Πανεπιστήμιο Πειραιώς

Σχολή Τεχνολογιών Πληροφορικής και Τηλεπικοινωνιών

Τμήμα Ψηφιακών Συστημάτων

Προπτυχιακό Πρόγραμμα Σπουδών

ΓΕΩΡΓΙΟΣ ΤΣΙΤΣΙΡΗΣ - Ε21179

Εργασία Εξαμήνου

Προστασία της Ιδιωτικότητας στην Ψηφιακή Εγκληματολογία

Privacy in Digital Forensics

Επιβλέπων Καθηγητής: Στέφανος Γκρίτζαλης

Πειραιάς

Απρίλιος 2025

Abstract

Η ραγδαία εξέλιξη της τεχνολογίας που επέφερε και την εκθετική αύξηση στην χρήση ψηφιακών συσκευών στην καθημερινή ζωή των ανθρώπων, έχει οδηγήσει σε μεγάλη αύξηση των ψηφιακών εγκλημάτων. Για αυτόν τον λόγο έχει αναδυθεί πολύ η ανάγκη για την εξαγωγή ερευνών Ψηφιακής Εγκληματολογίας για την εξιχνίαση τέτοιων εγκλημάτων. Όμως, λόγω της φύσης της Ψηφιακής Εγκληματολογίας, προκύπτουν πολλά ερωτήματα που αφορούν ιδιωτικότητα των εμπλεκόμενων ατόμων και αν και κατά πόσο παραβιάζεται κατά την διάρκεια της έρευνας. Η παρούσα εργασία εξετάζει αυτό το ερώτημα αναλύοντας νομικά, ηθικά και τεχνικά ζητήματα που αφορούν την ιδιωτικότητα και την Ψηφιακή Εγκληματολογία. Παρουσιάζονται σχετικές νομοθεσίες, όπως ο GDPR, μέθοδοι, τεχνικοί και μη, προστασίας της ιδιωτικότητας αλλά και προκλήσεις που αντιμετωπίζονται κατά την διάρκεια μιας έρευνας.

Εννοιολογικό πλαίσιο

hash (κατακερματισμός): η έξοδος μιας hash συνάρτησης. η οποία είναι μια συνάρτηση που με κάποιον τρόπο μετατρέπει τα δεδομένα εισόδου σε μια σειρά χαρακτήρων προκαθορισμένου μεγέθους. Το πιο σημαντικό χαρακτηριστικό των συναρτήσεων κατακερματισμού είναι ότι κάθε είσοδος έχει συγκεκριμένη έξοδο και δεν γίνεται να βρεθεί η αρχική είσοδος με την χρήση των δεδομένων της εξόδου

υποκείμενο των δεδομένων: οποιοδήποτε φυσικό πρόσωπο από το οποίο συλλέγονται προσωπικά δεδομένα για οποιονδήποτε σκοπό και και από οποιονδήποτε φορέα

κρυπτανάλυση (cryptanalysis): η επιστήμη του "σπασίματος" αλγορίθμων κρυπτογράφησης, όπου ανασυναρμολογείται το αρχικό απλό κείμενο χωρίς την χρήση του κλειδιού αποκρυπτογράφησης

αλυσίδα επιμέλειας (Chain of Custody - CoC): η αδιάλειπτη τεκμηρίωση της διαδρομής των αποδεικτικών στοιχείων από τη στιγμή της συλλογής τους μέχρι την παρουσίασή τους στο δικαστήριο. Περιλαμβάνει πληροφορίες για το ποιος τα χειρίστηκε, πότε, πού και με ποιο τρόπο, ώστε να διασφαλίζεται η ακεραιότητά τους

Περιεχόμενα

1. Εισαγωγή στην Ψηφιακή Εγκληματολογία (Digital Forensics)

Η ψηφιακή εγκληματολογία (digital forensics) είναι μια σχετικά νέα μορφή εγκληματολογίας, που πρωτοεμφανίστηκε τη δεκαετία του ‘70, κυρίως ως ένα είδος έρευνας και ανάκτησης δεδομένων από ελαττωματικές συσκευές, παρά για την εξιχνίαση εγκλημάτων. Αιτία αυτού ήταν η ελάχιστη διαθεσιμότητα και χρήση των υπολογιστών από τον άνθρωπο στην καθημερινότητά του, λόγω κόστους και όγκου. Την δεκαετία του ’90, η χρήση υπολογιστών για την υποστήριξη εγκλημάτων, κυρίως απάτης, έγινε πολύ πιο συχνή και για αυτό διοργανώθηκαν συνέδρια για την ανάλυση υπολογιστικών αποδεικτικών στοιχείων, όπου συμμετείχαν ερευνητές από διάφορες χώρες, χρησιμοποιώντας εργαλεία που αναπτύχθηκαν για την ανάλυση τέτοιων δεδομένων (Mark Pollitt, 2017)[1].

Σήμερα, όμως, η χρήση των ηλεκτρονικών συσκευών, και ειδικότερα των κινητών τηλεφώνων, έχει πλεον ενταχθεί στην καθημερινότητα όλων των ανθρώπων, ασχέτου τάξης και ηλικίας. Εξαιτίας της φύσης των δεδομένων που αποθηκεύονται στις σημερινές συσκευές, αλλά και του τεράστιου όγκου τους που παράγεται καθημερινά, η διερεύνηση ηλεκτρονικών και ψηφιακών μέσων για στοιχεία που έχουν σχέση με εγκλήματα γίνεται όλο και πιο δύσκολη. Έτσι και η διατήρηση της ιδιωτικότητας αυτών των δεδομένων γίνεται μια δυσμενής διαδικασία (T. B. Ogunseyi & O. M. Adedayo, 2023)[2]. Για την καταπολέμηση αυτής της δυσκολίας, σχεδιάζονται συνεχώς εργαλεία και μέθοδοι για να αποφευχθεί η παραβίαση της ιδιωτικότητας των χρηστών κατά την διάρκεια μιας έρευνας (A. Nieto, R. Rios, & J. Lopez, 2019)[3].

Η διερεύνηση ψηφιακών εγκλημάτων εγείρει σημαντικά νομικά και ηθικά ζητήματα, επειδή οι αρχές θα πρέπει να βρουν μια ισορροπία μεταξύ των αντικρουόμενων διαδικασιών της συλλογής αποδεικτικών στοιχείων και της προστασίας της ιδιωτικότητας του ιδιοκτήτη αυτών των δεδομένων (T. B. Ogunseyi & O. M. Adedayo, 2023)[2]. Νομοθεσίες όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) στην Ευρωπαϊκή Ένωση, εφαρμόζουν πολύ αυστηρούς κανόνες για την προστασία των προσωπικών δεδομένων των πολιτών της, επιβάλλοντας τεράστια πρόστιμα στους παραβάτες, δίνοντας όμως συγκεκριμένο ορισμό του “τι αποτελούν” τα προσωπικά δεδομένα και τρόπους προστασίας τους. Παρόλα αυτά, αυτή η υποχρέωση συνεχίζει να προκαλεί τους ειδικούς της ψηφιακής εγκληματολογίας, κυρίως λόγω της συνεχής και ταχύτατης εξέλιξης την τεχνολογίας που, συχνά, ξεπερνά τα όρια που έχουν τεθεί από τα υπάρχων νομικά πλαίσια (Ludwig Englbrecht & Günther Pernul, 2020)[4].

Digital Forensic Procedures	**Privacy Issues**
Indiscriminate acquisition/collection of digital data	**Third Party Privacy** Breach (TPPB) must be avoided
Full disk images are created and analysed	Deleted files can lead to **false accusations**
Data can be collected from personal devices	Need for **informed consents** complete and understandable by the users
During the investigation, the data to be acquired may be hosted on servers in different countries	Different **jurisdictions** can understand privacy differently
Warrants can be necessary during private investigation.	Matching of **privacy policies** and **warrants** (formally defined) for automated analysis.
Correlation is needed in order to build a timeline	**Multi-device** context (more and more data)
Digital forensics tools and methodologies must be accepted and tested by a broad group of experts in the field	Privacy requirements must be integrated by design in **existing tools and methodologies**
Digital forensic principles must be guaranteed	The **manipulation of data** (e.g., encryption) to protect privacy must be done considering digital forensic principles 8.2.2.1

Σχήμα 1. Πρακτικές στην Ψηφιακή εγκληματολογία και ανησυχίες για την ιδιωτικότητα[3]

1.1 Κατηγορίες Ψηφιακής Εγκληματολογίας

Η ψηφιακή εγκληματολογία εξετάζει πολλές διαφορετικές κατηγορίες ψηφιακών δεδομένων που παράγονται από διαφορετικά μέσα και συσκευές.
Μπορεί να χωριστεί σε έξι βασικούς τύπους (N. Kumari & A. K. Mohapatra, 2016)[5]:

- Computer Forensics
- Network Forensics
- Mobile Forensic
- Memory Forensics
- Email Forensics
- Database Forensics

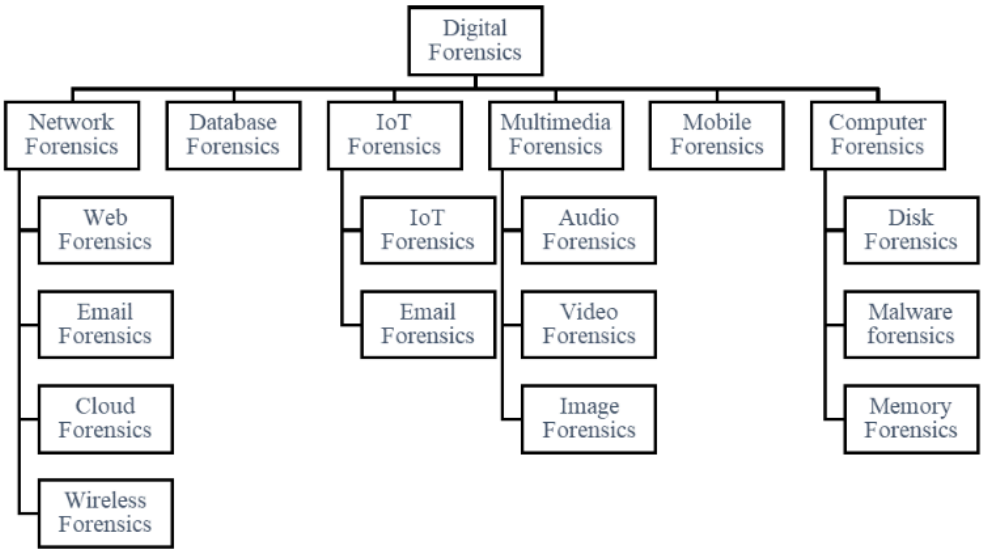
Computer Forensics ονομάζεται η διαδικασία που χρησιμοποιεί την πληροφορική για να αναλύσει αποδεικτικά στοιχεία και δεδομένα που προκύπτουν από μια ψηφιακή έρευνα[5].

Network Forensics χρησιμοποιούνται για την ανάλυση αρχεία καταγραφής και δραστηριότητα εγκληματιών πάνω σε ένα δίκτυο[5].

Το Mobile Forensics είναι όμοιο με το Computer Forensics, με βασική διαφορά ότι συλλέγονται δεδομένα και αποδεικτικά στοιχεία από κινητές συσκευές που, συνήθως, λειτουργούν με διαφορετικό τρόπο από τους κλασικούς υπολογιστές ως προς τον αποθηκευτικό χώρο και ότι τα κινητά έχουν ενσωματωμένα συστήματα επικοινωνίας (GSM, 5G κλπ.)[5].

Memory Forensics χρησιμοποιούνται για την συλλογή και ανάλυση δεδομένων από την προσωρινή μνήμη συσκευών (RAM, cache κλπ.)[5].

Όταν διερευνώνται τα Email Forensics, αναλύονται οι επικοινωνίες που γίνονται μέσω υπηρεσιών ηλεκτρονικού ταχυδρομείου που σήμερα χρησιμοποιούνται συχνά για την ανταλλαγή ευαίσθητων πληροφοριών και είναι στόχος επιτιθέμενων[5].



Σχήμα 2. Υποκατηγορίες της Ψηφιακής Εγκληματολογίας[2]

1.2. Διαδικασίες στην Ψηφιακή Εγκληματολογία

Οι έρευνες της Ψηφιακής Εγκληματολογίας ακολουθούν κάποιες βασικές διαδικασίες κατά την διάρκεια τους (όπως φαίνεται και στο Σχήμα 2). Αυτές είναι η ταυτοποίηση, η συντήρηση, η απόκτηση, η εξέταση, η ανάλυση και η παρουσίαση των δεδομένων/αποδεικτικών στοιχείων ενός εγκλήματος. Αυτές οι διαδικασίες είναι επαναλαμβανόμενες και γενικές για να εφαρμόζονται σε κάθε περίπτωση.

Κατά την ταυτοποίηση, ο στόχος είναι να προσδιοριστεί τι έγκλημα ή περιστατικό έχει συμβεί για να μπορεί να εξεταστεί σωστά και να βρεθούν οι κατάλληλες αποδείξεις. Για την διαδικασία αυτή, συνήθως χρησιμοποιούνται έξι (6) ερωτήσεις, οι οποίες είναι: Ποιος, Που, Πότε, Πως, Τι, Γιατι (Who, Where, Why, When, What, How [5W1H])[6].

Το “Ποιος” αναφέρεται στα άτομα που εμπλέκονται στην έρευνα, δηλαδή οι δράστες, τα θύματα και οι μάρτυρες.

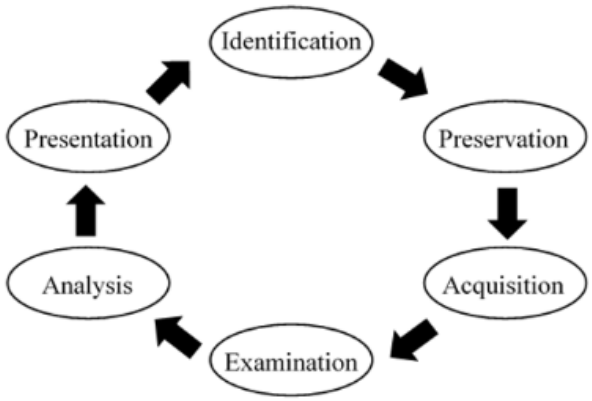
Το “Που” αναφέρεται στον τόπο του εγκλήματος και όπου αλλού έχει σχέση με αυτό. Σχετικά με το ψηφιακό έγκλημα, η απάντηση αυτής της ερώτησης γίνεται πιο περίπλοκη κυρίως λόγω του διαδικτύου.

Το “Πότε” αναφέρεται στην χρονική στιγμή που έγινε το έγκλημα και άλλες δράσεις που έχουν σχέση με αυτό. Για αυτόν το σκοπό δημιουργούνται χρονολόγια για την μπουν σε σωστή χρονική σειρά όλα τα γεγονότα που οδήγησαν στο έγκλημα.

Το “Πως” αναφέρεται στον τρόπο που έγινε το έγκλημα, ώστε να μπορεί να αποφευχθεί μελλοντικά.

Το “Τι” αναφέρεται στο τι έγινε, δηλαδή τι γεγονότα διαδραματίστηκαν στον τόπο του εγκλήματος.

Τέλος, το "Γιατι" αναφέρεται στον λόγο που έγινε το έγκλημα και τι κίνητρο μπορεί να είχε ο δράστης για να το διαπράξει.



Σχήμα 3. Οι βασικές διαδικασίες της Ψηφιακής Εγκληματολογίας[2]

Από την διαδικασία της ταυτοποίησης ξεκινάει και το Chain of Custody (CoC: Αλυσίδα Επιμέλειας), που αναφέρει λόγο, χρόνο, τόπο, μέθοδο και διαδικασία συλλογής των αποδείξεων αλλά και τα άτομα που τις χειρίζονται εκείνη την στιγμή. Το CoC πρέπει να συνεχίσει να καταγράφεται σωστά καθ'όλη την διάρκεια της έρευνας. Για την διατήρηση της αλυσίδας επιμέλειας, έχει δημιουργηθεί ένα πρότυπο από τον ISO (International Organization for Standardization: Διεθνής Οργανισμός Τυποποίησης). Ο ISO/PC 308 TC περιέχει έναν γενικό ορισμό του CoC αλλά και πλαίσια και οδηγούς για τρόπους διαχείρισης, εφαρμογής και επαλήθευσης της αλυσίδας για την διασφάλιση της ακεραιότητας των ψηφιακών στοιχείων της έρευνας (A. Nieto, R. Rios, & J. Lopez, 2019)[3].

Η συντήρηση, που συχνά εντάσσεται στην διαδικασία της απόκτησης, αναφέρεται στην αποθήκευση και συντήρηση των αποδεικτικών στοιχείων σε άριστη και αμετάβλητη, απο την αρχική, κατάσταση. Αυτό συνήθως επιτυγχάνεται με την δημιουργία πιστών αντιγράφων και με την δημιουργία hash για κάθε αρχείο ή μέσο που εξετάζεται..

Κατά την διαδικασία της απόκτησης εξάγονται όλα τα απαραίτητα δεδομένα, σε χρήσιμη για την έρευνα μορφή, ώστε να μπορεί να γίνει η εξέταση και ανάλυσή τους σε επόμενη φάση. Επειδή δουλεύουμε με φυσικούς υπολογιστές αλλά και απομακρυσμένους (cloud) υπάρχουν προβλήματα που μπορεί να προκύψουν όπως το Order of Volatility (σειρά μεταβλητότητας) του κάθε μέσου αποθήκευσης του υπολογιστή (π.χ. η μνήμη που αποθηκεύει τα δεδομένα προσωρινά ή ο σκληρός δίσκος όπου μένουν για χρόνια) και η άγνοια του πως λειτουργεί ένας απομακρυσμένος υπολογιστής.

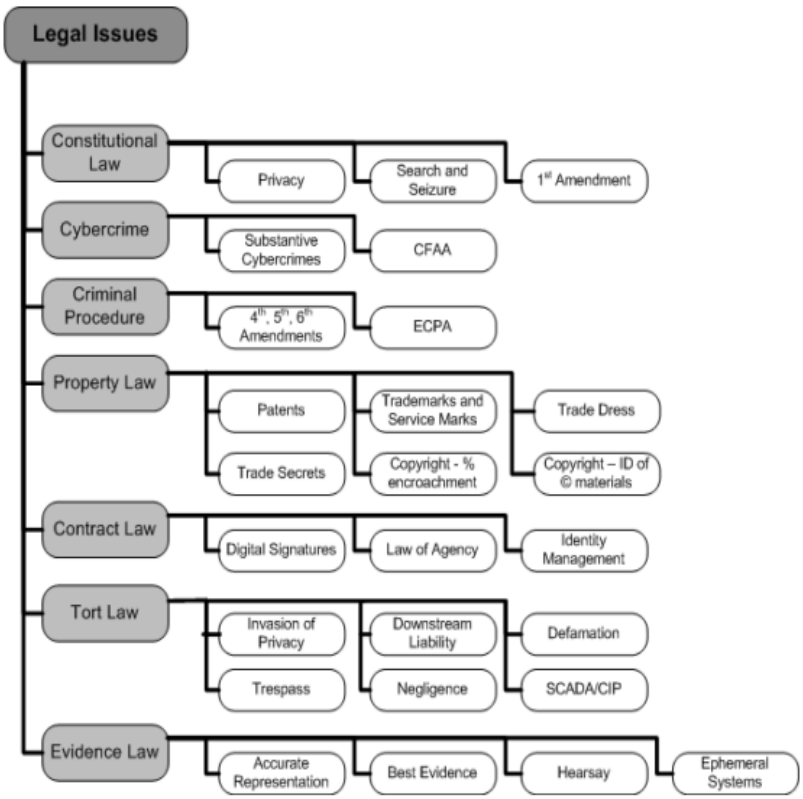
Επόμενη φάση μιας έρευνας Ψηφιακής Εγκληματολογίας είναι η εξέταση των δεδομένων που συλλέχθηκαν στις προηγούμενες φάσεις για να βρεθούν αποδεικτικά στοιχεία που μπορούν να χρησιμοποιηθούν αργότερα σε κάποια δίκη.

Στη συνέχεια, γίνεται η ανάλυση αυτών των αποδείξεων για να αποσπαστούν γεγονότα και πρόσωπα από ένα έγκλημα και εξετάζεται η σημασία αυτών των αποδείξεων σε σχέση με την έρευνα, διατηρώντας ταυτόχρονα την ακεραιότητά τους. Αυτή η διαδικασία γίνεται επαναληπτικά μέχρι να δημιουργηθεί ένα επαρκής χρονοδιάγραμμα, συνδυάζοντας, επίσης, δεδομένα από διαφορετικά μέσα που έχουν εξεταστεί.

Τέλος, βάσει των ευρημάτων από τις προηγούμενες φάσεις, δημιουργείται μια έκθεση (report) που, συνήθως, παρουσιάζεται κατά την διάρκεια μιας δίκης. Για αυτό θα πρέπει να περιέχει όλα τα σημαντικά δεδομένα αλλά και κάθε βήμα που πάρθηκε για να οδηγήσει στο τελικό συμπέρασμα της έρευνας. Επίσης, πρέπει να είναι γραμμένη σε μορφή κατανοητή από ανθρώπους χωρίς τεχνολογικές γνώσεις και με χρήση διαγραμμάτων, εικόνων και άλλων μέσων απεικόνισης δεδομένων, ώστε να έχει την δυνατότητα να βγάλει ένα συμπέρασμα ο δικαστής.

2. Κανονιστικές αρχές και Ψηφιακή Εγκληματολογία

Για να πραγματοποιηθεί μια έρευνα Ψηφιακής Εγκληματολογίας, είναι αναγκαίο να συλλεχθούν πάρα πολλά δεδομένα, όπου ένα μέρος τους θα είναι προσωπικά ή και ευαίσθητα. Για αυτόν τον λόγο έχει δυσκολευτεί η διαδικασία μιας έρευνας λόγω των διαφόρων νόμων που προστατεύουν αυτά τα δεδομένα των πολιτών, επειδή δεν επιτρέπεται η συλλογή οποιουδήποτε είδους προσωπικού δεδομένου χωρίς συγκατάθεση ή ένταλμα, των οποίων η απόκτηση είναι πολύ χρονοβόρα, πράγμα που πάει αντίθετα στο πρόβλημα της μεταβλητότητας των ψηφιακών συστημάτων. Επίσης, η Ψηφιακή εγκληματολογία εφαρμόζεται σε διάφορα είδη εγκλημάτων για τα οποία, ανάλογα με το νομικό πλαίσιο κάθε χώρας, ισχύει και ο αντίστοιχος νόμος. Αυτό, κυρίως, ισχύει στις Η.Π.Α., αφού η Ε.Ε. επιβάλλει έναν γενικό κανονισμό που ισχύει για κάθε τομέα, όπως και η Αυστραλία. Παραδείγματα περιλαμβάνουν αδικοπρακτικό δίκαιο, δηλαδή για αστικά αδικήματα, περιουσιακό δίκαιο, συμβατικό δίκαιο και άλλα (K. Nance & D. J. Ryan)[14].



Σχήμα 4. Νομικά θέματα που εξετάζονται (στην Αμερική)[14]

2.1. Νόμοι για την ιδιωτικότητα των δεδομένων

Η ιδιωτικότητα μπορεί να περιγραφεί ως το θεμελιώδες δικαίωμα κάθε ατόμου να διατηρεί και να ελέγχει τις προσωπικές πληροφορίες που του αφορούν και θεωρείται βασικό ανθρώπινο δικαίωμα από την *Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου* (ΕΣΔΑ) (Raphaël Gellert & Serge Gutwirth, 2013)[15] αλλά και από το Άρθρο 12 της *Οικουμενική Διακήρυξη για τα Ανθρώπινα Δικαιώματα* των Ηνωμένων Εθνών (ΟΗΕ) (A. Nieto, R. Rios, & J. Lopez, 2019)[3]. Κάθε χώρα ερμηνεύει την ιδιωτικότητα και τα προσωπικά δεδομένα με διαφορετικό τρόπο, άρα υπάρχουν διαφορές μεταξύ των νόμων που επιβάλλουν, όμως έχουν επικυρωθεί συμφωνίες μεταξύ κάποιων χωρών για την μεταφορα των ιδιωτικών δεδομένων (π.χ. το EU-US Privacy Shield[1]) μεταξύ τους για την αποφυγή προβλημάτων δικαιοδοσίας (A. Nieto, R. Rios, & J. Lopez, 2019)[3]. Οι πιο γνωστοί κανονισμοί που αφορούν την ιδιωτικότητα των δεδομένων είναι ο Γενικό Κανονισμό για την Προστασία των Δεδομένων (ΓΚΠΔ/GDPR), ο Personal Information Protection and Electronic Documents Act (PIPEDA), ο California Consumer Privacy Act (CCPA) κ.α. (Atheer Aljeraisy et al., 2022)[7]. Αυτές οι νομοθεσίες παίζουν πολύ σημαντικό ρόλο στον κόσμο της Ψηφιακή Εγκληματολογίας, επειδή για να διεξαχθεί μια έρευνα πρέπει να παραβιαστεί, εν μέρει, η ιδιωτικότητα των εμπλεκόμενων προσώπων. Στην συνέχεια θα αναλυθούν αυτές οι τρεις νομοθεσίες, με μεγαλύτερη έμφαση στον GDPR.

2.1.1. California Consumer Privacy Act (CCPA)

Αυτός ο κανονισμός ψηφίστηκε και υπογράφηκε ως νόμος τον Ιούνιο του 2018, ένα μήνα μετά την αρχή της ισχύς του GDPR, και τέθηκε σε ισχύ τον Ιανουάριο του 2020 και δίνει στους πολίτες της Καλιφόρνιας δικαιώματα για τον έλεγχο των προσωπικών τους δεδομένων. Συγκεκριμένα, τους δίνονται τα παρακάτω δικαιώματα (Atheer Aljeraisy et al., 2022)[7]:

- Δικαίωμα να γνωρίζουν τι προσωπικά δεδομένα συλλέγει και επεξεργαζεται ένας οργανισμός
- Δικαίωμα να γνωρίζουν αν έχουν πουληθεί τα προσωπικά δεδομένα τους και σε ποιον
- Δικαίωμα να απορρίψουν την πώληση των προσωπικών δεδομένων τους
- Δικαίωμα να έχουν πρόσβαση στα προσωπικά δεδομένα τους που έχουν συλλεχθεί
- Δικαίωμα σε ισάξιες υπηρεσίες και τιμές, ανεξάρτητα από το αν ασκήσουν ή όχι τα παραπάνω δικαιώματα τους

2.1.2. Personal Information Protection and Electronic Documents Act (PIPEDA)

Ο PIPEDA έγινε νόμος τον Απρίλιο του 2000 και θεμελιώνει κανόνες για τους τρόπους διαχείρισης των προσωπικών δεδομένων που συλλέγονται από ιδιωτικές επιχειρήσεις για τις εμπορικές δραστηριότητές

[1] https://www.privacyshield.gov/ps/eu-us-framework

τους. Αυτό δίνει στους χρήστες μεγαλύτερο έλεγχο στα δεδομένα που δίνουν σε υπηρεσίες του ιδιωτικού τομέα. Συγκεκριμένα, ο PIPEDA περιέχει τις παρακάτω αρχές (Atheer Aljeraisy et al., 2022)[7]:

- Αρχή της λογοδοσίας (*κάθε οργανισμός είναι υποχρεωμένος να ακολουθεί πιστά τους νόμους που αφορούν τα προσωπικά δεδομένα και να αναθέτουν έναν υπεύθυνο για την συμμόρφωση με τον νόμο*)
- Αρχή του προσδιορισμού των σκοπών (*κάθε οργανισμός είναι υποχρεωμένος να δίνει το σκοπό της συλλογής των δεδομένων πριν ή/και κατά την συλλογή τους*)
- Αρχή της συγκατάθεσης (*απαιτείται η συγκατάθεση του χρήστη για την συλλογή, την χρήση και την δημοσιοποίηση των προσωπικών τους δεδομένων*)
- Αρχή του περιορισμού της συλλογής (*όταν απαιτείται η συλλογή προσωπικών δεδομένων, πρέπει αυτά να είναι σχετικά με τον σκοπό του οργανισμού και να συλλέγονται τα λιγότερα δυνατά για αυτόν*)
- Αρχή του περιορισμού χρήσης, δημοσιοποίησης και διατήρησης (*κάθε οργανισμός είναι υποχρεωμένος να χρησιμοποιήσει ή δημοσιοποιήσει δεδομένα μόνο για τον σκοπό για τον οποίον συλλέχθηκαν*)
- Αρχή της ακρίβειας (*κάθε οργανισμός είναι υποχρεωμένος να κάνει προσπάθεια για την διασφάλιση της ακρίβειας και της ενημερότητας των συλλεγέντων δεδομένων ώστε να είναι χρήσιμα για τον σκοπό που θα χρησιμοποιηθούν*)
- Αρχή της εγγύησης (*κάθε οργανισμός είναι υποχρεωμένος να διασφαλίζει την συνεχή και αποτελεσματική προστασία των προσωπικών δεδομένων που συλλέγει*)
- Αρχή της διαφάνειας (*κάθε οργανισμός είναι υποχρεωμένος να παρέχει λεπτομερείς πληροφορίες για τις πολιτικές και τις διαδικασίες που αφορούν την επεξεργασία των προσωπικών δεδομένων, και αυτές να είναι άμεσα και δημόσια διαθέσιμες*)
- Αρχή της μεμονωμένης πρόσβασης (*κάθε οργανισμός είναι υποχρεωμένος να διασφαλίζει ότι πρόσβαση σε προσωπικά δεδομένα έχουν μόνο εξουσιοδοτημένα άτομα και για συγκεκριμένο λόγο*)
- Αρχή της συμμόρφωσης (*κάθε οργανισμός είναι υποχρεωμένος να μπορεί να αποδείξει οποιαδήποτε στιγμή ότι συμμορφώνεται με τις νομοθεσίες περί προστασίας προσωπικών δεδομένων που εφαρμόζονται σε αυτόν)*

και τις παρακάτω υποχρεώσεις των επιχειρήσεων προς τους χρήστες του (Atheer Aljeraisy et al., 2022)[7]:

- Οι ιδιωτικοί οργανισμοί υποχρεούνται να συλλέγουν και να χρησιμοποιούν προσωπικά δεδομένα με δίκαιες και νόμιμες μεθόδους και για λογικούς και σαφείς λόγους
- Οι ιδιωτικοί οργανισμοί υποχρεούνται να προστατεύουν τα προσωπικά δεδομένα των χρηστών τους με αποτελεσματικές τεχνικές και να διαγράφονται όταν τελειώσει η περίοδος χρησιμότητάς τους
- Οι ιδιωτικοί οργανισμοί υποχρεούνται να κρατούν σωστά και ενημερωμένα όλα τα προσωπικά δεδομένα που συλλέγουν από τους χρήστες τους
- Οι χρήστες έχουν το δικαίωμα πρόσβασης στα συλλεγμένα δεδομένα τους και ενημέρωσης τους, σε περίπτωση που είναι ανακριβείς
- Οι χρήστες έχουν το δικαίωμα να αποσύρουν την συγκατάθεσή τους οποιαδήποτε στιγμή, εντός των νομικών ορίων και με επαρκή ενημέρωση

2.1.3. Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ/GDPR)

Ο Γενικό Κανονισμό για την Προστασία των Δεδομένων (ΓΚΠΔ/GDPR) τέθηκε σε ισχύ τον Μάιο του 2018, είναι ένας από τους σημαντικότερους κανονισμούς που αφορούν την προστασία δεδομένων αφού

εφαρμόζεται σε όλα τα 27 κράτη μέλη της Ευρωπαϊκής Ένωσης και αφορά οποιονδήποτε οργανισμό που επεξεργάζεται δεδομένα Ευρωπαίων πολιτών και εστιάζεται στην ικανότητα των χρηστών να ελέγχουν τα δεδομένα τους που συλλέγονται και τον τρόπο που γίνεται αυτό (Neil C. Rowe)[13].

2.1.3.1. Νόμιμη επεξεργασία προσωπικών δεδομένων βάσει του GDPR

Με βάση τον GDPR τα προσωπικά δεδομένα είναι *"πληροφορίες που ταυτοποιούν ένα υποκείμενο των δεδομένων. Ταυτοποιήσιμα είναι τα υποκείμενα που μπορούν να ταυτοποιηθούν, έμμεσα ή άμεσα, μέσα από αναγνωρίστικα στοιχεία, δηλαδή προσωπικά δεδομένα, όπως είναι το ονοματεπώνυμο, ο αριθμός ταυτότητας κ.α. ή και από στοιχεία που περιγράφουν κάποια κατάσταση που βρίσκεται το υποκείμενο, όπως ψυχολογική, φυσική, οικονομική, θρησκευτική, κοινωνική κ.α. κατάσταση."* *(https://gdpr.eu/eu-gdpr-personal-data/)* . Όλα τα δεδομένα τέτοιου τύπου απαιτούνται, από τον GDPR να προστατεύονται σε κάθε περίπτωση που χρειάζεται η επεξεργασία τους, άρα και κατά την διάρκεια μιας έρευνας Ψηφιακής Εγκληματολογίας (Ludwig Englbrecht & Günther Pernul, 2020)[4].

Ο GDPR αναφέρει ότι πρέπει να υπάρχει νόμιμος λόγος για την επεξεργασία προσωπικών δεδομένων. Τέτοιος λόγος μπορεί να είναι:

- με την συγκατάθεση του υποκειμένου των δεδομένων
- για την εκπλήρωση συμβατικής υποχρέωσης του υποκειμένου των δεδομένων
- για την εκπλήρωση νομικών υποχρεώσεων του υπευθύνου επεξεργασίας δεδομένων
- για την προστασία συμφερόντων ζωτικής σημασίας του υποκειμένου των δεδομένων
- για την εκτέλεση έργου δημοσίου συμφέροντος
- για νόμιμα συμφέροντα του υπευθύνου επεξεργασίας δεδομένων ή τρίτου με την προϋπόθεση ότι δεν υπερισχύουν των συμφερόντων του υποκειμένου των δεδομένων

Επίσης, η συγκατάθεση πρέπει να δίνεται ελεύθερα, χωρίς μειονεκτήματα σε περίπτωση άρνησης, και οι όροι χρήσης να είναι διατυπωμένοι με σαφήνεια και σε μορφή κατανοητή σε οποιοδήποτε, που όμως καθίσταται απίθανο λόγω των πολυσέλιδων όρων που χρησιμοποιούν όλοι οι οργανισμοί σήμερα. Όσων αφορά την Ψηφιακή Εγκληματολογία, μπορεί να καλυφθεί από τον δεύτερο και πέμπτο νόμιμο λόγο, όταν, όμως, πραγματοποιείται από την αστυνομία για θέματα εθνικής ασφάλειας (Neil C. Rowe)[13].

2.1.3.2. Αρχές και δικαιώματα του GDPR

Οι οργανισμοί που επηρεάζονται από τον GDPR λόγω επεξεργασίας προσωπικών δεδομένων, υποχρεούνται να παρέχουν κάποια δικαιώματα στους χρήστες τους (Neil C. Rowe)[13]. Αυτά είναι (Atheer Aljeraisy et al., 2022)[7]:

- Δικαίωμα της ενημέρωσης για την συλλογή και επεξεργασία των δεδομένων τους

- Δικαίωμα στην πρόσβαση των δεδομένων τους που έχουν συλλεχθεί
- Δικαίωμα στην διόρθωση των δεδομένων τους (*τα υποκείμενα των δεδομένων πρέπει να έχουν την επιλογή να ζητήσουν την διαγραφή των δεδομένων τους που κρατάει ένας οργανισμός*)
- Δικαίωμα στην διαγραφή των δεδομένων (*τα υποκείμενα των δεδομένων πρέπει να έχουν την ικανότητα να ζητούν την διαγραφή των δεδομένων τους που κατέχει ένας οργανισμός*)
- Δικαίωμα της φορητότητας των δεδομένων (*τα υποκείμενα των δεδομένων πρέπει να έχουν την δυνατότητα να λάβουν άμεσα τα δεδομένα τους σε χρήσιμη μορφή για την μεταφορά τους σε άλλο οργανισμό*)
- Δικαίωμα στην απόσυρση της συγκατάθεσης, οποιαδήποτε στιγμή και για οποιονδήποτε λόγο, χωρίς επιπτώσεις
- Δικαίωμα του περιορισμού επεξεργασίας των δεδομένων (*τα υποκείμενα των δεδομένων πρέπει να έχουν την ικανότητα να ζητούν τον περιορισμό ή/και την κατάργηση της επεξεργασίας των δεδομένων τους*)
- Τα δικαιώματα σε σχέση με την αυτοματοποιημένη λήψη αποφάσεων (*τα υποκείμενα των δεδομένων έχουν το δικαίωμα να αρνηθούν κάποια απόφαση που πάρθηκε από αυτοματοποιημένη διαδικασία*)

Επίσης, με βάση τον GDPR, οι οργανισμοί πρέπει να ακολουθούν ορισμένες αρχές, οι οποίες είναι παρόμοιες με τις αρχές των νόμων που αναφέρθηκαν προηγουμένως (Atheer Aljeraisy et al., 2022)[7]:

- Αρχή της διαφάνειας
- Αρχή του περιορισμού του σκοπού (*κάθε οργανισμός πρέπει να δίνει το σκοπό της συλλογής των δεδομένων πριν ή κατά την συλλογή τους*)
- Αρχή της ελαχιστοποίησης στην συλλογή δεδομένων
- Αρχή της ακρίβειας
- Αρχή του περιορισμού χρήσης, δημοσιοποίησης και διατήρησης
- Αρχή της ακεραιότητας και εμπιστευτικότητας των δεδομένων (*κάθε οργανισμός πρέπει να εφαρμόζει μηχανισμούς προστασίας προσωπικών δεδομένων για την αποφυγή της διαρροής, λάθος χρήσης κ.α.*)
- Αρχή της λογοδοσίας

Επιπλέον, ο GDPR χαρακτηρίζει ένα υποσύνολο των προσωπικών δεδομένων ως ευαίσθητα ειδικού τύπου και εφαρμόζει περαιτέρω περιορισμούς για αυτά, και είναι τα δεδομένα που αφορούν φυλετική προέλευση, θρησκευτικές και πολιτικές πεποιθήσεις και σεξουαλικές προτιμήσεις.

2.1.3.3. Ιδιωτικότητα από σχεδιασμό και από προεπιλογή (Privacy by design and by default)

Ο GDPR, στο άρθρο 25, αναφέρει τους όρους “privacy by design” και “privacy by default” που αναφέρονται σε τυπικές πρακτικές προστασίας δεδομένων που πρέπει να ακολουθούνται όταν αναπτύσσεται οποιοδήποτε είδος πληροφοριακού συστήματος ή λογισμικού που θα επεξεργάζεται προσωπικά δεδομένα. Τέτοιες πρακτικές μπορεί να είναι η χρήση κρυπτογράφησης και η εφαρμογή συστήματος ελέγχου πρόσβασης (Neil C. Rowe)[13].

Συγκεκριμένα, ο όρος "privacy by design" (ιδιωτικότητα από σχεδιασμό) αναφέρεται στην απαίτηση της χρήσης όλων των δυνατών προστατευτικών μέτρων από την αρχή της ανάπτυξης ενός ψηφιακού προϊόντος. Ο όρος "privacy by default" (ιδιωτικότητα από προεπιλογή) αναφέρεται στην απαίτηση της χρήσης απαραίτητων μέτρων που διασφαλίζουν ότι, από προεπιλογή, μόνο τα απαραίτητα, για τον σκοπό που ζητούνται, δεδομένα, να συλλέγονται και να επεξεργάζονται (GDPR Art. 25)[16].

2.1.3.4. Ανωνυμοποίηση και ψευδωνυμοποίηση δεδομένων

Μια μέθοδος προστασίας της ιδιωτικότητας είναι με την χρήση τεχνικών ανωνυμοποίησης ή ψευδωνυμοποίησης, όπου οι δύο όροι διαφέρουν σε σημαντικό επίπεδο. Βάσει του άρθρου 4(5) του GDPR, η ψευδωνυμοποίηση είναι "*η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο δεδομένων χωρίς τη χρήση πρόσθετων πληροφοριών, υπό την προϋπόθεση ότι αυτές οι πρόσθετες πληροφορίες τηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα για να διασφαλιστεί ότι τα προσωπικά δεδομένα δεν αποδίδονται σε αναγνωρισμένο ή αναγνωρίσιμο φυσικό πρόσωπο*" (GDPR Art. 4)[17]. Η ψευδωνυμοποίηση, συνήθως, χρησιμοποιείται σε περιπτώσεις χειρισμού ευαίσθητων δεδομένων (π.χ. ιατρικών) που, όμως, χρειάζεται η αντιστοίχιση του προσώπου με αυτά, για παράδειγμα, για την ενημέρωση του ασθενή για κάποια διάγνωση. Από την άλλη μεριά, η ανωνυμοποίηση καταργεί πλήρως κάθε σύνδεση μεταξύ των δεδομένων και της ταυτότητας του υποκειμένου, καθιστώντας αδύνατη οποιαδήποτε εξατομίκευση και απαιτείται σε περιπτώσεις χρήσης δεδομένων πολιτών για επιστημονικές έρευνες. Ενώ έχουν ερευνηθεί πολλές μέθοδοι ανωνυμοποίησης, υπάρχουν πολλοί που δεν λειτουργούν γενικά ή σε συγκεκριμένες περιπτώσεις (A. Dehghantanha & K. Franke, 2014)[11].

2.1.3.5. Υπεύθυνος προστασία δεδομένων (DPO) και επιπτώσεις μη συμμόρφωσης

Προσθέτως, ο GDPR υποχρεώνει οργανισμούς να διορίσουν έναν "Data Protection Officer" (DPO), ο οποίος θα είναι υπεύθυνος της καταγραφής των διαδικασιών, σχετικά με την επεξεργασία των δεδομένων, της εταιρείας και θα εξασφαλίζει την συμμόρφωση της με τους υπάρχοντες νόμους (Neil C. Rowe)[13].

Σε περίπτωση μη συμμόρφωσης με όλα τα παραπάνω, ο GDPR μπορεί να επιβάλει κυρώσεις στον οργανισμό. Ειδικότερα, με βάση το άρθρο 83, ο GDPR μπορει να δώσει μια απλή προειδοποίηση, σε περίπτωση ακούσιας και πρώτης παράβασης ή να επιβάλλει χρηματικές ποινές αξίας έως και 20.000.000 EUR ή το 4% του ετήσιου παγκόσμιου τζίρου της εταιρείας, όποιο είναι υψηλότερο, και όπου το ποσό εξαρτάται από τα άρθρα που παραβιάστηκαν και από άλλα κριτήρια[2] (Neil C. Rowe)[13]. Για παράδειγμα, τον Σεπτέμβριο του 2024, η Ιρλανδική Επιτροπή Προστασίας Δεδομένων (DPC) έδωσε στην Meta πρόστιμο αξίας 91.000.000 EUR λόγω αποθήκευσης κωδικών χρηστών σε απλό κείμενο, χωρίς κρυπτογράφηση, στα συστήματά της[3].

2.2. Όρια και κανόνες για την συλλογή ψηφιακών αποδεικτικών στοιχείων

Μέσα από τους νόμους που αναφέρθηκε προηγουμένως, μπορούμε να καταλάβουμε ότι θέτονται πολλοί κανόνες και όρια όσων αφορά τις έρευνες Ψηφιακής Εγκληματολογίας, θέμα που δυσκολεύει την σωστή

[2] https://gdpr-info.eu/art-83-gdpr/

[3] https://www.lifo.gr/now/tech-science/meta-prostimo-eu91-ekat-sto-facebook-gia-parabiaseis-toy-gdpr-apo-tin-irlandia

διεκπεραίωση τους. Την ευθύνη για την τήρηση αυτών των κανόνων την έχουν οι ερευνητές, οι οποίοι πρέπει να έχουν πολύ καλή γνώση των νόμων που επιβάλλονται στην δικαιοδοσία που γίνεται η έρευνα και να τους ακολουθεί πιστά, επειδή μπορεί να καταστραφεί η ακεραιότητα της έρευνας, άρα να θεωρηθεί αμελητέα (A. Nieto, R. Rios, & J. Lopez, 2019)[3]. Για αυτόν τον λόγο πρέπει να υπάρχει απαραίτητη εκπαίδευση του προσωπικού.

Τα όρια που τίθενται από τους περισσότερους νόμους προστασίας της ιδιωτικότητας αφορούν την συλλογή και επεξεργασία των προσωπικών δεδομένων των πολιτών, άνευ χαρακτηρισμού (εγκληματίας ή όχι). Ειδικότερα, σε κάποιες χώρες, όπως στην Αμερική, απαιτείται η έκδοση εντάλματος από το δικαστήριο, σε ορισμένες περιπτώσεις, για την συλλογή οποιουδήποτε αποδεικτικού στοιχείου, όπου, πάλι, η παραβίαση των ορίων του εντάλματος μπορεί να χαλάσει μια έρευνα (A. Nieto, R. Rios, & J. Lopez, 2019)[3]. Επίσης, και στα επόμενα στάδια της έρευνας, δηλαδή στην διατήρηση και ανάλυση των δεδομένων, υπάρχουν όρια που, και κατά λάθος, μπορούν να υπερβούν οι ερευνητές. Για παράδειγμα, μπορεί να δουν κατά λάθος ευαίσθητα δεδομένα που δεν αφορούν την έρευνα κατά την διάρκεια της ανάλυσης ή μπορεί να αποκτήσουν τα δεδομένα που έχουν συλλεχθεί κρυφά και παράνομα και να τα χρησιμοποιήσουν για προσωπικό κέρδος, π.χ. πουλώντας τα σε κακόβουλα πρόσωπα.

3. Ηθικά ζητήματα για την προστασία της ιδιωτικότητας ευαίσθητων αποδεικτικών στοιχείων

Κατά την διάρκεια μιας έρευνας Ψηφιακής Εγκληματολογίας μπορούν να προκύψουν πολλά ηθικά ζητήματα. Αυτό που εμφανίζεται συχνότερα είναι το ζήτημα της διαχείρισης ευαίσθητων δεδομένων που βρέθηκαν, αλλά είναι άσχετα με την έρευνα που πραγματοποιείται. Σε αυτή την περίπτωση, η σύμφωνη γνώμη είναι η απλή αγνόηση αυτών των δεδομένων, όμως, κάποιες φορές, μπορεί να αποκαλυφθούν πληροφορίες που έχουν αρνητικά αποτελέσματα στην ψυχολογία του εξεταστή. Άλλα ζητήματα που ανακύπτουν είναι οι προκαταλήψεις του ερευνητή κατά την διάρκεια της έρευνας, η αναγνώριση λαθών στην συλλογή ή ανάλυση των δεδομένων, και άλλα, που μπορούν να οδηγήσουν σε λάθος καταδίκες (Karie N.M. & Venter H.S., 2015)[10].

4. Προστασία της Ιδιωτικότητας κατά τη Διερεύνηση Ψηφιακών Αποδεικτικών Στοιχείων

Όπως αναφέρθηκε προηγουμένως, οι σημερινές ψηφιακές συσκευές μπορούν να αποθηκεύουν χιλιάδες αρχεία και διάφορα στοιχεία για τον χρήστη. Αυτό δημιουργεί πρόβλημα στην προσπάθεια να προστατευτούν τα άσχετα για μια έρευνα προσωπικά δεδομένα, επειδή, συνήθως, τα χρήσιμα στοιχεία

είναι ένα μικρό υποσύνολο των διαθέσιμων δεδομένων (F. Y. W. Law et al., 2011)[8]. Όμως, η προστασία της ιδιωτικότητας κατά την διερεύνηση ψηφιακών αποδεικτικών στοιχείων γίνεται απαραίτητη προϋπόθεση λόγω της ανάγκης για συμμόρφωση με νόμους και κανονιστικές αρχές, όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR). Για τον λόγο αυτό παρουσιάζονται συνεχώς καινούργιοι τρόποι για την επίτευξη αυτού του στόχου.

4.1. Μέθοδοι ελαχιστοποίησης της παραβίασης της ιδιωτικότητας κατά την έρευνα

Μέθοδοι για την προστασία της ιδιωτικότητας μπορεί να είναι είτε τεχνικοί είτε κανονιστικοί, που επιβάλλονται από κάποια αρχή. Επειδή το θέμα της ιδιωτικότητας στην διερεύνηση ψηφιακών εγκλημάτων είναι μια, σχετικά, νέα απαίτηση, δεν έχουν υλοποιηθεί ακόμα συγκεκριμένοι νόμοι ή κανονισμοί, άρα ακολουθούνται οι ήδη υπάρχοντες που αφορούν την ιδιωτικότητα της ζωής των ανθρώπων. Ταυτόχρονα, όμως, η φύση και ο σκοπός της Ψηφιακής Εγκληματολογίας είναι τελείως αντικρουόμενα με την απαίτηση για προστασία της ιδιωτικότητας, επειδή, πάντα, οι ερευνητές προσπαθούν να εξορύξουν τα περισσότερα δυνατά δεδομένα ώστε να εξάγουν ικανοποιητικά και σωστά συμπεράσματα.

4.1.1. Πολιτικές Προστασίας

Ένας σημαντικός τρόπος για εξασφαλισμένη ιδιωτικότητα είναι η ανάπτυξη πολιτικών ιδιωτικότητας που προσαρμόζονται πάνω στις έρευνες Ψηφιακής Εγκληματολογίας. Αυτές οι πολιτικές πρέπει αρχικά να σέβονται τους υπάρχοντες νόμους περί ιδιωτικότητας, και στην συνέχεια να αναπτύσσονται με τον στόχο να καταπραΰνουν τις ανησυχίες των χρηστών για την ιδιωτικότητά τους (A. Dehghantanha & K. Franke, 2014)[11]. Αυτοί οι κανόνες θα περιλαμβάνουν προϋποθέσεις που θα αφορούν όλη την διαδικασία της Ψηφιακής Εγκληματολογίας, όπως αυτή περιγράφηκε στο **Κεφάλαιο 1.2**, από την συλλογή, την αποθήκευση, την ανάλυση, μέχρι και την παρουσίαση των στοιχείων.

Οι πολιτικές προστασίας ενδείκνυται να γενικοποιούνται ώστε να υπάρχει περιθώριο για αλλαγές σε πιο περίπλοκες περιπτώσεις. Για παράδειγμα, ο (Halboob et al., 2015)[12] πρότεινε ένα μοντέλο τριών (3) επιπέδων ως προς την συλλογή και την πρόσβαση στα δεδομένα μιας έρευνας, όπου ξεχωρίζονται ποιος μπορεί να προβάλει ένα σύνολο δεδομένων, δηλαδή υλοποίηση ενός ελέγχου πρόσβασης. Συγκεκριμένα, χωρίζει τα δεδομένα σε σχετικά και μη-ιδιωτικά που μπορούν να χρησιμοποιηθούν από οποιονδήποτε ερευνητή, σε σχετικά αλλά ιδιωτικά, για τα οποία πρέπει να χρησιμοποιηθεί κάποια τεχνική για την χρήση τους και, τέλος, σε άσχετα για μια έρευνα δεδομένα τα οποία δεν πρέπει να είναι επιτρεπτή η χρήση τους για οποιονδήποτε λόγο. Αυτό το μοντέλο μπορεί να αξιοποιηθεί για την ανάπτυξη εργαλείων εγκληματολογίας (Neil C. Rowe)[13], για αυτόματο φιλτράρισμα των συλλεγέντων δεδομένων.

No.	Level Name	Description
1	Direct Accessible Data (DAD)	Data are relevant and non-private so it can be directly imaged and analyzed.
2	Privacy-Preserved Accessed Data (PAD)	Data are relevant as well as private. Therefore, a privacy preservation technique(s) needs to be applied during the data imaging and analysis.
3	Non-Accessible Data (NAD)	These data are not relevant to the investigated crime and are not accessible at all.

Σχήμα 5. Επίπεδα ιδιωτικότητας στην Ψηφιακή εγκληματολογία[12]

4.1.2. Τεχνικές Μέθοδοι

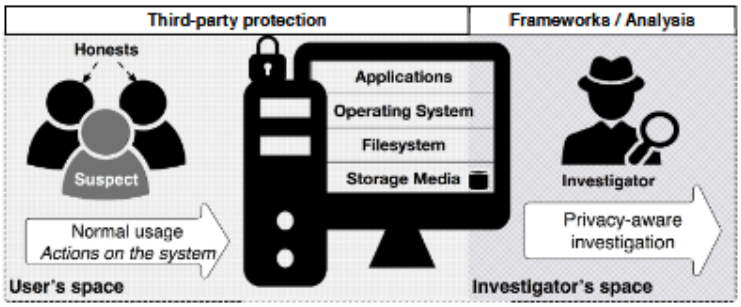
Για να μπορούν να λειτουργήσουν οι πολιτικές προστασίας και οι νόμοι, χρειάζονται εργαλεία και τεχνικές που θα τα εφαρμόζουν στο πλαίσιο της έρευνας. Επίσης, οι ίδιοι οι χρήστες μπορούν να πάρουν μέτρα για να προστατεύσουν την ιδιωτικότητά τους, ακόμα και από έρευνες Ψηφιακής Εγκληματολογίας (Neil C. Rowe)[13]. Τέτοια μέτρα ονομάζονται anti-forensics (αντί εγκληματολογικά) και χρησιμοποιούνται συχνά από εγκληματίες για αποφυγή ανίχνευσης.

Μια τεχνική διατήρησης της ιδιωτικότητας είναι η δημιουργία πλαισίου για την εγκληματολογική ετοιμότητα (forensic readiness), η οποία είναι μια από τις βασικές αρχές για τις εγκληματολογικές έρευνες και εννοεί την προετοιμασία που γίνεται πριν εξεταστεί ένα έγκλημα και συλλεχθούν τα απαραίτητα στοιχεία. Αναπτύσσοντας την καλύτερη δυνατή ετοιμότητα πριν αρχίσει η διαδικασία της συλλογής των ψηφιακών δεδομένων, δύναται να συνδράμει στην ελαχιστοποίηση των δεδομένων που να συγκεντρωθούν με αποτέλεσμα την αποφυγή ενός μέρους από τα περιττά δεδομένα που μπορεί να παραβιάσουν την ιδιωτικότητα των εξεταζόμενων ατόμων (A. Dehghantanha & K. Franke, 2014)[11]. Δυστυχώς, όμως, λόγω της συνεχής ανάπτυξης της τεχνολογίας και της απρόβλεπτης φύσης των ηλεκτρονικών συσκευών, γίνεται, συχνά, αδύνατη η ετοιμότητα, άρα χρειάζονται πιο πρακτικές μέθοδοι για να διασφαλιστεί η ιδιωτικότητα. Είναι, επίσης, δύσκολο να καθοριστεί ποια δεδομένα χρειάζονται και ποια όχι για να αποδειχθεί η αθωότητα ή η ενοχή του κατηγορουμένου, πριν ξεκινήσει η έρευνα. Έτσι, θέτοντας τέτοια πλαίσια, μπορεί να περιοριστούν οι δυνατότητες της έρευνας (Ludwig Englbrecht and Günther Pernul, 2020)[4].

Η απλή διαγραφή των δεδομένων μιας συσκευής είναι μια απλή και αποτελεσματική μέθοδος για την αποφυγή συλλογής προσωπικών και ευαίσθητων δεδομένων, γενικά ή και σε περίπτωση που ξέρουν οι χρήστες ότι θα ελεγχθούν οι συσκευές τους. Όμως, χρειάζονται περαιτέρω βήματα για να μην είναι προσβάσιμα με κανέναν τρόπο. Ένας γνωστός τρόπος για την ασφαλή διαγραφή δεδομένων είναι η αντικατάστασή τους με άλλα τυχαία (π.χ. σκέτα μηδενικά) μέσα στον αποθηκευτικό χώρο (F. Y. W. Law et al., 2011)[8].

Η πιο διαδεδομένη μέθοδος για την προστασίας μιας μυστικής πληροφορίας, δηλαδή της εμπιστευτικότητας της, που σε αυτή την περίπτωση είναι τα δεδομένα ενός ατόμου που δεν απαιτούνται για μια έρευνα, είναι με την χρήση κρυπτογραφικών αλγορίθμων. Λόγω, όμως, του όγκου των δεδομένων που συνήθως συλλέγονται, αυτή η διαδικασία καθιστάται αργή αλλά και πολύπλοκη στην υλοποίηση, επειδή είναι δύσκολη η αναζήτηση σε κρυπτογραφημένα δεδομένα και απίθανη η αποκρυπτογράφηση ξεχωριστών κομματιών τους (F. Y. W. Law et al., 2011)[8].

Ένας τρόπος για να γίνει δυνατή η αναζήτηση κρυπτογραφημένων δεδομένων είναι με την εφαρμογή λέξεων κλειδιών, δηλαδή η αποκρυπτογράφηση θα γίνεται μόνο στα δεδομένα που περιέχουν έναν συγκεκριμένο αριθμό λέξεων κλειδιών που αναζήτησε ο ερευνητής, ώστε να διασφαλίζεται η αποκλειστική χρήση σχετικών για την έρευνα δεδομένων (T. B. Ogunseyi & O. M. Adedayo, 2023)[2]. Με παρόμοιο τρόπο, μπορεί να υλοποιηθεί ένα σύστημα ελέγχου πρόσβασης, σε συνδυασμό με τις πολιτικές προστασίας, όπου τα συλλεγμένα δεδομένα ταξινομούνται, με βάση την ευαισθησία και την σημασία τους, και κρυπτογραφούνται. Κάθε επίπεδο μπορεί να προσπελαστεί από συγκεκριμένους ερευνητές, που έχουν την κατάλληλη εξουσιοδότηση, και μόνο αν πληρούνται κάποια προκαθορισμένα κριτήρια. Και οι δύο μέθοδοι, όμως, έχουν το πρόβλημα του τρόπου που θα ταξινομούνται τα δεδομένα και ποιος θα είναι ο υπεύθυνος για αυτό (A. Nieto, R. Rios, & J. Lopez, 2019)[3].



Σχήμα 6. Προσέγγιση ευαισθητοποιημένης Ψηφιακής Εγκληματολογίας ως προς την εγκληματολογία[3]

Μια ακόμη προσέγγιση είναι η δημιουργία αντιγράφων των αρχικών δεδομένων, αλλά αποκλειστικά με τα στοιχεία που αφορούν την έρευνα. Αυτή η τεχνική θεωρείται λάθος βάσει των αρχών των σωστών και επιστημονικών εγκληματολογικών ερευνών (forensic soundness) επειδή τροποποιούνται τα αρχικά δεδομένα, όμως λόγω των σημερινών κανονισμών αλλά και του όγκου των δεδομένων που συλλέγεται, η ιδέα αυτή γίνεται όλο και πιο δελεαστική. Αυτή η μέθοδος προτείνει τρεις (3) κατηγορίες τρόπων δημιουργίας αντιγράφων (Ludwig Englbrecht & Günther Pernul, 2020)[4]:

- Χειροκίνητη δημιουργία αντιγράφων
- Ημι-αυτόματη δημιουργία αντιγράφων
- Αυτόματη δημιουργία αντιγράφων

Στην χειροκίνητη ο ερευνητής αποφασίζει ποια δεδομένα είναι κρίσιμα για τον σκοπό της έρευνας και ποια όχι, που, όμως, δημιουργεί προβλήματα επειδή πρέπει να έχει πρόσβαση σε όλα τα δεδομένα στην αρχή της διαδικασίας, αρα δεν προστατεύεται η ιδιωτικότητα με αυτόν τον τρόπο. Με την ημι-αυτόματη δημιουργία αντιγράφων, ο ερευνητή θα μπορεί να επιλέξει συγκεκριμένα αρχεία με βάση διάφορα κριτήρια, όπως τον τύπο ή το περιεχόμενο ενός αρχείου, και το λογισμικό θα δημιουργεί το αντίγραφο βάσει αυτών των επιλογών. Όπως, όμως, ειπώθηκε προηγουμένως, αυτή η μέθοδος παραβιάζει την ακεραιότητα των δεδομένων και μπορεί να μην γίνουν δεκτά ως αποδεικτικά στοιχεία τα ευρήματα που βρέθηκα με την συγκεκριμένη μέθοδο. Για την αποφυγή αυτού του προβλήματος πρέπει να βρεθεί τρόπος που να αποδεικνύει την ακεραιότητα των αντεγραμμένων δεδομένων στην δίκη στην οποία θα παρουσιαστούν. Για την αυτόματη δημιουργία αντιγράφων πρέπει να αναπτυχθεί λογισμικό που θα έχει τις γνώσεις ενός ειδικευμένου ερευνητή ψηφιακών αποδεικτικών στοιχείων, αλλά και ενός δικαστή ώστε να μπορεί να διακρίνει σωστά μεταξύ των δεδομένων. Μετά από τον διαχωρισμό των δεδομένων θα δημιουργείται και ένα αρχείο ευρετήριο που περιέχει τα hash όλων των αρχείων και τις αλλαγές που έγιναν, αλλά και τους ειδικούς που είναι μέρος της έρευνας (Ludwig Englbrecht & Günther Pernul, 2020)[4].

4.2 Ιδιωτικότητα και Ψηφιακή Εγκληματολογία σε συστήματα Έξυπνου Σπιτιού (Smart Home)

Σε αυτό το κεφάλαιο θα αναλυθεί σύντομα πως εφαρμόζεται η Ψηφιακή Εγκληματολογία σε συστήματα Έξυπνου Σπιτιού (Smart Home).

Όπως κάθε πληροφοριακό σύστημα, έτσι και συσκευές έξυπνου σπιτιού (IoT) έχουν την πιθανότητα να δεχθούν κάποια επίθεση από κακόβουλους για να κλέψουν δεδομένα ή να τα χρησιμοποιήσουν προς πλεονεκτήματά τους για να παραβιάσουν το ίδιο το σπίτι. Επίσης, μπορεί να χρειαστεί η ανάλυση τους

στο πλαίσιο μιας έρευνας για την εξιχνίαση εγκλήματος. Όμως, επειδή ένα τέτοιο σύστημα αποτελείται από δίκτυο και πολλές διαφορετικές συσκευές, η συλλογή των δεδομένων από αυτά περιπλέκεται επειδή μπορεί να απαιτούνται και εξειδικευμένα εργαλεία (Plachkinova, M., Vo, A. & Alluhaidan, A., 2016)[19].

Οι περισσότερες συσκευές έξυπνου σπιτιού λειτουργούν με υπηρεσίες νέφους (cloud), υπάρχει πρόβλημα με την μεταβλητότητα των δεδομένων που αποθηκεύουν, επειδή με την αποσύνδεση των συσκευών από το δίκτυο μπορεί να χαθούν κάποια δεδομένα που δεν είχαν σταλεί για μόνιμη αποθήκευση. Αυτό δυσκολεύει μια έρευνα επειδή μπορεί να κρυφτεί η πηγή κάποιων σημαντικών δεδομένων και κάνει πολύπλοκη την διατήρηση χρονοδιαγράμματος για το Chain of Custody (Αλυσίδα Επιμέλειας). Μπορεί να δυσκολευτεί, επίσης, και από νομική άποψη λόγω του νέφους, αν οι υποδομές της υπηρεσίας που χρησιμοποιείται βρίσκονται σε άλλη χώρα χωρίς νομικές συμφωνίες (Plachkinova, M., Vo, A. & Alluhaidan, A., 2016)[19].

Σε αυτή την περίπτωση, θέματα ιδιωτικότητας υπάρχουν επειδή για να συλλεχθούν τα κατάλληλα δεδομένα πρέπει να παραβιαστεί η ιδιωτική ζωή στο σπίτι του εμπλεκόμενου, που μπορεί να περιλαμβάνει και προβολή καμερών ασφαλείας, ανάγνωση αρχείων καταγραφής του δικτύου που αποκαλύπτουν πολλά ιδιωτικά χαρακτηριστικά που δεν έχουν καμία σχέση με το έγκλημα για το οποίο διεξάγεται η έρευνα.

5. Προκλήσεις στην διατήρηση της ιδιωτικότητας στην Ψηφιακή Εγκληματολογία

Λόγω των διαφόρων νόμων που επιβάλλονται στην επεξεργασία δεδομένων αλλά και λόγω τεχνολογικών περιορισμών, μπορούν να εμφανιστούν πολλές προκλήσεις κατά την διάρκεια μια έρευνας
Ψηφιακής Εγκληματολογίας, ειδικά όταν υπάρχει απαίτηση για προστασία της ιδιωτικότητας των εμπλεκόμενων προσώπων. Προβλήματα προκαλούνται σε περιπτώσεις ερευνών πάνω σε καινούργιες τεχνολογίες, όπως σε υποδομές Διαδικτύου των Πραγμάτων (Internet of Things/IoT) όπου δεν έχει εμβαθύνει κάποια έρευνα ή νέφους (cloud) που εμφανίζονται θέματα δικαιοδοσίας (A. Nieto, R. Rios, & J. Lopez, 2019)[3].

Characteristic	Digital Forensic Challenge
Growing **size** of storage devices	Insufficient **time** to create a forensic image or to process the data
Prevalence of **embedded** flash storage and proliferation of HW interfaces	Storage devices can no longer be easily removed or imaged. **Embedded storage is routinely ignored** during forensic investigations (e.g., persistent memory inside GPUs)
Proliferation of **Operating Systems and file formats**	Increase the requirements, **complexity and cost** of digital forensic **tools**
Multiple devices in a single case	**Correlation** of digital evidence is needed
Pervasive **encryption**	Hinders or **avoids the processing** of data
Cloud for remote processing and storage	Complicates the **identification and acquisition** of digital evidence. Makes **impossible to perform basic forensic methodologies** of data preservation and isolation
Malware not written in persistent storage and capable of using **anti-forensic** techniques	Need for RAM forensics tools which are more difficult to create than disk tools and new systems to **capture the malware for in-depth analysis**
Law & Privacy	Limits the scope of forensic investigations

Σχήμα 7. Προκλήσεις της Ψηφιακής Εγκληματολογίας[3]

5.1. Νομικές προκλήσεις

Προκλήσεις εξαιτίας νομοθεσιών που πρέπει να ακολουθηθούν προκύπτουν από πολλές διαφορετικές όψεις και με διαφορετικά επίπεδα βαρύτητας. Αυτά μπορεί να είναι προβλήματα λόγω λάθους ή παράνομης συλλογής και χειρισμού δεδομένων, λόγω διαφορετικών νόμων σε περιπτώσεις διεθνών ερευνών, ή και λόγω αγνόησης των νομικών ορίων από επιτήδιους ή εξαιτίας κακής εκπαίδευσης.

Μια από τις σημαντικότερες αρχές της Ψηφιακής Εγκληματολογίας, που πρέπει να ακολουθείται πιστά για να θεωρηθεί έγκυρη μια έρευνα στο δικαστήριο, είναι η διασφάλιση της ακεραιότητας των αποδεικτικών στοιχείων που συλλέγονται, αναλύονται και διατηρούνται καθ'όλη την διάρκεια της έρευνας. Υπάρχουν κάποιες κατευθυντήριες οδηγίες που θέτουν κριτήρια για την επιστημονικότητα των στοιχείων που παρουσιάζονται, αλλά είναι περιληπτικές και είναι ανοιχτές σε διαφορετικές ερμηνείες, που μπορεί να οδηγήσει σε ασυνέπειες στον τρόπο αξιολόγησης των αποδείξεων. Γενικά, οι πιο διαδεδομένοι και σίγουροι τρόποι διασφάλισης της ακεραιότητας είναι με την χρήση διαφόρων τεχνικών όπως η κρυπτογράφηση, η χρονοσήμανση, ο κατακερματισμός κ.α. (Hussam N. Fakhouri et al., 2024)[18]. Πετυχαίνοντας την ακεραιότητα γίνεται να προστατευθεί και η ιδιωτικότητα, ως ένα ποσοστό, επειδή σε περίπτωση παράνομης παραβίασης άχρηστων δεδομένων, μπορεί να βρεθεί ο ένοχος με διάφορους τρόπου που αναφέρθηκαν και προηγουμένως στο Κεφάλαιο 4.

Μεγάλο πρόβλημα προκαλείται και σε περιπτώσεις που ένα έγκλημα διαπράττεται σε πολλές χώρες και πρέπει να συλλεχθούν αποδεικτικά στοιχεία από διάφορες δικαιοδοσίες. Αυτό εμφανίζεται κυρίως σε εγκλήματα στα οποία χρησιμοποιούνται πλατφόρμες νέφους (cloud) για την διακίνηση δεδομένων, που τα τελευταία χρόνια έχουν αναπτυχθεί με ραγδαίους ρυθμούς και εδραιώνονται παγκοσμίως. Με αυτόν τον τρόπο, εγκληματίες μπορούν να επιλέγουν υπηρεσίες νέφους που βρίσκονται σε περιοχές εκτός της δικαιοδοσίας της χώρας διαμονής τους, που επίσης δεν έχουν κάποια δικαστικη συμφωνία (Karie N.M. & Venter H.S., 2015)[10]. Ακόμα και με την ύπαρξη συμφωνιών, υπάρχει ακόμα το πρόβλημα της αισθητής διαφοράς των νόμων περί ιδιωτικότητας κάθε χώρας, όπου μπορεί να διαφοροποιείται ο τρόπος της νόμιμης συλλογής στοιχείων ή η διάκριση μεταξύ ευαίσθητων, και μη, δεδομένων, που προκαλεί προβλήματα στην αποδοχή των αποδείξεων από το νομικό σύστημα (Hussam N. Fakhouri et al., 2024)[18].

Επιπροσθέτως, προκλήσεις μπορούν να προκύψουν και από την χρήση εργαλείων και τεχνικών εγκληματολογίας. Αυτό συμβαίνει επειδή ένα λογισμικό ή μια μέθοδος συλλογής, ανάλυσης ή αποθήκευσης ψηφιακών αποδεικτικών στοιχείων, θα πρέπει να έχει πιστοποιηθεί κατάλληλα για χρήση σε δικαστικές και, γενικότερα, νομικές διαδικασίες. Σε αντίθετη περίπτωση, το δικαστήριο μπορεί να απορρίψει ευρήματα μιας έρευνας ως άκυρα. Επίσης, κάθε δεδομένο που παράγεται ως αποδεικτικό στοιχείο κατά την διάρκεια μιας έρευνας, πρέπει να υπάρχει η ικανότητα αναδημιουργίας του αποτελέσματος με τον ίδιο ή και διαφορετικό, εμπειρικό, τρόπο (Karie N.M. & Venter H.S., 2015)[10]. Σε αυτή την περίπτωση, προβλήματα ιδιωτικότητας μπορεί να δημιουργηθούν ακόμα και με έγκυρες τεχνικές και εργαλεία αν δεν τεθούν εξ' αρχής οι απαιτήσεις για την διάκριση μεταξύ των συλλεγέντων δεδομένων. Ως προς την διασφάλιση της ιδιωτικότητας, κάθε εργαλείο ή ερευνητής μπορεί να χρησιμοποιεί διαφορετικές μεθόδους για την επίτευξή της, άρα υπάρχει η πιθανότητα απόκλισης για το αν πραγματικά προστατεύεται η ιδιωτικότητα των ατόμων που εξετάζονται, που μπορεί να προκαλέσει προβλήματα σε όλη την δικαστική διαδικασία. Για παράδειγμα, μπορεί να δημιουργηθεί πρόβλημα σε περίπτωση που βρεθούν ενοχοποιητικά στοιχεία που αφορούν κάποιο άλλο έγκλημα που διαπράχθηκε, ανεξάρτητο από αυτό που εξετάζεται (Karie, N.M. and Venter, 2015)[10]. Επίσης, υπάρχουν περιπτώσεις που πρέπει να εξεταστούν συσκευές ατομων, εκτός του κατηγορούμενου (μάρτυρες, θύματα), για τα οποία μπορεί να ισχύουν άλλοι κανόνες που προστατεύουν τα δεδομένα τους (Graeme Horsman, 2022)[9].

5.2. Τεχνικές προκλήσεις

Αυτές οι προκλήσεις αφορούν τα προβλήματα που εμφανίζονται στις τεχνολογίες που χρησιμοποιούνται για την εκπλήρωση μιας έρευνας Ψηφιακής Εγκληματολογίας και μπορεί να είναι προβλήματα με τον τρόπο αποθήκευσης και διατήρησης των στοιχείων, η διασφάλισης της ακεραιότητάς τους, με την ανάλυσή τους, αλλά και πολλά άλλα που θα περιγραφούν στην συνέχεια.

Με την επέκταση του ψηφιακού κόσμου, ακολουθεί και τεράστια, εκθετική, αύξηση στα δεδομένα που παράγονται και αποθηκεύονται άρα και στις συσκευές αποθήκευσης καταναλωτών και οργανισμών. Αυτό δυσκολεύει την δουλειά των ερευνητών επειδή πρέπει να ψάξουν για χρήσιμες πληροφορίες ανάμεσα σε σωρούς άχρηστων δεδομένων, το οποίο είναι πολύ χρονοβόρο και είναι εύκολο να παραληφθούν, κατά λάθος, τα σημαντικά για την έρευνα δεδομένα. Αυτό το θέμα έχει ιδιαίτερη ισχύ σήμερα λόγω των εφαρμογών που λειτουργού σε πραγματικό χρόνο και έχουν χρονική ευαισθησία ως προς την συλλογή τους (Hussam N. Fakhouri et al., 2024)[18]. Εξαιτίας αυτού, επιπτώσεις δημιουργούνται και στην προστασία της ιδιωτικότητας, επειδή είναι χρονικά απίθανο να ασφαλιστούν όλα τα δεδομένα που έχουν συλλεχθεί με τα υπάρχοντα εργαλεία, ιδιαίτερα κρίσιμο στις χρονικές απαιτήσεις του δικαστηρίου (Karie N.M. & Venter H.S., 2015)[10], άρα μπορεί να χρειαστεί η ύπαρξη ενός επιπέδου αποδοχής παραβίασης της ιδιωτικότητας των κατηγορουμένων.

Προβλήματα προκαλεί και η συλλογή κρυπτογραφημένων δεδομένων, που με την ραγδαία ανάπτυξη των τεχνικών και των αλγορίθμων κρυπτογράφησης δισχερένει σε μεγάλο βαθμό την δουλειά των ερευνητών, επειδή πρέπει να προηγηθεί η διαδικασία της κρυπτανάλυσης πριν μπορούν να χρησιμοποιηθούν τα

δεδομένα, που, βάσει του αλγορίθμου που χρησιμοποιήθηκε, μπορεί να διαρκέσει και χρόνια αν δεν δεχτεί ο κατηγορούμενος να συνεργαστεί παρέχοντας χρήσιμα στοιχεία του κλειδιού αποκρυπτογράφησης ή το ίδιο το κλειδί. Σε κάποιες χώρες, όπως το Ηνωμένο Βασίλειο, δεν υποχρεούται η συνεργασία του κατηγορουμένου και έχει το δικαίωμα να απορρίψει να δώσει οποιοδήποτε τέτοιο στοιχείο. Για αυτόν τον λόγο, οι ερευνητές, συνήθως, αναγκάζονται να αγνοήσουν τα κρυπτογραφημένα δεδομένα χωρίς να τα χρησιμοποιήσουν επειδή, απλά, δεν υπάρχει χρονικό περιθώριο αλλά και λόγω περιορισμένων υπολογιστικών πόρων (Karie N.M. & Venter H.S., 2015)[10]. Επίσης, μπορεί κανείς να θεωρήσει το "σπάσιμο" της κρυπτογράφησης ως παραβίαση της ιδιωτικότητας του κατηγορουμένου επειδή γίνεται προσπάθεια πρόσβασης ενός μυστικού που δεν πρέπει να ξέρει κανείς εκτός του ιδιοκτήτη.

Μέθοδοι απόκρυψης, όπως η κρυπτογράφηση, δεδομένων που θα αναλυθούν για αποδεικτικά στοιχεία ενός εγκλήματος είναι ένα συχνό πρόβλημα που αντιμετωπίζετε κατά την διάρκεια ερευνών Ψηφιακής Εγκληματολογίας, και ονομάζονται αντι-εγκληματολογικά (anti-forensics) (Karie N.M. & Venter H.S., 2015)[10] και χρησιμοποιούνται από εγκληματίες με σκοπό την εκμετάλλευση των νόμων για την ιδιωτικότητα αλλά και τους ερευνητικούς περιορισμούς που υπάρχουν, για να προσπαθήσουν να αποφύγουν την αποκάλυψη όσο το δυνατόν περισσότερων ενοχοποιητικών στοιχείων για μειωμένη ποινή ή και αθώωση. Και αυτές οι μέθοδοι έχουν αναπτυχθεί πάρα πολύ τα τελευταία χρόνια και έχουν αναπτυχθεί πολλά εργαλεία για την εξυπηρέτηση τέτοιων αναγκών. Για παράδειγμα, μπορεί να χρησιμοποιηθεί κάποιο κακόβουλο λογισμικό (malware) που ανιχνεύει εργαλεία εγκληματολογίας και αυτόματα ενεργοποιεί αντίμετρα, όπως είναι η διαγραφή ή η κρυπτογράφηση ενοχοποιητικών στοιχείων στην μνήμη, από όπου δεν μπορεί να ανακτηθούν μετά, και στον σκληρό δίσκο (Hussam N. Fakhouri et al., 2024)[18].

5.3. Διαδικαστικές προκλήσεις και οργανωτικά προβλήματα

Οι διαδικαστικές προκλήσεις που εμφανίζονται είναι επίσης μεγάλης σημασίας επειδή επηρεάζουν όλα τα στάδια μιας έρευνας, από την τυποποίηση της διαδικασίας μέχρι το νομικό πλαίσιο της συλλογής και ανάλυσης των δεδομένων. Δηλαδή, υπαγορεύουν τον τρόπο διεξαγωγής της έρευνας άρα και την ακεραιότητα της και την αποδοχή της από το δικαστήριο (Hussam N. Fakhouri et al., 2024)[18]. Χωρίς συγκεκριμένες διαδικασίες δυσκολεύεται πολύ η έρευνα γενικά αλλά και η προσπάθεια για την προστασία της ιδιωτικότητας των δεδομένων.

Παρά την ύπαρξη διαφόρων προτύπων για τις διαδικασίες της Ψηφιακής Εγκληματολογίας, όπως των ISO και NIST, δεν έχουν αρκετή ανάπτυξη και υπάρχουν ασυνέπειες στις μεθοδολογίες και πρακτικές που συνιστούν και μπορεί να οδηγήσει σε δυσανασχετήσεις για την για την αξιοπιστία της έρευνας λόγω

της ασυμφωνίας για αυτά τα πρότυπα. Για αυτόν τον λόγο πρέπει να παγκοσμιοποιηθούν και να ομαδοποιηθούν τα πρότυπα ώστε να υπάρχει καλύτερη συνεργασία μεταξύ χωρών για διασυνοριακά νομικά θέματα (Hussam N. Fakhouri et al., 2024)[18].

Προβλήματα με την ιδιωτικότητα εμφανίζονται και όταν οι οργανισμοί που επεξεργάζονται δεδομένα και δεν έχουν κατάλληλα συστήματα και διαδικασίες ανίχνευσης, αντίδρασης, πρόληψης και διόρθωσης επιπτώσεων. Αυτό ισχύει είτε έχουν δικά τους συστήματα αποθήκευσης και επεξεργασίας δεδομένων, είτε εξάγουν την ευθύνη σε τρίτους, όπως σε υπηρεσίες νέφους (cloud). Η εξασφάλιση τέτοιας διαδικασίας είναι ζωτικής σημασίας επειδή, συνήθως, επιθέσεις σημειώνονται με σκοπό την κλοπή προσωπικών και εταιρικών δεδομένων. Για αυτό πρέπει να μπορεί ο οργανισμός να αντιδράσει εγκαίρως ώστε να συμμορφώνεται και με τους νόμους περί ιδιωτικότητας που απαιτούν την ενημέρωση των επηρεαζόμενων σε περίπτωση επίθεσης (Karie N.M. & Venter H.S., 2015)[10].

Το ανθρώπινο δυναμικό είναι άλλη μια μεγάλη πρόκληση που αντιμετωπίζετε από εταιρείες που διεξάγουν έρευνες Ψηφιακής Εγκληματολογίας. Η αύξηση της ανάγκης για την Ψηφιακή Εγκληματολογία, σημαίνει και αύξηση σε ανάγκες προσωπικού που, αν και μεγαλώνει η δημοτικότητά της, δεν καλύπτεται εύκολα. Επίσης, αυτό ισχύει ιδιαίτερα για έμπειρο και εκπαιδευμένο προσωπικό που οδηγεί σε χρήση ακατάλληλα εκπαιδευμένων εργαζομένων που μπορεί να προκαλέσει προβλήματα στην παράδοση σωστων και επιστημονικών αποτελεσμάτων. Μπορεί να παραβιαστει και η ιδιωτικότητα κατά λάθος, αλλά και με απώτερα κίνητρα (Karie N.M. & Venter H.S., 2015)[10].

6. Συμπεράσματα και Προοπτικές

Όσο αναπτύσσεται η τεχνολογία και γίνεται πιο προσβάσιμη από τον καθημερινό άνθρωπο, τόσο θα απαιτείται η ασφάλεια αυτών των ανθρώπων μέσα από την δικαιοσύνη, διατηρώντας όμως την ιδιωτικότητα στην πορεία. Η Ψηφιακή Εγκληματολογία, αν και απαραίτητη για τη διερεύνηση εγκλημάτων στον σύγχρονο ψηφιακό κόσμο, χρειάζεται συχνά η επεξεργασία προσωπικών και ευαίσθητων δεδομένων, όπου η χρήση τους, ακόμα και για νομικού σκοπούς λόγω εγκλημάτων, βρίσκεται σε γκρι ζώνη ως προς την νομιμότητα τους στο πλαίσιο μιας έρευνας.

Λόγω αυτής της τεχνολογικής εξέλιξης, οι νομοθεσίες που πρέπει να διασφαλίζουν την προστασία των δεδομένων τείνουν να μένουν πίσω και να μην μπορούν να καλύψουν επαρκώς καινούργια δεδομένα που προκύπτουν. Με αυτόν τον τρόπο, δυσκολεύονται πολύ οι έρευνες Ψηφιακής Εγκληματολογίας και γίνεται απίθανη η εξαγωγή συμπερασμάτων για ένα έγκλημα.

Για τον λόγο αυτό, πρέπει να αναπτυχθούν περαιτέρω πρότυπα για τις έρευνες Ψηφιακής Εγκληματολογίας που θα μπορούν να συμμορφώνονται με τους περισσότερους νόμους, σε οποιαδήποτε περίοδο, εξ' αρχής. Για παράδειγμα, με την ενσωμάτωση της αρχής, που αναφέρει ο GDPR, ιδιωτικότητα από σχεδιασμό (privacy by design) μπορεί να βοηθήσει πολύ την έρευνα να διασφαλίσει την ιδιωτικότητα από το ξεκίνημά της.

Επίσης, θα πρέπει να αναπτυχθούν πολιτικές προστασίας που θα ορίζουν συγκεκριμένες διαδικασίες για την σωστή διαχείριση των ψηφιακών αποδεικτικών στοιχείων. Επιπλέον, πρέπει να εκπαιδεύεται επαρκώς το προσωπικό για την σωστή και ηθική χρήση εργαλείων Ψηφιακής Εγκληματολογίας, που, επίσης, θα πρέπει να αναπτυχθούν για να βοηθήσουν τους ερευνητές να προστατευουν την ιδιωτικότητα χωρίς να χρειαστεί να χάσουν υπερβολικό χρόνο κάνοντάς το χειροκίνητα.

Βιβλιογραφία

[1]: Pollitt, M. (2010). A History of Digital Forensics. In: Chow, KP., Shenoi, S. (eds) Advances in Digital Forensics VI. DigitalForensics 2010. IFIP Advances in Information and Communication Technology, vol 337. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-15506-2_1

[2]: T. B. Ogunseyi and O. M. Adedayo, "Cryptographic Techniques for Data Privacy in Digital Forensics," in IEEE Access, vol. 11, pp. 142392-142410, 2023, doi: https://doi.org/10.1109/ACCESS.2023.3343360

[3]: A. Nieto, R. Rios, and J. Lopez, "Privacy-Aware Digital Forensics", Security and Privacy for Big Data, Cloud Computing and Applications, 2019. NICS Lab. https://www.nics.uma.es:8082/pub/papers/1777.pdf

[4]: Ludwig Englbrecht and Günther Pernul. 2020. A privacy-aware digital forensics investigation in enterprises. In Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES '20). Association for Computing Machinery, New York, NY, USA, Article 58, 1–10. https://doi.org/10.1145/3407023.3407064

[5]: N. Kumari and A. K. Mohapatra, "An insight into digital forensics branches and tools," *2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT)*, New Delhi, India, 2016, pp. 243-250, doi: 10.1109/ICCTICT.2016.7514586. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7514586&isnumber=7514538

[6]: Stefan Axelsson, "Digital Forensics - Process", Digital Forensics (DiFo), Stockholm 2024

[7]: Atheer Aljeraisy, Masoud Barati, Omer Rana, and Charith Perera. 2021. Privacy Laws and Privacy by Design Schemes for the Internet of Things: A Developer's Perspective. ACM Comput. Surv. 54, 5, Article 102 (June 2022), 38 pages. https://doi.org/10.1145/3450965

[8]: F. Y. W. Law et al., "Protecting Digital Data Privacy in Computer Forensic Examination," 2011 Sixth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering, Oakland, CA, USA, 2011, pp. 1-6, doi: https://doi.org/10.1109/SADFE.2011.15

[9]: Graeme Horsman, Defining principles for preserving privacy in digital forensic examinations, Forensic Science International: Digital Investigation, Volume 40, 2022, 301350, ISSN 2666-2817, doi: https://doi.org/10.1016/j.fsidi.2022.301350.

[10]: Karie, N.M. and Venter, H.S. (2015), Taxonomy of Challenges for Digital Forensics. J Forensic Sci, 60: 885-893. doi: https://doi.org/10.1111/1556-4029.12809

[11]: A. Dehghantanha and K. Franke, "Privacy-respecting digital investigation," *2014 Twelfth Annual International Conference on Privacy, Security and Trust*, Toronto, ON, Canada, 2014, pp. 129-138, doi: https://doi.org/10.1109/PST.2014.6890932.

[12]: Waleed Halboob, Ramlan Mahmod, Nur Izura Udzir, Mohd. Taufik Abdullah, Privacy Levels for Computer Forensics: Toward a More Efficient Privacy-preserving Investigation, Procedia Computer Science, Volume 56, 2015, Pages 370-375, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2015.07.222.

[13]: Neil C. Rowe, Current Privacy Concerns with Digital Forensics, US Naval Postgraduate School, United States, https://faculty.nps.edu/ncrowe/forensicpriv.pdf

[14]: K. Nance and D. J. Ryan, "Legal Aspects of Digital Forensics: A Research Agenda," *2011 44th Hawaii International Conference on System Sciences*, Kauai, HI, USA, 2011, pp. 1-6, doi: https://doi.org/10.1109/HICSS.2011.282.

[15]: Raphaël Gellert, Serge Gutwirth, The legal construction of privacy and data protection, Computer Law & Security Review, Volume 29, Issue 5, 2013, Pages 522-530, ISSN 2212-473X, https://doi.org/10.1016/j.clsr.2013.07.005.

[16]: Art. 25 GDPR, *Data protection by design and by default*, https://gdpr-info.eu/art-25-gdpr/

[17]: Art. 4 GDPR, *Definitions, https://gdpr-info.eu/art-4-gdpr/*

[18]: H. N. Fakhouri, M. A. AlSharaiah, A. k. Al hwaitat, M. Alkalaileh and F. F. Dweikat, "Overview of Challenges Faced by Digital Forensic," *2024 2nd International Conference on Cyber Resilience (ICCR)*, Dubai, United Arab Emirates, 2024, pp. 1-8, doi: https://doi.org/10.1109/ICCR61006.2024.10532850

[19]: Plachkinova, M., Vo, A. and Alluhaidan, A., 2016. Emerging trends in smart home security, privacy, and digital forensics, https://web.archive.org/web/20200323123821id_/https://aisel.aisnet.org/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1434&context=amcis2016