρίων αποτελούν οι πληροφορίες από ανοικτές πηγές. Ως τέτοια θεωρείται η πληροφορία η οποία φιλοξενείται σε οποιαδήποτε πηγή του Διαδικτύου και είναι ελεύθερης πρόσβασης ή είναι δυνατή η πρόσβαση σε αυτή κατόπιν εγγραφής του χρήστη.[184] Οι πληροφορίες που είναι ευρέως διαθέσιμες αφορούν φυσικά πρόσωπα, συνδεδεμένες υπολογιστικές συσκευές, καθώς και τους συσχετισμούς αυτών. Αντιπροσωπευτικότερη κατηγορία ανοικτής πηγής για συλλογή προσωπικών δεδομένων και δυνητικών αποδεικτικών στοιχείων αποτελούν τα μέσα κοινωνικής δικτύωσης.

Στον όρο κοινωνικά δίκτυα συγκαταλέγονται όλα τα κανάλια επικοινωνίας που χρησιμοποιούνται για την αλληλεπίδραση, την συνεργασία και την ανταλλαγή περιεχομένου εντός του δικτύου/της κοινότητας.[185] Αποτελούν πλούσια πηγή πληροφορίας για πιθανούς υπόπτους, θύματα αλλά και μάρτυρες ενώ περιλαμβάνει αναρτήσεις κειμένου, λίστες φίλων, εικόνες, βίντεο, δεδομένα γεωγραφικής θέσης τα οποία ενδείκνυνται για την σκιαγράφηση της συμπεριφοράς των ατόμων, τις προτιμήσεις τους, τις μεταξύ τους σχέσεις, την παρατήρηση επιχειρηματικών τάσεων, ακόμα και ενδείξεις ιατρικών καταστάσεων (πχ αν κάποιος βιώνει κατάθλιψη κτλ.). Το 2014, μια έρευνα κατέδειξε την σημαντικότητα αυτής της αχαρτογράφητης πηγής πληροφοριακού πλούτου, χαρακτηρίζοντας την εγκληματολογία των μέσων κοινωνικής δικτύωσης ως **ψηφιακή εγκληματολογία 2.0** και οι συγγραφείς πρότειναν ότι η υποκατηγορία αυτή αποτελεί το μέλλον της ψηφιακής εγκληματολογίας.[186] Στατιστικά δε, σημειώνεται ταχεία αύξηση των δικών που περιλαμβάνουν στοιχεία από τα μέσα κοινωνικής δικτύωσης, αρχής γενομένης το 2012 και με εκθετική πορεία έκτοτε.[187]

Ωστόσο είναι σημαντικό να τονισθεί ότι από δικανικής πλευράς οι πληροφορίες που αποκτήθηκαν από ανοικτές πηγές ενδέχεται να μην είναι παραδεκτές, καθώς η εγκυρότητα των πηγών μπορεί να αμφισβητηθεί, ειδικά όταν δεν συνοδεύονται από τα σχετικά μεταδεδομένα που αυθεντικοποιούν την ταυτότητα του χρήστη/υπόπτου. Οι ανοικτές πηγές

[183] Humphries, G., Nordvik, R., Manifavas, H., Cobley, P., & Sorell, M. (2021). Law Enforcement educational challenges for mobile forensics. *Forensic science international: Digital investigation*, *38*, 301129.
[184] Καντζάβελου Ι.-Κάτος Β. (2021) «Ψηφιακή Δικανική» **Κεφ. 16** στο συλλογικό τόμο "Ασφάλεια Πληροφοριών & Συστημάτων στον Κυβερνοχώρο", Σωκράτης Κάτσικας, Στέφανος Γκρίτζαλης, και Κωνσταντίνος Λαμπρινουδάκης (Επιστημονική Επιμέλεια), Εκδόσεις Νέων Τεχνολογιών, σελ.116
[185] Arshad, H., Jantan, A., & Omolara, E. (2019). Evidence collection and forensics on social networks: Research challenges and directions. *Digital Investigation*, *28*, 126-138.
[186] Keyvanpour, M., Moradi, M., & Hasanzadeh, F. (2014). Digital forensics 2.0: A review on social networks forensics. *Computational Intelligence in Digital Forensics: Forensic Investigation and Applications*, 17-46.
[187] Arshad, H., Jantan, A., & Omolara, E. (2019). Evidence collection and forensics on social networks: Research challenges and directions. *Digital Investigation*, *28*, 126-138.

στην πλειοψηφία τους άλλωστε δεν είναι σχεδιασμένες για δικανική χρήση, τα δεδομένα είναι ευμετάβλητα, ενδεχομένως ημιτελή και ανανεώνονται με τρόπο δυναμικό.

Για το παραδεκτό του αποδεικτικού υλικού που έχει συλλεχθεί από τα κοινωνικά μέσα, για δικαστηριακή χρήση, απαιτείται να επιβεβαιωθεί **η αυθεντικότητα του συντάκτη** του δυνάμει αποδεικτικού στοιχείου καθώς και να διασφαλισθεί η **αυθεντικότητα** και η **ακεραιότητα** του υλικού αυτού καθ' αυτού. Οι προκλήσεις και τα ερευνητικά κενά βέβαια είναι ακόμα πολλά σε αυτό το νέο αναδυόμενο εγκληματολογικό μοντέλο, όμως οι ερευνητικοί στόχοι για τον εξορθολογισμό και την σύννομη αξιοποίηση φαίνεται πως κινούνται προς την σωστή κατεύθυνση.

10. (ΨΗΦΙΑΚΗ) ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΗ ΕΡΕΥΝΑ ΜΕ ΓΝΩΜΟΝΑ ΤΗΝ ΙΔΙΩΤΙΚΗ ΖΩΗ

Η ψηφιακή εγκληματολογία και η ιδιωτική ζωή είναι δυο έννοιες **εγγενώς αλληλοσυγκρουόμενες** και αυτό διότι με την ιδιωτικότητα εκφράζεται η επιθυμία των ανθρώπων να αποφασίζουν οι ίδιοι πότε, πως και σε ποιο βαθμό οι προσωπικές τους πληροφορίες μοιράζονται με άλλους ενώ σκοπός της ψηφιακής έρευνας αποτελεί η απόκτηση και ανάλυση τέτοιων δεδομένων από συσκευές με τρόπο σύννομο ώστε να είναι και αποδεκτό.[188]

Οι ψηφιακές εγκληματολογικές έρευνες διεξάγονται συνήθως αφού προηγηθεί κατάσχεση των συσκευών από υπόπτους και τρίτους, οι οποίοι εν συνεπεία χάνουν τον έλεγχο των δεδομένων στα οποία έχει πρόσβαση ο ερευνητής. Επιπλέον, τα ψηφιακά εγκληματολογικά εργαλεία δύνανται να ανακτήσουν ακόμα και πληροφορίες που δεν υπάρχουν πλέον στην υπό διερεύνηση συσκευή γιατί ο χρήστης είχε αποφασίσει να τις διαγράψει. Να σημειωθεί εδώ ότι τα εργαλεία αυτά, μπορούν ακόμα να συσχετίσουν πληροφορίες από διαφορετικές πηγές, περικλείοντας νέους παράγοντες (τρίτους) στην έρευνα των οποίων η ιδιωτική ζωή μπορεί να επηρεαστεί. Πρόκειται για τρίτα πρόσωπα[189] άσχετα με την ψηφιακή έρευνα και τους υπόπτους, των οποίων τα προσωπικά δεδομένα έρχονται ουσιαστικά στο φως λόγω του ότι ανευρίσκονται αποθηκευμένα στις διερευνώμενες ψηφιακές συσκευές.

Είναι εμφανής λοιπόν και όλο και περισσότερο αποφασιστικής σημασίας η ανάγκη θωράκισης της ιδιωτικότητας τόσο τεχνολογικά/τεχνικά όσο και νομικά/κανονιστικά, ώστε ο χρήστης και ο σεβασμός της ιδιωτικής του ζωής να αποτελεί την κατευθυντήρια δύναμη σε κάθε ψηφιακή έρευνα χωρίς ωστόσο να παρακωλύεται το έργο της εγκληματολογικής έρευνας. Και ενώ τα κανονιστικά κείμενα ιδιαιτέρως τα ευρωπαϊκά ενισχύονται ολοένα και περισσότερο {βλ. Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου (άρθρο 8-σεβασμός στην ιδιωτικότητα) αλλά και Γενικό Κανονισμό Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, γίνονται συστηματικές έρευνες και προσπάθειες από την ακαδημαϊκή

[188] Ren, W., Wang, L., Xhafa, F., & Choo, K. K. R. (Eds.). (2019). *Security and Privacy for Big Data, Cloud Computing and Applications* (Vol. 28). Computing and Networks.

[189] **Γνωστό και ως παραβίαση της ιδιωτικής ζωής τρίτων (Third Party Privacy Breach-TPPB)**

κοινότητα και όχι μόνο ώστε να δημιουργηθούν και τεχνολογίες που θα ενσωματώνουν την απαίτηση για ιδιωτικότητα στις εγκληματολογικές έρευνες.

Υπάρχουν κατά βάση δύο τρόποι θωράκισης του ψηφιακού απορρήτου από τεχνολογική σκοπιά, αυτές είναι τα **PETs *(Privacy Enhancing Technologies),*** τεχνολογίες που ενσωματώνουν τις θεμελιώδεις αρχές προστασίας των δεδομένων, ελαχιστοποιώντας τη χρήση προσωπικών δεδομένων και μεγιστοποιώντας την ασφάλεια και τον έλεγχο αυτών από τα υποκείμενα των δεδομένων (τους χρήστες) αλλά και την ενσωμάτωση της απαίτησης για **σεβασμό της ιδιωτικότητας κατά τον σχεδιασμό των τεχνολογιών *(Privacy by design-άρθρο 25 ΓΚΠΔ)*.** Σε αυτή την κατηγορία τεχνολογικών εργαλείων σύμφωνα με την βιβλιογραφία, εμπίπτουν τεχνολογίες που προσφέρουν **ανακλητή ανωνυμία** ή **κρυπτογράφηση με δυνατότητα αναζήτησης (***κυρίως για τις ψηφιακές έρευνες που επικεντρώνονται στον διακομιστή).* Η ανακλητή ανωνυμία αναφέρεται στην διαδικασία που επιτρέπει στους χρήστες να περιηγούνται και να λαμβάνουν υπηρεσίες ανώνυμα, εκτός αν η διαδικτυακή τους συμπεριφορά εγείρει υποψίες, οπότε και μπορούν να ταυτοποιηθούν εκ νέου με την συνδρομή ενός έμπιστου τρίτου μέρους.[190]

Αυτό είναι το είδος της προσέγγισης που ακολουθείται από το **PPINA** *(Protect Private Information, Not Abuser)*[191]. Η ιδέα αυτή επιτρέπει στους χρήστες να συνδεθούν στο διακομιστή μέσω ενός ανώνυμου δικτύου επικοινωνίας, αλλά πριν το κάνουν αυτό, οφείλουν να δημιουργήσουν ένα ζεύγος δημόσιου/ιδιωτικού κλειδιού και ένα διακριτικό πρόσβασης. Το διακριτικό πρόσβασης συνδέεται κρυπτογραφικά με το δημόσιο κλειδί του χρήστη. Εν συνεχεία, το διακριτικό αποστέλλεται σε ένα έμπιστο τρίτο μέρος (την εγκληματολογική υπηρεσία), το οποίο επαληθεύει την εγκυρότητα του διακριτικού και το αποθηκεύει με την ταυτότητα του χρήστη. Ο διακομιστής λαμβάνει επίσης ένα αντίγραφο του αναγνωριστικού επιβεβαιωμένο όμως αυτή την φορά από το έμπιστο τρίτο μέρος. Στην συνέχεια το επαληθεύει χωρίς να γνωρίζει την ταυτότητα του χρήστη, ο οποίος και εγκαθιστά σύνδεση με αυτόν μέσω ενός ανώνυμου δικτύου. Ο διακομιστής αποθηκεύει επίσης το διακριτικό και όλα τα μηνύματα που υπογράφονται με το κλειδί που αντιστοιχεί σε αυτό. Σε περίπτωση που ο χρήστης συμπεριφέρεται ύποπτα, ο διακομιστής στέλνει όλα τα μηνύματα και το διακριτικό στην εγκληματολογική υπηρεσία για να αποφασίσει αν έγινε επίθεση ή όχι και αν πρέπει να προβεί στην αποκάλυψη της ταυτότητας του χρήστη.

Στο ίδιο πνεύμα κινείται και το πρωτόκολλο **ERPINA**[192], το οποίο επίσης έχει ως γνώμονα τον σεβασμό τόσο της επιθυμίας του χρήστη για ανωνυμία κατά την πρόσβαση σε ένα διακομιστή όσο και το δικαίωμα αυτού του διακομιστή να μπορεί να έχει πρόσβαση στην

---

[190] Nieto, A., Rios, R., Lopez, J., Ren, W., Wang, L., Choo, K. K. R., & Xhafa, F. (2019). Privacy-aware digital forensics.

[191] Antoniou, G., Wilson, C., & Geneiatakis, D. (2006). PPINA–a forensic investigation protocol for privacy enhancing technologies. In *Communications and Multimedia Security: 10th IFIP TC-6 TC-11 International Conference, CMS 2006, Heraklion, Crete, Greece, October 19-21, 2006. Proceedings 10* (pp. 185-195). Springer Berlin Heidelberg.

[192] Antoniou, G., Sterling, L., Gritzalis, S., & Udaya, P. (2008). Privacy and forensics investigation process: The ERPINA protocol. *Computer Standards & Interfaces*, *30*(4), 229-236.

ταυτότητα του χρήστη στην περίπτωση που ο τελευταίος εμφανίζει παραβατική συμπεριφορά. Η κύρια διαφορά με το προηγούμενο πρωτόκολλο έγκειται ότι εν προκειμένω, το διακριτικό που λαμβάνει ο χρήστης ενσωματώνει μια πολιτική χρήσης. Όσον αφορά την **κρυπτογράφηση με δυνατότητα αναζήτησης**, είναι μια κρυπτογραφική τεχνική που επιτρέπει την υποβολή ερωτημάτων σε μια κρυπτογραφημένη βάση δεδομένων με την μορφή λέξης-κλειδί, μια τεχνική πολλά υποσχόμενη για την προστασία της ιδιωτικής ζωής των χρηστών κατά την διεξαγωγή ψηφιακών ερευνών. Κατ' αυτόν τον τρόπο ο ερευνητής κάνει στοχευμένη έρευνα και αναζήτηση αποδεικτικού υλικού χωρίς να διακυβεύονται τα προσωπικά δεδομένα τρίτων.

Μια ακόμα όψη του σεβασμού της ιδιωτικότητας ακόμα και στις πιο διεισδυτικές επεμβάσεις στην ιδιωτική ζωή όπως είναι η διεξαγωγή εγκληματολογικών ερευνών, σε μια ψηφιοποιημένη ζωή τέτοιου βαθμού δε, αποτελεί η ευαισθητοποίηση και παρακίνηση ανάπτυξης δεξιοτήτων όχι μόνο από τους εγκληματολόγους αλλά απ' όλα τα μέλη της κοινωνίας της πληροφορίας.

Η ηθική των υπολογιστών η οποία αποτελεί κλάδο της Ηθικής, μας εισάγει πρακτικά σε κάτι τέτοιο και περιλαμβάνει την ελευθερία, την ισότητα, καθήκοντα και υποχρεώσεις για τα μέλη, επιλογές αλλά και αιτιολόγηση αυτών. Είναι η συστηματική μελέτη του ηθικού και κοινωνικού αντικτύπου των υπολογιστών στην ΚτΠ και ενσωματώνει την απόκτηση, διανομή, αποθήκευση, επεξεργασία και την διάδοση ψηφιακών δεδομένων καθώς και τον τρόπο με τον οποίο τα άτομα και οι ομάδες αλληλοεπιδρούν με τα συστήματα και τα δεδομένα. Επανεξετάζει ουσιαστικά τις ηθικές διαστάσεις των Κυβερνοεγκλημάτων και των ερευνών που σχετίζονται με αυτά.[193] Με την πάροδο των ετών, η ηθική των υπολογιστών έχει αποκτήσει ολοένα και μεγαλύτερη σημασία. Δεν συνδέεται μόνο με θέματα που αφορούν το έγκλημα στον κυβερνοχώρο και την Κυβερνοασφάλεια, αλλά συνδέεται επίσης με τις ψηφιακές εγκληματολογικές έρευνες και τις νοηματοδοτεί. Καθώς η ψηφιακή εγκληματολογία απαιτεί '***έναν ισορροπημένο συνδυασμό τεχνικών δεξιοτήτων, νομικής οξυδέρκειας και ηθικής συμπεριφοράς***' η προσθήκη αυτού του μαθήματος στο πλαίσιο ενίσχυσης της εγκληματολογικής παιδείας θα ήταν εξαιρετικά σημαντική για τους ερευνητές και όχι μόνο.[194]

[193] Choi, K., Back, S., & Toro-Alvarez, M. M. (2022). *Digital Forensics & Cyber Investigation*. Cognella Academic.

[194] Choi, K., Back, S., & Toro-Alvarez, M. M. (2022). *Digital Forensics & Cyber Investigation*. Cognella Academic.

ΑΝΤΙ ΕΠΙΛΟΓΟΥ

Είναι προφανές ότι εφόσον το Διαδίκτυο δεν έχει σύνορα, έτσι και τα εγκλήματα που σχετίζονται με αυτό θα είναι διασυνοριακά και θα απαιτούν διασυνοριακή πρόσβαση σε ψηφιακά αποδεικτικά στοιχεία. Όσο και αν τα εθνικά κράτη νομοθετούν διατάξεις ουσιαστικού Ποινικού Δικαίου που τιμωρούν τις καταχρήσεις των νέων τεχνολογιών, το βασικό πρόβλημα εξακολουθεί να εδράζεται στην δυσκολία **συλλογής** και **αξιοποίησης αποδεικτικών στοιχείων** που θα οδηγήσουν τους Κυβερνοεγκληματίες στον φυσικό τους δικαστή.[195] Για αυτό η στόχευση προς την δημιουργία αξιόπιστων, ταχέων και σύννομων μεθόδων απόκτησης τους θα πρέπει να αποτελεί προτεραιότητα των διωκτικών αρχών. Χαρακτηριστική ερευνητική προσπάθεια προς αυτή την κατεύθυνση αποτελεί η πλατφόρμα **LOCARD ,** η οποία συνιστά ένα πρόγραμμα που χρηματοδοτήθηκε από την Ευρωπαϊκή Ένωση στο πλαίσιο του Horizon 2020, και αποσκοπεί στην **αυτοματοποίηση** της συλλογής **δικαστικά παραδεκτών ψηφιακών πειστηρίων**, κάθε μορφής, με στόχο την αύξηση της εμπιστοσύνης στην διαχείριση και επεξεργασία των ψηφιακών δεδομένων.[196] Το 'κυνήγι απειλών στον Κυβερνοχώρο' ή αλλιώς προληπτική εγκληματολογία πρέπει να ενισχυθεί και να προσανατολιστεί επίσης στις σύγχρονες, αυξανόμενες απαιτήσεις **εξειδίκευσης του επιστημονικού προσωπικού** που διεξάγουν ψηφιακές έρευνες με έμφαση στους πρώτους ανταποκριτές (εκείνους που καταφθάνουν πρώτοι στην σκηνή του εγκλήματος) καθώς είναι καταλυτικός ο ρόλος που θα διαδραματίσουν κατά την ανίχνευση, συλλογή και προτεραιοποίηση της αξιολόγησης του αποδεικτικού υλικού. Παράλληλα, είναι σημαντικό να γίνει κατανοητό ότι η **έλλειψη τυποποίησης εγκληματολογικών εργαλείων** (ειδικά στις περιπτώσεις εγκληματολογικής έρευνας σε 'έξυπνα κινητά') αφήνει 'αναξιοποίητο' πλούσιο ψηφιακό αποδεικτικό πεδίο που μοιραία οδηγεί στην έλλειψη επιβολής από μέρους των διωκτικών αρχών. Η προβληματική αυτή αναδεικνύει την ανάγκη πρόβλεψης **πιστοποιήσεων** και **εγγυήσεων** για τα εργαλεία αυτά, που θα διασφαλίζουν την αποτελεσματικότητα τους στα διαφορετικά περιβάλλοντα και λειτουργικά των κινητών τηλεφώνων. Πέρα από την αξιοπιστία που πρέπει να παρέχουν, η οποία συμπαρασύρει και την αξιοπιστία της ίδιας της διαδικασίας συλλογής των ψηφιακών αποδεικτικών στοιχείων και κατ' επέκταση **την αξιοπιστία** και το **παραδεκτό** αυτών, η εφαρμογή τους στις ψηφιακές έρευνες θα πρέπει να εποπτεύεται από μια **ανεξάρτητη αρχή** που θα λειτουργεί εξισορροπητικά ώστε να μην φαλκιδεύεται η διαδικασία της ψηφιακής εγκληματολογικής έρευνας και να μην καταστρατηγούνται τα δικαιώματα και οι ελευθερίες των υπό διερεύνηση ατόμων.

Οι παραπάνω απαιτήσεις όπως και οι αρχές που πρέπει να διέπουν τον χειρισμό των ψηφιακών δεδομένων φαίνεται να είναι ακόμα πιο δαιδαλώδεις σε περιβάλλοντα

---

[195]Βασιλάκη Ε. (2022) 'Η εξέλιξη του Ποινικού Δικαίου Πληροφορικής το έτος 2022' Επιθεώρηση Δικαίου Πληροφορικής, ***Information Law Journal*** https://doi.org/10.26262/infolawj.v3i2.9236

[196] 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. Συγκεκριμένα, υποστήριξε ότι η επαφή ενός υποκειμένου ή αντικειμένου με ένα άλλο, έχει ως αποτέλεσμα την ανταλλαγή υλικού, όπως πχ 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. Ματάμη, Ε. (2022). Ψηφιακά πειστήρια και αποδεικτικές απαγορεύσεις στην ποινική δίκη σε εθνικό και υπερεθνικό επίπεδο.

Διαδικτύου των Πραγμάτων (ΔτΠ) ειδικότερα λόγω των διαστάσεων που μπορεί να λάβει μια επίθεση και της δυσκολίας ανεύρεσής των εμπλεκόμενων συσκευών που χρησιμοποιούνται τις περισσότερες φορές ως «δούρειος ίππος» για την επίθεση του τελικού στόχου. Ομοίως, ιδιαίτερα απαιτητική παρουσιάζεται η ψηφιακή έρευνα σε περιβάλλον νεφοϋπολογιστικής λόγω της εικονικότητας, της πολυμισθωτικής φύσης, της αστάθειας των δεδομένων εκεί, της αβέβαιης χρονοσήμανσης που θα οδηγούσε στην χρονική αλληλουχία των γεγονότων αλλά και της αβεβαιότητας ως προς την δικαιοδοσία αυτών, ειδικά όταν η διερεύνηση και δίωξη εγκλημάτων συνδέονται αυστηρά με την εδαφική κυριαρχία και την εδαφικά καθορισμένη δικαιοδοσία.[197]

Ίσως, η Τεχνητή Νοημοσύνη (ΤΝ), η συνθετότητα της και η ταχύτητα με την οποία εξελίσσεται αποτελέσει ένα εξαιρετικά χρήσιμο εργαλείο, τόσο στην πρόληψη όσο και στην καταστολή του εγκλήματος σε ιδιωτικό και δημόσιο τομέα και ειδικότερα στα όργανα επιβολής του νόμου, βελτιώνοντας την ποιότητα των ερευνών, μειώνοντας σημαντικά τον χρόνο αναζήτησης και εύρεσης νέων στοιχείων και βοηθώντας στην ανάπτυξη αντιμέτρων.

Και εδώ ωστόσο, είναι στο χέρι μας να δημιουργήσουμε ρυθμιστικούς/εποπτικούς φορείς και σύνολο κανόνων μέσα από τους οποίους θα απολαμβάνουμε τα πλεονεκτήματά που προσφέρει η ΤΝ χωρίς όμως να θυσιάζονται θεμελιώδη προσωπικά δικαιώματα και ατομικές ελευθερίες[198] ούτε να διαιωνίζονται ρατσιστικές και άλλες προκαταλήψεις.[199]

[197] Marangos, N., Rizomiliotis, P., & Mitrou, L. (2012, December). Digital forensics in the cloud computing era. In 2012 IEEE Globecom Workshops (pp. 775-780). IEEE.

[198] Χρυσοχού Χ. (2018) Τεχνητή Νοημοσύνη & Έγκλημα: Μια άλλη διάσταση, Crime Times ΚΕΜΕ https://www.crimetimes.gr/%CF%84%CE%B5%CF%87%CE%BD%CE%B7%CF%84%CE%AE-%CE%BD%CE%BF%CE%B7%CE%BC%CE%BF%CF%83%CF%8D%CE%BD%CE%B7-%CE%AD%CE%B3%CE%BA%CE%BB%CE%B7%CE%BC%CE%B1-%CE%BC%CE%B9%CE%B1-%CE%AC%CE%BB%CE%BB%CE%B7-%CE%B4%CE%B9/

[199] Η Καθημερινή, 2022 «Τεχνητή νοημοσύνη προβλέπει με ακρίβεια 90% τα εγκλήματα σε μία πόλη, μία εβδομάδα πριν» (Πρόκειται για το ακριβέστερο αλγοριθμικό εργαλείο που έχει αναπτυχθεί μέχρι σήμερα) https://www.kathimerini.gr/life/science/561936034/techniti-noimosyni-provlepei-me-akriveia-90-ta-egklimata-se-mia-poli-mia-evdomada-prin/

ΒΙΒΛΙΟΓΡΑΦΙΑ

❖ ΞΕΝΟΓΛΩΣΣΗ ΗΛΕΚΤΡΟΝΙΚΗ ΚΑΙ ΕΝΤΥΠΗ

- Alabdulsalam, S., Schaefer, K., Kechadi, T., & Le-Khac, N. A. (2018). Internet of things forensics–challenges and a case study. In Advances in Digital Forensics XIV: 14th IFIP WG 11.9 International Conference, New Delhi, India, January 3-5, 2018, Revised Selected Papers 14 (pp. 35-48). Springer International Publishing.
- Antoniou, G., Sterling, L., Gritzalis, S., & Udaya, P. (2008). Privacy and forensics investigation process: The ERPINA protocol. Computer Standards & Interfaces, 30(4), 229-236
- Antoniou, G., Wilson, C., & Geneiatakis, D. (2006). PPINA–a forensic investigation protocol for privacy enhancing technologies. In Communications and Multimedia Security: 10th IFIP TC-6 TC-11 International Conference, CMS 2006, Heraklion, Crete, Greece, October 19-21, 2006. Proceedings 10 (pp. 185-195). Springer Berlin Heidelberg.
- Arshad, H., Jantan, A., & Omolara, E. (2019). Evidence collection and forensics on social networks: Research challenges and directions. Digital Investigation, 28, 126-138.
- Beck, U. (2015). Κοινωνία της διακινδύνευσης: Καθ'οδόν προς μία άλλη νεωτερικότητα (μτφρ.: Οικονόμου Η.). Αθήνα: Πεδίο.
- Bernal, P. (2016). Data gathering, surveillance and human rights: recasting the debate. Journal of Cyber Policy, 1(2), 243-264
- Cardenas, A. A., Manadhata, P. K., & Rajan, S. P. (2013). Big data analytics for security. IEEE Security & Privacy, 11(6), 74-76.
- Caviglione, L., Wendzel, S., Vrhovec, S., & Mileva, A. (2022). Security and Privacy Issues of Home Globalization. IEEE Security & Privacy, 20(1), 10-11
- CHETAN SHARMA, «CORRECTING THE IOT HISTORY», 2016
- Choi, K., Back, S., & Toro-Alvarez, M. M. (2022). Digital Forensics & Cyber Investigation. Cognella Academic
- Davidoff, S., & Ham, J. (2012). Network forensics: tracking hackers through cyberspace (Vol. 2014). Upper Saddle River: Prentice hall
- Diaz Linares, I., Pardo, A., Patch, E., Dehghantanha, A., & Choo, K. K. R. (2022). IoT Privacy, Security and Forensics Challenges: An Unmanned Aerial Vehicle (UAV) Case Study. Handbook of Big Data Analytics and Forensics, 7-39
- ENISA, Introduction to Network Forensics Handbook, final version 1.0, Jan 2019 p.10-13
- European Commission, Information Society and Media, ό.π, σελ. 9, GAUL B./KOEHLER, L.M., Mitarbeiterdaten in der Computer Cloud: Datenschutzrechtliche Grenzen des Outsourcing, BB 2011, σελ. 2229
- FDA (2017), Safety Communications - Cybersecurity Vulnerabilities Identified in St. Jude Medicals Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication, 2017
- Green, N., & Smith, S. (2004). 'A Spy in your Pocket'? The Regulation of Mobile Data in the UK. Surveillance and Society

- Grobler, C., Louwrens, C., Von Solms, S.: A Multi -component View of Digital Forensics. In: Aleksy, M., Ghernaouti-Helie, S., Quirchmayr, G. International Conference on Avail ability Reliability and Security (ARES '10), 2010 p. 647-652
- Haeberlen, A. (2010). A case for the accountable cloud. ACM SIGOPS Operating Systems Review, 44(2), 52-57
- Harbawi, M., & Varol, A. (2017, April). An improved digital evidence acquisition model for the Internet of Things forensic I: A theoretical framework. In 2017 5th International Symposium on Digital Forensic and Security (ISDFS) (pp. 1-6). IEEE.
- Hegarty, R., Merabti, M., Shi, Q., & Askwith, B. (2009, June). Forensic analysis of distributed data in a service oriented computing platform. In proceedings of the 10th Annual Postgraduate Symposium on The Convergence of Telecommunications, Networking & Broadcasting, PG Net
- Humphries, G., Nordvik, R., Manifavas, H., Cobley, P., & Sorell, M. (2021). Law Enforcement educational challenges for mobile forensics. Forensic science international: Digital investigation, 38, 301129.
- Janarthanan, T., Bagheri, M., & Zargari, S. (2021). IoT forensics: An overview of the current issues and challenges. Digital Forensic Investigation of Internet of Things (IoT) Devices, 223-254.
- Keum, D. H., Kim, S. K., Koo, J., Lee, G. H., Jeon, C., Mok, J. W., ... & Hahn, S. K. (2020). Wireless smart contact lens for diabetic diagnosis and therapy. Science advances, 6(17), eaba3252.
- Keyvanpour, M., Moradi, M., & Hasanzadeh, F. (2014). Digital forensics 2.0: A review on social networks forensics. Computational Intelligence in Digital Forensics: Forensic Investigation and Applications, 17-46.
- Kott, A., Swami, A., & West, B. J. (2016). The internet of battle things. Computer, 49(12), 70-75
- Landau, S. (2020, October). Categorizing uses of communications metadata: Systematizing knowledge and presenting a path for privacy. In New Security Paradigms Workshop 2020 (pp. 1-19)
- Lutta, P., Sedky, M., Hassan, M., Jayawickrama, U., & Bastaki, B. B. (2021). The complexity of internet of things forensics: A state-of-the-art review. Forensic Science International: Digital Investigation, 38, 301210
- M. Scott Boone, Ubiquitous Computing, Virtual Worlds, and the Displacement of Property Right, 4 Journal of Law & Policy for the Information Society 2008, σ. 91
- Marangos, N., Rizomiliotis, P., & Mitrou, L. (2012, December). Digital forensics in the cloud computing era. In 2012 IEEE Globecom Workshops (pp. 775-780). IEEE
- Marangos, N., Rizomiliotis, P., & Mitrou, L. (2012, December). Digital forensics in the cloud computing era. In 2012 IEEE Globecom Workshops (pp. 775-780). IEEE
- Mattern, F., & Floerkemeier, C. (2010). From the Internet of Computers to the Internet of Things (pp. 242-259). Springer Berlin Heidelberg
- Mukasey, M. B., Sedgwick, J. L., & Hagy, D. W. (2008). Electronic crime scene investigation: A guide for first responders. NCJ, 219941.
- Mylonas, A., Meletiadis, V., Tsoumas, B., Mitrou, L., & Gritzalis, D. (2012). Smartphone forensics: A proactive investigation scheme for evidence acquisition. In Information Security and Privacy Research: 27th IFIP TC 11 Information Security and Privacy

Conference, SEC 2012, Heraklion, Crete, Greece, June 4-6, 2012. Proceedings 27 (pp. 249-260).
- Nieto, A., Rios, R., Lopez, J., Ren, W., Wang, L., Choo, K. K. R., & Xhafa, F. (2019). Privacy-aware digital forensics.
- Oriwoh, E., Jazani, D., Epiphaniou, G., & Sant, P. (2013, October). Internet of things forensics: Challenges and approaches. In 9th IEEE International Conference on Collaborative computing: networking, Applications and Worksharing (pp. 608-615). IEEE
- Paullet, K., Pinchot, J., & Mishra, S. (2017). IMPLEMENTING A SUCCESSFUL TRAIN-THE-TRAINER PROGRAM IN MOBILE FORENSICS AND SECURITY. Issues in Information Systems, 18(1).
- Perumal, S., Norwawi, N. M., & Raman, V. (2015, October). Internet of Things (IoT) digital forensic investigation model: Top-down forensic approach methodology. In 2015 Fifth International Conference on Digital Information Processing and Communications (ICDIPC) (pp. 19-23). IEEE.
- Popken, B. (2017). Hacked Home Devices Can Spy On You-NBC News, OCT 26 2017, 2017
- Ren, W., Wang, L., Xhafa, F., & Choo, K. K. R. (Eds.). (2019). Security and Privacy for Big Data, Cloud Computing and Applications (Vol. 28). Computing and Networks.
- Simou, S., Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2014). Cloud forensics solutions: A review. In Advanced Information Systems Engineering Workshops: CAiSE 2014 International Workshops, Thessaloniki, Greece, June 16-20, 2014. Proceedings 26 (pp. 299-309). Springer International Publishing
- Stergiou, C., Psannis, K. E., Kim, B. G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. Future Generation Computer Systems, 78, 964-975
- Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. IEEE Communications Surveys & Tutorials, 22(2), 1191-1221.
- Taylor, M., Haggerty, J., Gresty, D., & Hegarty, R. (2010). Digital evidence in cloud computing systems. Computer law & security review, 26(3), 304-308.
- Tsavli, M., Efraimidis, P. S., Katos, V., & Mitrou, L. (2015). Reengineering the user: privacy concerns about personal data on smartphones. Information & Computer Security, 23(4), 394-405
- Watson, D. L., & Jones, A. (2013). Digital forensics processing and procedures: Meeting the requirements of ISO 17020, ISO 17025, ISO 27001 and best practice requirements. Newnes.
- Wicker, S. B. (2013). Cellular convergence and the death of privacy. Oxford University Press, USA.
- Williams, J. (2012). Acpo good practice guide for digital evidence. Metropolitan Police Service, Association of chief police officers, GB, 1556-6013
- Yaacoub, J. P. A., Noura, H. N., Salman, O., & Chehab, A. (2022). Advanced digital forensics and anti-digital forensics for IoT systems: Techniques, limitations and recommendations. Internet of Things, 19, 100544.

❖ ΕΛΛΗΝΙΚΗ ΗΛΕΚΤΡΟΝΙΚΗ ΚΑΙ ΕΝΤΥΠΗ

- Αναστασίου, Ι. (2019). Ψηφιακή εγκληματολογία και ανάλυση σε κινητές συσκευές (Doctoral dissertation, University of Piraeus (Greece))
- Γκύζης Δ, (2023) Αντεισαγγελέας Εφετών 'Ψηφιακή ανακριτική πράξη' Ηλεκτρονικό Έγκλημα (Ουσιαστικές και δικονομικές όψεις), NB σελ.358, 374
- Δαγκλής Ν., Δαλακούρας Θ., Δανιήλ Γ., Κιούπης Δ., Ναζίρης Γ., Νούσκαλης Γ.,Παπαθανασίου Α., Νάιντος Χ., Γκύζης Δ., Καργόπουλος Α.-Ι., Κάτος Β., Κουδελή Μ., Μοροζίνης Ι.,Σαββίδης (2023) Ηλεκτρονικό Έγκλημα (Ουσιαστικές και δικονομικές όψεις) NB σελ 351
- Ζιώγου, Α. (2023). Τεχνητή νοημοσύνη στο Διαδίκτυο των Πραγμάτων
- Ζουμπουλάκης Κ. (2019)«Η πρόσβαση των αρχών στα ηλεκτρονικά αποδεικτικά στοιχεία: Τι συμβαίνει με τα προσωπικά μας δεδομένα;» Homo Digitalis
- Κανέλλος Λ, (2020)'The GDPR Handbook' Για DPOs, Επιχειρήσεις & Οργανισμούς, NB σελ.287
- Καντζάβελου Ι.- Κάτος Β. (2021) «Ψηφιακή Δικανική» Κεφ 16 στο συλλογικό τόμο "Ασφάλεια Πληροφοριών & Συστημάτων στον Κυβερνοχώρο", Σωκράτης Κάτσικας, Στέφανος Γκρίτζαλης, και Κωνσταντίνος Λαμπρινουδάκης (Επιστημονική Επιμέλεια), Εκδόσεις Νέων Τεχνολογιών σελ.128
- Καργόπουλος Α.Ι, 2023 'Τα ψηφιακά δεδομένα στο ισχύον δικονομικό πλαίσιο: Δικαιικοί άξονες & προβληματισμοί', Ηλεκτρονικό Έγκλημα (Ουσιαστικές και δικονομικές όψεις), NB
- Κάτος Β. (2023) Ψηφιακά Πειστήρια, Ηλεκτρονικό Έγκλημα (Ουσιαστικές και δικονομικές όψεις),NB σελ. 400-401
- Κουσουνή-Πανταζοπούλου Α. (2022) 'Cloud Computing & νομικά ζητήματα' NB, σελ. 5, 83, 144
- Μαρκόπουλος, Ν. (2018) 08-05-2018 «Η συνταγματική προστασία των εξωτερικών στοιχείων της επικοινωνίας», Πρακτικά Ημερίδας της Αρχής Διασφάλισης Απορρήτου Επικοινωνιών με θέμα Απόρρητο Επικοινωνιών – Σύγχρονες Προκλήσεις. Αθήνα,Α.Δ.Α.Ε., σελ. 65
- Ματάμη, Ε. (2022). Ψηφιακά πειστήρια και αποδεικτικές απαγορεύσεις στην ποινική δίκη σε εθνικό και υπερεθνικό επίπεδο.
- Μιχαηλάκη, Α. (2021). Δίκαιο και δεοντολογία στις εφαρμογές της επαυξημένης πραγματικότητας: τεχνολογικές προεκτάσεις και προβληματισμοί (Doctoral dissertation, Ιόνιο Πανεπιστήμιο. Σχολή Επιστήμης της Πληροφορίας και Πληροφορικής. Τμήμα Αρχειονομίας, Βιβλιοθηκονομίας και Μουσειολογίας)
- Μπαντή-Μαρκούτη, Β. (2015), ό.π., σελ. 3
- Μυλωνόπουλος Χ. (2021), Διεθνές & Ευρωπαϊκό Ποινικό Δίκαιο, Νομική Βιβλιοθήκη, σελ. 64-65
- Παναγοπούλου-Κουτνατζή, Φ. (2014). Διαδίκτυο των πραγμάτων (Internet of Things-IoT): Αποικισμός της καθημερινής ζωής ή νέα τεχνολογική πρόκληση. ΔiΜΕΕ, 3/2014, 346-358
- ΠΑΠΑΔΟΠΟΥΛΟΣ Μ./ ΕΥΓΕΝΙΔΗΣ Π., Νεφοϋπολογιστική (Cloud Computing) και προστασία προσωπικών δεδομένων, ΔιΜΕΕ 2016, σελ. 182 επ

- Παπαδόπουλος, Θ. (2020). Η Ανακριτική Διερεύνηση Ηλεκτρονικών Εγκλημάτων. Όρια και έκταση εφαρμογής της εγχώριας και διεθνούς πρακτικής υπό το φως των εγγυήσεων προστασίας των ατομικών δικαιωμάτων και της νομολογίας του ΕΔΔΑ
- Παπαθανασίου Α.Χ, (2023) Κυβερνοέγκλημα, Ψηφιακή Εγκληματολογία και Κατάσχεση Ψηφιακών Δεδομένων, Ηλεκτρονικό Έγκλημα (Ουσιαστικές και δικονομικές όψεις),ΝΒ σελ.273
- Τσόγκας Λ.Σ, (2021)Αντεισαγγελέας Εφετών Θράκης «ΨΗΦΙΑΚΗ ΕΠΟΧΗ ΚΑΙ ΔΙΚΑΙΟΣΥΝΗ ΣΥΓΧΡΟΝΕΣ ΜΟΡΦΕΣ ΕΓΚΛΗΜΑΤΙΚΟΤΗΤΑΣ - ΔΙΕΘΝΗΣ ΣΥ Ναζίρης Γ. (2023) Η κατάσχεση των ψηφιακών δεδομένων», Ηλεκτρονικό Έγκλημα (Ουσιαστικές και δικονομικές όψεις), ΝΒ σελ.501ΝΕΡΓΑΣΙΑ-ΣΥΓΧΡΟΝΑ ΜΕΣΑ»
- Φαρμακίδης Ε. (2021), Ευρωπαϊκή Εντολή Υποβολής και Ευρωπαϊκή Εντολή Διατήρησης στοιχείων - Η προσαρμογή των θεσμών δικαστικής συνεργασίας σε ποινικές υποθέσεις στην ψηφιακή εποχή, ΠοινΔικ, 1/2021, σελ. 28 – 43
- Φερενίκη Παναγοπούλου-Κουτνατζή, ΔiΜΕΕ, 3/2014, σελ. 346 – 35

❖ ΔΙΑΔΙΚΤΥΑΚΕΣ ΠΗΓΕΣ

(τελευταία προσπέλαση σε όλες τις διαδικτυακές πηγές πραγματοποιήθηκε στις **27.08.2023**)

- Μνήμη Τυχαίας Προσπέλασης (RAM,Random Access Memory) Βικιπαιδεία, ανακτήθηκε από https://el.wikipedia.org/wiki/%CE%9C%CE%BD%CE%AE%CE%BC%CE%B7_%CF%84%CF%85%CF%87%CE%B1%CE%AF%CE%B1%CF%82_%CF%80%CF%81%CE%BF%CF%83%CF%80%CE%AD%CE%BB%CE%B1%CF%83%CE%B7%CF%82
- Δίκτυο Ευρείας Περιοχής (WAN, Wide Area Network) Βικιπαιδεία, ανακτήθηκε από https://el.wikipedia.org/wiki/%CE%94%CE%AF%CE%BA%CF%84%CF%85%CE%BF_%CE%B5%CF%85%CF%81%CE%B5%CE%AF%CE%B1%CF%82_%CF%80%CE%B5%CF%81%CE%B9%CE%BF%CF%87%CE%AE%CF%82
- Διεθνές Πρότυπο ISO/IEC 27037:2012 ανακτήθηκε από https://www.iso.org/standard/44381.html
- Η τεχνική επιτροπή (TC) ISO/PC 308 σχετικά με την αλυσίδα φύλαξης ανακτήθηκε από https://www.iso.org/committee/6266669.html
- Teicher J (2018) The little-known story of the first IoT device ,IBM blog ανακτήθηκε από https://www.ibm.com/blog/little-known-story-first-iot-device/
- Sharma C (2016) Correcting the IoT history. Chetan Sharma Consulting Blog ανακτήθηκε από http://www.chetansharma.com/correcting-the-iot-history
- Cloud Credential Council (CCC) 'Knowledge Byte: The Different Types Of IoT' ανακτήθηκε από https://www.cloudcredential.org/blog/knowledge-byte-the-different-types-of-iot/
- Proxy Server (ορισμός) ανακτήθηκε από https://texnologia.net/

- The Onion Router (Tor) Network, Βικιπαιδεία ανακτήθηκε από https://en.wikipedia.org/wiki/Tor_(network)
- Εξυπηρετητής/Διακομιστής (Server), Βικιπαιδεία, ανακτήθηκε από https://el.wikipedia.org/wiki/%CE%95%CE%BE%CF%85%CF%80%CE%B7%CF%81%CE%B5%CF%84%CE%B7%CF%84%CE%AE%CF%82
- The NIST Definition of Cloud Computing, NIST Special Publication (2011) ανακτήθηκε από http://csrc.nist.gov/publications/PubsSPs.html#800-145
- Ζουμπουλάκης Κ. (2019)«Η πρόσβαση των αρχών στα ηλεκτρονικά αποδεικτικά στοιχεία: Τι συμβαίνει με τα προσωπικά μας δεδομένα;» Homo Digitalis ανακτήθηκε από https://www.homodigitalis.gr/posts/3928
- European Council (2023) Better access to e-evidence to fight crime ανακτήθηκε από https://www.consilium.europa.eu/en/policies/e-evidence/
- 'Smarter Coffee' ανακτήθηκε από https://firebox.com/Smarter-Coffee/p6991
- 'Family Hub Refrigerator' ανακτήθηκε από https://www.samsung.com/us/explore/family-hub-refrigerator/overview/
- Popken, B. (2017). Hacked Home Devices Can Spy On You-NBC News ανακτήθηκε από https://www.nbcnews.com/tech/security/hacked-home-devices-can-spy-you-n814671
- Z-Wave, Βικιπαιδεία ανακτήθηκε από https://en.wikipedia.org/wiki/Z-Wave

- Zigbee, Βικιπαιδεία ανακτήθηκε από https://en.wikipedia.org/wiki/Zigbee
- Chrichton, D.2015«With Mimo, MIT Alums Are Disrupting the Baby Nursery, Onesie at a Time ανακτήθηκε από https://techcrunch.com/2015/01/27/withmimo-mit-alums-are-disrupting-the-baby-nursery-onesie-at-a-time, σε Hillary Brill και Scott Jones
- Αυτό είναι το έξυπνο σουτιέν της Microsoft! (2013), newsit.gr ανακτήθηκε από https://www.inewsgr.com/61/afto-einai-to-exypno-soutien-tis-Microsoft.htm
- Food and Drug Administration ανακτήθηκε από https://ti-einai.gr/fda/
- Davis, D. (2014) "Your mobile phone is watching YOU", *Mail Online* ανακτήθηκε από https://www.dailymail.co.uk/news/article-2537828/Your-mobile-phone-watching-YOU-writes-DAVID-DAVIS-Campaigning-former-Shadow-Home-Secretarys-phone-log-reveals-insidious-tracking-move.html
- Χρυσοχού Χ. (2018) Τεχνητή Νοημοσύνη & Έγκλημα: Μια άλλη διάσταση, Crime Times ΚΕΜΕ ανακτήθηκε από https://www.crimetimes.gr/%CF%84%CE%B5%CF%87%CE%BD%CE%B7%CF%84%CE%AE-%CE%BD%CE%BF%CE%B7%CE%BC%CE%BF%CF%83%CF%8D%CE%BD%CE%B7-%CE%AD%CE%B3%CE%BA%CE%BB%CE%B7%CE%BC%CE%B1-%CE%BC%CE%B9%CE%B1-%CE%AC%CE%BB%CE%BB%CE%B7-%CE%B4%CE%B9/
- Η Καθημερινή, 2022 «Τεχνητή νοημοσύνη προβλέπει με ακρίβεια 90% τα εγκλήματα σε μία πόλη, μία εβδομάδα πριν» (Πρόκειται για το ακριβέστερο αλγοριθμικό εργαλείο που έχει αναπτυχθεί μέχρι σήμερα) ανακτήθηκε από https://www.kathimerini.gr/life/science/561936034/techniti-noimosyni-provlepei-me-akriveia-90-ta-egklimata-se-mia-poli-mia-evdomada-prin/