Κεφάλαιο 9. Ψηφιακή εγκληματολογία και οικονομικές έρευνες

Υπεύθυνος εταίρος για το κεφάλαιο: BayHfoD

Co-funded by the European Union

9. Κεφάλαιο 9. Ψηφιακή Εγκληματολογία και Οικονομικές Έρευνες

9.1 Εισαγωγή

Στον σημερινό ψηφιακό κόσμο, τα όρια μεταξύ εικονικής και πραγματικής ζωής είναι συχνά δυσδιάκριτα, γεγονός που ισχύει και για τις σκοτεινές μηχανορραφίες της εμπορίας ανθρώπων με σκοπό την εργασιακή εκμετάλλευση (εν συντομία: εργασιακή εκμετάλλευση ή εμπορία εργατικού δυναμικού). Το παρόν κεφάλαιο της εκπαίδευσης με τίτλο «Ψηφιακή Εγκληματολογία και Οικονομικές Έρευνες» υπογραμμίζει τον κρίσιμο ρόλο αυτών των δύο επιστημονικών κλάδων στην ανίχνευση και την καταπολέμηση της εργασιακής εκμετάλλευσης. Η ψηφιακή εγκληματολογία επικεντρώνεται στην ανάλυση ηλεκτρονικών δεδομένων για τη συλλογή ψηφιακών αποδεικτικών στοιχείων εγκληματικών δραστηριοτήτων που σχετίζονται με την εργασιακή εκμετάλλευση, ενώ οι οικονομικές έρευνες στοχεύουν στην παρακολούθηση των ροών χρημάτων και στην αποκάλυψη των οικονομικών δικτύων που κρύβονται πίσω από αυτά τα εγκλήματα. Οι ερευνητές/-τριες συνδυάζοντας αυτές τις δύο προσεγγίσεις μπορούν όχι μόνο να εντοπίσουν τους δράστες, αλλά και να αποκαλύψουν τις συχνά πολύπλοκες συνδέσεις μεταξύ των ψηφιακών ιχνών και των οικονομικών συναλλαγών που καθιστούν δυνατή την εργασιακή εκμετάλλευση. Σε αυτό το πλαίσιο, παρουσιάζονται διαδικασίες, βέλτιστες πρακτικές, μέθοδοι και πιθανά εργαλεία που επιτρέπουν στους/στις επαγγελματίες να αξιοποιήσουν τις δυναμικές αλληλεπιδράσεις μεταξύ της ψηφιακής επικοινωνίας και των χρηματικών

ροών για να βοηθήσουν τα θύματα της εμπορίας ανθρώπων και να αναλάβουν νομική δράση κατά των δραστών.

Το κεφάλαιο της εκπαίδευσης ξεκινά με τους μαθησιακούς στόχους ενός συμμετέχοντα στην εκπαίδευση (Ενότητα 2). Αυτοί παρατίθενται ξεχωριστά για την «ψηφιακή εγκληματολογία» και τις «οικονομικές έρευνες». Ακολουθούν οι ορισμοί των πιο σημαντικών όρων για αυτό το κεφάλαιο (Ενότητα 3). Η Ενότητα 4, που αποτελεί τον πυρήνα του κεφαλαίου της εκπαίδευσης, περιέχει το θεωρητικό και ενημερωτικό υπόβαθρο των θεμάτων. Ακολουθεί μια πρακτική δραστηριότητα, η οποία επιτρέπει στα συμμετέχοντα άτομα να εργαστούν με τις θεωρητικές πληροφορίες που έχουν μάθει εκ των προτέρων και να τις επεξεργαστούν σε μεγαλύτερο βάθος (Ενότητα 5). Το κεφάλαιο ολοκληρώνεται με τις βιβλιογραφικές και δικτυογραφικές αναφορές (Ενότητα 6).

9.2 Μαθησιακοί Στόχοι

Αυτό το κεφάλαιο της εκπαίδευσης παρέχει στα συμμετέχοντα άτομα τις απαραίτητες γνώσεις για την ψηφιακή εγκληματολογία και τις οικονομικές έρευνες που σχετίζονται με την εμπορία ανθρώπων και την εργασιακή εκμετάλλευση. Μετά το τέλος αυτού του κεφαλαίου, τα συμμετέχοντα άτομα θα είναι σε θέση:

Ψηφιακή εγκληματολογία

- Να κατανοούν τις αρχές της ψηφιακής εγκληματολογίας, συμπεριλαμβανομένης της συλλογής, διατήρησης και ανάλυσης δεδομένων, διασφαλίζοντας παράλληλα την ακεραιότητα της αλυσίδας επιτήρησης.

- Να γνωρίζουν πώς να δημιουργούν εγκληματολογικά αντίγραφα ασφαλείας (εικόνες και λογικά αντίγραφα).
- Να γνωρίζουν πού να αναζητήσουν ψηφιακά ίχνη και αποδεικτικά στοιχεία που έχουν αφήσει οι διακινητές και τι μπορεί να εξαχθεί από διαφορετικές πηγές ψηφιακών αποδεικτικών στοιχείων.
- Να κατανοούν το νομικό πλαίσιο που διέπει τα ψηφιακά αποδεικτικά στοιχεία και να διασφαλίζουν τη συμμόρφωση με τις διαδικαστικές απαιτήσεις.

Οικονομικές έρευνες

- Να εντοπίζουν ύποπτες χρηματοοικονομικές δραστηριότητες που ενδέχεται να υποδηλώνουν εμπορία ανθρώπων.
- Να εφαρμόζουν μια μεθοδολογία βήμα προς βήμα για τη διεξαγωγή οικονομικών ερευνών που σχετίζονται με την εμπορία ανθρώπων.
- Να κατανοούν τους οικονομικούς παράγοντες που οδηγούν στην εμπορία ανθρώπων.
- Να γνωρίζουν τις προκλήσεις στις χρηματοοικονομικές έρευνες, συμπεριλαμβανομένης της χρήσης κρυπτονομισμάτων, υπεράκτιων (offshore) λογαριασμών και τεχνικών ψηφιακής συσκότισης.
- Να κατανοούν τον ρόλο της Σύμπραξης Δημόσιου-Ιδιωτικού Τομέα (ΣΔΙΤ) στις χρηματοοικονομικές έρευνες και τη διεθνή συνεργασία για την καταπολέμηση της εμπορίας ανθρώπων.

9.3 Ορισμοί

Στη συνέχεια, θα περιγραφούν εν συντομία σημαντικές λέξεις-κλειδιά και για τα δύο θέματα.

Λέξεις-κλειδιά σχετικές με την ψηφιακή εγκληματολογία

9.3.1

Ψηφιακή Εγκληματολογία

Η ψηφιακή εγκληματολογία ασχολείται με την ταυτοποίηση, τη διατήρηση και την εξέταση ψηφιακών αποδεικτικών στοιχείων για την υποστήριξη ποινικών ερευνών. Περιλαμβάνει μεθόδους απόκτησης, ανάλυσης και τεκμηρίωσης δεδομένων για τον εντοπισμό ψηφιακών ιχνών εγκληματικών δραστηριοτήτων.

Δημιουργία Αντιγράφων Ασφαλείας Εγκληματολογικών Δεδομένων

Η δημιουργία ακριβών αντιγράφων ψηφιακών μέσων αποθήκευσης με διατήρηση της ακεραιότητας και της ιχνηλασιμότητας των δεδομένων (αλυσίδα επιτήρησης). Περιλαμβάνει φυσικά αντίγραφα ασφαλείας εικόνων (RAW, E01) και λογικά αντίγραφα ασφαλείας (L01, AD1).

Αλυσίδα Επιτήρησης

Συνεχής, χρονολογική τεκμηρίωση της διαχείρισης ψηφιακών αποδεικτικών στοιχείων για τη διασφάλιση της αυθεντικότητας και της ακεραιότητάς τους σε νομικές διαδικασίες.

Αντι-Ψηφιακή Εγκληματολογία (Anti-Digital Forensics)

Μέτρα που λαμβάνονται από έναν/μια χρήστη/-στρια με στόχο να δυσχεράνουν ή ακόμη και να αποτρέψουν την αξιολόγηση των ψηφιακών ιχνών. Για παράδειγμα, κρυπτογράφηση δεδομένων (FDE, container), TOR/ιδιωτική περιήγηση, εικονικοποίηση (virtualisation) → διαγραφή της Εικονικής Μηχανής (Virtual Machine - VM), προγράμματα για διαγραφή αρχείων (wiping), εκκαθάριση, αλλαγή χρονικών σημάνσεων (timestomping) απόκρυψη δεδομένων, π.χ. στεγανογραφία, πολλαπλή συσκευασία (multiple packing) κ.λπ.

eDiscovery

Η στοχευμένη χρήση της ψηφιακής εγκληματολογίας για την ανάλυση μεγάλου όγκου δεδομένων με σκοπό την εξαγωγή πληροφοριών σχετικών με έρευνες ή νομικές διαδικασίες. Με άλλα λόγια, το eDiscovery (ηλεκτρονική ανακάλυψη) είναι η ανάλυση δεδομένων για συγκεκριμένες υποθέσεις (π.χ. οργανωμένο έγκλημα, οικονομικό έγκλημα, αδικήματα κατά της κρατικής ασφάλειας). Για τη διεξαγωγή του eDiscovery απαιτούνται συγκεκριμένες γνώσεις σχετικά με τα αδικήματα και τη συγκεκριμένη υπόθεση. Επιπλέον, καθώς τα δεδομένα αυξάνονται συνεχώς, οι εγκληματολογικές εκθέσεις απαιτούν **αποσπάσματα δεδομένων**. Αυτό που θα μπορούσε να διευκολύνει το eDiscovery είναι το Electronic Discovery Reference Model EDRM, ένα πλαίσιο που περιλαμβάνει τα πρότυπα ανακάλυψης και ανάκτησης ψηφιακών δεδομένων, όπως για παράδειγμα:

- Βασικές γνώσεις υλικού (hardware)·
- Βασικές αρχές της ψηφιακής εγκληματολογίας·
- Δομή των φορέων δεδομένων και των συστημάτων αρχείων·
- Σύντομη εισαγωγή στα εργαλεία εγκληματολογικής ανάλυσης·

- Βασικές εγκληματολογικές δραστηριότητες·
- Δομή και λειτουργικότητα του λειτουργικού συστήματος Windows·
- Εγκληματολογικά τεκμήρια από συστήματα Windows.

Εγκληματολογικά Μέσα Εκκίνησης

Εξειδικευμένα λειτουργικά συστήματα (π.χ. συστήματα βασισμένα σε Linux ή Windows) που χρησιμοποιούνται για την εκκίνηση ψηφιακών συσκευών και τη διεξαγωγή εγκληματολογικών αναλύσεων χωρίς να αλλοιώνονται τα αρχικά δεδομένα.

Πλεονάζουσα Συστοιχία Ανεξάρτητων Δίσκων (Redundant Array of Independent Disks -RAID)

Σύστημα που συνδυάζει πολλαπλούς σκληρούς δίσκους για την ενίσχυση της ασφάλειας και της απόδοσης των δεδομένων, το οποίο απαιτεί εξειδικευμένες τεχνικές εγκληματολογικής ανάλυσης για τη συλλογή δεδομένων.

9.3.2

Λέξεις-κλειδιά σχετικές με οικονομικές έρευνες

Οικονομικές Έρευνες

Η εξέταση χρηματοοικονομικών συναλλαγών με σκοπό την αποκάλυψη παράνομων δραστηριοτήτων, όπως νομιμοποίηση εσόδων από παράνομες δραστηριότητες, χρηματοδότηση της τρομοκρατίας ή εμπορία ανθρώπων, και τον εντοπισμό των δραστών.

Ξέπλυμα Μαύρου Χρήματος/ Νομιμοποίηση Εσόδων από Παράνομες Δραστηριότητες (Money Laundering-ML)

Η διαδικασία απόκρυψης της παράνομης προέλευσης κεφαλαίων μέσω μιας σειράς χρηματοοικονομικών συναλλαγών, ώστε να φαίνονται νόμιμα. (Αντίθετο: Καταπολέμηση της Νομιμοποίησης Εσόδων από Παράνομες Δραστηριότητες/ Anti-Money Laundering)

Γνωρίστε τον/την Πελάτη/-τισσά Σας (Know Your Customer-KYC)

Κανονιστική απαίτηση για τα χρηματοπιστωτικά ιδρύματα να επαληθεύουν την ταυτότητα και το χρηματοοικονομικό ιστορικό των πελατών/-τισσών τους, προκειμένου να αποτρέπουν το ξέπλυμα χρήματος και τη χρηματοδότηση της τρομοκρατίας.

Αναφορές Ύποπτων Συναλλαγών (Suspicious Transaction Reports-STR)

Αναφορές που πρέπει να υποβάλλουν τα χρηματοπιστωτικά ιδρύματα όταν μια συναλλαγή θεωρείται δυνητικά ύποπτη ή συνδέεται με ξέπλυμα χρήματος ή χρηματοδότηση της τρομοκρατίας.

Ανάλυση Blockchain

Η διερεύνηση συναλλαγών με κρυπτονομίσματα για τον εντοπισμό παράνομων δραστηριοτήτων, όπως νομιμοποίηση εσόδων από παράνομες δραστηριότητες, απάτη ή χρηματοδότηση της τρομοκρατίας, και για τον εντοπισμό δικτύων παραβατών.

Κρυπτονομίσματα και Τεχνικές Συσκότισης

Ψηφιακά νομίσματα (π.χ. Bitcoin, Monero) και μέθοδοι όπως mixers, tumblers ή chain-hopping που χρησιμοποιούνται για την απόκρυψη χρηματοοικονομικών συναλλαγών.

9.4 Θεωρητικό/Ενημερωτικό Μέρος

Ψηφιακή εγκληματολογία

9.4.1 Η παρούσα ενότητα παρέχει μια γενική επισκόπηση της ψηφιακής εγκληματολογίας, η οποία αναλύεται εκτενέστερα στην Ενότητα 9.6.2, δίνοντας βασικές πληροφορίες για το τι είναι, πώς μπορεί να κατηγοριοποιηθεί και πώς είναι μια τυπική διαδικασία ψηφιακής εγκληματολογίας. Ακόμη, η ενότητα περιγράφει τις βασικές αρχές που πρέπει να λαμβάνει υπόψη ένας/μια ψηφιακός/-κή επιστήμονας ή επαγγελματίας. Στη συνέχεια, η Ενότητα 9.6.2 ασχολείται με τις βασικές γνώσεις σχετικά με τα αντίγραφα ασφαλείας δεδομένων, καθώς αυτά αποτελούν τη βάση μιας σταθερής και επιτυχημένης διαδικασίας ψηφιακής εγκληματολογίας. Ωστόσο, μια περαιτέρω βασική τεχνική εισαγωγή στην ψηφιακή εγκληματολογία (μέσω αυτού του πρώτου βήματος της δημιουργίας αντιγράφων ασφαλείας) θα ήταν υπερβολική σε αυτό το σημείο, ιδίως διότι, για παράδειγμα, οι μέθοδοι ανάλυσης είναι πολύ διαφορετικές για να καλυφθούν στο παρόν έγγραφο. Συνεπώς, δεν κρίνεται σκόπιμο, δεδομένου ότι η εφαρμογή αφορά την εμπορία ανθρώπων και την εργασιακή εκμετάλλευση, να προχωρήσουμε σε περαιτέρω βήματα. Για τον λόγο αυτό, η Ενότητα 9.4.1.3 ασχολείται με την ψηφιακή εγκληματολογία στο πλαίσιο της εμπορίας ανθρώπων.

9.4.2

Επισκόπηση

Η εγκληματολογία είναι η εφαρμογή επιστημονικών μεθόδων για την ανάλυση και τη δίωξη ποινικών αδικημάτων. Η ψηφιακή εγκληματολογία, συγκεκριμένα, ασχολείται με ερωτήματα όπως:

- Πού δημιουργούνται τα ψηφιακά ίχνη;
- Πώς μπορούν να αναγνωριστούν και να αξιολογηθούν τα ψηφιακά ίχνη;
- Πώς μπορούν να εξασφαλιστούν και να αξιοποιηθούν τα ψηφιακά ίχνη;

Ακόμη και αν η ψηφιακή εγκληματολογία έχει ήδη οριστεί στην Ενότητα 3, αξίζει να αναφερθούμε σε περισσότερες λεπτομέρειες. Η ψηφιακή εγκληματολογία περιλαμβάνει (1) την αναζήτηση, την ταυτοποίηση, (2) την περιγραφή και (3) την εξέταση ψηφιακών αποδεικτικών στοιχείων, συμπεριλαμβανομένης της αξιολόγησης της αξιοπιστίας, της εγκυρότητας και της συνάφειας τους με τη συγκεκριμένη υπόθεση. Ως τελευταίο βήμα, η (4) ψηφιακή εγκληματολογία περιλαμβάνει την αναφορά αυτών των αποδεικτικών στοιχείων (Maras, 2014). Ασχολείται με μεθόδους για την απόκτηση, ανάλυση και τεκμηρίωση δεδομένων με σκοπό τον εντοπισμό ψηφιακών αποτυπωμάτων εγκληματικών δραστηριοτήτων, ιχνών σε ψηφιακές συσκευές που μπορούν και πρέπει να αναλυθούν για σκοπούς ποινικής δίωξης.

Κανονικά, υπάρχουν **εξειδικευμένες μονάδες** στις Υπηρεσίες Επιβολής του Νόμου (YEN) για την ψηφιακή εγκληματολογία. Γι' αυτό και τα τμήματα καταπολέμησης της εμπορίας ανθρώπων συνεργάζονται κυρίως με τμήματα ψηφιακής εγκληματολογίας και συνήθως δεν ασχολούνται με θέματα ψηφιακής εγκληματολογίας χωρίς βοήθεια. Επομένως, είναι προτιμότερο να δημιουργηθεί και να διατηρηθεί η συνεργασία με τα εν λόγω τμήματα. Επιπλέον, είναι σκόπιμο να γνωρίζετε τις διάφορες επαγγελματικές θέσεις στην υπηρεσία, π.χ. υπάρχει αστυνομικός/-κή υπάλληλος υπεύθυνος/-νη για

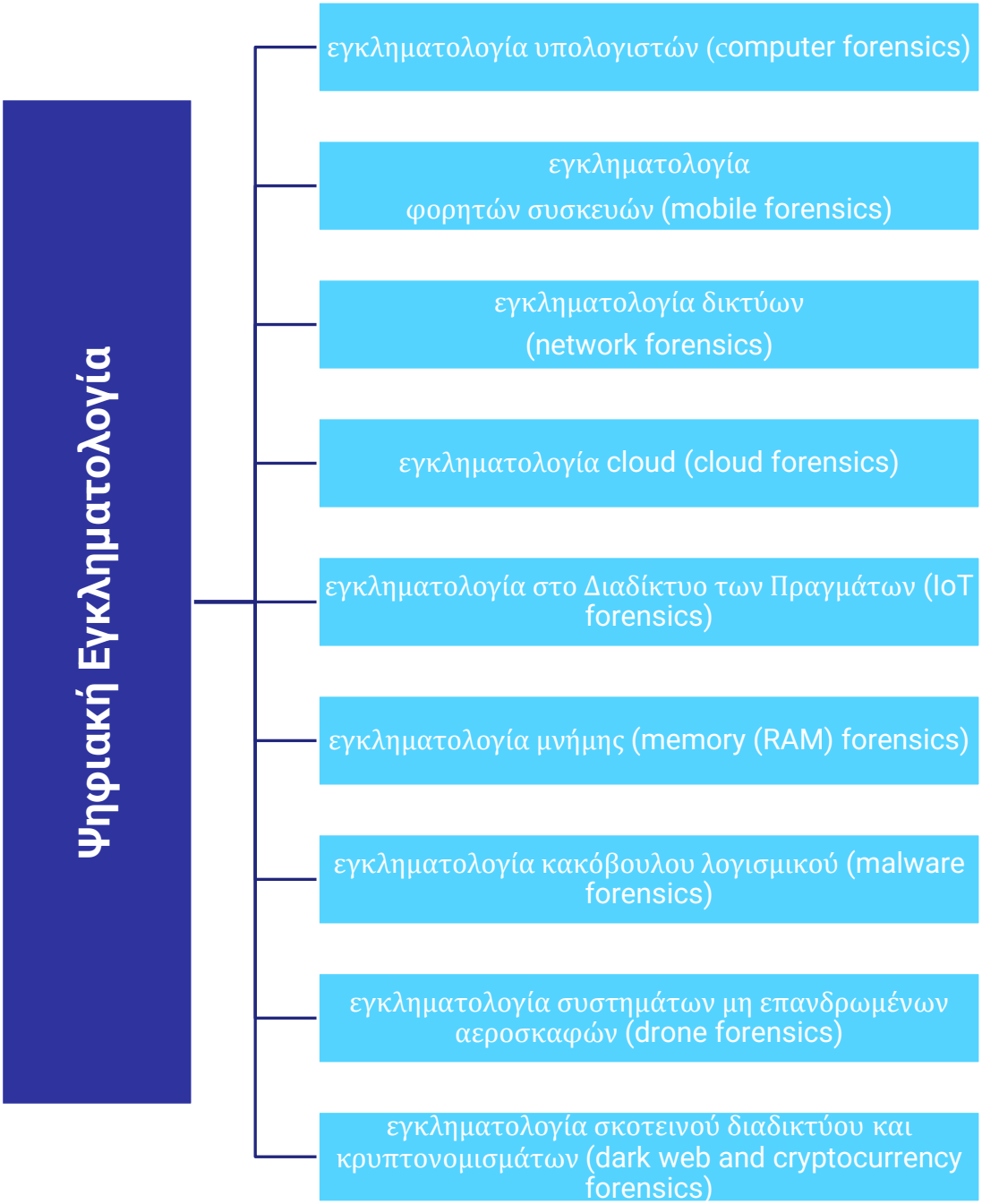
Η ψηφιακή εγκληματολογία περιλαμβάνει την ταυτοποίηση, την εξασφάλιση και τη διερεύνηση ψηφιακών αποδεικτικών στοιχείων, λαμβάνοντας παράλληλα υπόψη (1) τις νομικές περιστάσεις και τις συνθήκες πλαισίου (για να εξασφαλιστεί η χρηστικότητα στο δικαστήριο) και (2) τη διατήρηση και την τεκμηρίωση της αλυσίδας επιτήρησης και της ακεραιότητας των δεδομένων. Ως εκ τούτου, είναι σημαντικό για την ψηφιακή εγκληματολογία κάθε προσπάθεια και κάθε βήμα να είναι αποδεκτά από το δικαστήριο και να μπορούν να χρησιμοποιηθούν στη δικαστική τεκμηρίωση.

Τα τυπικά καθήκοντα των επιστημόνων ψηφιακής εγκληματολογίας περιλαμβάνουν: δημιουργία αντιγράφων ασφαλείας δεδομένων από υπολογιστές, φορείς δεδομένων, φορητές συσκευές και διαδικτυακούς χώρους αποθήκευσης, προετοιμασία και αξιολόγηση ηλεκτρονικών αποδεικτικών στοιχείων, παροχή συμβουλών και υποστήριξης κατά τη διάρκεια ερευνών.

Επιπρόσθετα, η ψηφιακή εγκληματολογία μπορεί να χωριστεί και να κατηγοριοποιηθεί σε διαφορετικούς κλάδους. Το Σχήμα 11 παρέχει μια επισκόπηση των πιθανών κλάδων της ψηφιακής εγκληματολογίας. Η εγκληματολογία υπολογιστών επικεντρώνεται στην ανάκτηση, ανάλυση και διατήρηση ψηφιακών αποδεικτικών στοιχείων από υπολογιστές, συμπεριλαμβανομένων σκληρών δίσκων, συστημάτων αρχείων, λειτουργικών συστημάτων και δεδομένων εφαρμογών. Βασικές τεχνικές είναι η δημιουργία εικόνων δίσκων, η ανάκτηση αρχείων και η ανάλυση μητρώων (βλ. π.χ. Casey, 2011). Η εγκληματολογία βάσεων δεδομένων (που

μερικές φορές αναφέρεται ξεχωριστά) ασχολείται με την εξέταση βάσεων δεδομένων (συμπεριλαμβανομένων των βάσεων δεδομένων SQL και NoSQL) και των μεταδεδομένων τους και περιλαμβάνει, για παράδειγμα, τη χρονοσήμανση μιας βάσης δεδομένων και την ανάλυση σε πραγματικό χρόνο (βλ. π.χ. Dubey, Bhatt & Negi, 2023) για την αποκάλυψη χειραγώγησης δεδομένων, μη εξουσιοδοτημένης πρόσβασης ή παραβίασης. Ωστόσο, η εγκληματολογική ανάλυση βάσεων δεδομένων μπορεί επίσης να θεωρηθεί υποπεδίο της εγκληματολογικής ανάλυσης υπολογιστών, καθώς οι βάσεις δεδομένων αποθηκεύονται κυρίως σε παραδοσιακά υπολογιστικά συστήματα, όπως διακομιστές (servers). Η εγκληματολογική ανάλυση φορητών συσκευών ασχολείται με την εξαγωγή και ανάλυση δεδομένων που είναι αποθηκευμένα σε φορητές συσκευές, όπως smartphone, tablet και συστήματα GPS (Dubey, Bhatt & Negi, 2023). Η εγκληματολογία δικτύων περιλαμβάνει την ανάλυση της δικτυακής κίνησης για τη λήψη πληροφοριών, την ανίχνευση εισβολών και τη συλλογή νομικών αποδεικτικών στοιχείων. Στο υποπεδίο της εγκληματολογίας τείχους προστασίας (firewall forensics), εξετάζονται όλα τα αρχεία καταγραφής του τείχους προστασίας για την εύρεση πολύτιμων αποδεικτικών στοιχείων. Η εγκληματολογία cloud διερευνά τα αποδεικτικά στοιχεία που είναι αποθηκευμένα σε περιβάλλοντα «νέφους» (cloud) αντιμετωπίζοντας προκλήσεις που σχετίζονται με την αποθήκευση δεδομένων σε πολλαπλές δικαιοδοσίες, τους περιορισμούς πρόσβασης και τη συνεργασία των παρόχων. Συνεπώς, απαιτεί εξειδικευμένες νομικές και τεχνικές εκτιμήσεις. Η εγκληματολογία IoT εξετάζει τα ψηφιακά ίχνη από συσκευές του Διαδικτύου των Πραγμάτων (IoT), όπως έξυπνες οικιακές συσκευές, φορητές συσκευές, βιομηχανικοί αισθητήρες και συστήματα αυτοκινήτων. Συχνά περιλαμβάνει ένα συνδυασμό ανάλυσης ενσωματωμένων συστημάτων, εγκληματολογίας δικτύων και παραδοσιακής εγκληματολογίας συσκευών. Η εγκληματολογία μνήμης (RAM) επικεντρώνεται στην εξαγωγή και ανάλυση της πτητικής μνήμης (RAM) για την

αποκάλυψη των εκτελούμενων διαδικασιών, των κλειδιών κρυπτογράφησης, του κακόβουλου λογισμικού και της δραστηριότητας του συστήματος σε πραγματικό χρόνο. Η εγκληματολογία κακόβουλου λογισμικού περιλαμβάνει την ανάλυση κακόβουλου λογισμικού (malware) για την κατανόηση της συμπεριφοράς του, τον προσδιορισμό της προέλευσής του και τον μετριασμό των επιπτώσεών του (π.χ. μέσω στατικής και δυναμικής ανάλυσης κακόβουλου λογισμικού, sandboxing, reverse engineering). Η εγκληματολογική ανάλυση drone ασχολείται με την εξαγωγή δεδομένων από μη επανδρωμένα αεροσκάφη (UAV), συμπεριλαμβανομένων των αρχείων πτήσεων, της ενσωματωμένης αποθήκευσης, της παρακολούθησης GPS και των συστημάτων επικοινωνίας. Η εγκληματολογική ανάλυση του dark web και των κρυπτονομισμάτων εστιάζει σε παράνομες δραστηριότητες στο dark web, συμπεριλαμβανομένης της εμπορίας ανθρώπων, του εμπορίου ναρκωτικών και του κυβερνοεγκλήματος. Οι τεχνικές εγκληματολογικής ανάλυσης κρυπτονομισμάτων βοηθούν στην ανίχνευση συναλλαγών σε Bitcoin ή άλλα ψηφιακά νομίσματα για τον εντοπισμό εγκληματικών παραγόντων.



Σχήμα1 . Πιθανοί κλάδοι της ψηφιακής εγκληματολογίας

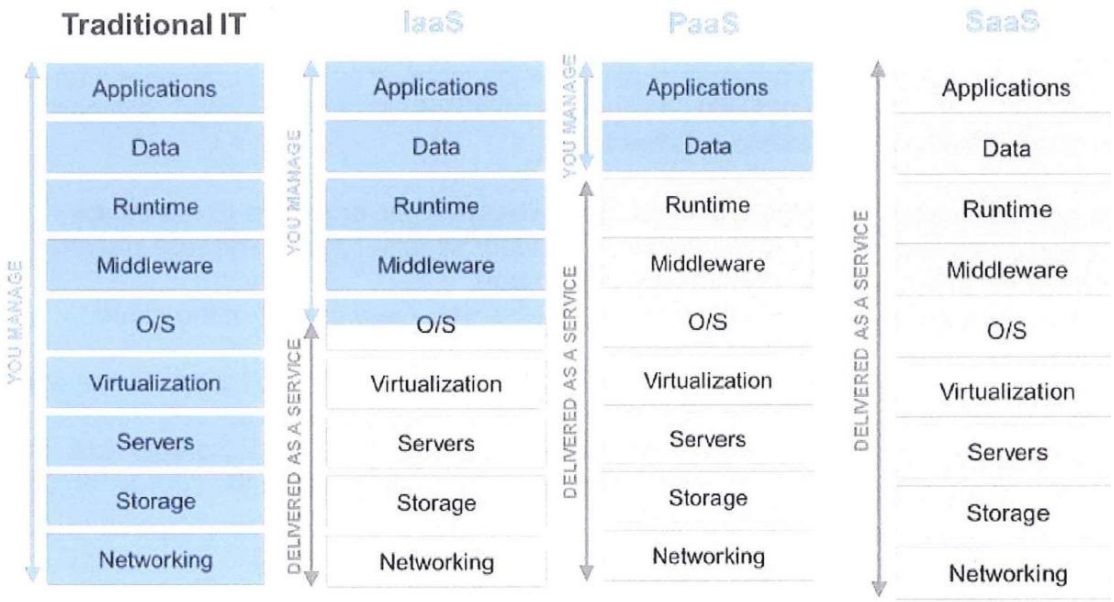
Επιπλέον, η σύνδεση μεταξύ των διαφόρων κλάδων της ψηφιακής εγκληματολογίας και του περιβάλλοντος της τεχνολογίας των πληροφοριών είναι ζωτικής σημασίας, καθώς ο τύπος της υποδομής καθορίζει πού αποθηκεύονται τα ψηφιακά αποδεικτικά στοιχεία, πώς είναι δυνατή η πρόσβαση σε αυτά και ποιες εγκληματολογικές προκλήσεις αντιμετωπίζουν οι ερευνητές/-τριες:

«Κλασική» ψηφιακή εγκληματολογία έναντι διαδικτυακής εγκληματολογίας

- Παραδοσιακές Τεχνολογίες Πληροφοριών→ Η εταιρεία διαχειρίζεται ολόκληρη την υποδομή πληροφορικής στις εγκαταστάσεις της. Οι διακομιστές, τα δίκτυα, η αποθήκευση, τα λειτουργικά συστήματα και το λογισμικό λειτουργούν φυσικά στις εγκαταστάσεις της εταιρείας. Περιλαμβάνει την κλασική ψηφιακή εγκληματολογία υπολογιστών, την εγκληματολογία δικτύων και την εγκληματολογία βάσεων δεδομένων που εφαρμόζεται σε φυσικές μηχανές, τοπικούς διακομιστές και εσωτερικά δίκτυα. Συνηθισμένες πηγές αποδεικτικών στοιχείων είναι οι σκληροί δίσκοι (HDD, SSD), οι τοπικές βάσεις δεδομένων και τα αρχεία καταγραφής του συστήματος. Απαιτείται φυσική πρόσβαση, αλλά ο πλήρης έλεγχος του υλικού μπορεί να απλουστεύσει τη δημιουργία εικόνων και την ανάλυση.
- IaaS (Infrastructure as a Service)→ (Υποδομή ως Υπηρεσία). Το IaaS παρέχει βασικούς πόρους πληροφορικής, όπως εικονικούς διακομιστές, αποθήκευση και δίκτυα μέσω του διαδικτύου. Οι εταιρείες ενοικιάζουν αυτήν την υποδομή από έναν πάροχο cloud. Οι σχετικοί κλάδοι εγκληματολογίας είναι η εγκληματολογία cloud και η εγκληματολογία δικτύων. Οι κύριες πηγές δεδομένων είναι οι εικονικές μηχανές, οι αποθηκευτικοί χώροι cloud και τα αρχεία καταγραφής της κίνησης δικτύου.

- PaaS (Platform as a Service) → (Πλατφόρμα ως Υπηρεσία). Το PaaS προσφέρει μια πλατφόρμα στην οποία οι προγραμματιστές/-στριες μπορούν να αναπτύσσουν, να δοκιμάζουν και να αναπτύσσουν εφαρμογές. Ο πάροχος διαχειρίζεται την υποκείμενη υποδομή και το middleware. Οι κυρίαρχοι κλάδοι είναι η εγκληματολογική ανάλυση βάσεων δεδομένων και η εγκληματολογική ανάλυση cloud. Οι πηγές δεδομένων είναι κυρίως αρχεία καταγραφής εφαρμογών, στιγμιότυπα βάσεων δεδομένων και αρχεία καταγραφής API.
- SaaS (Software as a Service) → (Λογισμικό ως Υπηρεσία). Το SaaS παρέχει πλήρως λειτουργικό λογισμικό μέσω του διαδικτύου. Οι χρήστες/-στριες έχουν πρόσβαση στο λογισμικό μέσω προγραμμάτων περιήγησης ιστού ή εφαρμογών χωρίς να χρειάζεται να ανησυχούν για την εγκατάσταση, τη διαχείριση ή τη συντήρηση. Δεν απαιτείται εγκατάσταση. Ενδεικτικό παράδειγμα είναι το Microsoft 365. Η εγκληματολογία cloud και δικτύων είναι οι κυρίαρχοι κλάδοι της εγκληματολογικής ανάλυσης σε αυτήν την περίπτωση. Σημαντικές πηγές δεδομένων περιλαμβάνουν αρχεία καταγραφής ελέγχου, ιστορικό εκδόσεων και αρχεία δραστηριότητας χρηστών/-στριών.

Το Σχήμα 11 παρουσιάζει μια επισκόπηση των διαφορετικών περιβαλλόντων τεχνολογίας πληροφοριών.



Σχήμα2 . Διαφορετικό περιβάλλον πληροφορικής[1]

Ακόμα και αν υπάρχουν ξεχωριστοί κλάδοι και πρέπει να ληφθεί υπόψη ο τύπος της υποδομής, η δομή μιας διαδικασίας ψηφιακής εγκληματολογίας παραμένει κατά κύριο λόγο η ίδια. Τα βήματα μπορούν εν συντομία να συνοψιστούν ως εξής: (1) απόκτηση ψηφιακών αποδεικτικών στοιχείων, (2) ανάλυσή τους συμπεριλαμβανομένης της ερμηνείας, και (3) παρουσίασή τους (π.χ. στους/στις επικεφαλής ερευνητές/-τριες της υπόθεσης, στο δικαστήριο) σύμφωνα με τους Dubey, Bhatt & Negi (2023). Ένα άλλο σημαντικό μοντέλο διαδικασίας είναι το μοντέλο διεπιστημονικής διαδικασίας ψηφιακής εγκληματολογικής έρευνας του Lutui (2016) που απεικονίζεται στο Σχήμα 12.

[1] Πηγή: Αστυνομία της Βαυαρίας. Απαγορεύεται η διανομή χωρίς άδεια.

Σχήμα3 . Επισκόπηση της διαδικασίας ψηφιακής εγκληματολογίας[2]

Επιπλέον, ένας άλλος οδηγός βήμα προς βήμα μπορεί να βοηθήσει τους/τις επαγγελματίες στη δομή της διαδικασίας ψηφιακής εγκληματολογίας, καθώς περιέχει μερικά περισσότερο πρακτικά στοιχεία από τα δύο μοντέλα διαδικασίας που παρουσιάστηκαν προηγουμένως:

Εννέα (9) πρακτικά στοιχεία της διαδικασίας ψηφιακής εγκληματολογίας

1. **Λήψη**: παραλαβή της συσκευής ως αποδεικτικού στοιχείου, παραλαβή αιτήματος για εξέταση.
2. **Ταυτοποίηση**: ταυτοποίηση των προδιαγραφών και των δυνατοτήτων της συσκευής, ταυτοποίηση των στόχων της εξέτασης, ταυτοποίηση της νομικής αρχής για την εξέταση.
3. **Προετοιμασία**: προετοιμασία των μεθόδων και των εργαλείων που θα χρησιμοποιηθούν, προετοιμασία των μέσων και του σταθμού εργασίας εγκληματολογικής έρευνας για την εξέταση.
4. **Απομόνωση**: προστασία των αποδεικτικών στοιχείων, αποτροπή απομακρυσμένης καταστροφής δεδομένων, απομόνωση από το δίκτυο, το Bluetooth και το Wi-Fi.
5. **Επεξεργασία**: διεξαγωγή εγκληματολογικής απόκτησης, εκτέλεση εγκληματολογικής ανάλυσης, σάρωση για κακόβουλο λογισμικό.

[2] Πηγή: Πρωτότυπη απεικόνιση του Lutui (2016), σ. 601

6. **Επαλήθευση**: επικύρωση της απόκτησης, επικύρωση των εγκληματολογικών ευρημάτων.
7. **Τεκμηρίωση/Αναφορά**: τήρηση σημειώσεων σχετικά με τα ευρήματα και τη διαδικασία, σύνταξη και ολοκλήρωση εγκληματολογικών αναφορών.
8. **Παρουσίαση**: προετοιμασία των εκθεμάτων, παρουσίαση των ευρημάτων.
9. **Αρχειοθέτηση**: διατήρηση ενός αντιγράφου των δεδομένων σε ασφαλές μέρος, τήρηση των δεδομένων σε κοινές μορφές για μελλοντική χρήση.

Εξίσου σημαντικό για τον/την ψηφιακό/-κή εγκληματολόγο/επαγγελματία είναι να έχει κατά νου ολόκληρη τη διαδικασία μιας εγκληματολογικής έρευνας:

Διαδικασία εγκληματολογικής έρευνας

1. Παράδοση των κατασχεθέντων αποδεικτικών στοιχείων στον/στην ψηφιακό/-κή εγκληματολόγο.
2. Διατήρηση (αποθήκευση αρχείων) δεδομένων και φορέων δεδομένων (κατάλογος, αυτοκόλλητα κ.λπ.).
3. Δημιουργία αντιγράφων ασφαλείας δεδομένων: αντίγραφα ασφαλείας φυσικών εικόνων, αντίγραφα ασφαλείας λογικών δεδομένων.
4. Ασφαλής αποθήκευση των αρχικών αποδεικτικών στοιχείων.
5. Τεκμηρίωση της αλυσίδας επιτήρησης.

Επιπλέον, θα πρέπει πάντα να εφαρμόζονται ορισμένες βασικές αρχές της ψηφιακής εγκληματολογίας:

Βασικές αρχές της ψηφιακής εγκληματολογίας

- Δημιουργία αντιγράφων ασφαλείας δεδομένων. Υπάρχουν διαφορετικοί τύποι που πρέπει να διακρίνονται:
    - αντίγραφα ένα προς ένα των ηλεκτρονικών αποδεικτικών στοιχείων·
    - φυσικά αντίγραφα ασφαλείας εικόνων (E01 [μορφή αρχείου εικόνας encase] ή RAW)·
    - λογικά αντίγραφα ασφαλείας δεδομένων (L01, AD1 ή CTR).
- Εξέταση των αντιγράφων ασφαλείας ή των αντιγράφων των δεδομένων (ανάλυση post mortem).
- Καμία αλλαγή στα ασφαλισμένα δεδομένα.
- Ακριβής τεκμηρίωση του ποιος/ποια έκανε τι και πότε με τα αντίγραφα ασφαλείας των δεδομένων, ώστε να διασφαλίζεται η τήρηση της αλυσίδας επιτήρησης. Το τελευταίο απαιτεί (1) χρονολογική τεκμηρίωση και (2) ιχνηλασιμότητα για την εξασφάλιση της μεταφοράς, της αξιολόγησης και της υποβολής των αποδεικτικών στοιχείων. Ακολουθεί την αρχή ότι εφαρμόζονται (επιστημονικά) αναγνωρισμένες μέθοδοι και ότι ο/η ειδικός ψηφιακής εγκληματολογίας προετοιμάζει πλήρη τεκμηρίωση.
- Δημιουργία αντιγράφων των αποδεικτικών στοιχείων του υπολογιστή σε αναλογία 1:1 λαμβάνοντας υπόψη:
    - τη διασφάλιση της ακεραιότητας και της αυθεντικότητας των αποδεικτικών στοιχείων·
    - την ενσωμάτωση προστασίας εγγραφής·

- την επαλήθευση.

- Μην αλλάζετε κάτι σκόπιμα! Οι αλλαγές γίνονται γρήγορα, π.χ. μέσω της εκκίνησης ενός συστήματος ή της τοποθέτησης ενός σκληρού δίσκου.
- **Προσέξτε το εξής:** Κάντε τα πάντα ανιχνεύσιμα πάντα και παντού (τεκμηρίωση).

Είναι σημαντικό να γνωρίζετε τις νομικές πτυχές, καθώς πρέπει να διασφαλίζεται η νομιμότητα της έρευνας και της κατάσχεσης. Ως εγκληματολόγος, γενικά δεν χρειάζεται να ανησυχείτε για απαγορεύσεις χρήσης (αποτελούν καθήκον του/της ανακριτή/-τριας και, εν τέλει, του/της εισαγγελέα). Τέλος, είναι σκόπιμο να συμβουλευτείτε τους/τις ανακριτές/-τριες σε περίπτωση τυχαίων ευρημάτων.

9.4.3 Δημιουργία αντιγράφων ασφαλείας δεδομένων

Στην ψηφιακή εγκληματολογία, η δημιουργία αντιγράφων ασφαλείας δεδομένων είναι ένα θεμελιώδες βήμα για τη διατήρηση και την ανάλυση ψηφιακών αποδεικτικών στοιχείων. Η διασφάλιση της ακεραιότητας και της διαθεσιμότητας των εγκληματολογικών δεδομένων είναι κρίσιμη για τις έρευνες, τις νομικές διαδικασίες και την αντιμετώπιση περιστατικών κυβερνοασφάλειας. Μια σωστή εγκληματολογική δημιουργία αντιγράφων ασφαλείας δίνει τη δυνατότητα στους/στις ανακριτές να εργάζονται με ένα ακριβές, αναλλοίωτο αντίγραφο των αρχικών δεδομένων, γεγονός που ελαχιστοποιεί τον κίνδυνο μόλυνσης ή απώλειας αποδεικτικών στοιχείων.

Αυτή η ενότητα εξετάζει τις βασικές πτυχές της δημιουργίας αντιγράφων ασφαλείας εγκληματολογικών δεδομένων ξεκινώντας από τις βασικές αρχές της (Ενότητα 9.6.3.1), συμπεριλαμβανομένης της ακεραιότητας, της αυθεντικότητας και

της αλυσίδας επιτήρησης των δεδομένων. Στη συνέχεια, παρέχει μια επισκόπηση των κοινών μορφών δημιουργίας αντιγράφων ασφαλείας εγκληματολογικών δεδομένων και της δομής τους (Ενότητα 9.6.3.2), ακολουθούμενη από μια εξέταση των μηχανισμών προστασίας εγγραφής που βασίζονται σε λογισμικό για την αποτροπή της παραποίησης δεδομένων (Ενότητα 9.6.3.3). Εξετάζονται συν τοις άλλοις οι διαφορετικοί τύποι φορέων δεδομένων και ο ρόλος τους στις εγκληματολογικές έρευνες (Ενότητα 9.6.3.4), παράλληλα με μια ανάλυση εξειδικευμένων λύσεων λογισμικού και υλικού για την εγκληματολογική δημιουργία αντιγράφων ασφαλείας (Ενότητα 9.6.3.5). Επιπλέον, η ενότητα καλύπτει τη δημιουργία και την εφαρμογή εγκληματολογικών μέσων εκκίνησης (Ενότητα 9.6.3.6), τα οποία διευκολύνουν τη συλλογή δεδομένων από online και offline συστήματα. Εξετάζονται επίσης μέθοδοι εγκληματολογικής δημιουργίας αντιγράφων ασφαλείας με βάση τα δίκτυα συμπεριλαμβανομένων τεχνικών απομακρυσμένης απόκτησης (Ενότητα 9.6.3.7). Τέλος, συζητούνται ειδικές παράμετροι για τη διαχείριση σύνθετων συστημάτων αποθήκευσης, όπως συστοιχίες RAID και συσκευές NAS (Ενότητα 9.6.3.8) επισημαίνοντας εν συντομία τις προκλήσεις και τις βέλτιστες πρακτικές για τη διατήρηση τέτοιων δομών δεδομένων.

Με την κατανόηση αυτών των εννοιών, ειδικοί και επαγγελματίες της εγκληματολογίας μπορούν να διασφαλίσουν αξιόπιστα, επαληθεύσιμα και αποδεκτά από τα δικαστήρια αντίγραφα ασφαλείας δεδομένων, τα οποία αποτελούν τη βάση μιας ορθής εγκληματολογικής έρευνας.

9.4.3.1 Αρχές της εγκληματολογικής δημιουργίας αντιγράφων ασφαλείας δεδομένων

Υπάρχουν ορισμένες θεμελιώδεις αρχές που πρέπει να ακολουθούνται όσον αφορά τα αντίγραφα ασφαλείας δεδομένων:

- **Δημιουργία εγκληματολογικών αντιγράφων και αποκλεισμός εγγραφής**:
    - Αποκλειστική εργασία σε εγκληματολογικά αντίγραφα, όχι στα αρχικά μέσα.
    - Δημιουργία εγκληματολογικών αντιγράφων ως εικόνων bitstream ή λογικών αντιγράφων ασφαλείας.
    - Αποτροπή αλλαγών στα αρχικά δεδομένα ή μέσα κατά τη δημιουργία αντιγράφων ασφαλείας, την έρευνα και την εξέταση.
    - Πρόσβαση μόνο για ανάγνωση κατά τη διαδικασία δημιουργίας αντιγράφων ασφαλείας (προστασία εγγραφής).
- **Διασφάλιση της ακεραιότητας των αντιγράφων ασφαλείας**:
    - Διασφάλιση ότι τα αντίγραφα ασφαλείας των δεδομένων παραμένουν κατάλληλα για ανάλυση.
    - Καμία αλλαγή στα δεδομένα που έχουν δημιουργηθεί αντίγραφα ασφαλείας (δεύτερο αντίγραφο μόνο εάν είναι απαραίτητο).
    - Χρήση διαγραμμένων μέσων δημιουργίας αντιγράφων ασφαλείας (κίνδυνος διασταυρούμενης μόλυνσης).

- Επαλήθευση των αντιγράφων ασφαλείας εικόνων (σύγκριση κατακερματισμού μεταξύ του πρωτότυπου και του αντιγράφου μετά τη διαδικασία δημιουργίας αντιγράφων ασφαλείας ή τις διαδικασίες αντιγραφής).

- **Τεκμηρίωση της αλυσίδας επιτήρησης**: Ακριβής τεκμηρίωση όλων των αλληλεπιδράσεων με τα αντίγραφα ασφαλείας των δεδομένων (διατήρηση της «αλυσίδας επιτήρησης»)

9.4.3.2 Επισκόπηση και δομή των κοινών μορφών αντιγράφων ασφαλείας για εγκληματολογικές έρευνες

Το πεδίο εφαρμογής των αντιγράφων ασφαλείας δεδομένων στην ψηφιακή εγκληματολογία περιλαμβάνει μαγνητικούς και SSD σκληρούς δίσκους από υπολογιστές, μεμονωμένες συσκευές αποθήκευσης όπως μονάδες USB ή μνήμες flash και οπτικά μέσα. Αυτά μπορούν να ασφαλιστούν χρησιμοποιώντας δύο βασικές μεθόδους: **αντίγραφα ασφαλείας εικόνας**, τα οποία δημιουργούν ολοκληρωμένα αντίγραφα τομέα προς τομέα, ή **λογικά αντίγραφα ασφαλείας**, τα οποία εστιάζουν σε συγκεκριμένα αρχεία και καταλόγους. Και οι δύο μέθοδοι υποστηρίζονται από εγκληματολογικά εργαλεία όπως τα X-Ways, EnCase, FTK, NUIX Imager και Magnet Acquire.

Η δημιουργία αντιγράφων ασφαλείας **δεδομένων εικόνας** είναι ένα αντίγραφο bit-for-bit μιας συσκευής αποθήκευσης, που καταγράφει όλα τα δεδομένα, συμπεριλαμβανομένων αρχείων, φακέλων και μη κατανεμημένων, ελεύθερων και απελευθερωμένων χώρων αποθήκευσης.

Η εικόνα διαφέρει από έναν κλώνο, καθώς η δημιουργία αντιγράφων ασφαλείας δεδομένων εικόνας δημιουργεί ένα συμπιεσμένο αρχείο (εικόνα) ενός δίσκου, διαμερίσματος ή συστήματος. Το αντίγραφο ασφαλείας εικόνας που αποθηκεύει δεδομένα σε ένα μεγάλο αρχείο πρέπει να αποκατασταθεί προτού μπορέσει να χρησιμοποιηθεί. Στην ψηφιακή εγκληματολογία, λαμβάνονται εγκληματολογικές εικόνες, για παράδειγμα, από τον σκληρό δίσκο ενός υπόπτου. Η δημιουργία εικόνας χρησιμοποιείται συνήθως για εκ των υστέρων ανάλυση, ενώ η **κλωνοποίηση** χρησιμοποιείται για την αντιγραφή συστημάτων ή τη δημιουργία πανομοιότυπων ρυθμίσεων (π.χ. κλωνοποίηση ενός παλιού σκληρού δίσκου σε SSD χωρίς επανεγκατάσταση του λειτουργικού συστήματος). Μερικές φορές μπορεί να εξυπηρετήσει και εγκληματολογικές ανάγκες. Ο κλωνοποιημένος δίσκος μπορεί να φορτωθεί και να χρησιμοποιηθεί αμέσως. Για παράδειγμα, στην ψηφιακή εγκληματολογία, θα μπορούσε κανείς να δημιουργήσει ένα ακριβές αντίγραφο bitstream του δίσκου ενός υπόπτου.

Υπάρχουν διάφορες **μορφές εικόνων** που χρησιμοποιούνται συνήθως **στην εγκληματολογία**:

- **Μορφή RAW:** Άμεσο αντίγραφο bitstream του μέσου αποθήκευσης. Ανάλογα με το λογισμικό δημιουργίας αντιγράφων ασφαλείας, δημιουργούνται κατακερματισμοί MD5 της πλήρους εικόνας ή μεμονωμένων τμημάτων της εικόνας.
- **Expert-Witness Format (EWF) (E01)**: Αμετάβλητη μορφή σχεδιασμένη για εγκληματολογική χρήση. Η κεφαλίδα EVF περιλαμβάνει μεταδεδομένα όπως τον αριθμό των μπλοκ και τα μεγέθη των τομέων. Ενσωματώνει κυκλικούς

ελέγχους πλεονασμού (CRC) για την επαλήθευση μεμονωμένων μπλοκ. Τμηματοποιημένη δομή με κεφαλίδες, δεδομένα και πίνακες τομέων.

- **Μορφή αρχείου αποδεικτικών στοιχείων EnCase (Ex01):** Αναπτύχθηκε από την Guidance/OpenText και βασίζεται στη μορφή E01. Πιο αποτελεσματική και αποδοτική σε σύγκριση με την E01 και υποστηρίζεται κυρίως από τα EnCase και NUIX.
- **Advanced Forensic Format (AFF):** Μορφή ανοιχτού κώδικα, ανεξάρτητη από τον κατασκευαστή, που συντηρείται από μια διαδικτυακή κοινότητα. Υποστηρίζει τις παραλλαγές AFF4 και AFF4-L. Λιγότερο συχνή χρήση στη Γερμανία. Συμβατή με εργαλεία όπως το FTK Imager και το Magnet Forensics AXIOM.

Η εγκληματολογική έρευνα περιλαμβάνει μεταξύ άλλων **λογικά αντίγραφα ασφαλείας**. Ένα λογικό αντίγραφο ασφαλείας είναι ένα αντίγραφο των πραγματικών δεδομένων σε μια συσκευή αποθήκευσης ή ένα διαμέρισμα, το οποίο καταγράφει μόνο τα αρχεία και τους φακέλους που υπάρχουν εκείνη τη στιγμή, και όχι τις μη εκχωρημένες περιοχές ή τα διαγραμμένα δεδομένα. Τα λογικά αντίγραφα ασφαλείας δημιουργούνται συνήθως επιτόπου ή κατά τη διάρκεια ερευνών της εταιρείας και από συστήματα NAS.

9.4.3.3Προστασία εγγραφής λογισμικού

Η προστασία εγγραφής λογισμικού αναφέρεται σε εργαλεία που αποτρέπουν την τροποποίηση των δεδομένων που είναι αποθηκευμένα σε έναν φορέα δεδομένω επιβάλλοντας πρόσβαση μόνο για ανάγνωση. Υπάρχουν διάφορα λογισμικά που διασφαλίζουν ότι κανένα δεδομένο δεν θα τροποποιηθεί ή θα διαγραφεί κατά λάθος κατά τη διάρκεια εγκληματολογικών ερευνών.

- **X-Ways forensics:** Προστατεύει ολόκληρους δίσκους ή συγκεκριμένα διαμερίσματα. Είναι αποτελεσματικό μόνο αφού τα Windows έχουν αναγνωρίσει και έχουν αποκτήσει πρόσβαση στο δίσκο.
- **Diskpart:** Χρησιμοποιείται για τη ρύθμιση ή την κατάργηση της προστασίας εγγραφής σε δίσκους ή τόμους. Είναι αποτελεσματικό μόνο αφού η συσκευή αναγνωριστεί από τα Windows.
- **FastBloc SE:** Λύση λογισμικού αποκλεισμού εγγραφής που επιτρέπει τη δημιουργία εγκληματολογικών εικόνων σε κανάλια IDE, SATA, SCSI, FireWire και USB χωρίς αποκλειστές εγγραφής υλικού (hardware write-blockers).
- **Προστασία βάσει μητρώου:** Ενεργοποιεί την προστασία εγγραφής για συσκευές αποθήκευσης τροποποιώντας τις ρυθμίσεις του συστήματος προκειμένου να περιορίσει την πρόσβαση εγγραφής.
- **Θύρες USB:** Προστασία εγγραφής μέσω diskpart (μη αξιόπιστη) ή τροποποιήσεις μητρώου: προστασία σε συσκευή USB.

9.4.3.4Φορείς δεδομένων

Οι **μαγνητικοί φορείς δεδομένων**, όπως οι σκληροί δίσκοι, αποθηκεύουν τα δεδομένα μαγνητικά σε περιστρεφόμενους δίσκους που χωρίζονται σε τομείς. Αυτοί οι τομείς έχουν συνήθως φυσικό μέγεθος 512 byte ή 4096 byte στους σύγχρονους δίσκους και τα δεδομένα διαβάζονται μηχανικά χρησιμοποιώντας μια κεφαλή ανάγνωσης/εγγραφής.

Οι **φορείς δεδομένων flash**, όπως οι SSD και οι μονάδες USB, αποθηκεύουν τα δεδομένα ηλεκτρονικά σε κελιά μνήμης οργανωμένα σε σελίδες και μπλοκ. Σε

αντίθεση με τους μαγνητικούς δίσκους, δεν έχουν κινούμενα μέρη. Η μνήμη flash χρησιμοποιεί ελεγκτές για να προσομοιάζει την παραδοσιακή δομή βάσει τομέων για συμβατότητα με τα υπάρχοντα συστήματα. Είναι ανθεκτική στους κραδασμούς, συμπαγής σε μέγεθος, προσφέρει υψηλή χωρητικότητα αποθήκευσης και καταναλώνει λιγότερη ενέργεια. Ωστόσο, έχει και κάποια μειονεκτήματα. Ένα σημαντικό μειονέκτημα είναι η περιορισμένη διάρκεια ζωής της. Υπάρχουν κυρίως δύο τύποι μνήμης flash: NAND και NOR. Η μνήμη flash NAND είναι πιο οικονομική και προσφέρει υψηλότερες χωρητικότητες αποθήκευσης. Λειτουργεί παρόμοια με μια συσκευή μπλοκ, όπως ένας σκληρός δίσκος, και περιέχει ένα σύστημα αρχείων που μπορεί να χωριστεί σε διαμερίσματα.

Οι μονάδες SSD (Solid-State Drives) χρησιμοποιούν μνήμη flash NAND και έχουν σχεδιαστεί με σκοπό να αντικαταστήσουν τους παραδοσιακούς σκληρούς δίσκους. Παρέχουν σημαντικές βελτιώσεις στην απόδοση, όπως μεγαλύτερες ταχύτητες ανάγνωσης και εγγραφής δεδομένων. Μια υβριδική λύση αποθήκευσης, γνωστή ως Hybrid Solid State Drives (SSHD), συνδυάζει έναν παραδοσιακό μαγνητικό σκληρό δίσκο με επιπλέον μνήμη flash. Τα δεδομένα που χρησιμοποιούνται συχνά αποθηκεύονται στη μνήμη flash, η οποία επιταχύνει τη συνολική απόδοση του συστήματος, αποθηκεύοντας τα δεδομένα στην προσωρινή μνήμη για ταχύτερη ανάκτηση.

9.4.3.5Λογισμικό και υλικό για εγκληματολογική δημιουργία αντιγράφων ασφαλείας

Η δημιουργία αντιγράφων ασφαλείας εγκληματολογικών δεδομένων περιλαμβάνει ένα συνδυασμό εξειδικευμένων εργαλείων **λογισμικού** και **υλικού**. Μεταξύ των πιο κοινών εργαλείων λογισμικού είναι τα εξής προγράμματα δημιουργίας εικόνων:

- **FTK Imager:** Φορητές και εγκαθιστώμενες εκδόσεις. Υποστηρίζει προεπισκόπηση τοπικών δίσκων, κοινόχρηστων δικτυακών πόρων και εικόνων. Δημιουργεί εικόνες bitstream σε μορφή RAW, E01 και SMART. Επιτρέπει την κατακερματισμένη αποθήκευση, την εξαγωγή αρχείων, τη διαίρεση, τη συγχώνευση εικόνων και τη λογική δημιουργία αντιγράφων ασφαλείας (μορφή AD1). Συμβατότητα μεταξύ πλατφορμών (Windows, Linux, macOS).
- **EnCase Imager:** Ιδιόκτητο εργαλείο δημιουργίας εικόνων με προηγμένες λειτουργίες.
- **Magnet Acquire:** Απλό εργαλείο για δημιουργία εικόνων σε κινητά τηλέφωνα και επιτραπέζιους υπολογιστές.
- **NUIX Imager:** Ασφαλής δημιουργία εικόνων για φυσικούς δίσκους και περιβάλλοντα cloud. Υποστηρίζει μοναδικές λογικές μορφές (*.nli) με επαλήθευση μεταδεδομένων και κατακερματισμού.

Επιπρόσθετα, οι ολοκληρωμένες σουίτες εγκληματολογικής ανάλυσης παρέχουν ένα ευρύτερο σύνολο εργαλείων για ψηφιακή εγκληματολογική ανάλυση, όπως:

- **X-Ways forensics:** Υποστηρίζει τη δημιουργία εικόνων φυσικών και λογικών δίσκων. Προσφέρει διάφορες λειτουργίες δημιουργίας εικόνων (πλήρης, ελάχιστη, καθαρή). Επιτρέπει τη δημιουργία αρχείων-δοχείων, τη μετατροπή μορφών και τη σποραδική συμπίεση.
- **EnCase forensics:** Ολοκληρωμένη σουίτα για δημιουργία εικόνων και ανάλυση.
- **Magnet forensics IEF/AXIOM:** Εστιάζει στην ανάλυση και την απεικόνιση ψηφιακών αποδεικτικών στοιχείων.

Για μια συγκεκριμένη επισκόπηση των εργαλείων ψηφιακής εγκληματολογίας που σχετίζονται με την εμπορία ανθρώπων, ανατρέξτε στην ενότητα 9.6.4.3. Η απόκτηση εγκληματολογικών δεδομένων απαιτεί επίσης συγκεκριμένα εργαλεία υλικού:

- Οι **αντιγραφείς δίσκων με μπλοκάρισμα εγγραφής** χρησιμοποιούνται για τη δημιουργία ακριβών αντιγράφων των μέσων αποθήκευσης, bit προς bit, αποτρέποντας ταυτόχρονα οποιαδήποτε αλλαγή στα αρχικά μέσα. Χαρακτηριστικά παραδείγματα είναι τα Logicube και VOOM Hardcopy. Επίσης, οι φορητές συσκευές εγκληματολογικής ανάλυσης είναι λύσεις που έχουν σχεδιαστεί για γρήγορη δημιουργία εικόνων σε επιτόπιες επιχειρήσεις και χρησιμοποιούνται συχνά με φορητούς υπολογιστές ή εξωτερικούς δίσκους.
- **Πρόσθετα χαρακτηριστικά και εργαλεία** περιλαμβάνουν την ασφαλή αντιγραφή εικόνων με τη βοήθεια εργαλείων όπως το NUIX Evidence Mover και την επαλήθευση της τιμής κατακερματισμού με τη χρήση λογισμικού όπως το HashMyFiles, το HashCalc και το MD5.exe. Αυτά τα εργαλεία ενσωματώνονται απρόσκοπτα σε λογισμικό εγκληματολογικής ανάλυσης, όπως το EnCase και το X-Ways, για να διασφαλίσουν την ακεραιότητα των αρχείων εικόνας E01.

Για την αφαίρεση δίσκων από συμπαγή συστήματα, πόροι όπως το iFixit, τα σεμινάρια του YouTube και οι επίσημες πύλες (π.χ. TeSIT) παρέχουν πολύτιμες οδηγίες. Σε περιπτώσεις στις οποίες δεν είναι εφικτή η φυσική πρόσβαση στους δίσκους, συνιστάται η χρήση μέσων εκκίνησης για τη διευκόλυνση της απόκτησης δεδομένων.

9.4.3.6 Δημιουργία και χρήση μέσων εκκίνησης εγκληματολογικής έρευνας

Τα εγκληματολογικά μέσα εκκίνησης είναι ένα απαραίτητο εργαλείο στην ψηφιακή εγκληματολογία, ιδιαίτερα όταν δεν είναι δυνατή η αφαίρεση ή η άμεση πρόσβαση σε μια συσκευή αποθήκευσης από έναν υπολογιστή ή όταν δεν είναι διαθέσιμο ένα πρόγραμμα αποκλεισμού εγγραφής.

Υπάρχουν δύο **κύριοι τύποι συστημάτων** που χρησιμοποιούνται για την εκκίνηση:

- Basic Input Output System (BIOS): Παραδοσιακή διεπαφή μεταξύ του υλικού του υπολογιστή και του λειτουργικού συστήματος. Υποστηρίζει εκκίνηση έως και τεσσάρων λειτουργικών συστημάτων σε έναν δίσκο. Ενεργοποιείται αμέσως μετά την ενεργοποίηση του υπολογιστή. Είναι σχεδιασμένο για φορείς δεδομένων που βασίζονται σε MBR.
- Extensible Firmware Interface (EFI): Διάδοχος του BIOS, με υποστήριξη για έως και 128 λειτουργικά συστήματα σε έναν μόνο δίσκο. Οι παραλλαγές περιλαμβάνουν: **UEFI** (Unified Extensible Firmware Interface) για Windows/Linux και **EFI** για macOS. Είναι απαραίτητο για δίσκους που βασίζονται σε GPT. Χρησιμοποιείται για την εκκίνηση του λειτουργικού συστήματος σε φορείς δεδομένων GPT. Υποστηρίζεται από όλα τα τρέχοντα λειτουργικά συστήματα. Προσφέρει βελτιωμένη ασφάλεια και λειτουργικότητα:
    - Μονάδα Υποστήριξης Συμβατότητας (Compatibility Support Module-CSM): Προσομοιώνει ένα BIOS για το υλικό και το λειτουργικό σύστημα. Λειτουργία συμβατότητας/λειτουργία παλαιού τύπου.

- Ασφαλής Εκκίνηση (Secure Boot): Αποτρέπει τη φόρτωση κακόβουλου λογισμικού πριν από την εκκίνηση του συστήματος.
- Αξιόπιστη Εκκίνηση (Trusted Boot): Επισημαίνει αρχεία πυρήνα/συστήματος από τα Windows 10 για τον αποκλεισμό κακόβουλου κώδικα και κακόβουλου λογισμικού.

- Ακολουθία εκκίνησης
  - BIOS: Ελέγχει διαδοχικά τις καθορισμένες μονάδες δίσκου για εκκινήσιμα λειτουργικά συστήματα και μεταφέρει τη διαδικασία εκκίνησης.
  - UEFI: Περιλαμβάνει ενσωματωμένο διαχειριστή εκκίνησης που επιτρέπει την άμεση επιλογή μονάδας δίσκου.

Μέσα εκκίνησης Linux

Τα μέσα εκκίνησης Linux είναι εξοπλισμένα με ένα ευρύ φάσμα δωρεάν εργαλείων εγκληματολογικής ανάλυσης για εργασίες όπως δημιουργία αντιγράφων ασφαλείας, ανάλυση και ανάκτηση δεδομένων. Μερικά παραδείγματα αυτών των εργαλείων περιλαμβάνουν: **Δημιουργία αντιγράφων ασφαλείας** (`Guymager`, `dcfldd`, `ddrescue`), **Ανάλυση** (`Sleuthkit`, `Autopsy`) και **Ανάκτηση** (`Foremost`, `TestDisk`).

Δημοφιλείς διανομές Linux είναι οι Knoppix, Helox, CAINE (Computer Aided INvestigative Environment), DeepThought, DEFT¸ Grml και Kali Linux.

Δημιουργία μέσων εκκίνησης Linux: Τα συστήματα Linux αποθηκεύονται σε κοντέινερ Casper με μορφοποίηση FAT32, ενώ τα αρχεία που δημιουργούνται από τον/τη χρήστη/-στρια αποθηκεύονται εξωτερικά. Τα μέσα εκκίνησης μπορούν να δημιουργηθούν χρησιμοποιώντας εργαλεία όπως **YUMI, Rufus** ή **Linux Live USB-**

Creator. Συσκευές όπως **Zalman** ή **IODD** μπορούν να χρησιμεύσουν ως υλικό δημιουργίας αντιγράφων ασφαλείας/εκκίνησης.

Δημιουργία εφεδρικού αντιγράφου εικόνας: Συνήθως χρησιμοποιούνται **εικόνες RAW**. Το «dd» είναι συνήθως διαθέσιμο σε κάθε σύστημα Linux. Σύνταξη: dd if=/dev/sdX of=/media/image.dd. Διαχωρισμός μεγάλων εικόνων. Παρακολούθηση προόδου με ενημερωμένες εκδόσεις `dd` ή βοηθητικά προγράμματα όπως `to Pipe Viewer (pv)`. Επαλήθευση με χρήση αλγορίθμων κατακερματισμού (`md5sum` ή παρόμοια). Συγχώνευση τμημάτων εικόνας μετά τον διαχωρισμό.

Εναλλακτικά προγράμματα δημιουργίας αντιγράφων ασφαλείας για Linux είναι τα Guymager, dcfldd, dc3dd και ddrescue. Ένα λογικό αντίγραφο ασφαλείας ημερομηνίας δημιουργείται χρησιμοποιώντας το tar (Tape Archiver), το οποίο είναι πλέον ενσωματωμένο στα Windows.

Μέσα εκκίνησης των Windows

Τα μέσα εκκίνησης των Windows παρέχουν εναλλακτική ή συμπληρωματική λειτουργικότητα στα μέσα εκκίνησης των Linux.

- Windows Preinstallation Environment (WinPE): Ένα μινιμαλιστικό, αυτόνομο λειτουργικό σύστημα (OS) ανεξάρτητο από το σύστημα που είναι εγκατεστημένο στη συσκευή. Επιτρέπει την ανάλυση και τη δημιουργία εικόνων του συστήματος χωρίς να επηρεάζει τα δεδομένα του εγκατεστημένου λειτουργικού συστήματος.
- Windows Forensic Environment (WinFE): Πρόκειται για προσαρμοσμένο WinPE που έχει διαμορφωθεί ειδικά για εγκληματολογική χρήση. Μερικές από τις εφαρμογές του είναι οι εξής:

- Δημιουργία αντιγράφων ασφαλείας εγκληματολογικών δεδομένων με χρήση X-Ways Forensics ή FTK Imager·
- Διαλογή και προεπισκόπηση αποδεικτικών στοιχείων·
- Παράκαμψη των δικαιωμάτων διαχειριστή/-στριας στα συστήματα-στόχους.

- Windows Image Format (WIM): Αποθηκεύει βασικές εικόνες συστήματος Windows (π.χ. Pro, Home, Education). Χρησιμοποιείται για την εκκίνηση του Windows PE («boot.wim»). Για την εγκατάσταση, ξεκινά το WinPE και το «install.wim» εγγράφεται στον σκληρό δίσκο. Είναι συμβατό με εργαλεία όπως το `7zip` για έλεγχο εικόνων. Μπορεί επίσης να παραδοθεί σε συμπιεσμένη μορφή ESD (Electronic Software Distribution).

Προηγμένες επιλογές μέσων εκκίνησης

- Ventoy: Εργαλείο που βασίζεται σε λογισμικό για εκκίνηση εικόνων ISO απευθείας από μονάδα USB. Οι λειτουργίες του περιλαμβάνουν συμβατότητα Secure Boot και υποστήριξη διαμερισμάτων GPT. Δημιουργεί δύο διαμερίσματα (FAT για το boot manager και exFAT για αποθήκευση ISO).
- Μέσα εκκίνησης Macintosh:
  - **Target Disk Mode (TDM):** Επιτρέπει στους υπολογιστές Mac να λειτουργούν ως εξωτερικές μονάδες δίσκου μέσω Thunderbolt ή FireWire.
  - **Λειτουργία Ανάκτησης:** Παρέχει πρόσβαση σε εργαλεία όπως το Disk Utility και το Terminal για τη δημιουργία εικόνων.

- **Αποκρυπτογράφηση FileVault:** Απαιτεί κωδικούς πρόσβασης ή κλειδιά ανάκτησης για πρόσβαση.
- **Σημειώσεις για το Τσιπ Ασφαλείας T2:** Περιορίζει την εξωτερική εκκίνηση και απαιτεί διαπιστευτήρια συγκεκριμένης συσκευής για τη δημιουργία εικόνων.

- Μέσα πολλαπλής εκκίνησης: Εργαλεία, όπως το YUMI, δημιουργούν εκκινήσιμα USB με πολλαπλές επιλογές λειτουργικού συστήματος (Linux, Windows, macOS). Εξασφαλίστε συμβατότητα με διάφορα συστήματα (BIOS/UEFI, macOS System Integrity Protection).

Ειδικές παράμετροι για macOS

- **FileVault και Τσιπ Ασφαλείας T2:** Η κρυπτογράφηση απαιτεί γνωστά διαπιστευτήρια. Το τσιπ T2 ενσωματώνει Secure Boot και περιορισμούς εξωτερικής εκκίνησης.
- **Fusion Drives:** Υβριδικό HDD και SSD, που απαιτεί ξεχωριστή δημιουργία εικόνας για κάθε στοιχείο και ανασύνθεση.

9.4.3.7 Δημιουργία αντιγράφων ασφαλείας δεδομένων μέσω δικτύου

Τα αντίγραφα ασφαλείας δεδομένων μέσω δικτύου παρέχουν μια αποτελεσματική μέθοδο για τη δημιουργία εικόνων και τη μεταφορά δεδομένων μεταξύ συστημάτων.

Τα **EnCase και LinEn** παρέχουν ένα ισχυρό πλαίσιο για δημιουργίες αντιγράφων ασφαλείας μέσω δικτύου επιτρέποντας στους/στις ερευνητές/-τριες να έχουν πρόσβαση και να δημιουργούν εικόνες απομακρυσμένων συστημάτων με ασφάλεια.

- **Διαδικασία:**
    - Εκκινήστε τον υπολογιστή-στόχο χρησιμοποιώντας μια διανομή Linux για εγκληματολογικές έρευνες, όπως το Deft.
    - Στον εφεδρικό υπολογιστή, εκκινήστε το EnCase Imager.
    - Δημιουργήστε μια φυσική σύνδεση μεταξύ των δύο υπολογιστών χρησιμοποιώντας ένα καλώδιο crossover.
    - Αναθέστε στατικές διευθύνσεις IP και στα δύο συστήματα: **Windows**: Διαμορφώστε μέσω του «Κέντρου Δικτύου και Κοινής Χρήσης» στην ενότητα «Ρυθμίσεις Προσαρμογέα». **Linux**: Χρησιμοποιήστε εντολές συστήματος για να ορίσετε την IP.
    - Επαληθεύστε τη σύνδεση εκτελώντας μια δοκιμή ping.
    - Αντιγράψτε το πρόγραμμα LinEn σε μια εξωτερική συσκευή αποθήκευσης και συνδέστε τη στο σύστημα-στόχο.
    - Μεταβείτε στη θέση του LinEn στο σύστημα προορισμού και εκτελέστε το. Επιλέξτε την επιλογή «Server» (Διακομιστής) στη διεπαφή του LinEn.
    - Στον εφεδρικό υπολογιστή, χρησιμοποιήστε το EnCase για να ξεκινήσετε τη διαδικασία δημιουργίας εικόνας μέσω των επιλογών «Προσθήκη αποδεικτικών στοιχείων» και «Προεπισκόπηση Crossover».
- **Πλεονεκτήματα:** Αποτρέπει την αυτόματη πρόσβαση εγγραφής σε συνδεδεμένες συσκευές αποθήκευσης. Τα συστήματα Linux μπορούν να αναγνωρίσουν σύνθετες διαμορφώσεις υλικού, όπως ελεγκτές RAID.

Τα **εργαλεία Unix** και τα μέσα εκκίνησης για εγκληματολογική ανάλυση που βασίζονται στο Linux προσφέρουν ευελιξία και έλεγχο κατά τη διάρκεια των διαδικασιών δημιουργίας εικόνων δικτύου.

- **Διαδικασία:**
    - Συνδέστε τα δύο συστήματα χρησιμοποιώντας είτε ένα καλώδιο crossover είτε ένα τυπικό καλώδιο patch. Χρησιμοποιήστε έναν διανομέα δικτύου ή έναν διακόπτη, αν χρειαστεί.
    - Αναθέστε στατικές διευθύνσεις IP σε κάθε υπολογιστή:

      Windows: Ορίστε τις ρυθμίσεις μέσω του «Κέντρου Δικτύου και Κοινής Χρήσης»

      Linux: Ορίστε την IP χρησιμοποιώντας εργαλεία όπως το ifconfig (π.χ. ifconfig eth0 192.168.100.1).
    - Ελέγξτε τη συνδεσιμότητα χρησιμοποιώντας μια εντολή ping για να βεβαιωθείτε ότι και οι δύο συσκευές επικοινωνούν.

Ο συνδυασμός των **dd και Netcat** επιτρέπει την απλή και αποτελεσματική μεταφορά δεδομένων μέσω του δικτύου.

- **Διαδικασία:**
    - **Προετοιμάστε τον υπολογιστή προορισμού:** Ξεκινήστε να παρακολουθείτε τα εισερχόμενα δεδομένα χρησιμοποιώντας το Netcat. Παράδειγμα: Αποθηκεύστε τα δεδομένα απευθείας σε ένα αρχείο ή μεταβιβάστε τα στο dd για εγγραφή.

- **Προετοιμάστε τον υπολογιστή προέλευσης:** Μεταδώστε τα δεδομένα του δίσκου στον προορισμό: Σε Linux: Χρησιμοποιήστε το dd για να διαβάσετε τα δεδομένα και να τα μεταφέρετε στο Netcat. Σε Windows: Χρησιμοποιήστε ένα συμβατό dd.exe για να εκτελέσετε παρόμοιες εργασίες.

- **Πρόσθετες παρατηρήσεις:** Απενεργοποιήστε προσωρινά τα τείχη προστασίας (firewalls) και το λογισμικό προστασίας από ιούς (antivirus) για να αποφύγετε παρεμβολές. Το Netcat ενδέχεται να ενεργοποιήσει ειδοποιήσεις ασφαλείας, καθώς συχνά ταξινομείται ως «δυνητικά ανεπιθύμητο πρόγραμμα».

Η χρήση **SSH** εξασφαλίζει ασφαλείς μεταφορές δεδομένων, ειδικά όταν εργάζεστε με συστήματα Linux ή macOS.

- **Διαδικασία:**
  - Χρησιμοποιήστε το dd για να δημιουργήσετε ένα αντίγραφο bitstream του δίσκου προέλευσης.
  - Διαβιβάστε την έξοδο μέσω μιας σύνδεσης SSH στο σύστημα προορισμού στο οποίο αποθηκεύεται ως εγκληματολογική εικόνα.
- **Πρόσθετα χαρακτηριστικά**
  - **Παρακολούθηση προόδου**: Χρησιμοποιήστε βοηθητικά προγράμματα όπως το Pipe Viewer (pv) για να παρακολουθείτε τη μεταφορά δεδομένων σε πραγματικό χρόνο.

- **Συμπίεση:** Μεταδώστε δεδομένα μέσω εργαλείων συμπίεσης, όπως το Gzip, για να μειώσετε τις απαιτήσεις αποθήκευσης.

9.4.3.8Ιδιαιτερότητες της δημιουργίας αντιγράφων ασφαλείας δεδομένων

Τα συστήματα **RAID** (Redundant Array of Independent Disks) έχουν σχεδιαστεί για να βελτιώνουν την απόδοση και την αξιοπιστία διανέμοντας τα δεδομένα σε πολλούς σκληρούς δίσκους.

- **Τύποι RAID:**
  - **Υλικό RAID:** Είναι διαχειρίσιμο με τη χρήση μιας ειδικής κάρτας ελεγκτή RAID που προσφέρει ισχυρή απόδοση και αξιοπιστία
  - **Λογισμικό RAID:** Ελέγχεται από το λειτουργικό σύστημα, είναι συνήθως λιγότερο ακριβό, αλλά εξαρτάται από τους πόρους του συστήματος
- **Επίπεδα RAID:**
  - **JBOD:** Όλοι οι σκληροί δίσκοι συνδυάζονται σε έναν ενιαίο μεγάλο χώρο αποθήκευσης. Το δίκτυο αποθήκευσης είναι ένα μεγάλο σύστημα αρχείων στο οποίο αποθηκεύονται τα δεδομένα.
  - **RAID0:** Όλοι οι σκληροί δίσκοι συνδυάζονται σε ένα ενιαίο μεγάλο σύστημα αποθήκευσης. Η λογική αποθήκευσης δεδομένων (μέγεθος λωρίδας) διασφαλίζει ότι τα δεδομένα αποθηκεύονται σε τμήματα στους σκληρούς δίσκους.

- **RAID10:** Δύο ή περισσότεροι σκληροί δίσκοι συνδυάζονται για να σχηματίσουν έναν ενιαίο χώρο αποθήκευσης (RAID0). Ο χώρος αποθήκευσης αντικατοπτρίζεται (RAID1 Mirroring).
- **RAID5 ή RAID6:** Τουλάχιστον 3 (RAID5) ή τουλάχιστον 4 (RAID6) σκληροί δίσκοι συνδυάζονται σε έναν ενιαίο χώρο αποθήκευσης. Οι πληροφορίες ισοτιμίας κατανέμονται στους δίσκους. Αν ένας (RAID5) ή δύο (RAID6) σκληροί δίσκοι παρουσιάσουν βλάβη, το περιεχόμενό τους μπορεί να αποκατασταθεί από τους υπόλοιπους φορείς δεδομένων. Ανάλογα με τον ελεγκτή/κατασκευαστή, οι πληροφορίες ισοτιμίας μπορούν να περιστραφούν «προς τα εμπρός» ή «προς τα πίσω» στους μεμονωμένους σκληρούς δίσκους.
- **Synology Hybrid RAID (SHR):** Μια παραλλαγή του RAID που χρησιμοποιεί λογισμικό RAID Linux (MD RAID και LVM2).

- **Βέλτιστες πρακτικές για δημιουργία αντιγράφων ασφαλείας RAID**:
  - Ακριβής τεκμηρίωση των διαμορφώσεων RAID (π.χ. ρυθμίσεις BIOS, τύπος ελεγκτή RAID, επίπεδο RAID, μέγεθος λωρίδας).
  - Δημιουργία αντιγράφων ασφαλείας μέσω ελεγκτή RAID, π.χ. εκκίνηση με Linux Live CD ή WinFE, τα οποία αναγνωρίζουν τον ελεγκτή RAID υλικού.
  - Δημιουργία αντιγράφων ασφαλείας λογικών δεδομένων, εάν είναι απαραίτητο, π.χ. με το FTK Imager «Custom Content Image».

Τα συστήματα **NAS** (Network Attached Storage) είναι συμπαγείς, αυτόνομοι διακομιστές που χρησιμοποιούν προσαρμοσμένα λειτουργικά συστήματα, συνήθως ελαφριές, προσαρμοσμένες εκδόσεις του Linux. Ο εσωτερικός φορέας δεδομένων

συνήθως αποτελείται από σκληρούς δίσκους SATA. Το πρώτο βήμα είναι η δημιουργία κλασσικών αντιγράφων ασφαλείας εικόνας. Κατά την αφαίρεση δίσκων από το σύστημα, είναι σημαντικό να επισημάνετε ποιος δίσκος βρισκόταν σε ποια υποδοχή. Τα συστήματα NAS διαθέτουν διεπαφή βασισμένη σε πρόγραμμα περιήγησης (Web GUI). Για να αποκτήσετε πρόσβαση σε αυτή τη διεπαφή, το NAS πρέπει να είναι συνδεδεμένο στο δίκτυο της έρευνας.

9.4.4 Ψηφιακή εγκληματολογία στο πλαίσιο της εμπορίας ανθρώπων και της εργασιακής εκμετάλλευσης

Η εμπορία ανθρώπων, συμπεριλαμβανομένης της εργασιακής εκμετάλλευσης, βασίζεται όλο και περισσότερο στην ψηφιακή επικοινωνία, τις χρηματοοικονομικές συναλλαγές και τη στρατολόγηση μέσω του διαδικτύου (Europol, 2020· 2024). Κατά συνέπεια, η ψηφιακή εγκληματολογία διαδραματίζει κρίσιμο ρόλο στην ταυτοποίηση των δραστών, στην αποκάλυψη των μοτίβων εκμετάλλευσης των θυμάτων και στη διασφάλιση αποδεικτικών στοιχείων για δίωξη. Αυτή η υποενότητα εξετάζει τον τρόπο με τον οποίο οι μεθοδολογίες ψηφιακής εγκληματολογίας μπορούν να εφαρμοστούν σε υποθέσεις εμπορίας ανθρώπων αντιμετωπίζοντας τόσο τεχνικά όσο και ηθικά ζητήματα. Η ενότητα ξεκινά με τις βασικές πηγές ψηφιακών αποδεικτικών στοιχείων στον τομέα της εμπορίας ανθρώπων (και όπου είναι δυνατόν να συγκεντρωθούν πληροφορίες, ειδικά για την εργασιακή εκμετάλλευση, Ενότητα 9.6.4.1). Στη συνέχεια, η Ενότητα 9.6.4.2 ασχολείται με την ανάλυση των τυπικών ψηφιακών αποδεικτικών στοιχείων της εμπορίας ανθρώπων (π.χ. τι αναζητούν οι ερευνητές/-τριες;). Ακολουθεί η Ενότητα 9.6.4.3, η οποία παρουσιάζει ορισμένα πιθανά εργαλεία ψηφιακής εγκληματολογίας που μπορούν να χρησιμοποιηθούν από

τις αρχές επιβολής του νόμου. Έπειτα, συζητούνται οι κύριες προκλήσεις που είναι ιδιαίτερα σημαντικές για τη διαδικασία ψηφιακής εγκληματολογίας κατά τη διάρκεια των ερευνών για την εμπορία ανθρώπων (Ενότητα 9.6.4.4). Η ενότητα ολοκληρώνεται με νομικά και ηθικά ζητήματα που πρέπει να ληφθούν υπόψη (Ενότητα 9.6.4.5). Μια περαιτέρω επισκόπηση της τεχνολογίας που χρησιμοποιείται για την πρόληψη και την καταπολέμηση της εμπορίας ανθρώπων συντάχθηκε από το Γραφείο των Ηνωμένων Εθνών για τον Έλεγχο των Ναρκωτικών και την Πρόληψη του Εγκλήματος (UNODC) – Ενότητα 14: Σύνδεσμοι μεταξύ Εγκληματικότητας στον Κυβερνοχώρο, Εμπορίας Ανθρώπων και Παράνομης Διακίνησης Μεταναστών/-στριών.

9.4.4.1 Βασικές πηγές ψηφιακών αποδεικτικών στοιχείων

Οι διακινητές και οι εκμεταλλευτές χρησιμοποιούν διάφορες ψηφιακές πλατφόρμες και τεχνολογίες αφήνοντας πίσω τους σημαντικά εγκληματολογικά ίχνη, αλλά οι αρχές επιβολής του νόμου μπορούν να χρησιμοποιήσουν ψηφιακά αποδεικτικά στοιχεία για να εντοπίσουν την εμπορία ανθρώπων μέσω του διαδικτύου και τους δράστες, καθώς και να βρουν νομικά αποδεικτικά στοιχεία για να τους κατηγορήσουν για αυτό το έγκλημα (Cellebrite, 2024). Οι συνήθεις πηγές αποδεικτικών στοιχείων περιλαμβάνουν τα εξής:

Προσωπικές ψηφιακές συσκευές

Στο πλαίσιο των ερευνών για εργασιακή εκμετάλλευση, οι προσωπικές ψηφιακές συσκευές, όπως τα κινητά τηλέφωνα και οι υπολογιστές, μπορούν να χρησιμεύσουν ως σπουδαίες πηγές αποδεικτικών στοιχείων. Οι εν λόγω συσκευές συχνά περιέχουν επικοινωνίες, επαφές, οικονομικές συναλλαγές και δεδομένα τοποθεσίας που μπορούν να αποκαλύψουν πρακτικές εκμετάλλευσης.

- **Φορητές συσκευές**: Οι διακινητές χρησιμοποιούν συχνά φορητές συσκευές για τον συντονισμό παράνομων δραστηριοτήτων. Τα αποδεικτικά στοιχεία από αυτές τις συσκευές μπορούν να περιλαμβάνουν: (1) αρχεία κλήσεων και λίστες επαφών που αποκαλύπτουν μοτίβα επικοινωνίας και δίκτυα, (2) μηνύματα κειμένου και ιστορικό συνομιλιών που περιέχουν λεπτομέρειες σχετικά με δραστηριότητες στρατολόγησης (πρόσληψης), συντονισμού και εκμετάλλευσης, (3) αρχεία πολυμέσων, όπως φωτογραφίες και βίντεο που μπορεί να τεκμηριώνουν θύματα, τοποθεσίες ή παράνομες πράξεις, και (4) δεδομένα τοποθεσίας (οι πληροφορίες GPS μπορούν να εντοπίσουν κινήσεις και να προσδιορίσουν βασικές τοποθεσίες).
- **Υπολογιστές:** Υπάρχουν διάφοροι τύποι αποθηκευμένων ή προσβάσιμων μέσω υπολογιστή δεδομένων που μπορεί να παρουσιάζουν ιδιαίτερο ενδιαφέρον για την έρευνα της εμπορίας ανθρώπων (ενδεχομένως σε συνδυασμό με δεδομένα από φορητές συσκευές): (1) αρχεία επικοινωνίας όπως μηνύματα ηλεκτρονικού ταχυδρομείου (e-mail) και γραπτά μηνύματα, δραστηριότητες στα μέσα κοινωνικής δικτύωσης (social media) ή διαδικτυακές διαφημίσεις ή αγγελίες εργασίας, (2) οικονομικά δεδομένα, όπως τραπεζικές συναλλαγές και αρχεία πληρωμών ή αρχεία κρυπτονομισμάτων, (3) δεδομένα προσωπικής ταυτοποίησης, όπως ψηφιακά αντίγραφα εγγράφων ταυτότητας ή δεδομένα τοποθεσίας, (4) αρχεία απασχόλησης και συνθηκών εργασίας, όπως συμβάσεις εργασίας, παράνομα προγράμματα εργασίας, συστήματα χρονομέτρησης και παρακολούθησης παρουσιών (π.χ. για τον εντοπισμό υπερβολικών ωρών εργασίας), (5) δεδομένα ταξιδιών, όπως πληροφορίες κρατήσεων ταξιδιών από αεροπορικές εταιρείες ή ταξιδιωτικά γραφεία ή αγορές εισιτηρίων και δρομολόγια, (6) ιστορικό δραστηριοτήτων στο (σκοτεινό ή επιφανειακό)

διαδίκτυο, (7) αρχεία υγείας και ιατρικά αρχεία που αποθηκεύονται , π.χ. από επισκέψεις των θυμάτων σε γιατρό μετά από σωματικές επιθέσεις, ή (8) δεδομένα από κάμερες παρακολούθησης ή συστήματα ασφαλείας σε χώρους εργασίας ή ιδιωτικές ιδιοκτησίες που δείχνουν τις συνθήκες διαβίωσης και εργασίας των θυμάτων.

Αποθήκευση στο cloud

Η αποθήκευση στο cloud μπορεί να χρησιμοποιηθεί από τους διακινητές λόγω της ευκολίας, της απομακρυσμένης πρόσβασης και της δυνατότητας αποθήκευσης μεγάλου όγκου δεδομένων, γεγονός που την καθιστά μια σημαντική πηγή ψηφιακών αποδεικτικών στοιχείων σε τέτοιες περιπτώσεις. Τα δεδομένα που συλλέγονται από την αποθήκευση στο cloud μπορεί να είναι παρόμοια με αυτά που αναφέρονται παραπάνω για τις φορητές συσκευές και τους υπολογιστές. Επιπλέον, ειδικά δεδομένα που μπορούν να βρεθούν πιο συχνά σε αποθηκευτικούς χώρους στο cloud είναι ψηφιακά ημερολόγια που ενδέχεται να αποκαλύπτουν πραγματοποιημένες ή προγραμματισμένες συναντήσεις, μετακινήσεις των θυμάτων ή άλλες πληροφορίες σχετικά με τις επιχειρήσεις που κοινοποιήθηκαν στο δίκτυο εμπορίας ανθρώπων. Ως εκ τούτου, οι αποθηκευτικοί χώροι στο cloud μπορούν να προσφέρουν μεγαλύτερη πιθανότητα αποκάλυψης των δομών του δικτύου εμπορίας ανθρώπων ή των θυμάτων που υφίστανται οργανωμένη εργασιακή εκμετάλλευση. Η πρόσβαση και η ανάλυση των δεδομένων που είναι αποθηκευμένα στο cloud απαιτεί, ωστόσο, νομικές διαδικασίες και ειδική τεχνική εμπειρογνωσία για να διασφαλιστεί η ακεραιότητα των αποδεικτικών στοιχείων (εάν τα διαπιστευτήρια του/της χρήστη/-στριας δεν είναι γνωστά). Τεχνικοί τρόποι (τουλάχιστον μερικής) πρόσβασης είναι, για παράδειγμα, η συνεργασία με τον πάροχο υπηρεσιών cloud, η εφαρμογή εργαλείων εξαγωγής

δεδομένων cloud, η χρήση API υπηρεσιών cloud, η πρόσβαση μέσω κατασχεθέντων συσκευών (σύνδεση με διαπιστευτήρια χρήστη/-στριας, χρήση αντιγράφων ασφαλείας συσκευών και έλεγχος εάν η συσκευή συγχρόνισε δεδομένα με το cloud), η διεξαγωγή ανάλυσης μεταδεδομένων με τα αρχεία που είναι αποθηκευμένα στο cloud, η εφαρμογή δικτυακής εγκληματολογίας (Ενότητα 4.1.1) ή η πρόσβαση στα αρχεία καταγραφής των υπηρεσιών αποθήκευσης cloud από τους παρόχους υπηρεσιών cloud, π.χ. για τη λήψη του ιστορικού σύνδεσης ή του ιστορικού λήψης αρχείων.

Πλατφόρμες επικοινωνίας και πρόσληψης

Το διαδίκτυο παρέχει στους διακινητές πρόσβαση σε πιθανά θύματα μέσω διαφόρων ψηφιακών καναλιών, συμπεριλαμβανομένων των μέσων κοινωνικής δικτύωσης και των ιστότοπων πρόσληψης (UNODC, 2019α). Ο Fraser (2016) ανέλυσε λεπτομερώς τον τρόπο με τον οποίο οι διαδικασίες μεταξύ των διακινητών ανθρώπων και των θυμάτων αλλάζουν με τη μετάβαση από τα γεωγραφικά δίκτυα στα διαδικτυακά δίκτυα. Ο Fraser επισημαίνει ότι οι διακινητές στις μέρες μας γνωρίζουν πώς να χρησιμοποιούν τα διαδικτυακά μέσα κοινωνικής δικτύωσης και το σκοτεινό διαδίκτυο. Το έγγραφο περιγράφει επίσης τον τρόπο με τον οποίο αυτά τα δίκτυα επηρεάζουν την ανισορροπία ισχύος στην εμπορία ανθρώπων και διαμορφώνουν τις εμπειρίες των θυμάτων (Fraser, 2016). Τα ψηφιακά αποδεικτικά στοιχεία από αυτές τις πλατφόρμες περιλαμβάνουν (1) προφίλ και αναρτήσεις που μπορεί να περιέχουν προσπάθειες πρόσληψης, παραπλανητικές προσφορές εργασίας ή διαφημίσεις για παράνομες υπηρεσίες, (2) άμεσα μηνύματα (που διευκολύνουν την ιδιωτική επικοινωνία μεταξύ διακινητών και θυμάτων) και (3) συμμετοχές σε ομάδες που υποδηλώνουν συμμετοχή σε δίκτυα ή φόρουμ διακίνησης. Η ανάλυση αυτών των

στοιχείων μπορεί να αποκαλύψει, για παράδειγμα, στρατηγικές πρόσληψης και να ταυτοποιήσει τόσο τα θύματα όσο και τους δράστες.

- **Πλατφόρμες μέσων κοινωνικής δικτύωσης**: Μια έκθεση των Kunz et al. (2018) συνοψίζει ποιοι ιστότοποι χρησιμοποιούνται για σκοπούς σεξουαλικής εκμετάλλευσης. Μεταξύ αυτών συγκαταλέγονται (1) ιστότοποι για προβολή και σχολιασμό, όπως το Facebook, το Instagram και το Snapchat, αλλά και το YikYak και το Wispher, (2) ιστότοποι για συνομιλία, όπως το Tinder, το Blendr, το WhatsApp και το KIK, αλλά και το Yellow και το #1 Chat Avenue ως λιγότερο συνηθισμένοι ιστότοποι, (3) ιστότοποι με κάμερες web, όπως το Chatroulette, το Omegle και το Monkey, και (4) ιστότοποι για διαφήμιση και πωλήσεις, όπως το Cityxguide, το skipthegames, το bedpage, το seekingarrangement.com ή το sugar-babies.com. Σε ό,τι αφορά την εργασιακή εκμετάλλευση, δεν ήταν δυνατό να βρεθεί μια τέτοια επισκόπηση. Εντούτοις, είναι γνωστό ότι οι **mainstream πλατφόρμες των social media** χρησιμοποιούνται για την πρόσληψη εργαζομένων με σκοπό την εκμετάλλευση, μαζί με διαδικτυακές πύλες εργασίας και αγγελίες (βλ. π.χ. Europol, 2024).
- **Ιστότοποι διαδικτυακής πρόσληψης προσωπικού**: Ακόμη και αν αυτές οι πύλες και οι ιστότοποι με αγγελίες είναι νόμιμες, οι διακινητές μπορούν να δημοσιεύουν παραπλανητικές προσφορές εργασίας, στοχεύοντας ευάλωτους πληθυσμούς που αναζητούν απασχόληση. Σε δεύτερο στάδιο, οι διακινητές χρησιμοποιούν εφαρμογές άμεσων μηνυμάτων για την ανταλλαγή επιχειρησιακών λεπτομερειών, καθώς αυτές παρέχουν ένα ασφαλέστερο περιβάλλον (Europol, 2024).

- **Διαφημίσεις στο διαδίκτυο**: Η διαφορά σε σχέση με τις πλατφόρμες των μέσων κοινωνικής δικτύωσης, τις εφαρμογές άμεσων μηνυμάτων και τους ιστότοπους πρόσληψης προσωπικού στο διαδίκτυο είναι ότι οι διαφημίσεις στο διαδίκτυο μπορούν να θεωρηθούν ως *μονόδρομη επικοινωνία*, ενώ οι άλλες πηγές στοχεύουν συνήθως στην *αμφίδρομη επικοινωνία* μεταξύ ατόμων (π.χ. πιθανό θύμα και ύποπτος διακινητής). Τα χαρακτηριστικά των διαφημίσεων στο διαδίκτυο για εμπορία ανθρώπων με σκοπό την εργασιακή εκμετάλλευση περιλαμβάνουν τα εξής:
    - **Έλλειψη συγκεκριμένων στοιχείων**: Οι διαφημίσεις συχνά παρέχουν ασαφείς περιγραφές θέσεων εργασίας με ελάχιστες λεπτομέρειες σχετικά με τον ρόλο, τις ευθύνες ή τις συνθήκες εργασίας. Αυτή η ασαφής περιγραφή βοηθά στο να προσελκύσει ένα ευρύτερο φάσμα υποψηφίων χωρίς να αποκαλύπτει πιθανές καταστάσεις εκμετάλλευσης (Volodko, Cockbain & Kleinberg, 2020).
    - **Μη ρεαλιστικές υποσχέσεις**: Οι προσφορές μπορεί να περιλαμβάνουν ασυνήθιστα υψηλούς μισθούς, ταχεία επεξεργασία βίζας ή άλλα οφέλη που φαίνονται πολύ καλά για να είναι αληθινά, με στόχο να προσελκύσουν άτομα που αναζητούν καλύτερες ευκαιρίες (βλ. π.χ. Fraser, 2016).
    - **Στοχευμένες δημογραφικές ομάδες**: Οι προσπάθειες πρόσληψης συχνά επικεντρώνονται σε συγκεκριμένους πληθυσμούς, όπως μετανάστες/-στριες ή άτομα από οικονομικά μειονεκτούντα περιβάλλοντα, τα οποία είναι πιο ευάλωτα στην εκμετάλλευση (Volodko, Cockbain & Kleinberg, 2020).

- Παρόλο που έχουν γίνει προσπάθειες για τη διερεύνηση των διαδικτυακών διαφημίσεων για σεξουαλική εκμετάλλευση με τη χρήση σύγχρονων τεχνολογικών μεθόδων, όπως η Επεξεργασία Φυσικής Γλώσσας (Natural Language Processing-NLP) (π.χ. Perez & Rivas, 2023· Lugo-Graulich et al, 2024), το έγκλημα της εργασιακής εκμετάλλευσης, καθώς και άλλες μορφές εμπορίας ανθρώπων, εξακολουθούν να στερούνται επιστημονικής έρευνας σε αυτόν τον τομέα.

- **Σκοτεινό διαδίκτυο (dark web) έναντι επιφανειακού διαδικτύου (surface web)**: Οι καταχωρίσεις και οι διαφημίσεις στο dark web φιλοξενούνται σε κρυπτογραφημένα δίκτυα που απαιτούν εξειδικευμένο λογισμικό για πρόσβαση και προσφέρουν υψηλότερο βαθμό ανωνυμίας. Αυτή η απόκρυψη δημιουργεί σημαντικές προκλήσεις για τις αρχές επιβολής του νόμου, καθώς αυτές οι πλατφόρμες συχνά εφαρμόζουν προηγμένα τεχνικά μέτρα για την προστασία της ταυτότητας των χρηστών/-στριών. Αντίθετα, οι καταχωρίσεις και οι διαφημίσεις στο surface web είναι προσβάσιμες στο κοινό και συχνά βρίσκονται σε mainstream πλατφόρμες, όπως τα social media και οι ιστότοποι με αγγελίες. Αν και μπορεί να χρησιμοποιούν κωδικοποιημένη γλώσσα και εικόνες για να αποφύγουν τον εντοπισμό, ο δημόσιος χαρακτήρας τους επιτρέπει την πιο άμεση παρακολούθηση από τις αρχές επιβολής του νόμου. Οι διακινητές χρησιμοποιούν τόσο τις πλατφόρμες του επιφανειακού διαδικτύου όσο και του σκοτεινού διαδικτύου για να διαφημίζουν υπηρεσίες ή ευκαιρίες εκμετάλλευσης. Τα σχετικά ψηφιακά αποδεικτικά στοιχεία στο σκοτεινό διαδίκτυο περιλαμβάνουν, για παράδειγμα, (1) αγγελίες και καταχωρίσεις που ενδέχεται να προσφέρουν παράνομες υπηρεσίες ή παραπλανητικές ευκαιρίες απασχόλησης, και (2) αναρτήσεις σε φόρουμ και επικοινωνίες στις οποίες

συζητούνται μέθοδοι, ανταλλάσσονται πληροφορίες ή διεξάγονται διαπραγματεύσεις για συναλλαγές (π.χ. μια ανάρτηση σε φόρουμ που αναφέρει «διαθέσιμοι/-μες εργάτες/-τριες για εργασία χαμηλού κόστους»), ή (3) πλαστά έγγραφα που αποκτήθηκαν από αγορές του σκοτεινού διαδικτύου, όπως πλαστές βίζες και άδειες εργασίας για μετανάστες/-στριες χωρίς έγγραφα.

Παρακολούθηση και εντοπισμός

Τα δεδομένα παρακολούθησης και εντοπισμού αναφέρονται στα δεδομένα που μπορούν να αποκαλύψουν την τοποθεσία, τις κινήσεις ή τις ενέργειες ατόμων, τα οποία συχνά συλλέγονται μέσω ηλεκτρονικών μέσων και αξιοποιούνται από την ψηφιακή εγκληματολογία. Τα σύγχρονα περιβάλλοντα που είναι εξοπλισμένα με συστήματα παρακολούθησης και συσκευές IoT μπορούν να καταγράψουν ακούσια δραστηριότητες εμπορίας ανθρώπων. Η έρευνα μπορεί επίσης να επιτρέψει (εάν επιβεβαιωθεί νομικά) την παρακολούθηση και τον έλεγχο υπόπτων.

Παρακολούθηση που ξεκινά από τις αρχές επιβολής του νόμου (συνήθως απαιτείται δικαστική εντολή)

- **Παρακολούθηση μέσω GPS, π.χ. παρακολούθηση οχημάτων:** Μπορεί να χρησιμοποιηθεί από τις αρχές επιβολής του νόμου για την παρακολούθηση των κινήσεων. Οι αρχές μπορούν, για παράδειγμα, να παρακολουθούν τις κινήσεις του αυτοκινήτου ενός υπόπτου που μεταφέρει τακτικά θύματα από και προς διάφορους χώρους εργασίας. Τα μοτίβα στα δεδομένα θέσης του οχήματος θα μπορούσαν να βοηθήσουν τις αρχές να εντοπίσουν κέντρα εμπορίας ανθρώπων ή να προσδιορίσουν τις διαδρομές μετακίνησης ή τις ώρες εργασίας των θυμάτων.

- **Κάμερες παρακολούθησης:** Τα βίντεο από δημόσιες ή ιδιωτικές κάμερες παρακολούθησης μπορούν να χρησιμοποιηθούν για την παρακολούθηση των κινήσεων των διακινητών ή των θυμάτων σε συγκεκριμένες τοποθεσίες (π.χ. σε χώρους εργασίας, κοντά σε σύνορα).
- **Παρακολούθηση επικοινωνιών (υποκλοπές):** Οι υποκλοπές (π.χ. τηλεφωνικές κλήσεις, μηνύματα ηλεκτρονικού ταχυδρομείου, άμεσα μηνύματα) μπορούν να παράσχουν πληροφορίες για τις δραστηριότητες εμπορίας ανθρώπων. Οι υποκλοπές μπορούν να βοηθήσουν τις αρχές να παρακολουθήσουν τους διακινητές ενώ οργανώνουν ταξίδια, πληρωμές, απειλούν τα θύματα κ.λπ.
- **Συσκευές εντοπισμού σε κινητά τηλέφωνα:** Η τριγωνοποίηση κινητών τηλεφώνων και τα δεδομένα GPS από κινητά τηλέφωνα μπορούν να χρησιμοποιηθούν για τον ακριβή εντοπισμό της θέσης του θύματος ή του διακινητή και, π.χ., για τη χαρτογράφηση των θέσεών τους κατά τη διάρκεια του χρόνου.
- **Μη επανδρωμένα αεροσκάφη ή εναέρια παρακολούθηση:** Τα drone που είναι εξοπλισμένα με κάμερες μπορούν να χρησιμοποιηθούν για την παρακολούθηση κινήσεων σε μεγαλύτερες περιοχές (ειδικά σε αγροτικές ή δυσπρόσιτες περιοχές στις οποίες η παρακολούθηση από τον άνθρωπο μπορεί να είναι δύσκολη).

Παρακολούθηση που ξεκινά από τους διακινητές (δεδομένα που συλλέγονται από τους διακινητές)

- **Παρακολούθηση φορητών συσκευών από τους διακινητές**: Οι διακινητές μπορούν να χρησιμοποιούν τα τηλέφωνα των θυμάτων ή τις δικές τους συσκευές για να παρακολουθούν τα θύματα. Αυτό μπορεί να περιλαμβάνει τη

χρήση εφαρμογών παρακολούθησης GPS ή ακόμη και την εγκατάσταση λογισμικού υποκλοπής (π.χ. mSpy, FlexiSPY) για την παρακολούθηση της θέσης και των επικοινωνιών του θύματος.

- **Δεδομένα θέσης από συσκευές IoT**: Οι συσκευές IoT, όπως τα έξυπνα ρολόγια ή ακόμη και τα συνδεδεμένα οχήματα, μπορούν να χρησιμοποιηθούν από τους διακινητές για την παρακολούθηση της θέσης των θυμάτων. Τα αρχεία καταγραφής από αυτές τις συσκευές μπορούν να αναλυθούν, π.χ. για να εντοπιστούν ασυνήθιστοι χρόνοι πρόσβασης ή αλλαγές στο περιβάλλον.
- **Παρακολούθηση στο διαδίκτυο**: Οι διακινητές παρακολουθούν συχνά τους λογαριασμούς των θυμάτων τους στα μέσα κοινωνικής δικτύωσης για να ελέγχουν τις επικοινωνίες τους ή ακόμη φτάνουν στο σημείο να τα υποδύονται για να ελέγχουν την παρουσία τους στο διαδίκτυο και, π.χ., να τα εμποδίζουν να ζητήσουν βοήθεια. Οι αρχές επιβολής του νόμου θα μπορούσαν επομένως να εξετάσουν εάν ο διακινητής είχε τα διαπιστευτήρια χρήστη του/των θύματος/θυμάτων για να συνδεθεί σε διάφορα μέσα κοινωνικής δικτύωσης ή άλλες πλατφόρμες.
- **Παρακολούθηση με βίντεο και ήχο**: Οι διακινητές μπορεί να τοποθετούν κρυφές κάμερες ή συσκευές ηχογράφησης σε δωμάτια ή χώρους εργασίας για να παρακολουθούν συνεχώς τα θύματα, π.χ. για να διασφαλίζουν ότι εκτελούν τις εργασίες τους. Οι αρχές επιβολής του νόμου θα μπορούσαν να επικεντρωθούν στην ανίχνευση τέτοιων συσκευών και στη συνέχεια να αξιολογήσουν τα δεδομένα τους για να καθορίσουν το εύρος της εργασιακής εκμετάλλευσης και να είναι σε θέση να παρουσιάσουν αξιόπιστα αποδεικτικά στοιχεία στο δικαστήριο.

Χρηματοοικονομικές συναλλαγές και μέθοδοι πληρωμής

Χρηματοοικονομικές συναλλαγές και συναλλαγές με κρυπτονομίσματα (εγχώριες και διεθνείς): Οι διακινητές συχνά εκμεταλλεύονται τα ψηφιακά συστήματα εγκληματολογικής ανάλυσης για να κάνουν «ξέπλυμα μαύρου χρήματος» και να αποκρύψουν κέρδη. Βασικά ψηφιακά αποδεικτικά στοιχεία είναι τα εξής: (1) τραπεζικά εκκαθαριστικά και ιστορικά συναλλαγών που υποδεικνύουν ασυνήθιστα μοτίβα τα οποία υποδηλώνουν παράνομες δραστηριότητες, (2) πορτοφόλια κρυπτονομισμάτων και συναλλαγές που χρησιμοποιούνται για την απόκρυψη χρηματοοικονομικών ιχνών, οι οποίες απαιτούν εξειδικευμένη εγκληματολογική ανάλυση. Η χρηματοοικονομική ανάλυση (βλ. Ενότητα 9.2) είναι μείζονος σημασίας για τον εντοπισμό της ροής των χρημάτων, την εξάρθρωση των δραστηριοτήτων εμπορίας ανθρώπων και τη δίωξη των παραβατών (Thomson Reuters, 2025).

- **Παραδοσιακές τραπεζικές συναλλαγές**
- **Συναλλαγές κρυπτονομισμάτων**
- **Προπληρωμένα και ψηφιακά συστήματα πληρωμών**

9.4.4.2Ανάλυση και συσχέτιση αποδεικτικών στοιχείων

Μετά την κατάσχεση και τη διατήρηση των ψηφιακών αποδεικτικών στοιχείων (π.χ. κατάσχεση κινητών τηλεφώνων, υπολογιστών, μονάδων USB, λογαριασμών cloud, δεδομένων social media), τα δεδομένα πρέπει να εξαχθούν από αυτές τις συσκευές ή τους αποθηκευτικούς χώρους εφαρμόζοντας διαφορετικούς τύπους εγκληματολογικών μεθόδων που περιγράφονται στην Ενότητα 9.1.1 (π.χ. εγκληματολογική ανάλυση cloud, εξαγωγή δεδομένων σε επίπεδο υλικού, όπως chip

off ή μέθοδοι όπως παραβίαση/αποκρυπτογράφηση κωδικών πρόσβασης). Στη συνέχεια, οι ερευνητές/-τριες μπορούν να αναλύσουν και να συσχετίσουν τα ψηφιακά αποδεικτικά στοιχεία. Οι ψηφιακές εγκληματολογικές διαδικασίες και αρχές που παρουσιάζονται παρακάτω είναι αφενός ενδεικτικές και αφετέρου δεν είναι απολύτως μοναδικές για την εμπορία ανθρώπων: πολλές τεχνικές επικαλύπτονται με τις έρευνες για εγκλήματα στον κυβερνοχώρο, το οργανωμένο έγκλημα και τις απάτες. Ωστόσο, ορισμένες πτυχές καθιστούν την εμπορία ανθρώπων μοναδική σε αυτό το πλαίσιο, όπως η **έμφαση στα μέσα κοινωνικής δικτύωσης και στις αγγελίες πρόσληψης** (σε αντίθεση με τα οικονομικά εγκλήματα, οι υποθέσεις εμπορίας ανθρώπων βασίζονται σε μεγάλο βαθμό στη διαδικτυακή εξαπάτηση και την παρακολούθηση των επικοινωνιών). Επιπλέον, ένα μεγάλο μέρος των **αποδεικτικών στοιχείων** (τα οποία ανασυνθέτουν οι ομάδες ψηφιακής εγκληματολογίας) **επικεντρώνεται στα θύματα**, καθώς οι διακινητές διατηρούν τον έλεγχο των θυμάτων τους μέσω, για παράδειγμα, απειλητικών μηνυμάτων, εκβιασμού ή παρακολούθησης μέσω GPS. Ακόμη, τα θύματα εμπορίας συχνά δεν διαθέτουν δικούς τους επιτραπέζιους ή φορητούς υπολογιστές, αλλά smartphone και λογαριασμούς cloud. Αυτό καθιστά τις έρευνες για την εμπορία ανθρώπων πιο εξαρτημένες από από την **εγκληματολογική ανάλυση φορητών συσκευών και cloud** (βλ. Ενότητα 9.1.1).

Σε περιπτώσεις εμπορίας ανθρώπων, οι εμπειρογνώμονες ψηφιακής εγκληματολογίας μπορούν να αναζητήσουν συγκεκριμένα:

- **Μοτίβα επικοινωνίας**: Συχνά, οι διακινητές χρησιμοποιούν κωδικοποιημένη γλώσσα ή αργκό στα μηνύματα και, ως εκ τούτου, αναζητούν διαφορετικές λέξεις-κλειδιά όπως «εύκολη δουλειά», «πληρωμή με μετρητά», «δωρεάν ταξίδι» στο πλαίσιο της εργασιακής εκμετάλλευσης ή «μοντελινγκ» και «συνοδεία» στο πλαίσιο της σεξουαλικής εκμετάλλευσης. Συχνά, αυτές οι

λέξεις-κλειδιά που σχετίζονται με την εργασία, τη διαμονή και τους μισθούς χρησιμοποιούνται επαναληπτικά. Οι Tong et al. (2017), για παράδειγμα, διαπίστωσαν ότι οι διακινητές στις ΗΠΑ και τον Καναδά τροποποιούν τη γλώσσα τους για να αποφύγουν τον εντοπισμό από τις αρχές επιβολής του νόμου. Επιπρόσθετα, αλλάζουν την ορολογία, γεγονός που δυσχεραίνει την ανάπτυξη λιστών με λέξεις-κλειδιά για τον εντοπισμό διαφημίσεων που σχετίζονται με την εμπορία ανθρώπων. Αυτό δημιουργεί ένα λεξιλόγιο που εξελίσσεται συνεχώς. Για παράδειγμα, αντί να αναφέρουν ρητά «νεαρή κοπέλα», οι διακινητές χρησιμοποιούν ασαφή κείμενα, emoji ή αργκό (π.χ. «Y ♥ ng G!rl»). Πολλές διαφημίσεις δεν έχουν σωστή γραμματική δομή, γεγονός που μειώνει την αποτελεσματικότητα των παραδοσιακών τεχνικών NLP. Οι διαφημίσεις περιέχουν συχνά σύμβολα, emoji και μη τυποποιημένους χαρακτήρες. Η σειρά των λέξεων είναι συχνά ασυνεπής θυμίζοντας περισσότερο τα social media ή τα μηνύματα κειμένου παρά τη δομή του γραπτού λόγου (π.χ. «@» αντί για «at» ή «m33t» αντί για «meet»). Η πολυπλοκότητα των μονογραμμάτων, των διγραμμάτων και των τριγραμμάτων είναι υψηλή. Η υψηλή μεταβλητότητα των λέξεων προκύπτει από το γεγονός ότι οι διακινητές τροποποιούν σκόπιμα τις λέξεις για να αποφύγουν την αυτόματη ανίχνευση (ασυνήθιστοι συνδυασμοί λέξεων, σπάνιες λέξεις, τροποποιημένες φράσεις). Οι διαφημίσεις είναι συνήθως σύντομες (μέσος όρος 133 λέξεων) και δεν περιέχουν εκτενείς περιγραφές. Οι Tong et al. (2017) καταλήγουν στο συμπέρασμα ότι οι διακινητές προσαρμόζουν συνεχώς τη γλώσσα τους, γεγονός που απαιτεί ευέλικτα μοντέλα ανίχνευσης. Οι λίστες λέξεων-κλειδιών από μόνες τους δεν αρκούν και για τον λόγο αυτό, οι ερευνητές/-τριες χρειάζονται μοντέλα Τεχνητής Νοημοσύνης (AI) που να αναγνωρίζουν το πλαίσιο.

Ένας άλλος τρόπος για να κατανοήσουμε και να ανατρέξουμε σε συγκεκριμένα μοτίβα επικοινωνίας για ψηφιακές εγκληματολογικές έρευνες είναι να εξετάσουμε τις στρατηγικές πρόσληψης που εφαρμόζουν οι διακινητές. Αυτές μπορούν να κατηγοριοποιηθούν σε ενεργητικές και παθητικές μεθόδους (Europol, 2020): Η **ενεργητική πρόσληψη** είναι σαν το «ψάρεμα με αγκίστρι», καθώς οι εγκληματίες δημοσιεύουν ψεύτικες αγγελίες εργασίας σε αξιόπιστους ιστότοπους εύρεσης εργασίας και σε κοινωνικά δίκτυα. Μπορούν ακόμη και να δημιουργήσουν ψεύτικους ιστότοπους πρόσληψης που φαίνονται επαγγελματικοί, μερικές φορές με ζωντανή συνομιλία (live chat) για να φαίνονται νόμιμοι. Το Γραφείο των Ηνωμένων Εθνών για τον Έλεγχο των Ναρκωτικών και την Πρόληψη του Εγκλήματος αποκαλεί αυτό το φαινόμενο «στρατηγική κυνηγιού» (UNODC, 2020). Η ενεργητική πρόσληψη περιλαμβάνει κυρίως άμεσα μηνύματα και συνομιλίες μέσω που στοχοποιούν ευάλωτα άτομα. Μπορεί να περιλαμβάνει μορφές εξαναγκασμού, χειραγώγησης και ψευδών προσφορών εργασίας. Επίσης, δεν είναι ασυνήθιστο να διαγράφονται ξαφνικά μηνύματα ή λογαριασμοί μετά την αρχική επαφή (δηλαδή, όταν ο διακινητής διαπιστώνει ότι το άτομο που πρόκειται να διακινηθεί δεν είναι διαθέσιμο για την προσφορά εργασίας). Η **παθητική πρόσληψη** είναι πιο διακριτική και πιο δύσκολο να ανιχνευθεί από τις αρχές επιβολής του νόμου. Λειτουργεί όπως το «ψάρεμα με δίχτυα» (ή «στρατηγική ψαρέματος», UNODC, 2020), καθώς οι διακινητές παρακολουθούν τις αναρτήσεις των ατόμων που αναζητούν εργασία στο διαδίκτυο και επικοινωνούν απευθείας μαζί τους. Υπόσχονται ευκαιρίες εργασίας στο εξωτερικό ζητώντας από τα υποψήφια θύματα ένα ποσό για να εξασφαλίσουν τη θέση εργασίας και να καλύψουν τα έξοδα ταξιδιού ή τοποθέτησης. Τα θύματα συνειδητοποιούν ότι έχουν εξαπατηθεί μόνο όταν φτάνουν στη ξένη χώρα (Europol, 2020).

Τέλος, αξιόπιστα επιστημονικά στοιχεία σχετικά με τις τεχνικές έρευνας για τα πρότυπα επικοινωνίας είναι πολύ σπάνια (βλ. για παράδειγμα τον Χάρτη Evidence Gap Map της Διεθνούς Οργάνωσης Εργασίας, 2023, για πιθανές ενημερώσεις σχετικά με επιστημονικές μελέτες).

- **Παρακολούθηση γεωγραφικής θέσης**: Όπως και στην περίπτωση της κατανόησης των προτύπων επικοινωνίας, μπορεί να βοηθήσει στην κατανόηση της οπτικής γωνίας του δράστη. Συσκευές που επιτρέπουν την παρακολούθηση της γεωγραφικής θέσης θα μπορούσαν να έχουν χρησιμοποιηθεί για την παρακολούθηση θυμάτων σε πραγματικό χρόνο, π.χ. μέσω GPS, ενσωματωμένων καμερών σε smartphone, εφαρμογών κοινής χρήσης τοποθεσίας (Europol, 2020). Η δυνατότητα τηλεχειρισμού μειώνει τα όρια αναστολής των δραστών για εκμετάλλευση και επίσης περιπλέκει τις προσπάθειες ταυτοποίησης από τις αρχές επιβολής του νόμου σύμφωνα με τη Europol (2020, σ. 3):

  > [Ενώ] ιστορικά, οι οργανωμένες εγκληματικές ομάδες θα έπρεπε να ασκούν φυσικό έλεγχο και μονοπώλιο σε συγκεκριμένες γειτονιές της πόλης και γενικά θα αποτελούσαν ένα μεγάλο δίκτυο μελών, οι νεοεισερχόμενοι στον τομέα της εμπορίας ανθρώπων μπορούν πλέον να διαχειρίζονται αποτελεσματικά μια διαδικτυακή επιχείρηση χωρίς την ανάγκη φυσικής εγκληματικής υποδομής και με μειωμένο εργατικό δυναμικό. Επομένως, η γνώση της τεχνολογίας μπορεί να κάνει μια εγκληματική ομάδα πιο απειλητική, αλλά και λιγότερο αναγνωρίσιμη από τις αρχές επιβολής του νόμου.

  Περισσότερες πληροφορίες σχετικά με την παρακολούθηση της γεωγραφικής θέσης μπορείτε να βρείτε στην προηγούμενη Ενότητα 9.1.3.1.

- **Οικονομική ανάλυση**: Η οικονομική ανάλυση και η ψηφιακή εγκληματολογία μπορούν να συνδυαστούν, ιδίως σε σχέση με τις οικονομικές συναλλαγές που πραγματοποιούν οι διακινητές για να αναρτήσουν αγγελίες στο διαδίκτυο (Europol, 2020). Τα θύματα συχνά πραγματοποιούν τραπεζικές μεταφορές προς τους διακινητές. Στην Ενότητα 9.2 μπορείτε να βρείτε μια πιο λεπτομερή ανάλυση σχετικά με τα χρηματικά μέσα, τις οικονομικές συναλλαγές και τις οικονομικές έρευνες.
- **Ταυτοποίηση θυμάτων**: Για την ταυτοποίηση των θυμάτων, οι επιστήμονες και οι επαγγελματίες της ψηφιακής εγκληματολογίας μπορούν να εφαρμόσουν την αναγνώριση προσώπου για να τα εντοπίσουν, π.χ. σε διαφημίσεις ή αναρτήσεις στα μέσα κοινωνικής δικτύωσης. Πέραν αυτού, η αντίστροφη αναζήτηση εικόνων μπορεί να αποκαλύψει αν τα θύματα διαφημίζονταν σε ιστότοπους για ενήλικες ή σε πλατφόρμες της μαύρης αγοράς.
- **Ανάλυση του deep και dark web**: Η χρήση φόρουμ του σκοτεινού διαδικτύου δεν είναι ασυνήθιστη για τους διακινητές. Οι ερευνητές/-τριες μπορούν να χρησιμοποιήσουν εργαλεία ψηφιακής εγκληματολογίας TOR και παρακολούθησης του σκοτεινού διαδικτύου για να εντοπίσουν, για παράδειγμα, μηνύματα πρόσληψης, περιεχόμενο εκμετάλλευσης θυμάτων ή παράνομες συναλλαγές.

9.4.4.3Ψηφιακές εγκληματολογικές προσεγγίσεις και εργαλεία

Για την αποτελεσματική συλλογή και ανάλυση αποδεικτικών στοιχείων σε περιπτώσεις εμπορίας ανθρώπων και εργασιακής εκμετάλλευσης, η ψηφιακή εγκληματολογία βασίζεται σε μεγάλο βαθμό στα εξής:

- Εγκληματολογία φορητών συσκευών·
- Εγκληματολογία δικτύων και cloud·
- Ανάλυση χρηματοοικονομικών στοιχείων και κρυπτονομισμάτων·
- Έρευνες στο σκοτεινό διαδίκτυο.

Για να προχωρήσουμε χρονολογικά, ακολουθούν οι σχετικές αρχές της ψηφιακής εγκληματολογίας που πρέπει να ληφθούν υπόψη στην πράξη, επίσης στο πλαίσιο της εμπορίας ανθρώπων: Στην πρώτη φάση της αναγνώρισης και της διατήρησης, οι πρώτοι ανταποκριτές πρέπει να αναγνωρίσουν και να ασφαλίσουν άμεσα τις ψηφιακές συσκευές για να αποτρέψουν την παραποίηση ή την απώλεια δεδομένων (π.χ. απομόνωση από δίκτυα, UNODC, 2019b). Στη συνέχεια, για τη διαχείριση των ψηφιακών αποδεικτικών στοιχείων, είναι σημαντικό να καταγράφονται λεπτομερώς οι συνθήκες κάθε συσκευής, συμπεριλαμβανομένης της κατάστασης λειτουργίας (π.χ. ενεργοποιημένη, απενεργοποιημένη, σε κατάσταση αναμονής), του μοντέλου και τυχόν ορατών ζημιών. Οι φωτογραφίες και οι γραπτές σημειώσεις βοηθούν στη διατήρηση της αλυσίδας επιτήρησης και ενισχύουν την ακεραιότητα των αποδεικτικών στοιχείων (UNODC, 2019b). Η εξαγωγή δεδομένων μπορεί κατόπιν να πραγματοποιηθεί με εξειδικευμένα εργαλεία εγκληματολογικής ανάλυσης για την ανάκτηση δεδομένων χωρίς να αλλοιωθεί το αρχικό περιεχόμενο (βλ. Ενότητα 9.6.2 για μια γενική επισκόπηση). Σε ορισμένες συσκευές, αυτό μπορεί να συνεπάγεται την παράκαμψη χαρακτηριστικών ασφαλείας όπως η κρυπτογράφηση ή οι κωδικοί πρόσβασης. Ειδικά στο πλαίσιο της εμπορίας ανθρώπων/εργασιακής εκμετάλλευσης, οι αρχές επιβολής του νόμου χρησιμοποιούν εργαλεία ψηφιακής εγκληματολογικής ανάλυσης που διευκολύνουν τη διερεύνηση αυτού του εγκλήματος.

Στο παρόν έγγραφο, δεν είναι δυνατόν να παρασχεθεί μια πλήρης επισκόπηση των ψηφιακών εγκληματολογικών εργαλείων που θα μπορούσαν να χρησιμοποιηθούν και χρησιμοποιούνται στην επιβολή του νόμου, λόγω (1) της ποικιλομορφίας των εργαλείων που χρησιμοποιούν οι διάφορες αρχές επιβολής του νόμου σε όλη την Ευρώπη (λαμβάνοντας υπόψη την ψηφιακή εγκληματολογία στο σύνολό της και την ψηφιακή εγκληματολογία για τη διερεύνηση της εμπορίας ανθρώπων ως έναν κλάδο της), (2) της αλληλένδετης χρήσης διαφορετικών τεχνικών και εργαλείων που εξαρτώνται από την εκάστοτε περίπτωση, και (3) της μη δημόσιας πρόσβασης στον τρόπο με τον οποίο λειτουργούν οι αρχές επιβολής του νόμου σε αυτό το πλαίσιο, για να αναφέρουμε μόνο μερικούς από τους λόγους. Ωστόσο, μπορούν να παρουσιαστούν επιφανειακά ορισμένα ψηφιακά εργαλεία εγκληματολογικής ανάλυσης και εταιρείες που προσφέρουν λύσεις λογισμικού για τη διερεύνηση υποθέσεων εμπορίας ανθρώπων:

- **Cellebrite Pathfinder**: Εργαλείο εγκληματολογίας φορητών συσκευών που εξάγει, αναλύει και αποκωδικοποιεί δεδομένα από smartphone, tablet και πηγές cloud. Μπορεί να ανακτήσει διαγραμμένα μηνύματα, αρχεία κλήσεων και τοποθεσίες GPS.

  Πιθανή εφαρμογή σε περίπτωση εμπορίας ανθρώπων/εργασιακής εκμετάλλευσης:

  ➔ Εξάγει π.χ. μηνύματα WhatsApp, Telegram μεταξύ διακινητών και θυμάτων.

  ➔ Ανακτά διαγραμμένες συνομιλίες στις οποίες υποσχέθηκαν στα θύματα ψεύτικες θέσεις εργασίας.

  ➔ Αναγνωρίζει τοποθεσίες GPS από το τηλέφωνο του θύματος για να καταγράψει τα μοτίβα μετακίνησης.

- **MAGNET FORENSICS**: Η εταιρεία προσφέρει διάφορες λύσεις λογισμικού για τη δημόσια ασφάλεια, τον στρατό, τις υπηρεσίες πληροφοριών κ.λπ.

  Το MAGNET AXIOM σχετίζεται ιδιαίτερα με την εμπορία ανθρώπων: Το εργαλείο ειδικεύεται στην εγκληματολογία υπολογιστών και cloud αναλύοντας δεδομένα από σκληρούς δίσκους, social media, e-mail και κρυπτογραφημένα αρχεία.

  Πιθανή εφαρμογή σε περίπτωση εμπορίας ανθρώπων/εργασιακής εκμετάλλευσης:

  ➔ Ερευνά αναρτήσεις στα social media και δραστηριότητα σε ιστότοπους εύρεσης εργασίας στους οποίους οι διακινητές δημοσιεύουν ψεύτικες αγγελίες εργασίας.

  ➔ Εξάγει κρυφά αρχεία (π.χ. συμβόλαια θυμάτων, αεροπορικά εισιτήρια, άδειες εργασίας) από τους υπολογιστές των διακινητών.

  ➔ Αναλύει τα αρχεία καταγραφής επικοινωνιών μεταξύ πολλαπλών υπόπτων σε διαφορετικές χώρες.

  Το MAGNET OUTRIDER μπορεί επίσης να υποστηρίξει θετικά τη διαδικασία ψηφιακής εγκληματολογικής έρευνας, καθώς σαρώνει φορητές συσκευές iOS και Android και αποκαλύπτει, π.χ. παράνομες εφαρμογές, λίστα επαφών, μηνύματα SMS και εφαρμογές που χρησιμοποιήθηκαν πρόσφατα.

  Πιθανή εφαρμογή σε περίπτωση εμπορίας ανθρώπων/εργασιακής εκμετάλλευσης:

➔ Αποκαλύπτει κρυφές διαδικτυακές δραστηριότητες και εντοπίζει διακινητές που χρησιμοποιούν φόρουμ του dark web ή ψεύτικους λογαριασμούς στα social media.

➔ Μπορεί να ανιχνεύσει ψεύτικες συμβάσεις εργασίας, αγγελίες εργασίας και οικονομικά αρχεία.

Το MAGNET GRAYKEY, που ειδικεύεται στην παραβίαση κρυπτογραφημένων φορητών συσκευών, μπορεί και αυτό να συμβάλει στη διαδικασία ψηφιακής εγκληματολογικής έρευνας. Παρακάμπτει τα κλειδώματα οθόνης και εξάγει δεδομένα του συστήματος αρχείων.

Πιθανή εφαρμογή σε περίπτωση εμπορίας ανθρώπων/εργασιακής εκμετάλλευσης:

➔ Ξεκλειδώνει τα κατασχεμένα τηλέφωνα των διακινητών και βοηθά στην ανάκτηση συνομιλιών από WhatsApp, Telegram, Signal, Viber κ.λπ.

Υπάρχουν και άλλα λογισμικά MAGNET που μπορούν να φανούν εξίσου χρήσιμα σε αυτή τη διαδικασία (βλ. Pizzuro, 2022).

- MSAB XRY: Εργαλείο εγκληματολογίας φορητών συσκευών που χρησιμοποιείται από τις αρχές επιβολής του νόμου για την εξαγωγή, ανάλυση και αποκωδικοποίηση δεδομένων από κινητά τηλέφωνα, tablet, συσκευές GPS και drone.

Πιθανή εφαρμογή σε περίπτωση εμπορίας ανθρώπων/εργασιακής εκμετάλλευσης

➔ Εξάγει επικοινωνίες κινητών τηλεφώνων αποκαλύπτοντας ενδεχομένως ψηφιακά στοιχεία σχετικά με την εμπορία ανθρώπων.

➔ Αναλύει τα μέσα κοινωνικής δικτύωσης και τις πλατφόρμες εργασίας.

➔ Ανακτά διαγραμμένα αρχεία και φωτογραφίες.

- **Maltego**: Η εταιρεία προσφέρει εργαλεία που χρησιμοποιούνται για τη χαρτογράφηση σχέσεων μεταξύ ατόμων, εταιρειών, λογαριασμών κοινωνικών μέσων και ιστότοπων (GRAPH), για τη διεξαγωγή αναζητήσεων OSINT σε ύποπτους παραβάτες (SEARCH), την παρακολούθηση των κοινωνικών μέσων σε πραγματικό χρόνο (MONITOR) και τη διεξαγωγή ανάλυσης κοινωνικών δικτύων (EVIDENCE).

  Πιθανή εφαρμογή σε περίπτωση εμπορίας ανθρώπων/εργασιακής εκμετάλλευσης:

  ➔ Αποκαλύπτει ψεύτικους ιστότοπους πρόσληψης και τους συνδέει με γνωστούς διακινητές.

  ➔ Χαρτογραφεί τις συνδέσεις μεταξύ διαφορετικών προφίλ κοινωνικών μέσων που χρησιμοποιούνται για προσλήψεις.

  ➔ Εντοπίζει κρυπτογραφικά πορτοφόλια και χρηματοοικονομικές συναλλαγές που συνδέονται με εμπόρους ανθρώπων.

  https://www.maltego.com/blog/shining-a-light-empowering-ngos-during-national-human-trafficking-prevention-month/

- **Autopsy**: Ένα δωρεάν, ανοιχτού κώδικα ψηφιακό εργαλείο εγκληματολογικής ανάλυσης που προσφέρει μια πλατφόρμα για έρευνες σκληρών δίσκων.

  Πιθανή εφαρμογή σε περίπτωση εμπορίας ανθρώπων/εργασιακής εκμετάλλευσης:

  ➔ Ανακτά διαγραμμένες συμβάσεις εργασίας ή πλαστά έγγραφα βίζας.

➔ Εντοπίζει το ιστορικό του προγράμματος περιήγησης (π.χ. επισκέψεις σε πλαστούς ιστότοπους εργασίας ή κρυπτογραφημένες πλατφόρμες συνομιλίας).

➔ Εξάγει το ιστορικό συσκευών USB για να διαπιστώσει εάν χρησιμοποιήθηκαν εξωτερικοί σκληροί δίσκοι για την αποθήκευση, π.χ. δεδομένων θυμάτων.

- **ADF PRO**: Ένα λογισμικό ψηφιακής εγκληματολογίας και διαλογής που έχει σχεδιαστεί για γρήγορη ανάλυση υπολογιστών, εξωτερικών δίσκων και φορητών συσκευών.

  Πιθανή εφαρμογή σε περίπτωση εμπορίας ανθρώπων/εργασιακής εκμετάλλευσης:

  ➔ Ταχεία κατάσχεση ψηφιακών αποδεικτικών στοιχείων σε χώρους επιδρομών (π.χ. σάρωση των μέσων κοινωνικής δικτύωσης, των φορητών υπολογιστών και των τηλεφώνων των υπόπτων).

  ➔ Αναγνώριση προσώπου: γρήγορη αναγνώριση και αντιστοίχιση προσώπων σε εικόνες και βίντεο (εφαρμόζεται για την αναγνώριση θυμάτων και δραστών).

- **Εργαλεία ανάλυσης blockchain** (π.χ. από Chainalysis, Elliptic, CipherTrace)

  Αυτά τα εργαλεία ειδικεύονται στην παρακολούθηση συναλλαγών κρυπτονομισμάτων, που συχνά χρησιμοποιούνται από τους διακινητές για να λάβουν πληρωμές για αμοιβές πρόσληψης ή εκμετάλλευση θυμάτων.

  Πιθανή εφαρμογή σε περίπτωση εμπορίας ανθρώπων/εργασιακής εκμετάλλευσης:

- ➔ Εντοπίζει συναλλαγές Bitcoin ή κρυπτονομισμάτων που πραγματοποιούνται από τα θύματα προς τους εκμεταλλευτές που τα προσλαμβάνουν.
- ➔ Συνδέει διευθύνσεις πορτοφολιών με γνωστά δίκτυα εμπορίας ανθρώπων.
- ➔ Εντοπίζει τεχνικές νομιμοποίησης εσόδων από παράνομες δραστηριότητες που χρησιμοποιούνται για την απόκρυψη παράνομων κερδών.

Σε ό,τι αφορά τις διαδικασίες ψηφιακής εγκληματολογίας για την καταπολέμηση της εμπορίας ανθρώπων, εισάγονται και περιγράφονται εν συντομία δύο ακόμη πιθανές προσεγγίσεις. Σε ορισμένο βαθμό, μπορεί επίσης να επικαλύπτονται με τα ήδη περιγραφέντα εργαλεία ή κλάδους της ψηφιακής εγκληματολογίας.

Η πρώτη είναι η προσέγγιση της χρήσης μεταδεδομένων από εικόνες και βίντεο στην εμπορία ανθρώπων για (ψηφιακές) εγκληματολογικές έρευνες. Αντί να βασίζονται αποκλειστικά σε υπολογιστικά δαπανηρές τεχνικές υπολογιστικής όρασης, τα μεταδεδομένα εικόνων και βίντεο θα μπορούσαν να βοηθήσουν τις αρχές επιβολής του νόμου στην ταυτοποίηση των θυμάτων και των διακινητών (Mattmann et al., 2016). Η εμπορία ανθρώπων συχνά περιέχει κειμενικά σημάδια, όπως τα φυσικά χαρακτηριστικά του θύματος, την τοποθεσία και στοιχεία πολυμέσων (δηλ. εικόνες, βίντεο σε διαφορετικές πλατφόρμες). Οι Mattmann et al. (2016) ανέπτυξαν ένα εργαλείο ψηφιακής εγκληματολογίας μεταδεδομένων για πολυμέσα, που περιλαμβάνει το ImageCat (κατάλογος εικόνων) και το ImageSpace. Το ImageCat είναι ένα σύστημα εξαγωγής, μετασχηματισμού και φόρτωσης (ETL) που έχει σχεδιαστεί για την επεξεργασία και την καταλογογράφηση μεταδεδομένων πολυμέσων, ιδίως στον τομέα των ερευνών για την εμπορία ανθρώπων. Μπορεί να συνδέσει πολλαπλές διαφημίσεις με κοινά μεταδεδομένα (π.χ. ίδια κάμερα που χρησιμοποιείται για διαφορετικά θύματα, ανάλυση ομοιότητας) και επιτρέπει τη γρήγορη αναζήτηση και

ανάκτηση αποδεικτικών στοιχείων πολυμέσων. Ως εκ τούτου, μπορεί να βοηθήσει τις αρχές επιβολής του νόμου να ταυτοποιήσουν τόσο τα θύματα όσο και τους διακινητές (Mattmann et al., 2016). Επιπλέον, το ImageSpace (που βασίζεται στο ImageCat) εξάγει μεταδεδομένα πολυμέσων (δηλ. χρωματικό χώρο RGB, μοντέλο κάμερας, γεωγραφική θέση, χρονικές σημάνσεις). Μπορεί να αναζητήσει και να υποβάλει ερωτήματα σε μεγάλες βάσεις δεδομένων πολυμέσων επιτρέποντας στις αρχές επιβολής του νόμου να αναζητήσουν εικόνες και βίντεο χρησιμοποιώντας κείμενο, μεταδεδομένα ή ομοιότητα εικόνων. Επιπρόσθετα, η διαδραστική περιήγηση και οπτικοποίηση εικόνων βοηθά τις αρχές επιβολής του νόμου να εμφανίσουν αυτά τα αποδεικτικά στοιχεία σε μια οργανωμένη γκαλερί για εγκληματολογική εξέταση και παρέχει διαδραστικά ιστογράμματα και διαγράμματα πυκνότητας. Το ImageSpace επιτρέπει συν τοις άλλοις την αντιστοίχιση ομοιότητας μεταξύ εικόνων και βίντεο για την ομαδοποίηση σχετικών αρχείων βοηθώντας τους/τις ερευνητές/-τριες να εντοπίζουν, για παράδειγμα, θύματα σε διαφορετικές διαφημίσεις και πλατφόρμες. Παράλληλα, μπορεί να βελτιστοποιήσει τα αποτελέσματα αναζήτησης με την πάροδο του χρόνου και υποστηρίζει την οπτική αναγνώριση χαρακτήρων και την εξαγωγή κειμένου (δηλ. εξαγωγή αριθμών τηλεφώνου, διευθύνσεων ηλεκτρονικού ταχυδρομείου, διευθύνσεων) από τις εικόνες και τα βίντεο. Αυτή η συγκεκριμένη προσέγγιση πολυμέσων παρέχει μια εναλλακτική μέθοδο για τη σύνδεση διαφημίσεων, θυμάτων και διακινητών μέσω της ανάλυσης προτύπων μεταδεδομένων αντί του περιεχομένου εικόνων ή βίντεο μόνο.

Μια άλλη προσέγγιση που ενσωματώνεται εν μέρει στα εργαλεία που παρουσιάστηκαν προηγουμένως και αντικατοπτρίζεται σε πολλές από τις μέχρι τώρα επεξεργασίες σχετικά με τις έρευνες εμπορίας ανθρώπων και την ψηφιακή εγκληματολογία είναι η έρευνα ανοιχτού κώδικα (Open-Source INTelligence-OSINT). Η

έρευνα OSINT αναφέρεται στη συλλογή και ανάλυση δημόσια διαθέσιμων δεδομένων για την υποστήριξη ερευνών. Διαδραματίζει κρίσιμο ρόλο στην ψηφιακή εγκληματολογία για τις έρευνες εμπορίας ανθρώπων εντοπίζοντας μοτίβα, παρακολουθώντας ψηφιακά ίχνη και συνδέοντας υπόπτους με εγκληματικές δραστηριότητες. Δεδομένου ότι τα ιδιαίτερα χρήσιμα στοιχεία OSINT έχουν ήδη αναφερθεί, αυτή η σύντομη ενότητα σχετικά με αυτό το θέμα έχει ως σκοπό μόνο να περιγράψει τη σημασία και τις μεγάλες δυνατότητές του. Το OSINT είναι απαραίτητο για τον εντοπισμό προτύπων πρόσληψης και επικοινωνίας, διότι βοηθά στην αποκάλυψη βασικών πλατφορμών, γλωσσικών προτύπων και στρατηγικών πρόσληψης που χρησιμοποιούνται σε ενεργητικές («κυνήγι») και παθητικές («ψάρεμα») μεθόδους πρόσληψης. Το OSINT, το οποίο μπορεί να χωριστεί σε πληροφορίες από τα μέσα κοινωνικής δικτύωσης (SOCMINT), γεωχωρικές πληροφορίες (GEOINT) και ανθρώπινες πληροφορίες (HUMINT), περιλαμβάνει, μεταξύ άλλων, την παρακολούθηση των μέσων κοινωνικής δικτύωσης και των αγγελιών εργασίας, την ανάλυση συζητήσεων σε φόρουμ, τις δραστηριότητες στο σκοτεινό διαδίκτυο και την αντίστροφη αναζήτηση εικόνων και βίντεο. Χρησιμεύει στη σύνδεση των διαδικτυακών αγγελιών με τα δίκτυα εμπορίας ανθρώπων μέσω της ανίχνευσης και ανάλυσης αγγελιών εργασίας, της παρακολούθησης κρυπτονομισμάτων και πληρωμών, καθώς και της ανάλυσης τομέων και ιστότοπων. Μπορεί να είναι σημαντικό για τον εντοπισμό της γεωγραφικής θέσης των θυμάτων και των διακινητών μέσω της ανάλυσης εικόνων και βίντεο (και των μεταδεδομένων τους) ή της χρήσης γεωγραφικού εντοπισμού μέσω crowdsourcing (π.χ. Google Street View, δορυφορικές εικόνες). Επιπλέον, το OSINT μπορεί να βοηθήσει στην αποκάλυψη ψεύτικων ταυτοτήτων και δικτύων μέσω της ανάλυσης δεδομένων κοινωνικών μέσων (ή και του dark web) με τη μέθοδο της αντεπισκόπησης (cross-referencing), της ανάλυσης ψηφιακών αποτυπωμάτων και του ελέγχου προσωπικών δεδομένων (βλ.

π.χ. https://epieos.com/ για την αντίστροφη αναζήτηση εάν μια διεύθυνση ηλεκτρονικού ταχυδρομείου ή ένας αριθμός τηλεφώνου συνδέεται με συγκεκριμένους λογαριασμούς, όπως ένας λογαριασμός Google) ή μέσω ανάλυσης συμπεριφοράς (π.χ. συμπεριφορές δημοσίευσης, γλωσσικά μοτίβα, χρονισμός των διαδικτυακών δραστηριοτήτων).

9.4.4.4Προκλήσεις στις ψηφιακές εγκληματολογικές έρευνες

Η διερεύνηση υποθέσεων εμπορίας ανθρώπων παρουσιάζει μοναδικά εμπόδια για την ψηφιακή εγκληματολογία, όπως:

- Κρυπτογραφημένη και αυτοκαταστρεφόμενη επικοινωνία.
- Διαγραφή και απόκρυψη δεδομένων.
- Διασυνοριακά ζητήματα δεδομένων.
- Προστασία των θυμάτων και προσωπικού απορρήτου.

Για να γίνει μια πιο συστηματική επισκόπηση των προκλήσεων, μπορεί κανείς να τις χωρίσει σε προκλήσεις που σχετίζονται με το αντικείμενο και σε δομικές προκλήσεις.

Προκλήσεις που σχετίζονται με το αντικείμενο

Οι προκλήσεις που σχετίζονται με το αντικείμενο είναι προκλήσεις που προκύπτουν από το θέμα της ψηφιακής εγκληματολογίας και των ερευνών για την εμπορία ανθρώπων. Ως εκ τούτου, είναι εγγενείς στο ίδιο το έγκλημα. Για παράδειγμα, μπορεί να γίνει διάκριση μεταξύ προληπτικών και αντιδραστικών ερευνών. Οι **προληπτικές έρευνες** είναι πολύ πιο περίπλοκες στην έναρξή τους, επειδή οι αρχές

επιβολής του νόμου πρέπει να εντοπίσουν σημάδια εκμετάλλευσης που θα μπορούσαν να υποδηλώνουν εκμετάλλευση. Είναι δύσκολο να φιλτραριστούν αυτές οι αναφορές από τον μεγάλο αριθμό διαθέσιμων διαδικτυακών διαφημίσεων, για παράδειγμα (Europol, 2020). Ως εκ τούτου, «οι **αντιδραστικές έρευνες** είναι ευκολότερες, επειδή έχουν ένα σημείο εκκίνησης, όπως η κατάθεση ενός αναγνωρισμένου θύματος ή/και ο λογαριασμός ή ο ιστότοπος που χρησιμοποιείται για σκοπούς πρόσληψης ή εκμετάλλευσης» (Europol, 2020, σ. 5).

Ακόμη, τα ψηφιακά αποδεικτικά στοιχεία με τα οποία ασχολούνται κυρίως οι ερευνητές/-τριες σε περιπτώσεις εμπορίας ανθρώπων, δημιουργούν προκλήσεις. Επειδή πολλοί διακινητές χρησιμοποιούν εφαρμογές άμεσων μηνυμάτων όπως το WhatsApp, το Signal ή το Telegram, η ενσωματωμένη κρυπτογράφηση από άκρο σε άκρο (E2EE) δυσχεραίνει την ανάκτηση των μηνυμάτων. Αξίζει μεταξύ άλλων να σημειωθεί ότι οι διακινητές διαγράφουν συχνά τα ψηφιακά αποδεικτικά στοιχεία (οι ίδιοι ή χρησιμοποιούν λειτουργίες αυτόματης διαγραφής, π.χ. στις συνομιλίες WhatsApp). Η πρόσβαση στα διαγραμμένα δεδομένα είναι περιορισμένη και οι ερευνητές/-τριες μπορούν μόνο να προσπαθήσουν να έχουν πρόσβαση σε αντίγραφα ασφαλείας που έχουν δημιουργηθεί στο παρελθόν. Επιπλέον, οι διακινητές ενδέχεται να λειτουργούν σε κρυφές υπηρεσίες Tor (dark web, χρήση VPN), καθιστώντας δύσκολη την παρακολούθηση. Εκτός από αυτό, οι διακινητές προσπαθούν να συγκαλύψουν τα ίχνη τους με μια ακραία διαφοροποίηση της ψηφιακής τους παρουσίας, για παράδειγμα χρησιμοποιώντας πολλές κάρτες SIM και κινητά τηλέφωνα, διάφορους λογαριασμούς (συμπεριλαμβανομένων ψεύτικων λογαριασμών) κ.λπ. Αυτή η δυσκολία αποτελεί παράδειγμα μιας άλλης πρόκλησης: ο/η ερευνητής/-τρια που ασχολείται με την υπόθεση πρέπει συχνά να επεξεργαστεί έναν τεράστιο όγκο δεδομένων (ειδικά ψηφιακών), να εξετάσει αυτά τα δεδομένα, να τα

κατηγοριοποιήσει ως σχετικά ή άσχετα με το έγκλημα ή τα εγκλήματα για τα οποία θα απαγγελθούν κατηγορίες, να διατηρήσει μια συνολική εικόνα και να σχεδιάσει περαιτέρω στρατηγικά βήματα. Αναφορικά με αυτή την πρόκληση υπάρχει και μια άλλη νομική πτυχή που μπορεί να γίνει προβληματική: μια υπόθεση μπορεί να γίνει εξαιρετικά περίπλοκη, καθώς συχνά δεν μπορεί να απαγγελθεί κατηγορία μόνο για εμπορία ανθρώπων/εκμετάλλευση εργατικού δυναμικού, αλλά και, για παράδειγμα, για φοροδιαφυγή, παραβιάσεις του εργατικού δικαίου και των υποχρεώσεων κοινωνικής ασφάλισης, καταναγκαστική εργασία, επίθεση, απάτη, πλαστογράφηση εγγράφων ή παραβιάσεις των ανθρωπίνων δικαιωμάτων. Αυτό μπορεί επίσης να επηρεάσει την ψηφιακή εγκληματολογία, για παράδειγμα, διότι μια πιο περίπλοκη υπόθεση απαιτεί περισσότερη και συνεπή ανταλλαγή πληροφοριών μεταξύ του/της επικεφαλής ανακριτή/-τριας της υπόθεσης και του/της ειδικού ψηφιακής εγκληματολογίας.

Δομικές προκλήσεις

Οι προκλήσεις μπορούν να θεωρηθούν δομικές όταν προκύπτουν από το σύστημα (π.χ. από την οργάνωση της επιβολής του νόμου σε μια χώρα, τις νομοθετικές συνθήκες). Για παράδειγμα, οι ψηφιακές τεχνολογίες που εφαρμόζουν οι διακινητές εξελίσσονται συνεχώς. Για τον λόγο αυτό, οι αρχές επιβολής του νόμου πρέπει να προσαρμοστούν στις (πιο πρόσφατες) τεχνικές εξελίξεις που εφαρμόζουν οι δράστες (Europol, 2020). Παράλληλα, οι αρχές επιβολής του νόμου πρέπει να διαθέτουν τους κατάλληλους ανθρώπινους πόρους για αυτές τις έρευνες. Αυτό δεν ισχύει μόνο για τους ανθρώπινους πόρους των εξειδικευμένων ερευνητών/-τριών εμπορίας ανθρώπων και των επιστημόνων και επαγγελματιών ψηφιακής εγκληματολογίας, αλλά και για άλλο προσωπικό που απαιτείται επειγόντως για τη διερεύνηση τέτοιων υποθέσεων, όπως διερμηνείς (π.χ. για τη μετάφραση δεδομένων τηλεπικοινωνιακής

παρακολούθησης). Ομοίως, τα νομοθετικά μέσα πρέπει να βελτιωθούν για να διασφαλιστεί η δίωξη και η καταδίκη (Europol, 2020).

Η επέκταση των νομοθετικών δυνατοτήτων είναι ιδιαίτερα σημαντική, διότι τα θύματα συχνά διστάζουν να κάνουν σημαντικές ομολογίες και δηλώσεις, καθώς βρίσκονται ήδη υπό μεγάλη ψυχολογική πίεση – απειλές, εκβιασμούς, καθώς και τον εγγενή κίνδυνο δημόσιας ταπείνωσης μέσω των social media (π.χ. με τη δημοσιοποίηση της εκμετάλλευσής τους). Η ευκολότερη πρόσβαση σε διαθέσιμα σύνολα δεδομένων για ψηφιακή εγκληματολογία είναι επομένως σημαντική σε αυτό το πλαίσιο, προκειμένου να προωθηθούν οι έρευνες και, τελικά, να υποστηριχθεί ή ακόμη και να καταστεί δυνατή η ποινική δίωξη (Europol, 2020).

Σε ό,τι αφορά τα νομικά ζητήματα, πρέπει να επισημανθεί ότι οι προσπάθειες διασυνοριακής συνεργασίας μπορούν να επιδεινωθούν, εάν η δικαστική συνεργασία και οι ισχύοντες κανόνες δεν αποσαφηνιστούν. Αυτό μπορεί να εμποδίσει, για παράδειγμα, την ανταλλαγή αποδεικτικών στοιχείων μεταξύ χωρών. Λόγω της έλλειψης τυποποιημένης διεθνούς συνεργασίας, δεν υπάρχει προς το παρόν κεντρική παγκόσμια βάση δεδομένων για την καταπολέμηση της διακίνησης ανθρώπων, η οποία να παρακολουθεί τις διαδικτυακές δραστηριότητες των διακινητών σε παγκόσμιο επίπεδο.

9.4.4.5Νομικές και ηθικές πτυχές

Λόγω της ευαίσθητης φύσης των υποθέσεων εμπορίας ανθρώπων, οι εγκληματολογικές έρευνες πρέπει να τηρούν αυστηρά ηθικά και νομικά πρότυπα, ορισμένα από τα οποία έχουν ήδη παρουσιαστεί προηγουμένως. Με την ενσωμάτωση αυτών των παραμέτρων, οι επαγγελματίες της ψηφιακής εγκληματολογίας μπορούν

να πλοηγηθούν στο περίπλοκο τοπίο των ερευνών για την εμπορία ανθρώπων και την εργασιακή εκμετάλλευση με ηθικό, νόμιμο και αποτελεσματικό τρόπο διασφαλίζοντας ότι η επιδίωξη της δικαιοσύνης συνάδει με την προστασία των ατομικών δικαιωμάτων και των κοινωνικών αξιών.

Προσέγγιση με επίκεντρο το θύμα

Μια προσέγγιση που επικεντρώνεται στο θύμα δίνει προτεραιότητα στα δικαιώματα, τις ανάγκες και την ευημερία των θυμάτων καθ' όλη τη διάρκεια της ερευνητικής διαδικασίας. Αυτή η μεθοδολογία δίνει έμφαση στη μεταχείριση των θυμάτων με σεβασμό και ευαισθησία διασφαλίζοντας ότι ενημερώνονται και υποστηρίζονται, και συμμετέχουν ενεργά στις αποφάσεις που επηρεάζουν τη ζωή τους. Οι ερευνητές/-τριες εστιάζοντας στην εμπειρία του θύματος μπορούν να χτίσουν μια σχέση εμπιστοσύνης, η οποία είναι ζωτικής σημασίας όχι μόνο για τη συλλογή ακριβών πληροφοριών, αλλά και για την παροχή κατάλληλων υπηρεσιών υποστήριξης στο θύμα. Η εν λόγω προσέγγιση όχι μόνο βοηθά στην ανάκαμψη των θυμάτων, αλλά και ενισχύει τη συνολική ακεραιότητα της έρευνας (International Labour Organization, 2018). «Η ασφάλεια των θυμάτων και των οικογενειών και των αγαπημένων τους προσώπων είναι πάντα πρωταρχικής σημασίας και αποτελεί ευθύνη του ανακριτή και του εισαγγελέα» (International Labour Organization, 2018, σ. 47). Αυτό υπογραμμίζει μεταξύ άλλων την ανάγκη να εστιάζουμε όχι μόνο στο θύμα ως άτομο, αλλά και στις οικογένειες ή στους/στις συγγενείς τους, καθώς η πιθανότητα για αντίποινα εναντίον μελών της οικογένειας από τους διακινητές είναι μεγάλη (International Labour Organization, 2018).

Ειδικά όσον αφορά την ψηφιακή εγκληματολογία, συνιστάται να ελαχιστοποιείται η παρεμβατική ψηφιακή παρακολούθηση εστιάζοντας σε αυτό το θέμα στους

διακινητές και όχι στα θύματα. Η εμπιστευτικότητα των δεδομένων των θυμάτων πρέπει να διασφαλίζεται ανά πάσα στιγμή, προκειμένου να αποφεύγονται αντίποινα ή η δημόσια έκθεση. Ο/Η ανακριτής/-τρια θα πρέπει να αποφεύγει να πιέζει τα θύματα να επαναλαμβάνουν πολλές φορές τις ψηφιακές αλληλεπιδράσεις τους (και να χρησιμοποιεί αντίθετα εργαλεία εγκληματολογίας) και να σέβεται τη συγκατάθεση του θύματος πριν αποκτήσει πρόσβαση σε προσωπικές συσκευές. Συνεχίζοντας, θα πρέπει να αποφεύγονται οι επιθετικές τεχνικές ανάκρισης που βασίζονται σε ψηφιακά ευρήματα (π.χ. η αντιπαράθεση του θύματος με τα αρχεία καταγραφής των συνομιλιών του με τρόπο που προκαλεί άγχος). Μια άλλη σημαντική πρόκληση στη δίωξη των διακινητών μπορεί να είναι η εξάρτηση από την κατάθεση του θύματος, η οποία μπορεί να είναι τραυματική για το θύμα, αλλά και ενδεχομένως αναξιόπιστη λόγω, για παράδειγμα, του φόβου. Από αυτή την άποψη, η ψηφιακή εγκληματολογία μπορεί να ενισχύσει τις υποθέσεις και να μειώσει την εξάρτηση από τα θύματα στο δικαστήριο, γεγονός που, με τη σειρά του, μπορεί να μειώσει το βάρος για τα θύματα. Οι εμπειρογνώμονες ψηφιακής εγκληματολογίας μπορούν να αποτρέψουν την εκδίκηση και την εκ νέου εμπορία των θυμάτων σαρώνοντας τις συσκευές τους, εάν συμφωνηθεί/είναι επιθυμητό, για spyware και αφαιρώντας στη συνέχεια τα εργαλεία παρακολούθησης.

Προστασία δεδομένων

Κατά τη διάρκεια της διαδικασίας έρευνας: Η προστασία των ατόμων που αποκαλύπτουν δραστηριότητες εμπορίας ανθρώπων είναι μείζονος σημασίας για την ενθάρρυνση της αναφοράς εγκλημάτων. Επίσης, η προστασία των μαρτύρων δημοσίου συμφέροντος διασφαλίζει ότι όσα άτομα υποβάλλουν καταγγελία δεν θα υποστούν αντίποινα, γεγονός που δημιουργεί ένα περιβάλλον στο οποίο οι πληροφορίες μπορούν να κοινοποιούνται με

ασφάλεια. Παράλληλα, η ηθική αναφορά από τα μέσα ενημέρωσης και τις αρχές διασφαλίζει ότι τα θύματα δεν θα υποστούν εκ νέου θυματοποίηση μέσω της έκθεσής τους και ότι οι πληροφορίες που διαδίδονται εξυπηρετούν το δημόσιο συμφέρον χωρίς να προκαλούν βλάβη.

Το UNODC συνέταξε μια επισκόπηση της προστασίας του απορρήτου και των δεδομένων στην Ενότητα 10 σχετικά με την Προστασία του Απορρήτου και των Δεδομένων που πρέπει να λαμβάνεται υπόψη για θέματα που σχετίζονται με τον κυβερνοχώρο.

- **Κατάσχεση αποδεικτικών στοιχείων:** Η διασφάλιση της ακεραιότητας και της εμπιστευτικότητας των ψηφιακών αποδεικτικών στοιχείων είναι καίριας σημασίας. Θα πρέπει να υπάρχουν κατάλληλα μέτρα προστασίας των δεδομένων για την αποτροπή της μη εξουσιοδοτημένης πρόσβασης, της παραποίησης ή της απώλειας αποδεικτικών στοιχείων. Η διατήρηση μιας σαφούς αλυσίδας φύλαξης των αποδεικτικών στοιχείων είναι απαραίτητη για την παραδεκτότητα των αποδεικτικών στοιχείων στο δικαστήριο, καθώς τεκμηριώνει τον χειρισμό των αποδεικτικών στοιχείων από τη συλλογή έως την παρουσίασή τους. Η τήρηση των νομικών προτύπων και πρωτοκόλλων προστατεύει τα δικαιώματα όλων των εμπλεκόμενων μερών και διαφυλάσσει την αξιοπιστία της διαδικασίας έρευνας.

Διεθνής συνεργασία

Η εμπορία ανθρώπων και η εργασιακή εκμετάλλευση είναι συχνά διακρατικά εγκλήματα που απαιτούν διασυνοριακή συνεργασία. Η διεθνής συνεργασία περιλαμβάνει την εναρμόνιση των νομικών πλαισίων, την ανταλλαγή πληροφοριών και τον συντονισμό των προσπαθειών μεταξύ των διαφόρων δικαιοδοσιών. Αυτή η

συλλογική προσέγγιση ενισχύει την ικανότητα εντοπισμού των δραστών, προστασίας των θυμάτων και αποτελεσματικής εξάρθρωσης των δικτύων εμπορίας ανθρώπων. Η Ενότητα 11 – Διεθνής Συνεργασία για την Καταπολέμηση του Διακρατικού Οργανωμένου Εγκλήματος του UNODC μπορεί να βοηθήσει στην κατανόηση των νομικών δυνατοτήτων σε αυτό το θέμα.

Αναλογικότητα και αναγκαιότητα

Οι έρευνες πρέπει να εξισορροπούν την ανάγκη για πληροφορίες με τον σεβασμό της ιδιωτικής ζωής των ατόμων. Η συλλογή ψηφιακών αποδεικτικών στοιχείων πρέπει να είναι ανάλογη με τη σοβαρότητα του εγκλήματος και απαραίτητη για την έρευνα. Αυτή η αρχή διασφαλίζει ότι τα ερευνητικά μέτρα δεν υπερβαίνουν τα όρια ή παραβιάζουν τα θεμελιώδη δικαιώματα διατηρώντας τα ηθικά πρότυπα κατά την επιδίωξη της δικαιοσύνης.

Ενσωμάτωση της Τεχνητής Νοημοσύνης

Η ενσωμάτωση της Τεχνητής Νοημοσύνης στην ψηφιακή εγκληματολογία προσφέρει αποτελεσματικότητα, αλλά εγείρει επίσης ανησυχίες σχετικά με την ακρίβεια και τη μεροληψία. Τα αυτοματοποιημένα εργαλεία πρέπει να σχεδιάζονται προσεκτικά και να αξιολογούνται τακτικά προκειμένου να αποφεύγονται μεροληψίες που θα μπορούσαν να οδηγήσουν σε αδικαιολόγητες κατηγορίες ή να παραβλέψουν ορισμένα προφίλ θυμάτων. Η ανθρώπινη εποπτεία παραμένει ζωτικής σημασίας για την ερμηνεία των δεδομένων που παράγονται από την Τεχνητή Νοημοσύνη στο κατάλληλο νομικό και ηθικό πλαίσιο. Ειδικά σε σχετικά ή ακόμη και κρίσιμα σημεία της ερευνητικής διαδικασίας, η χρήση της Τεχνητής Νοημοσύνης δεν πρέπει να αντικαθιστά την ανθρώπινη κρίση.

Ηθική χρήση του OSINT και παρακολούθηση του σκοτεινού ιστού

Αν και το OSINT και η παρακολούθηση του dark web είναι πολύτιμες για την αποκάλυψη παράνομων δραστηριοτήτων, πρέπει να διεξάγονται εντός των νομικών ορίων. Οι ερευνητές/-τριες πρέπει να αποφεύγουν τη μη εξουσιοδοτημένη πρόσβαση ή τις παραπλανητικές πρακτικές που θα μπορούσαν να θέσουν σε κίνδυνο την ακεραιότητα της έρευνας ή να παραβιάσουν τα ηθικά πρότυπα. Ο σεβασμός της ιδιωτικής ζωής και η νόμιμη απόκτηση πληροφοριών είναι θεμελιώδεις για τη διατήρηση της εμπιστοσύνης του κοινού και την τήρηση του κράτους δικαίου.

9.5 Οικονομικές έρευνες

Οι χρηματοοικονομικές έρευνες είναι ένα ουσιαστικό εργαλείο για την καταπολέμηση των χρηματοοικονομικών εγκλημάτων, όπως το ξέπλυμα χρήματος (ML), η χρηματοδότηση της τρομοκρατίας (TF) και η εμπορία ανθρώπων. Αυτές οι έρευνες επικεντρώνονται στην ανάλυση χρηματοοικονομικών συναλλαγών για τον εντοπισμό παράνομων δραστηριοτήτων, την ανίχνευση παράνομων κεφαλαίων και την ταυτοποίηση των δραστών και των δικτύων τους. Οι βασικές έννοιες και οι στόχοι των χρηματοοικονομικών ερευνών περιστρέφονται γύρω από την **παρακολούθηση της διαδρομής των χρημάτων** για την αποκάλυψη και την τεκμηρίωση των χρηματοοικονομικών εγκλημάτων. Οι πρωταρχικοί στόχοι περιλαμβάνουν τον εντοπισμό εγκληματικών δικτύων, την ανίχνευση παράνομων κεφαλαίων και τη συλλογή αποδεικτικών στοιχείων που μπορούν να χρησιμοποιηθούν σε ποινικές διώξεις. Μια άρτια διεξαχθείσα χρηματοοικονομική έρευνα ενισχύει τις προσπάθειες επιβολής του νόμου στερώντας από τους εγκληματίες τους οικονομικούς τους

πόρους και διαλύοντας την οικονομική υποδομή που υποστηρίζει το οργανωμένο έγκλημα.

Η σημασία των χρηματοοικονομικών αναλύσεων στο πλαίσιο της **εμπορίας ανθρώπων** είναι ιδιαίτερα σημαντική, καθώς οι διακινητές εξαρτώνται από τις χρηματοοικονομικές συναλλαγές για τη μεταφορά, την αποθήκευση και το ξέπλυμα των παράνομων εσόδων τους. Με την εξέταση των αρχείων συναλλαγών, των τραπεζικών καταστάσεων και των ψηφιακών μεθόδων πληρωμής , οι ερευνητές/-τριες μπορούν να αποκαλύψουν τις χρηματοοικονομικές συνδέσεις μεταξύ των διακινητών και των συνεργατών τους. Αυτό όχι μόνο βοηθά στη δίωξη των εγκληματιών, αλλά και στην ταυτοποίηση των θυμάτων μέσω της ανίχνευσης χρηματοοικονομικών προτύπων που υποδηλώνουν εκμετάλλευση. Συνεπώς, οι χρηματοοικονομικές έρευνες διαδραματίζουν καθοριστικό ρόλο στην εξάρθρωση των δικτύων εμπορίας ανθρώπων στοχεύοντας στις χρηματοοικονομικές πηγές που τα συντηρούν. «Ωστόσο, η ευρεία αναγνώριση, εφαρμογή και εναρμόνιση των ερευνητικών στρατηγικών και τακτικών που στοχεύουν ειδικά στις χρηματοοικονομικές πηγές της εμπορίας ανθρώπων εξακολουθεί να αποτελεί έργο σε εξέλιξη» (OSCE, 2019, σ. 37).

Η Ενότητα 9.7.1 περιγράφει τις βασικές αρχές της χρηματοοικονομικής έρευνας, ακολουθούμενη από μια εισαγωγή στις επιχειρηματικές δομές της εμπορίας ανθρώπων, προκειμένου να τονιστεί η σημασία της χρηματοοικονομικής έρευνας στο θέμα της εμπορίας ανθρώπων και της εργασιακής εκμετάλλευσης (Ενότητα 9.7.2). Η Ενότητα 9.7.3 περιγράφει βήμα προς βήμα τον τρόπο διεξαγωγής μιας χρηματοοικονομικής έρευνας σε υποθέσεις εμπορίας ανθρώπων. Η Ενότητα 9.7.4 παρουσιάζει δείκτες συναλλαγών που υποδηλώνουν ύποπτες χρηματοοικονομικές δραστηριότητες στον τομέα της εμπορίας ανθρώπων και ιδίως της εργασιακής

εκμετάλλευσης. Η Ενότητα 9.7.5 περιγράφει τις προκλήσεις στις χρηματοοικονομικές έρευνες, ενώ η Ενότητα 9.7.6 εξετάζει τις τεχνικές καινοτομίες και τάσεις. Η Ενότητα 9.7.7 ολοκληρώνεται με ορισμένες πρόσθετες συστάσεις.

Επισκόπηση

9.5.1 Οι χρηματοοικονομικές έρευνες διαδραματίζουν κρίσιμο ρόλο στην επιβολή του νόμου και τη δίωξη, ιδίως σε υποθέσεις που αφορούν νομιμοποίηση εσόδων από παράνομες δραστηριότητες, χρηματοδότηση της τρομοκρατίας και οργανωμένο έγκλημα (FATF, 2012). Οι Οδηγίες της Ομάδας Χρηματοοικονομικής Δράσης (FATF) για τις Χρηματοοικονομικές Έρευνες περιγράφουν τις βασικές αρχές, τα εργαλεία και τις στρατηγικές που είναι απαραίτητα για τη διεξαγωγή αποτελεσματικών χρηματοοικονομικών ερευνών. Ο πρωταρχικός στόχος μιας χρηματοοικονομικής έρευνας είναι **να εντοπίσει και να τεκμηριώσει την κίνηση παράνομων κεφαλαίων** συμβάλλοντας στον εντοπισμό εγκληματικών δικτύων, στην αποκάλυψη χρηματοοικονομικών δομών και στη δημιουργία ισχυρών νομικών υποθέσεων (FATF, 2012). Οι ερευνητές/-τριες εξετάζοντας τις χρηματοοικονομικές πτυχές των εγκληματικών δραστηριοτήτων μπορούν να ανακαλύψουν νέες πληροφορίες, να χαρτογραφήσουν ολόκληρα δίκτυα εγκληματικών δραστηριοτήτων – συμπεριλαμβανομένων των διακρατικών συνδέσεών τους – και να συγκεντρώσουν πολύτιμα αποδεικτικά στοιχεία για τη δίωξη υπόπτων και την κατάσχεση παράνομων περιουσιακών στοιχείων.

9.5.1.1 Βασικές πτυχές των χρηματοοικονομικών ερευνών

Βασικό στοιχείο των χρηματοοικονομικών ερευνών είναι οι **παράλληλες έρευνες** κατά τις οποίες οι χρηματοοικονομικές έρευνες διεξάγονται παράλληλα με τις ποινικές έρευνες. Η προσέγγιση αυτή διασφαλίζει ότι, ενώ οι αρχές επιβολής του νόμου εστιάζουν σε εγκλήματα όπως η εμπορία ανθρώπων, η διαφθορά ή η διακίνηση ναρκωτικών, μια ταυτόχρονη χρηματοοικονομική έρευνα παρακολουθεί τη ροή των χρημάτων που παράγονται από αυτές τις δραστηριότητες (FATF, 2012). Οι παράλληλες έρευνες βοηθούν στον εντοπισμό παράνομων περιουσιακών στοιχείων, στην αναγνώριση επιπλέον υπόπτων και στη στήριξη της κατάσχεσης των εσόδων από εγκληματικές δραστηριότητες. Για την ενίσχυση της αποτελεσματικότητας, συχνά δημιουργούνται πολυεπιστημονικές ομάδες εργασίας, στις οποίες συμμετέχουν χρηματοοικονομικοί/-κές αναλυτές/-τριες, λογιστές/-στριες-εγκληματολόγοι, εμπειρογνώμονες ψηφιακής εγκληματολογίας και εισαγγελείς. Οι ομάδες αυτές βελτιώνουν την ανταλλαγή πληροφοριών, μειώνουν την αλληλεπικάλυψη των προσπαθειών και εξασφαλίζουν μια ολοκληρωμένη προσέγγιση του οικονομικού εγκλήματος (FATF, 2012).

Ένας βασικός στόχος των χρηματοοικονομικών ερευνών είναι η **ανάκτηση και** η **κατάσχεση περιουσιακών στοιχείων** (βλ. κεφάλαιο 10 της εκπαίδευσης). Οι εγκληματίες στηρίζονται στο οικονομικό κέρδος ως βασικό κίνητρο και η στέρηση των παράνομων εσόδων τους αποδυναμώνει τις δραστηριότητές τους. Οι υπηρεσίες επιβολής του νόμου πρέπει να εντοπίζουν, να «παγώνουν» και να κατάσχουν παράνομα περιουσιακά στοιχεία χρησιμοποιώντας προηγμένες τεχνικές χρηματοοικονομικής εγκληματολογίας. Η κατάσχεση χωρίς καταδίκη συνιστάται επίσης ως αποτελεσματικό νομικό εργαλείο, καθώς επιτρέπει στις αρχές να κατάσχουν

εγκληματικά περιουσιακά στοιχεία ακόμη και σε περιπτώσεις όπου η καταδίκη δεν είναι δυνατή. Η δημιουργία εξειδικευμένων μονάδων ανάκτησης περιουσιακών στοιχείων και κεντρικών βάσεων δεδομένων χρηματοοικονομικών πληροφοριών ενισχύει σημαντικά τις χρηματοοικονομικές έρευνες βελτιώνοντας την αποτελεσματικότητα και τον συντονισμό.

Μια επιτυχημένη χρηματοοικονομική έρευνα **βασίζεται σε πολλαπλές πηγές πληροφοριών**. Οι αρχές επιβολής του νόμου πρέπει να έχουν πρόσβαση σε εκθέσεις χρηματοοικονομικών πληροφοριών, συμπεριλαμβανομένων των STR, των εκθέσεων συναλλαγών σε ξένο νόμισμα και των διασυνοριακών δηλώσεων μετρητών. Ακόμη, κρίσιμες πληροφορίες παρέχουν τα τραπεζικά και χρηματοοικονομικά αρχεία, τα μητρώα εταιρειών, οι φορολογικές δηλώσεις, τα τελωνειακά δεδομένα και το OSINT. Είναι απαραίτητο οι αξιωματικοί επιβολής του νόμου να διαθέτουν τη νομική εξουσία να έχουν πρόσβαση και να αναλύουν αυτά τα αρχεία διασφαλίζοντας παράλληλα τη συμμόρφωση με τους νόμους περί προστασίας δεδομένων.

Τεχνικές έρευνας

Στις χρηματοοικονομικές έρευνες χρησιμοποιούνται διάφορες τεχνικές έρευνας (για τις αναφερόμενες τεχνικές, βλ. FATF, 2012, εάν δεν αναφέρεται άλλη πηγή).

- **Φυσική παρακολούθηση**: Η τεχνική αυτή περιλαμβάνει την παρακολούθηση υπόπτων για την κατανόηση των χρηματοοικονομικών δραστηριοτήτων τους, όπως μετακινήσεις μεγάλων ποσών μετρητών ή αλληλεπιδράσεις με χρηματοοικονομικούς διαμεσολαβητές. Είναι ιδιαίτερα χρήσιμη σε περιπτώσεις νομιμοποίησης εσόδων από παράνομες δραστηριότητες και χρηματοδότησης της τρομοκρατίας.

- **Συλλογή απορριμμάτων**: Οι ερευνητές/-τριες μπορούν να συλλέγουν και να αναλύουν νόμιμα απορριφθέντα χρηματοοικονομικά αρχεία και άλλα έγγραφα που ενδέχεται να αποκαλύψουν κρυφά περιουσιακά στοιχεία ή παράνομες συναλλαγές.
- **Υποχρεωτικά μέτρα**: Αυτά περιλαμβάνουν εντάλματα έρευνας, κλητεύσεις και διαταγές προσκόμισης για την απόκτηση κρίσιμων χρηματοοικονομικών αρχείων, όπως τραπεζικά εκκαθαριστικά, φορολογικές δηλώσεις και λογιστικά βιβλία. Οι σωστά εκτελεσμένες διαδικασίες έρευνας και κατάσχεσης διασφαλίζουν ότι τα ψηφιακά και φυσικά αποδεικτικά στοιχεία συλλέγονται νόμιμα και διατηρούνται υπό αλυσίδα επιτήρησης.
- **Παρακολούθηση επικοινωνιών**: Οι αρχές επιβολής του νόμου μπορούν να πραγματοποιούν υποκλοπές τηλεφωνικών συνδιαλέξεων, παρακολούθηση ηλεκτρονικού ταχυδρομείου και άλλες μορφές ηλεκτρονικής παρακολούθησης για να ελέγχουν τις χρηματοοικονομικές συναλλαγές και να εντοπίζουν συνωμότες. Αυτή η μέθοδος είναι ιδιαίτερα αποτελεσματική, αλλά πρέπει να συμμορφώνεται με τα νομικά πλαίσια για να αποφεύγονται παραβιάσεις απορρήτου.
- **Μυστικές επιχειρήσεις**: Σε ορισμένες περιπτώσεις, οι ερευνητές/-τριες μπορούν να χρησιμοποιήσουν ψευδείς ταυτότητες για να διεισδύσουν σε εγκληματικές οργανώσεις και να συλλέξουν άμεσα αποδεικτικά στοιχεία για οικονομικά αδικήματα. Αυτή η τεχνική απαιτεί πολλούς πόρους και εκτενή εκπαίδευση.
- **Ελεγχόμενες παραδόσεις**: Αυτή η μέθοδος περιλαμβάνει την παρακολούθηση της κίνησης παράνομων κεφαλαίων, είτε σε μετρητά είτε μέσω ψηφιακών

μεταφορών, υπό την εποπτεία των αρχών επιβολής του νόμου. Βοηθά στον εντοπισμό βασικών παραγόντων σε δίκτυα νομιμοποίησης εσόδων από παράνομες δραστηριότητες ή απάτης.

- **Δικαστική λογιστική**: Η δικαστική λογιστική είναι μια εξειδικευμένη πρακτική που συνδυάζει λογιστικές, ελεγκτικές και ερευνητικές δεξιότητες με σκοπό την εξέταση οικονομικών αρχείων για ενδείξεις παραβατικής συμπεριφοράς. Οι δικαστικοί/-κές λογιστές/-στριες μπορούν να αποκαλύψουν ασυμφωνίες στα βιβλία, να εντοπίσουν απάτες και να ανιχνεύσουν παράνομες οικονομικές δραστηριότητες μέσω λεπτομερών οικονομικών καταστάσεων. Εφαρμόζουν τόσο ποσοτικές μεθόδους, όπως ανάλυση δεδομένων και στατιστική μοντελοποίηση, όσο και ποιοτικές προσεγγίσεις, συμπεριλαμβανομένης της αξιολόγησης συμπεριφορικών προτύπων και οργανωτικής κουλτούρας, για τον εντοπισμό ανωμαλιών. Ο Νόμος του Benford προβλέπει την κατανομή της συχνότητας των ψηφίων σε φυσικά δεδομένα. Οι δικαστικοί/-κές λογιστές/-στριες χρησιμοποιούν αυτή την αρχή για να εντοπίζουν ανωμαλίες στα οικονομικά δεδομένα. Οι αποκλίσεις από την αναμενόμενη κατανομή μπορεί να υποδηλώνουν πιθανή χειραγώγηση ή απάτη. Ο Mark Nigrini, πρωτοπόρος στον τομέα αυτό, έχει ερευνήσει εκτενώς και εφαρμόσει τον Νόμο του Benford για τον εντοπισμό ανωμαλιών στα λογιστικά δεδομένα (βλ. π.χ. Gorenc, 2019· Siavoshi, 2025).
- **Μέθοδοι απόδειξης εισοδήματος**: Οι ερευνητές/-τριες χρησιμοποιούν άμεσες και έμμεσες μεθόδους για να προσδιορίσουν παράνομες πηγές εισοδήματος. Η μέθοδος της καθαρής θέσης (net worth) συγκρίνει τα περιουσιακά στοιχεία ενός ατόμου σε δύο χρονικά σημεία για να προσδιορίσει το αδήλωτο εισόδημα. Η μέθοδος της κατάθεσης τραπεζικού λογαριασμού αναλύει τις ανεξήγητες

εισροές σε τραπεζικούς λογαριασμούς. Η μέθοδος των δαπανών συγκρίνει τα μοτίβα δαπανών με γνωστές νόμιμες πηγές εισοδήματος.

- **Ανταλλαγή χρηματοοικονομικών πληροφοριών**: Οι αρχές επιβολής του νόμου συνεργάζονται με τις Μονάδες Χρηματοοικονομικών Πληροφοριών (Financial Intelligence Units-FIU), τις τράπεζες και τους διεθνείς ομολόγους τους για τη λήψη Αναφορών Ύποπτων Δραστηριοτήτων (Suspicious Activity Reports-SAR) και άλλων σχετικών χρηματοοικονομικών δεδομένων.
- **Η εξέταση των χρηματοοικονομικών συναλλαγών** βοηθά τους/τις ερευνητές/-τριες να εντοπίσουν ύποπτα τραπεζικά πρότυπα, τεχνικές διαστρωμάτωσης και μεθόδους ενοποίησης περιουσιακών στοιχείων.
- **Η ψηφιακή εγκληματολογία** (βλ. Ενότητα 9.6.1) διαδραματίζει βασικό ρόλο στην ανίχνευση ηλεκτρονικών μεταφορών χρημάτων, στην ανάλυση συναλλαγών με κρυπτονομίσματα και στην υποκλοπή παράνομων χρηματοοικονομικών επικοινωνιών.

Αξιοποίηση των συνεργιών της συνεργασίας

Οι Μονάδες Χρηματοοικονομικών Πληροφοριών διαδραματίζουν αποφασιστικό ρόλο στις χρηματοοικονομικές έρευνες, καθώς συλλέγουν, αναλύουν και διαδίδουν χρηματοοικονομικές πληροφορίες στις αρχές επιβολής του νόμου. Οι ΜΧΠ λαμβάνουν γνωστοποιήσεις AML/CFT, STR και αναφορές διασυνοριακών συναλλαγών, οι οποίες μπορούν να παράσχουν έγκαιρες προειδοποιήσεις για εγκληματικές χρηματοοικονομικές δραστηριότητες. Η ισχυρή εθνική συνεργασία μεταξύ των ΜΧΠ και των ανακριτών/-τριών διασφαλίζει ότι οι αρχές επιβολής του νόμου έχουν πρόσβαση σε έγκαιρες και αξιοποιήσιμες πληροφορίες. Για την ενίσχυση της αποτελεσματικότητας, οι ΜΧΠ και οι αρχές επιβολής του νόμου θα πρέπει να

δημιουργήσουν ασφαλείς πλατφόρμες ανταλλαγής δεδομένων σε πραγματικό χρόνο και να αναπτύξουν πρωτόκολλα για την ανάλυση χρηματοοικονομικών πληροφοριών.

Δεδομένου ότι το οικονομικό έγκλημα είναι συχνά διακρατικό, η διεθνής συνεργασία είναι εξίσου ζωτικής σημασίας. Οι εγκληματίες εκμεταλλεύονται τα διεθνή τραπεζικά συστήματα και τα υπεράκτια χρηματοοικονομικά κέντρα για να αποκρύψουν παράνομα κεφάλαια. Οι αρχές επιβολής του νόμου πρέπει να αξιοποιήσουν τις Συμβάσεις Αμοιβαίας Νομικής Συνδρομής (Mutual Legal Assistance Treaties-MLAT), την Interpol, την Europol και τα δίκτυα της FATF για να διευκολύνουν τις διασυνοριακές έρευνες. Η σύσταση κοινών ομάδων έρευνας και η απλούστευση των νομικών πλαισίων για την ανταλλαγή πληροφοριών ενισχύουν τον παγκόσμιο αγώνα κατά του οικονομικού εγκλήματος (FATF, 2012).

Για την ενίσχυση των οικονομικών ερευνών, οι αρχές επιβολής του νόμου και οι εισαγγελικές αρχές θα πρέπει να ενσωματώσουν την οικονομική εγκληματολογία σε όλες τις έρευνες για σοβαρά εγκλήματα, να αξιοποιήσουν τα συστήματα οικονομικών πληροφοριών για ανάλυση σε πραγματικό χρόνο και να ενισχύσουν τη διεθνή συνεργασία στον τομέα της ανάκτησης περιουσιακών στοιχείων και της ανταλλαγής πληροφοριών. Με την υιοθέτηση αυτών των βέλτιστων πρακτικών, οι οικονομικές έρευνες μπορούν να αποτελέσουν ένα ισχυρό εργαλείο για την εξάρθρωση των εγκληματικών οργανώσεων και τη διασφάλιση ότι το έγκλημα δεν αποδίδει.

9.5.1.2Οι προσπάθειες της Ευρωπαϊκής Ένωσης

Αναγνωρίζοντας την αυξανόμενη απειλή της διείσδυσης του οργανωμένου εγκλήματος στη νόμιμη οικονομία, η Ευρωπαϊκή Ένωση έχει τονίσει την ανάγκη ενίσχυσης των ικανοτήτων χρηματοοικονομικής έρευνας. Η Στρατηγική της ΕΕ για

την Καταπολέμηση του Οργανωμένου Εγκλήματος για το 2021 υπογράμμισε τη σημασία της προώθησης έγκαιρων χρηματοοικονομικών ερευνών σε όλες τις χώρες της ΕΕ. Η προσέγγιση αυτή αποσκοπεί στην εξάρθρωση της χρηματοοικονομικής υποδομής των εγκληματικών οργανώσεων, στην εξάλειψη των κερδών τους και στην αποτροπή της ένταξής τους στη νόμιμη οικονομία και κοινωνία (European Commission, χ.χ.). Για να υποστηρίξει αυτές τις προσπάθειες, η Ευρωπαϊκή Πολυεπιστημονική Πλατφόρμα κατά των Εγκληματικών Απειλών (EMPACT) έχει δώσει προτεραιότητα στις χρηματοοικονομικές έρευνες στην ατζέντα της. Η εν λόγω πλατφόρμα διευκολύνει τη συνεργασία μεταξύ των κρατών μελών της ΕΕ για την αντιμετώπιση διαφόρων εγκληματικών απειλών, συμπεριλαμβανομένης της διακίνησης ναρκωτικών και της εμπορίας ανθρώπων, ενσωματώνοντας τις χρηματοοικονομικές έρευνες ως κοινό στόχο σε όλες τις προτεραιότητες.

Επιπλέον, η Ευρωπαϊκή Επιτροπή παρέχει χρηματοδοτική στήριξη στο Δίκτυο Δράσης κατά του Ξεπλύματος Χρήματος (AMON), ένα παγκόσμιο δίκτυο ερευνητών/-τριών κατά του ξεπλύματος χρήματος που ιδρύθηκε το 2012. Το AMON διευκολύνει την ανταλλαγή γνώσεων μεταξύ των μονάδων επιβολής του νόμου και υποστηρίζει την ταχεία επιχειρησιακή συνεργασία στις έρευνες για το ξέπλυμα χρήματος, γεγονός που φανερώνει τον διασυνοριακό χαρακτήρα των εγκλημάτων αυτών.

Η Europol ενίσχυσε επίσης τις προσπάθειές της με την ίδρυση του Ευρωπαϊκού Κέντρου για την Καταπολέμηση του Οικονομικού και Χρηματοοικονομικού Εγκλήματος (EFECC) το 2020. Το EFECC παρέχει επιχειρησιακή υποστήριξη στα κράτη μέλη της ΕΕ σε υποθέσεις που αφορούν φορολογικά εγκλήματα, απάτη, διαφθορά, νομιμοποίηση εσόδων από παράνομες δραστηριότητες, ανάκτηση περιουσιακών στοιχείων, παραχάραξη ευρώ και εγκλήματα κατά της πνευματικής ιδιοκτησίας. Η

πρωτοβουλία αυτή αποσκοπεί στην καταπολέμηση ιδιαίτερα περίπλοκων υποθέσεων οικονομικού εγκλήματος που στοχεύουν ιδιώτες, εταιρείες και τον δημόσιο τομέα.

Επιπρόσθετα, ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κατάρτιση στον Τομέα της Επιβολής του Νόμου (CEPOL) προσφέρει τακτική εκπαίδευση στους/στις αξιωματούχους επιβολής του νόμου, προκειμένου να βελτιώσουν την κατανόησή τους σχετικά με τα συστήματα νομιμοποίησης εσόδων από παράνομες δραστηριότητες και τις τεχνικές διεθνούς χρηματοοικονομικής έρευνας. Η κατάρτιση αυτή αποσκοπεί στην ανάπτυξη των ικανοτήτων των ερευνητών/-τριών να αντιμετωπίζουν αποτελεσματικά τις χρηματοοικονομικές διαστάσεις του οργανωμένου εγκλήματος (European Commission, χ.χ.).

Συνοψίζοντας, η ολοκληρωμένη προσέγγιση της Ευρωπαϊκής Ένωσης όσον αφορά τις χρηματοοικονομικές έρευνες υπογραμμίζει τον καθοριστικό ρόλο τους στην εξουδετέρωση των εγκληματικών οργανώσεων, στην προστασία της νόμιμης οικονομίας και στην ενίσχυση της αποτελεσματικότητας της επιβολής του νόμου σε όλα τα κράτη μέλη.

9.5.2 Η εμπορία ανθρώπων ως επιχείρηση

Η εμπορία ανθρώπων λειτουργεί ως επιχείρηση με κίνητρο το κέρδος, όπως και οι νόμιμες επιχειρήσεις, και αξίζει να εξεταστεί αυτή η προοπτική προκειμένου (1) να γίνουν κατανοητοί οι βασικοί παράγοντες που οδηγούν στην εμπορία και (2) η ανάγκη διεξαγωγής χρηματοοικονομικών ερευνών. Οι οικονομικές θεωρίες του εγκλήματος υποδηλώνουν ότι οι δράστες κάνουν ορθολογικές επιλογές με βάση τα πιθανά κέρδη, τους κινδύνους και τις ευκαιρίες (βλ. π.χ. Belser, 2005). Αυτές οι ευκαιρίες προκύπτουν λόγω του γεγονότος ότι τα άτομα αναζητούν καλύτερες οικονομικές

συνθήκες, είτε μέσω της μετανάστευσης από φτωχές αγροτικές περιοχές σε πλουσιότερα αστικά κέντρα είτε μέσω της διέλευσης διεθνών συνόρων. Τα εγκληματικά δίκτυα εκμεταλλεύονται αυτές τις ευαλωτότητες δίνοντας ψευδείς υποσχέσεις για απασχόληση, αγάπη ή ασφάλεια, οδηγώντας τα θύματα σε εργασιακή ή σεξουαλική εκμετάλλευση ή σε άλλες μορφές εμπορίας (π.χ. αφαίρεση οργάνων). Το επιχειρηματικό μοντέλο για την εκμετάλλευση της εργασίας είναι απλό: τα θύματα εργάζονται υπό εξαναγκασμό ή χωρίς να έχουν επίγνωση της εκμεταλλευτικής κατάστασης, γεγονός που αποφέρει υψηλά κέρδη με ελάχιστο κόστος για τους διακινητές. Τομείς όπως η γεωργία, οι κατασκευές, η οικιακή εργασία και η φιλοξενία παρέχουν κάλυψη για την εμπορία εργατικού δυναμικού, ενώ η σεξουαλική εκμετάλλευση παραμένει μία από τις πιο κερδοφόρες αγορές για τους διακινητές (βλ. π.χ. Aronowitz, Theuermann & Tyurykanova, 2010).

Παρά την υψηλή κερδοφορία, οι κίνδυνοι για τους διακινητές παραμένουν χαμηλοί. Πολλά θύματα φοβούνται τις αρχές επιβολής του νόμου λόγω της νομικής τους κατάστασης, του κοινωνικού στίγματος ή των απειλών από τους εκμεταλλευτές τους. Σε χώρες στις οποίες η πορνεία είναι παράνομη, τα θύματα είναι πιο πιθανό να αντιμετωπίσουν σύλληψη παρά να λάβουν προστασία. Πέραν αυτού, τα ποσοστά ανίχνευσης και δίωξης των διακινητών παραμένουν χαμηλά, γεγονός που ενισχύει τη βιωσιμότητα του επιχειρηματικού μοντέλου. Οι δυνάμεις της αγοράς διαδραματίζουν επίσης σημαντικό ρόλο στη διαμόρφωση των δραστηριοτήτων εμπορίας ανθρώπων. Δεν είναι μόνο η ζήτηση από τους καταναλωτές που οδηγεί στην εμπορία ανθρώπων, αλλά μάλλον η ύπαρξη μιας μεγάλης προσφοράς ευάλωτων ατόμων. Οι εγκληματικές οργανώσεις προσαρμόζουν τις μεθόδους τους με βάση τα νομικά πλαίσια, τις οικονομικές συνθήκες και τους μηχανισμούς επιβολής του νόμου, όπως και οι νόμιμες

επιχειρήσεις που ανταποκρίνονται στις αλλαγές της αγοράς (Aronowitz, Theuermann & Tyurykanova, 2010).

Οι χρηματοοικονομικές έρευνες για την εμπορία ανθρώπων πρέπει να λαμβάνουν υπόψη αυτούς τους οικονομικούς παράγοντες. Μέσω της ανάλυσης των χρηματοοικονομικών συναλλαγών, των περιθωρίων κέρδους και των παράνομων ταμειακών ροών, οι αρχές επιβολής του νόμου μπορούν να εντοπίσουν μοτίβα εκμετάλλευσης, να διαλύσουν δίκτυα και να αποδυναμώσουν τα οικονομικά κίνητρα που κρύβονται πίσω από τις δραστηριότητες εμπορίας ανθρώπων. Η κατανόηση της εμπορίας ανθρώπων ως οικονομικής δραστηριότητας είναι μείζονος σημασίας για την ανάπτυξη αποτελεσματικών αντιμέτρων, συμπεριλαμβανομένων ρυθμιστικών πλαισίων, χρηματοοικονομικής εποπτείας και στοχευμένων παρεμβάσεων. Η επόμενη ενότητα περιγράφει το γενικό πλαίσιο των χρηματοοικονομικών ερευνών σε υποθέσεις εμπορίας ανθρώπων και τα συγκεκριμένα μέτρα που πρέπει να ληφθούν.

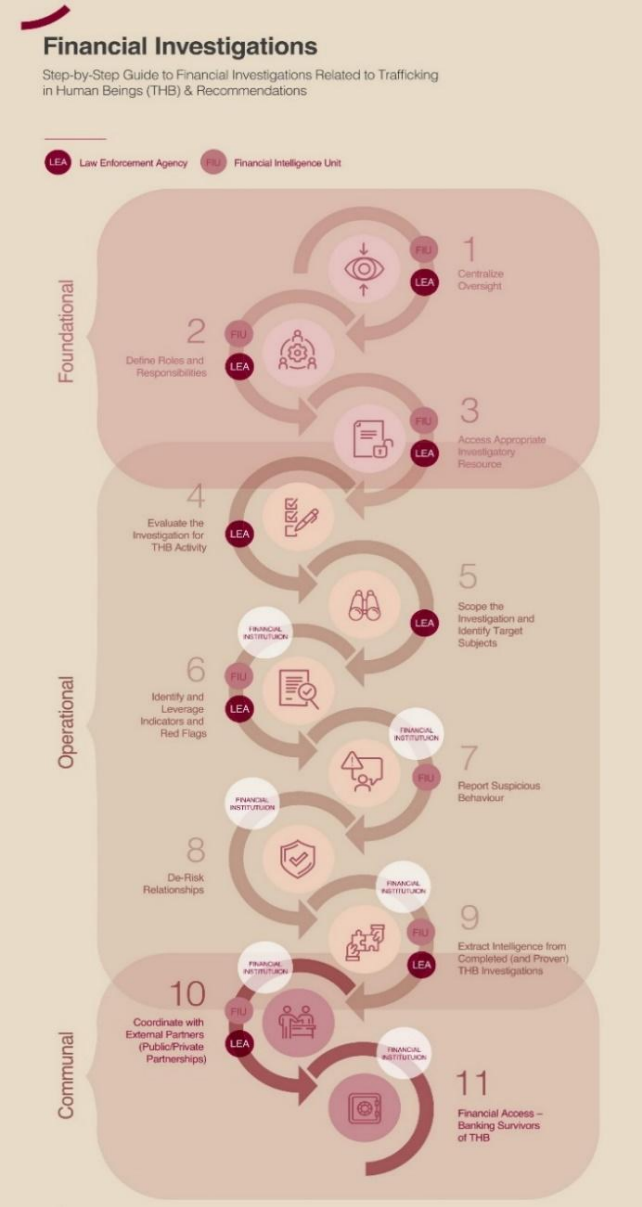
9.5.3 Οδηγός βήμα προς βήμα για τις χρηματοοικονομικές έρευνες που σχετίζονται με την εμπορία ανθρώπων

Αυτή η ενότητα περιγράφει **έντεκα (11) βασικά βήματα** για τη διεξαγωγή αποτελεσματικών χρηματοοικονομικών ερευνών σε περιπτώσεις εμπορίας ανθρώπων. Αυτά τα βήματα κατηγοριοποιούνται σε τρεις τομείς: *θεμελιώδη*, *επιχειρησιακά* και *κοινοτικά*.

Τα θεμελιώδη βήματα συνήθως πραγματοποιούνται μία φορά κατά τη δημιουργία του πλαισίου έρευνας και εφαρμόζονται ευρέως τόσο στον δημόσιο όσο και στον ιδιωτικό τομέα. Τα επιχειρησιακά βήματα εφαρμόζονται συχνότερα λόγω της συνάφειάς τους με μεμονωμένες έρευνες, αν και η εφαρμογή τους διαφέρει μεταξύ

δημόσιων και ιδιωτικών φορέων. Για παράδειγμα, τα βήματα 7 και 8 αφορούν κυρίως φορείς αναφοράς στον ιδιωτικό τομέα. Τέλος, τα κοινοτικά βήματα χωρίζονται ανάλογα με την εφαρμογή τους: και οι δύο τομείς έχουν κοινό ενδιαφέρον για το βήμα 10, ενώ οι πάροχοι χρηματοοικονομικών υπηρεσιών φέρουν μεγαλύτερη ευθύνη για το βήμα 11.

Το Σχήμα 14 παρουσιάζει αυτή τη σχηματική διαδικασία βήμα προς βήμα μεταξύ των αρχών επιβολής του νόμου και των Μονάδων Χρηματοοικονομικών Πληροφοριών. Το σχήμα αυτό είναι αντίγραφο από τον ΟΑΣΕ (2020).



Σχήμα 4 . Βήματα μιας χρηματοοικονομικής έρευνας

Βήμα 1ο: Το πρώτο βήμα για μια επιτυχημένη χρηματοοικονομική έρευνα σχετικά με την εμπορία ανθρώπων είναι η **δημιουργία ενός κεντρικού μηχανισμού εποπτείας**. Αυτό εξασφαλίζει μια συντονισμένη και ολοκληρωμένη ανταπόκριση σε κάθε ύποπτη υπόθεση, αν και η δομή του μπορεί να διαφέρει ανάλογα με το μέγεθος και την αποστολή του οργανισμού. Οι αρχές επιβολής του νόμου συχνά ενσωματώνουν τις έρευνες για την εμπορία ανθρώπων σε **εξειδικευμένες μονάδες**. Για παράδειγμα, το Αστυνομικό Τμήμα της Νέας Υόρκης (NYPD) και η Μητροπολιτική Αστυνομική Υπηρεσία του Λονδίνου (MPS) διαθέτουν ειδικές ομάδες, ενώ η Αστυνομική Υπηρεσία του Τορόντο (TPS) χειρίζεται υποθέσεις εμπορίας ανθρώπων στο πλαίσιο της Μονάδας Σεξουαλικών Εγκλημάτων αναγνωρίζοντας τη διαφορά τους από τα αδικήματα που σχετίζονται με την πορνεία. Ομοσπονδιακές υπηρεσίες όπως το FBI και η Interpol συγκεντρώνουν επίσης εμπειρογνωσία, όπως και οι ΜΧΠ, αν και οι τελευταίες λειτουργούν συχνά με λιγότερη δημοσιότητα.

Στον **ιδιωτικό τομέα**, ιδίως στις τράπεζες, η εποπτεία είναι λιγότερο δομημένη λόγω του μεγάλου όγκου συναλλαγών και των κανονιστικών απαιτήσεων. Ωστόσο, πολλά ιδρύματα διατηρούν **ειδικές ομάδες έρευνας** για την αντιμετώπιση οικονομικών εγκλημάτων, συμπεριλαμβανομένης της εμπορίας ανθρώπων. Η συγκέντρωση των ερευνητικών προσπαθειών προσφέρει πολλαπλά οφέλη, όπως τη μείωση της αλληλεπικάλυψης, τη βελτίωση της αποτελεσματικότητας, την ενίσχυση της εμπειρογνωσίας και τη δυνατότητα ολοκληρωμένης ανάλυσης δεδομένων. Ωστόσο, ενέχει επίσης κινδύνους, όπως τον περιορισμό της γνώσης σε μια επιλεγμένη ομάδα και πιθανές καθυστερήσεις στις έρευνες. Για να μετριαστούν αυτοί οι κίνδυνοι, τα ιδρύματα πρέπει να προωθούν πρωτοβουλίες ανταλλαγής γνώσεων και να επιτρέπουν ευελιξία στις ερευνητικές ευθύνες προκειμένου να αποφεύγονται τα εμπόδια. Σε τελική ανάλυση, με την καταγραφή και την κατάλληλη διαχείριση των

περιπτώσεων, οι έρευνες μπορούν να διεξάγονται από διαφορετικές ομάδες προς όφελος τόσο των εσωτερικών όσο και των εξωτερικών ενδιαφερόμενων μερών.

Βήμα 2ο: Μόλις καθοριστεί ένα πλαίσιο εποπτείας για τις έρευνες σχετικά με την εμπορία ανθρώπων, είναι σημαντικό να καθοριστούν με σαφήνεια οι ρόλοι και οι ευθύνες των εμπλεκόμενων. Αν και αυτό αποτελεί συνήθη πρακτική σε πολλά δημόσια και ιδιωτικά ιδρύματα, μερικές φορές παραβλέπεται. Ο **σαφής καθορισμός των ευθυνών** συμβάλλει στην αποφυγή της αλληλεπικάλυψης των προσπαθειών, ενισχύει την επιχειρησιακή αποτελεσματικότητα και προσφέρει πρόσθετα οφέλη, όπως ομαλότερη διαδοχή, αποτελεσματικότερη ταξινόμηση των υποθέσεων, καλύτερη ιεράρχηση των ερευνών και συνεπής επικοινωνία εντός και εκτός της ομάδας. Η **τεκμηρίωση των ρόλων** διασφαλίζει ότι οι έρευνες διεξάγονται πιο αποτελεσματικά και έγκαιρα. Στην ουσία, αυτή η προσέγγιση ακολουθεί την αρχή «διαίρει και βασίλευε» – όταν όλα τα άτομα κατανοούν τον ρόλο τους, μπορούν να επικεντρωθούν στην εκτέλεση. Χωρίς σαφείς ευθύνες, ακόμη και οι καλοπροαίρετες προσπάθειες μπορεί να οδηγήσουν σε μια ασυνεπή και αναποτελεσματική ερευνητική διαδικασία.

Βήμα 3ο: Μια επιτυχημένη έρευνα απαιτεί **πρόσβαση στους κατάλληλους πόρους**, οι οποίοι μπορεί να διαφέρουν ανάλογα με τη φύση της έρευνας. Οι χρηματοοικονομικές έρευνες, ιδίως εκείνες που εστιάζουν στο ξέπλυμα χρήματος και την εμπορία ανθρώπων, απαιτούν **εξειδικευμένα εργαλεία** διαφορετικά από αυτά που χρησιμοποιούνται στις επιτόπιες επιχειρήσεις. Δεδομένης της πολυπλοκότητας της ανίχνευσης των χρηματοοικονομικών ροών, οι ερευνητές/-τριες πρέπει να διαθέτουν επαρκείς πόρους για να αναλύουν αποτελεσματικά τις συναλλαγές, να συνδέουν σχετικές υποθέσεις και να προσαρμόζονται στις εξελισσόμενες εγκληματικές τακτικές.

Η παροχή των απαραίτητων εργαλείων στους/στις ερευνητές/-τριες ενισχύει την αποτελεσματικότητα, βελτιώνει την ποιότητα της έρευνας και αυξάνει την πιθανότητα επιτυχών συλλήψεων και καταδικών. Οι βασικοί πόροι περιλαμβάνουν:

- **Ψηφιακά συστήματα διαχείρισης υποθέσεων:** Μια κεντρική βάση δεδομένων για την αποθήκευση σημειώσεων και αποδεικτικών στοιχείων επιτρέπει την καλύτερη παρακολούθηση των υποθέσεων και τη σύνδεση των ερευνών.
- **Απεριόριστη πρόσβαση στο διαδίκτυο:** Οι ερευνητές/-τριες ενδέχεται να χρειαστούν πρόσβαση σε ιστότοπους με περιορισμένη πρόσβαση, όπως πλατφόρμες με περιεχόμενο για ενήλικες, κατά την παρακολούθηση δραστηριοτήτων εμπορίας ανθρώπων, υπό την προϋπόθεση ότι έχουν λάβει την κατάλληλη εκπαίδευση για την αποφυγή κατάχρησης.
- **Εκπαίδευση OSINT:** Η εξειδικευμένη εκπαίδευση σε διαδικτυακές έρευνες βοηθά στην αποκάλυψη κρίσιμων πληροφοριών και στην προστασία της ταυτότητας των ερευνητών/-τριών.
- **Πρόσβαση σε εσωτερικά δεδομένα:** Η άμεση διαθεσιμότητα σχετικών θεσμικών δεδομένων, όπως αρχεία συναλλαγών ή προηγούμενων υποθέσεων, είναι απαραίτητη. Η υπέρβαση των τεχνολογικών, νομικών και γραφειοκρατικών εμποδίων στην πρόσβαση στα δεδομένα βελτιώνει την αποτελεσματικότητα των ερευνών.
- **Συμβουλευτική από νομικούς/-κές εμπειρογνώμονες:** Τα οικονομικά εγκλήματα συχνά αφορούν τη φορολογία, τα χρεόγραφα και τα ακίνητα απαιτώντας τη συμβολή ειδικών. Η έγκαιρη αναγνώριση νομικών και οικονομικών εμπειρογνωμόνων ενισχύει τα αποτελέσματα των ερευνών.

Παρότι η πρόσβαση σε πόρους είναι ζωτικής σημασίας, οι οργανισμοί πρέπει να εξισορροπούν την αποτελεσματικότητα με νομικές και ηθικές παραμέτρους διασφαλίζοντας ότι οι ερευνητές/-τριες λειτουργούν εντός των ρυθμιστικών ορίων μεγιστοποιώντας παράλληλα τις ερευνητικές τους δυνατότητες.

Βήμα 4ο: Μία από τις βασικές προκλήσεις στις οικονομικές έρευνες που σχετίζονται με την εμπορία ανθρώπων είναι ο κίνδυνος εσφαλμένης αναγνώρισης των εγκλημάτων — είτε με την εκτίμηση ενός άλλου αδικήματος ως εμπορία ανθρώπων είτε με την παράβλεψη των δεικτών εμπορίας. Αυτό μπορεί να οφείλεται στην έλλειψη νομικών γνώσεων ή στην επικάλυψη χαρακτηριστικών εγκλημάτων, όπως η παράνομη διακίνηση ανθρώπων ή οι παραβιάσεις της εργατικής νομοθεσίας. Η διάκριση αυτών των αδικημάτων είναι μείζονος σημασίας, ιδίως για τους/τις ερευνητές/-τριες τόσο του δημόσιου όσο και του ιδιωτικού τομέα. Οι ιδιωτικοί φορείς θα πρέπει συν τοις άλλοις να καθορίσουν ποια προαπαιτούμενα αδικήματα θα εξετάζουν οι εξειδικευμένες ομάδες τους, καθώς οι μονάδες που ασχολούνται αποκλειστικά με την εμπορία ανθρώπων είναι σπάνιες λόγω περιορισμένων πόρων. Μόλις αποκτηθεί μια βασική κατανόηση των νόμων που σχετίζονται με την εμπορία ανθρώπων και των ερευνητικών ευθυνών, οι ερευνητές/-τριες μπορούν να βελτιώσουν την προσέγγισή τους για τη διαχείριση των παραπομπών. Οι δημόσιοι φορείς λαμβάνουν συνήθως μεγαλύτερο αριθμό παραπομπών που σχετίζονται με την εμπορία ανθρώπων λόγω των ευρύτερων αρμοδιοτήτων τους, ενώ οι ομάδες του ιδιωτικού τομέα μπορεί να έχουν λιγότερες υποθέσεις, αλλά περισσότερες ευκαιρίες για προληπτική έρευνα. Οι προληπτικές στρατηγικές περιλαμβάνουν:

- **Επανεξέταση παλαιότερων υποθέσεων:** Παλαιότερες υποθέσεις που έχουν χαρακτηριστεί εσφαλμένα ως πορνεία ή παράνομη διακίνηση προσώπων ενδέχεται να περιέχουν παραβλεφθέντα στοιχεία εμπορίας ανθρώπων.
- **Διεξαγωγή αναδρομικών αναζητήσεων σε αρνητικά δημοσιεύματα:** Η αναθεώρηση των ειδησεογραφικών αναφορών για ύποπτους διακινητές μπορεί να αποκαλύψει οικονομικούς δεσμούς ή μοτίβα στους λογαριασμούς ενός ιδρύματος.
- **Ανάλυση αναφορών ύποπτων συναλλαγών (SAR):** Η εξόρυξη ιστορικών δεδομένων SAR μπορεί να βοηθήσει στον εντοπισμό παραβλέψεων που σχετίζονται με την εμπορία ανθρώπων.
- **Παρακολούθηση επιχειρηματικών τομέων υψηλού κινδύνου:** Κλάδοι όπως τα κέντρα μασάζ, τα στριπτιζάδικα και η πορνογραφία έχουν συνδεθεί με την εμπορία ανθρώπων και απαιτούν πιο προσεκτική εξέταση.

Οι αποτελεσματικές χρηματοοικονομικές έρευνες απαιτούν τόσο αντιδραστικά όσο και προληπτικά μέτρα. Ωστόσο, η επιτυχία τους εξαρτάται από την ποιότητα των πληροφοριών που ανταλλάσσονται διασφαλίζοντας ότι οι άρτια τεκμηριωμένες αναφορές ύποπτων συναλλαγών (SAR) φτάνουν στις αρχές επιβολής του νόμου και οδηγούν σε άμεσες και ουσιαστικές ενέργειες.

<u>Βήμα 5ο</u>: Ένα σαφώς καθορισμένο πεδίο έρευνας είναι σημαντικό για να αποφευχθεί η υπερβολική διεύρυνση των υποθέσεων και η εσφαλμένη σύνδεση αθώων ατόμων με εγκληματικές δραστηριότητες. Στις έρευνες για την εμπορία ανθρώπων, οι διακινητές συχνά εκμεταλλεύονται τους τραπεζικούς λογαριασμούς των θυμάτων τους για προσωπικό όφελος καθιστώντας απαραίτητο για τους

οργανισμούς να διαθέτουν πολιτικές που αποτρέπουν την περαιτέρω θυματοποίηση. **Η σαφής διάκριση μεταξύ διακινητών και θυμάτων αποτελεί προτεραιότητα**, ακολουθούμενη από τον **εντοπισμό των βασικών δραστών πριν από τους δευτερεύοντες διαμεσολαβητές**. Αυτή η προσέγγιση βάσει κινδύνου βελτιστοποιεί τους πόρους και διασφαλίζει την αποτελεσματικότητα των ερευνών.

Για να καθοριστεί με ακρίβεια το πεδίο εφαρμογής μιας έρευνας, αυτή πρέπει να είναι όσο το δυνατόν πιο ολοκληρωμένη από την αρχή. Το Μοντέλο 360, για παράδειγμα, που αναπτύχθηκε από τον Peter Warrack, προσφέρει μια δομημένη μέθοδο για την αξιολόγηση της χρηματοοικονομικής δραστηριότητας για πιθανή νομιμοποίηση εσόδων από παράνομες δραστηριότητες και μπορεί να εφαρμοστεί τόσο σε ιδιωτικά χρηματοπιστωτικά ιδρύματα όσο και στις αρχές επιβολής του νόμου. Το μοντέλο αποτελείται από έξι βήματα:

1. **Εκκίνηση της έρευνας** – Η έρευνα ξεκινά με μια ειδοποίηση, όπως μια αναφορά ύποπτης δραστηριότητας (SAR), μια αυτόματη επισήμανση παρακολούθησης συναλλαγών, αρνητική δημοσιότητα, μια εσωτερική παραπομπή ή ένα αίτημα των αρχών επιβολής του νόμου.
2. **Κατανόηση του/της πελάτη/-τισσας** – Οι ερευνητές/-τριες συλλέγουν πληροφορίες σχετικά με το ιστορικό του υποκειμένου συμπεριλαμβανομένης της απασχόλησης, της οικονομικής κατάστασης και του γενικού προφίλ του.
3. **Κατανόηση της χρηματοοικονομικής δραστηριότητας** – Η χρηματοοικονομική συμπεριφορά του/της πελάτη/-τισσας αξιολογείται σε σχέση με το γνωστό ιστορικό του προκειμένου να προσδιοριστεί εάν συνάδει με τις προσδοκίες.

4. **Εξάλειψη της κανονικότητας** – Οι συναλλαγές που φαίνονται κανονικές για τον/την πελάτη/-τισσα φιλτράρονται, γεγονός που επιτρέπει στους/στις ερευνητές/-τριες να εστιάσου σε πραγματικά ύποπτες δραστηριότητες.
5. **Ανάλυση της υπόλοιπης χρηματοοικονομικής δραστηριότητας** – Η έρευνα επικεντρώνεται στη δραστηριότητα που προκάλεσε την αρχική υποψία αναλύοντας τα μοτίβα και τις πιθανές συνδέσεις με παράνομη συμπεριφορά.
6. **Αναφορά και εξέταση της αποεπένδυσης** – Αν η έρευνα επιβεβαιώσει την υποψία, υποβάλλεται αναφορά SAR στην τοπική ΜΧΠ και, σε περιπτώσεις επιβολής του νόμου, μπορεί να ζητηθεί ένταλμα σύλληψης.

Αυτή η δομημένη προσέγγιση διασφαλίζει ότι οι ερευνητικοί πόροι επικεντρώνονται σε νόμιμες απειλές ελαχιστοποιώντας τα ψευδώς θετικά αποτελέσματα και ενισχύοντας τη συνολική αποτελεσματικότητα.

Βήμα 6ο: Για να κατανοήσουμε τι συνιστά ύποπτη χρηματοοικονομική δραστηριότητα στο πλαίσιο της εμπορίας ανθρώπων, απαιτείται τόσο γενική γνώση των τραπεζικών πρακτικών όσο και σε βάθος γνώση των μεθόδων των διακινητών. Μολονότι οι βασικές τραπεζικές γνώσεις είναι σχετικά εύκολο να αποκτηθούν, η αναγνώριση των ανωμαλιών απαιτεί συχνά πρόσβαση σε σημαντικά δεδομένα και πρακτική εμπειρία στον τομέα των ερευνών. Ωστόσο, δεδομένης της εκτεταμένης τεκμηρίωσης που είναι διαθέσιμη σχετικά με τις χρηματοοικονομικές συμπεριφορές των διακινητών, η έρευνα μπορεί να αντισταθμίσει την έλλειψη άμεσης εμπειρίας.

Σε μακροοικονομικό επίπεδο, οι **δείκτες της εμπορίας ανθρώπων** μπορούν να ταξινομηθούν σε τρεις κατηγορίες:

1. **Δείκτες Συμπεριφοράς** – Αυτοί περιλαμβάνουν οπτικά στοιχεία που μπορεί να υποδηλώνουν ότι ένα άτομο είναι θύμα εμπορίας ανθρώπων ή ότι κάποιος είναι διακινητής.
2. **Δείκτες «Γνωρίστε τον/την Πελάτη/-τισσά Σας» (KYC)** – Προειδοποιητικά σημάδια που βασίζονται σε πληροφορίες που παρέχονται από τον/την πελάτη/-τισσα, όπως ασυνέπειες στην ταυτότητα ή στις διευθύνσεις.
3. **Δείκτες Συναλλαγών** – Ύποπτα χρηματοοικονομικά μοτίβα που μπορούν να εμφανιστούν ανά πάσα στιγμή μετά το άνοιγμα ενός λογαριασμού, συχνά χωρίς προσωπική επαφή, ιδίως με την άνοδο της ψηφιακής τραπεζικής (digital banking).

Αυτοί οι δείκτες μπορούν να εμφανιστούν ανεξάρτητα ή σε συνδυασμό και μπορούν να ανιχνευθούν από διαφορετικές ομάδες εντός ενός οργανισμού — το προσωπικό πρώτης γραμμής που εντοπίζει συμπεριφορικά σημάδια, οι ομάδες συλλογής δεδομένων που εντοπίζουν προειδοποιητικά σημάδια KYC και οι ομάδες παρακολούθησης συναλλαγών που αναγνωρίζουν οικονομικές ανωμαλίες. Η σαφής επικοινωνία και τα πρωτόκολλα κλιμάκωσης είναι απαραίτητα για να διασφαλιστεί ότι οι δυνητικά ύποπτες δραστηριότητες διερευνώνται διεξοδικά. Η κατάτμηση των δεικτών σε αυτές τις τρεις κατηγορίες ευθυγραμμίζεται με τα πλαίσια που έχουν αναπτυχθεί από την Thomson Reuters και την Banks Alliance στην Ευρώπη, την Ασία και τις Ηνωμένες Πολιτείες Αμερικής. Τα εργαλεία τους παρέχουν πρόσθετες πληροφορίες, συμπεριλαμβανομένης της σχετικής ισχύος κάθε δείκτη και της σύνδεσής του με συγκεκριμένες μορφές εμπορίας ανθρώπων, όπως εκείνης που αποσκοπεί στην εργασιακή εκμετάλλευση.

Είναι σημαντικό να αναγνωριστεί ότι ορισμένοι δείκτες, όπως οι συχνές αγορές φαρμάκων, μπορεί να μην είναι ύποπτοι μεμονωμένα. Ως εκ τούτου, οι αναλυτές/-τριες θα πρέπει να λαμβάνουν υπόψη πολλαπλούς παράγοντες για να διαπιστώσουν εύλογους λόγους υποψίας. Αυτό ευθυγραμμίζεται με τις οδηγίες των υπηρεσιών χρηματοοικονομικών πληροφοριών, μεταξύ των οποίων:

- **FINTRAC** (Καναδάς, 2016): «Μια μεμονωμένη συναλλαγή μπορεί να οδηγήσει σε λανθασμένη υπόθεση κανονικότητας. Η εξέταση όλων των δεικτών μπορεί να αποκαλύψει άγνωστες συνδέσεις που, στο σύνολό τους, θα μπορούσαν να οδηγήσουν σε εύλογους λόγους υποψίας για εμπορία ανθρώπων».
- **FinCEN** (ΗΠΑ, 2014): «Καμία μεμονωμένη συναλλαγή δεν αποτελεί σαφή ένδειξη δραστηριότητας που σχετίζεται με τη διακίνηση ή την εμπορία ανθρώπων. Πρέπει επίσης να λαμβάνονται υπόψη πρόσθετοι παράγοντες, όπως η αναμενόμενη χρηματοοικονομική δραστηριότητα ενός/μιας πελάτη/-τισσας».

Τόσο η FINTRAC όσο και η FinCEN τονίζουν τη σημασία μιας δομημένης ερευνητικής προσέγγισης, όπως το Μοντέλο 360 του Warrack, για να διασφαλιστεί ότι οι οικονομικές προειδοποιητικές ενδείξεις αξιολογούνται στο πλαίσιο τους και όχι μεμονωμένα. Για έναν ολοκληρωμένο κατάλογο συνθετικών δεικτών, ανατρέξτε στα παραρτήματα του **Συνοπτικού Εγχειριδίου Πόρων και του Οδηγού Βήμα προς Βήμα για τις Χρηματοοικονομικές Έρευνες που Σχετίζονται με την Εμπορία Ανθρώπων** του ΟΑΣΕ **(OSCE, 2019)**.

Βήμα 7ο: Οι **Αναφορές Ύποπτων Συναλλαγών (SAR)** διαδραματίζουν κρίσιμο ρόλο στις χρηματοοικονομικές έρευνες τόσο στον δημόσιο όσο και στον ιδιωτικό τομέα. Παραδοσιακά, μια SAR σηματοδοτεί το τέλος της έρευνας ενός ιδιωτικού ιδρύματος,

συνήθως ενός χρηματοπιστωτικού ιδρύματος όπως μια τράπεζα, το οποίο στη συνέχεια υποβάλλει την αναφορά στη ΜΧΠ του. Από την πλευρά του δημόσιου τομέα, μια τέτοια αναφορά μπορεί να προκαλέσει την έναρξη μιας έρευνας από τις αρχές επιβολής του νόμου. Ωστόσο, για να μεγιστοποιηθούν οι δυνατότητές τους, οι Αναφορές πρέπει να θεωρούνται πολύτιμα εργαλεία σε όλη τη διάρκεια της διαδικασίας έρευνας και όχι μόνο ως τελικό στάδιο ή ως έναρξη δημόσιων ερευνών. Μπορούν να παρέχουν χρήσιμες πληροφορίες σε διάφορα στάδια, είτε συμβάλλοντας σε τρέχουσες έρευνες είτε προσφέροντας το πλαίσιο για εσωτερικές έρευνες εντός ιδιωτικών ιδρυμάτων.

Στον **ιδιωτικό τομέα**, συνιστάται η χρήση τεχνικών λύσεων για την ελάφρυνση του διοικητικού φόρτου της εισαγωγής δεδομένων ρουτίνας επιτρέποντας στους/-στις ερευνητές/-τριες να επικεντρωθούν στις λεπτομέρειες των ύποπτων δραστηριοτήτων. Επιπλέον, τα δεδομένα από προηγούμενες SAR θα πρέπει να είναι εύκολα προσβάσιμα για τον εντοπισμό προτύπων, την αποκάλυψη μοναδικών αδικημάτων και την παρακολούθηση των εμπλεκόμενων οντοτήτων . Οι αναφορές SAR θα πρέπει να αναφέρονται σε προηγούμενες αναφορές που σχετίζονται με το ίδιο εγκληματικό δίκτυο προκειμένου να δημιουργηθεί μια συνεκτική αφήγηση και να αποφευχθούν διπλές καταχωρίσεις. Είναι σημαντικό τα ιδρύματα που υποβάλλουν αναφορές να ακολουθούν τις συμβάσεις ονοματολογίας που έχουν θεσπιστεί από τις εθνικές Μονάδες Χρηματοοικονομικών Πληροφοριών (FIU), ιδίως για αδικήματα υψηλού προφίλ, όπως η εμπορία ανθρώπων. Η τήρηση αυτών των συμβάσεων συμβάλλει στη διασφάλιση της συμμόρφωσης με τις κανονιστικές προσδοκίες, ενισχύει την αξιοπιστία των αναφορών του ιδρύματος και βοηθά στον εντοπισμό των τάσεων των οικονομικών εγκλημάτων. Για παράδειγμα, η FinCEN των ΗΠΑ συνιστά να επισημαίνονται οι αναφορές SAR που σχετίζονται με την εμπορία ανθρώπων ως

"Advisory Human Trafficking" (Συμβουλευτική για την εμπορία ανθρώπων), ενώ η FINTRAC του Καναδά προτείνει τη χρήση της ένδειξης "Project Protect" (Πρόγραμμα Προστασίας). Τα ιδρύματα που δεν διαθέτουν αυτά τα συστήματα κωδικοποίησης θα μπορούσαν να εξετάσουν το ενδεχόμενο σύναψης συμπράξεων δημόσιου/ιδιωτικού τομέα για την εφαρμογή τους.

Στον **δημόσιο τομέα**, συνιστάται η χρήση των βάσεων δεδομένων SAR των ΜΧΠ για όλες τις έρευνες σχετικά με την εμπορία ανθρώπων, καθώς αυτό το έγκλημα συνήθως συνεπάγεται οικονομικό όφελος. Οι αρχές επιβολής του νόμου θα πρέπει επίσης να χρησιμοποιούν εργαλεία όπως εντολές παραγωγής και εντάλματα για να ενθαρρύνουν τις τράπεζες και άλλους φορείς αναφοράς να υποβάλλουν SAR που σχετίζονται με ανοιχτές έρευνες. Παρά τη σημασία τους, οι αναφορές SAR έχουν επικριθεί για τον αυξανόμενο αριθμό αναφορών χαμηλής ποιότητας. Για παράδειγμα, μια έκθεση του ΟΑΣΕ του 2014 υπογράμμισε ότι, στην Ιταλία, μόνο 23 από τις 37.000 αναφορές SAR θεωρήθηκαν χρήσιμες για ποινικές έρευνες. Μια επιτροπή νομικής μεταρρύθμισης του Ηνωμένου Βασιλείου το 2019 επανέλαβε παρόμοιες ανησυχίες, υποδηλώνοντας την ανάγκη βελτίωσης των αναφορών SAR για τη μείωση του όγκου των υποβαλλόμενων αναφορών χαμηλής ποιότητας. Με την εφαρμογή ορισμένων από τις προτάσεις που απαριθμούνται, όπως η αναφορά σε ιστορικές αναφορές SAR, μπορεί να βελτιωθεί η ποιότητα των μελλοντικών εγγράφων.

<u>Βήμα 8ο</u>: Μετά την ολοκλήρωση μιας έρευνας σε έναν ιδιωτικό οργανισμό, όπως μια τράπεζα, πρέπει να ληφθεί απόφαση σχετικά με τη συνέχιση της σχέσης με τον/την πελάτη/-τισσα που ερευνάται. Αυτή η διαδικασία, γνωστή ως «**μείωση κινδύνου**», περιλαμβάνει τον τερματισμό της σχέσης, εάν είναι απαραίτητο. Είναι σημαντικό να γίνεται διάκριση μεταξύ θύματος και δράστη, ώστε να αποφεύγεται η

άδικη τιμωρία του θύματος, ειδικά σε περιπτώσεις όπως η εμπορία ανθρώπων. Αν ένας λογαριασμός ανήκει σε θύμα εμπορίας ανθρώπων, πρέπει να καταβληθούν προσπάθειες για τη διατήρηση της σχέσης, εκτός εάν υπάρχουν πολλαπλές παραβιάσεις ή συνενοχή. Η μείωση του κινδύνου πρέπει να αντιμετωπίζεται με προσοχή, καθώς η ώθηση ύποπτων δραστηριοτήτων σε παράνομες αγορές μπορεί να δυσχεράνει τις έρευνες των αρχών επιβολής του νόμου. Σε ορισμένες δικαιοδοσίες, οι αρχές επιβολής του νόμου μπορούν να ζητήσουν να παραμείνουν ανοιχτοί οι τραπεζικοί λογαριασμοί, προκειμένου να μην διαταραχθούν οι έρευνες. Αν η μείωση του κινδύνου καταστεί απαραίτητη, θα πρέπει να χρησιμοποιούνται τυποποιημένα μηνύματα, προκειμένου να αποφευχθούν ψευδείς κατηγορίες, και θα πρέπει να τηρούνται αρχεία των οντοτήτων για τις οποίες έχει προηγουμένως μειωθεί ο κίνδυνος, για μελλοντική αναφορά.

Βήμα 9ο: Η αναγνώριση πραγματικών περιπτώσεων εμπορίας ανθρώπων με βάση αποκλειστικά τις χρηματοοικονομικές συναλλαγές είναι δύσκολη λόγω της έλλειψης πληροφοριών σχετικά με το πλαίσιο. Επιπλέον, το αν οι ερευνητές/-τριες εργάζονται σε δημόσιο ίδρυμα ή σε ιδιωτικό οργανισμό επηρεάζει την πιθανότητα εύρεσης αποδεικτικών περιπτώσεων εμπορίας ανθρώπων. Οι ιδιωτικοί οργανισμοί, όπως οι πάροχοι χρηματοοικονομικών υπηρεσιών, δεν υποχρεούνται να αποδείξουν πέραν πάσης αμφιβολίας ότι έχει διαπραχθεί προαπαιτούμενο αδίκημα προτού υποβάλουν αναφορά ύποπτης δραστηριότητας (SAR) στη Μονάδα Χρηματοοικονομικών Πληροφοριών. Το όριο αναφοράς είναι συχνά χαμηλό, επειδή τα χρηματοπιστωτικά ιδρύματα μπορούν να δουν μόνο ένα μέρος της συνολικής εικόνας. Εκτός από αυτό, οι ΜΧΠ συνήθως δεν παρέχουν ανατροφοδότηση σχετικά με το αν οι αναφορές ύποπτης δραστηριότητας (SAR) οδηγούν σε επιβεβαιωμένα προαπαιτούμενα αδικήματα,

γεγονός που καθιστά πιο δύσκολη για τον ιδιωτικό τομέα την επικύρωση των δραστηριοτήτων που σχετίζονται με την εμπορία ανθρώπων.

Δεδομένου ότι η διαφάνεια σχετικά με το αποτέλεσμα των χρηματοοικονομικών ερευνών για εμπορία ανθρώπων δεν είναι πάντα δυνατή, οι αποδεδειγμένες υποθέσεις θα πρέπει να χρησιμοποιούνται για την εκπαίδευση και τη μελλοντική μείωση του κινδύνου. Οι πάροχοι χρηματοοικονομικών υπηρεσιών μπορούν να εντοπίσουν αποδεδειγμένες περιπτώσεις εμπορίας ανθρώπων με τους εξής τρόπους:

- Εξετάζοντας τις καθημερινές αρνητικές ειδήσεις των μέσων ενημέρωσης για συνδέσεις με εσωτερικές έρευνες.
- Εγγραφόμενοι σε ενημερώσεις από τις αρχές επιβολής του νόμου ή τις ΜΧΠ σχετικά με την επιβολή του νόμου για την εμπορία ανθρώπων και διασταυρώνοντας τις πληροφορίες αυτές με εσωτερικές υποθέσεις.
- Δημιουργώντας ένα κανάλι άμεσης παραπομπής για τις διωκτικές αρχές που σχετίζονται με έρευνες για εμπορία ανθρώπων.

Συνιστάται η ανταλλαγή πληροφοριών από αποδεδειγμένες υποθέσεις εμπορίας ανθρώπων με την ευρύτερη ομάδα έρευνας, και όχι μόνο με την εξειδικευμένη μονάδα εμπορίας ανθρώπων. Αυτό συνάδει με τις οδηγίες του 1ου Βήματος (Κεντρική Εποπτεία) και μπορεί να ενισχύσει το ηθικό των ερευνητών/-τριών, να δημιουργήσει ένα αίσθημα σκοπού και να βελτιώσει τις πιθανότητες κατανομής πόρων ή συνεργασίας μεταξύ των ομάδων.

<u>Βήμα 10ο</u>: Τα τελευταία χρόνια, η **σημασία και** η **επικράτηση των Συμπράξεων Δημόσιου-Ιδιωτικού Τομέα (ΣΔΙΤ) στην καταπολέμηση των οικονομικών**

εγκλημάτων, ιδίως της εμπορίας ανθρώπων στον επιχειρηματικό τομέα, **έχουν αυξηθεί σημαντικά**. Η παγκόσμια προσπάθεια για την εξάλειψη της εμπορίας ανθρώπων έχει οδηγήσει σε μεγαλύτερη συνεργασία μεταξύ των ανταγωνιστών του κλάδου για την αντιμετώπιση των οικονομικών εγκλημάτων. Οι επαγγελματίες που ασχολούνται με την καταπολέμηση του οικονομικού εγκλήματος έχουν συνειδητοποιήσει ότι οι διακινητές μετακινούνται μεταξύ διαφορετικών ιδρυμάτων και τραπεζών, γεγονός που έχει οδηγήσει στη συνεργασία για την αντιμετώπιση αυτών των ζητημάτων. Μερικές από τις κορυφαίες ΣΔΙΤ περιλαμβάνουν την Joint Money Laundering Intelligence Taskforce (JMLIT) του Ηνωμένου Βασιλείου, την Fintel Alliance της Αυστραλίας και το Project Protect του Καναδά. Οι ΗΠΑ διαθέτουν επίσης μηχανισμούς όπως τον Νόμο US: PATRIOT Act 314(a) για την ανταλλαγή πληροφοριών.

Τα κίνητρα για τη συμμετοχή σε ΣΔΙΤ περιλαμβάνουν την έκθεση σε διαφορετικές προσεγγίσεις στις χρηματοοικονομικές έρευνες, την ταχύτερη ανάπτυξη δεικτών εμπορίας ανθρώπων, την οικοδόμηση ισχυρότερων σχέσεων με ομοτίμους και τις αρχές επιβολής του νόμου, την ενίσχυση των ερευνών, την κοινή χρήση πόρων και τη δέσμευση για το κοινωνικό καλό. Ωστόσο, ο ΟΑΣΕ αναγνωρίζει τις προκλήσεις που υπάρχουν στην εδραίωση αποτελεσματικής συνεργασίας μεταξύ των ΜΧΠ, των αρχών επιβολής του νόμου και των φορέων που υποβάλλουν αναφορές STR. Μία από αυτές τις προκλήσεις είναι η μονόπλευρη ροή πληροφοριών από τις ΜΧΠ, η οποία συχνά περιορίζει την ικανότητά τους να μοιράζονται πληροφορίες εκτός του οργανισμού τους. Η ανατροφοδότηση σχετικά με αναφορές ύποπτων συναλλαγών υψηλής ποιότητας θα μπορούσε να βελτιώσει την εκπαίδευση, τις μεθόδους ανίχνευσης και την ποιότητα των αναφορών ύποπτων συναλλαγών.

Η έλλειψη ανατροφοδότησης από τις ΜΧΠ και η απουσία διεθνών βάσεων δεδομένων για τους εμπόρους ανθρώπων υπογραμμίζουν την ανάγκη για ΣΔΙΤ. Η

δημιουργία μιας ΣΔΙΤ δεν απαιτεί πάντα νέους νόμους. Μπορούν να χρησιμοποιηθούν τα υπάρχοντα νομικά πλαίσια. Για παράδειγμα, το Project Protect στον Καναδά λειτούργησε με επιτυχία στο πλαίσιο του νομικού πλαισίου της εθνικής κυβέρνησης εστιάζοντας σε γενικές τυπολογίες και δείκτες, ενώ σεβάστηκε τη νομοθεσία περί απορρήτου. Είναι μείζονος σημασίας να κατανοηθούν τα νομικά όρια και να εργαστούμε εντός αυτών για την προώθηση της συνεργασίας. Οι μακροπρόθεσμοι στόχοι των ΣΔΙΤ μπορούν να περιλαμβάνουν την προώθηση αλλαγών στη νομοθεσία με βάση επιτυχημένες συνεργασίες. Η έναρξη ή η συμμετοχή σε μια ΣΔΙΤ πρέπει να ακολουθεί τη θέσπιση μιας σταθερής διαδικασίας έρευνας, αλλά η έγκαιρη συνεργασία είναι πολύτιμη. Μπορεί να προσφέρει πληροφορίες που διαμορφώνουν τη διαδικασία έρευνας με τρόπους που θα ήταν δύσκολο να επιτευχθούν μετά την εφαρμογή της διαδικασίας. Η συμμετοχή σε μια ΣΔΙΤ θα ενισχύσει την πληρότητα μιας προσέγγισης για τη διερεύνηση της εμπορίας ανθρώπων.

Βήμα 11ο: Οι έρευνες για την εμπορία ανθρώπων, ιδίως στον τραπεζικό τομέα, μπορούν να έχουν αρνητικές συνέπειες στους/στις επιζώντες/-σες. Αυτό υπογραμμίζει τη σημασία του 4ου Βήματος (Αξιολόγηση της Έρευνας για Δραστηριότητες Εμπορίας Ανθρώπων), το οποίο διασφαλίζει ότι οι δραστηριότητες που σχετίζονται με την εμπορία ανθρώπων ορίζονται σαφώς σε επίπεδο ομάδας ή ιδρύματος. Η σωστή εκτέλεση του 4ου Βήματος μπορεί να συμβάλει στη μείωση της περιττής εργασίας αργότερα διασφαλίζοντας ότι αθώα άτομα δεν θα αποκλειστούν λανθασμένα. Δεδομένου ότι οι διακινητές συχνά εκμεταλλεύονται την οικονομική κατάσταση των θυμάτων τους, συνιστάται να δοθεί στους/στις επιζώντες/-σες που έχουν διαφύγει από την εμπορία ανθρώπων η ευκαιρία να ανασυγκροτήσουν το οικονομικό τους προφίλ.

Ένα επιτυχημένο παράδειγμα υποστήριξης των επιζώντων/-σών της εμπορίας ανθρώπων για οικονομικούς σκοπούς είναι ένα πρόγραμμα που ξεκίνησε η HSBC στο Ηνωμένο Βασίλειο τον Ιούνιο του 2019. Το πρόγραμμα αυτό βοηθά τους/τις επιζώντες/-σες που παραπέμπονται από τον Εθνικό Μηχανισμό Παραπομπής του Ηνωμένου Βασιλείου να αντιμετωπίσουν προκλήσεις όπως η παροχή αποδεικτικών στοιχείων διεύθυνσης και ταυτότητας. Επιπρόσθετα, το Σχέδιο Δράσης για την Κινητοποίηση Χρηματοδοτικών Πόρων κατά της Δουλείας και της Εμπορίας Ανθρώπων της Πρωτοβουλίας του Λιχτενστάιν, που δημιουργήθηκε σε συνεργασία με το Πανεπιστήμιο των Ηνωμένων Εθνών και διάφορες κυβερνήσεις έχει συγκεντρώσει διάφορα χρηματοπιστωτικά ιδρύματα για την επέκταση των προσπαθειών της HSBC σε διάφορα ιδρύματα και δικαιοδοσίες. Η Scotiabank, σε συνεργασία με το πρόγραμμα Deborah's Gate του Στρατού Σωτηρίας για την καταπολέμηση της εμπορίας ανθρώπων, ήταν η πρώτη τράπεζα που άνοιξε λογαριασμούς για επιζώντες/-σες στο πλαίσιο αυτής της πρωτοβουλίας χρηματοοικονομικής ένταξης. Αναμένεται ότι άλλα συμμετέχοντα χρηματοπιστωτικά ιδρύματα θα ακολουθήσουν το παράδειγμά της και θα αναπτύξουν παρόμοια προγράμματα.

Καθώς η προσοχή και οι προσπάθειες συνεχίζουν να επικεντρώνονται σε όσα άτομα διευκολύνουν την εμπορία ανθρώπων, **είναι σημαντικό να μην ξεχνάμε τα θύματα**. Οι Συμπράξεις Δημόσιου και Ιδιωτικού Τομέα και η συνεργασία με διακυβερνητικές ομάδες μπορούν να δημιουργήσουν μια ολοκληρωμένη προσέγγιση για την καταπολέμηση της εμπορίας ανθρώπων ωφελώντας όχι μόνο τα εμπλεκόμενα ιδρύματα αλλά και τα θύματα, συχνά με ελάχιστο κόστος υλοποίησης.

Εντοπισμός ύποπτων χρηματοοικονομικών δραστηριοτήτων

9.5.4

Ο ΟΑΣΕ δημοσίευσε έναν **κατάλογο χρηματοοικονομικών δεικτών συναλλαγών και των λεγόμενων προειδοποιητικών σημαδιών ("red flags") που ισχύουν για την εμπορία ανθρώπων και ειδικά για την εργασιακή εκμετάλλευση**. Ο ακόλουθος κατάλογος έχει ληφθεί από την έκθεση του ΟΑΣΕ και έχουν αφαιρεθεί τρεις φαινομενικά συγκεκριμένοι δείκτες για την αφαίρεση οργάνων καθώς και επτά για τη σεξουαλική εκμετάλλευση, ώστε να είναι πιο κατάλληλος για την εργασιακή εκμετάλλευση, ακόμη και αν σε ειδικές περιπτώσεις οι δείκτες μπορεί να διαφέρουν και να αλληλεπικαλύπτονται (OSCE, 2019, σ. 61ff).

- Χρήση εμπορικών λογαριασμών από προστάτες.
- Μη καταβολή φόρων, αποζημιώσεων εργαζομένων και άλλων τελών σε φορολογική αρχή.
- Το ποσοστό αμοιβής για κάθε περίοδο πληρωμής είναι πανομοιότυπο (χωρίς αλλαγές για υπερωρίες, διακοπές, αναρρωτικές άδειες, πληρωμές μπόνους κ.λπ.) σε θέσεις εργασίας όπου αυτό δεν θα ήταν αναμενόμενο.
- Επαναλαμβανόμενες πληρωμές μισθών σε αδικαιολόγητα χαμηλά ποσά (π.χ. πολύ χαμηλότερα από τον κατώτατο μισθό).
- Σημαντικό μερίδιο του κεφαλαίου της εταιρείας σε καταθέσεις χωρίς προθεσμία – δυσανάλογος χρηματοοικονομικός κύκλος εργασιών.
- Δάνεια που χορηγούνται από μέτοχο σε συνδεδεμένο νομικό πρόσωπο και επακόλουθη μεταβίβαση, πλασματικό δάνειο.

- Διαρθρωτική οργάνωση μέσω εμπορικών οντοτήτων και μεταφορά χρημάτων με τη χρήση σύμβασης δανείου.
- Υπερβολική χρήση υπηρεσιών "ride sharing" (κοινή χρήση οχήματος) μετά τα μεσάνυχτα.
- Έλλειψη εξόδων διαβίωσης, όπως τρόφιμα, βενζίνη, υπηρεσίες κοινής ωφέλειας και ενοίκιο.
- Αγορές σε εστιατόρια και υπηρεσία δωματίου, χωρίς δωμάτια.
- Χρήση πολλαπλών ατόμων για τη διενέργεια τραπεζικών συναλλαγών.
- Υψηλές ή/και συχνές δαπάνες σε αεροδρόμια, λιμάνια, άλλους συγκοινωνιακούς κόμβους ή στο εξωτερικό, που δεν συνάδουν με την προσωπική χρήση του ατόμου ή τη δηλωθείσα επιχειρηματική δραστηριότητά του στο εξωτερικό.
- Κατάθεση μετρητών σε διαφορετικές πόλεις σε ολόκληρη τη χώρα.
- Πληρωμές σε γραφεία ευρέσεως εργασίας ή φοιτητικών γραφείων που δεν διαθέτουν άδεια/δεν είναι εγγεγραμμένα ή που παραβιάζουν την εργατική νομοθεσία.
- Σχετικά υψηλές δαπάνες για είδη που δεν συνάδουν με τον δηλωμένο επιχειρηματικό σκοπό.
- Συναλλαγές που πραγματοποιούνται εκτός του γνωστού ωραρίου λειτουργίας της επιχείρησης.
- Διασυνοριακές μεταφορές κεφαλαίων που δεν συνάδουν με τον δηλωμένο επιχειρηματικό σκοπό του κατόχου του λογαριασμού ή/και μεταξύ ανεξήγητων

μοτίβων διασυνοριακών συναλλαγών μεταξύ γνωστών διαδρομών διακίνησης ή περιοχών όπου υπάρχει υψηλότερος κίνδυνος διακίνησης.

- Ευρεία χρήση μετρητών, μεταξύ άλλων για την αγορά περιουσιακών στοιχείων των επιχειρήσεων.
- Εσωτερικές μεταφορές από εταιρείες που δραστηριοποιούνται σε τομείς ευαίσθητους σε κοινωνική απάτη, τα χρήματα αποσύρονται σε μετρητά αμέσως μετά.
- Χρήση ιδρυμάτων που δεν ανήκουν στο χρηματοπιστωτικό σύστημα (μη παραδοσιακά).
- Χρήση μεταφορέων μετρητών και επαναλαμβανόμενες αναλήψεις μετρητών.
- Αγορά τραπεζικών επιταγών πληρωτέων σε καζίνο αμέσως μετά τις καταθέσεις.
- Ανεξήγητα/Αδικαιολόγητα μεγάλα κέρδη για μια εταιρεία.
- Κατάθεση μετρητών συχνά λίγο κάτω από το όριο αναφοράς.
- Κατάθεση μετρητών σε διάφορα καταστήματα ή ATM.
- Αγορά γραμματίων για την πληρωμή λογαριασμών αντί για την έκδοση προσωπικών επιταγών.
- Επαγγελματικοί λογαριασμοί με εμφανείς κρατήσεις από τους μισθούς των εργαζομένων για διάφορες κατηγορίες δαπανών, όπως στέγαση και διατροφή.
- Εξαργυρωμένες επιταγές μισθοδοσίας στις οποίες το μεγαλύτερο μέρος των χρημάτων είτε κατατίθεται ξανά στον λογαριασμό του εργοδότη είτε παρακρατείται από τον εργοδότη.

- Αποστολέας ή δικαιούχος με ελλιπείς πληροφορίες.
- Αγορά τραπεζικών επιταγών πληρωτέων σε καζίνο αμέσως μετά τις καταθέσεις.
- Μεταφορές από διαφορετικές περιοχές προς τα ίδια πρόσωπα σε χώρες που είναι γνωστό ότι ενέχουν υψηλότερο κίνδυνο για δραστηριότητες εμπορίας ανθρώπων.
- Οι επιταγές κρατικής βοήθειας κατατίθενται στον λογαριασμό, ακόμη και αν ο κάτοχος διαθέτει σημαντικό χρηματικό ποσό.
- Μπορούν επίσης να πραγματοποιηθούν ηλεκτρονικές μεταφορές/εμβάσματα.
- Συνδυασμός μετρητών με νόμιμες πηγές εισοδήματος.
- Δραστηριότητα εξευγενισμού (ανταλλαγή χαρτονομισμάτων μικρής ονομαστικής αξίας με χαρτονομίσματα μεγαλύτερης ονομαστικής αξίας).
- Συχνές αγορές πολλαπλών μικρών ποσών Bitcoin ή εικονικών νομισμάτων απευθείας από τον πελάτη ή μέσω ανταλλαγών.
- Μεταφορές κεφαλαίων που αφορούν τρίτους με εναλλακτικά ονόματα που αναφέρονται σε παρένθεση.
- Ο λογαριασμός λαμβάνει μισθούς από νόμιμες, συχνά εθνικές εταιρείες εύρεσης προσωπικού, αλλά τα χρήματα παραμένουν αχρησιμοποίητα για μεγάλες περιόδους.
- Εστιατόρια γρήγορου φαγητού (ταχυφαγεία): συχνές αγορές χαμηλής αξίας σε σχετικά σύντομο χρονικό διάστημα και ασυνεπείς με την αναμενόμενη δραστηριότητα.

- Ο λογαριασμός φαίνεται να λειτουργεί ως λογαριασμός διοχέτευσης.

Η ακόλουθη μελέτη περίπτωσης από τους Francavilla Lyon & De Cock (2024) αποτελεί παράδειγμα του τρόπου με τον οποίο τα μοτίβα χρηματοοικονομικών συναλλαγών μπορούν να χρησιμεύσουν ως δείκτες πιθανής εργασιακής εκμετάλλευσης στον τομέα της φιλοξενίας. Το παράδειγμα αυτό υπογραμμίζει τον κρίσιμο ρόλο της χρηματοοικονομικής ανάλυσης στον εντοπισμό των κινδύνων εμπορίας ανθρώπων και στην ανίχνευση κρυφών μορφών σύγχρονης δουλείας:

Αρχική κατάσταση: Ένας Κινέζος πολίτης ανοίγει έναν ιδιωτικό λογαριασμό και δηλώνει ότι εργάζεται στο εστιατόριο Χ. Η ανάλυση της επιχειρηματικής σχέσης δείχνει ότι η διεύθυνση αυτού του ατόμου και η διεύθυνση του εστιατορίου Χ είναι ίδιες. Μερικοί από τους εισερχόμενους μισθούς αποσύρονται ξανά σε μετρητά ή μεταφέρονται σε τρίτους (χωρίς προφανή οικογενειακή σχέση). Οι πληρωμές των μισθών γίνονται ακανόνιστα και σε ποικίλα ποσά. Κατά τη διάρκεια μιας συνομιλίας μεταξύ της τράπεζας και του πελάτη, ο τελευταίος ενημέρωσε την τράπεζα ότι οι πληρωμές από το εξωτερικό ήταν διατροφές που κατέβαλε στην πρώην σύζυγό του και για τα παιδιά τους. Ωστόσο, σύμφωνα με το KYC, ο πελάτης δεν έχει παιδιά. Επιπλέον, σύμφωνα με τη σύμβαση εργασίας του, ο πελάτης έχει μόνιμη θέση με σταθερό μισθό και δεν εργάζεται με ωρομίσθιο. Λείπουν τα αναμενόμενα καθημερινά έξοδα (φαγητό, ενοίκιο, ασφάλιση κ.λπ.).

Οι δείκτες πιθανής εργασιακής εκμετάλλευσης σε αυτό το σενάριο είναι οι εξής:

- Εθνικότητα κινδύνου (πελάτης)·
- Κίνδυνος τομέα για εργασιακή εκμετάλλευση·
- Συναλλαγές διαμεσολάβησης·

- Συναλλαγές σε μετρητά·
- Απουσία αναμενόμενων καθημερινών δαπανών·
- Ιδιωτική διεύθυνση ίδια με τη διεύθυνση εργασίας·
- Αντιφατικές δηλώσεις από τον πελάτη.

9.5.5 Προκλήσεις στις χρηματοοικονομικές έρευνες

Μια σημαντική πρόκληση στις χρηματοοικονομικές έρευνες είναι η εξελισσόμενη φύση των **τεχνικών συσκότισης** που χρησιμοποιούν οι εγκληματίες για να αποκρύψουν τα χρηματοοικονομικά ίχνη τους. Τεχνικές όπως οι **υπηρεσίες ανάμειξης**, το **chain-hopping** και η **χρήση κρυπτονομισμάτων** που εστιάζουν στην προστασία του απορρήτου αποτελούν σοβαρά εμπόδια για τους/τις ερευνητές/-τριες. Για παράδειγμα, οι υπηρεσίες ανάμειξης, γνωστές και ως tumblers, επιτρέπουν στους/στις χρήστες/-στριες να αποκρύψουν την προέλευση των κεφαλαίων τους συγκεντρώνοντάς τα και αναδιανέμοντάς τα. Το chain-hopping περιλαμβάνει τη γρήγορη μετατροπή κρυπτονομισμάτων μεταξύ διαφορετικών πλατφορμών καθιστώντας πιο δύσκολη την παρακολούθηση της κίνησης των κεφαλαίων. Επιπλέον, τα νομίσματα που εστιάζουν στην προστασία του απορρήτου, όπως το Monero και το Zcash, προσφέρουν βελτιωμένες λειτουργίες ανωνυμίας περιπλέκοντας περαιτέρω τις προσπάθειες των αρχών επιβολής του νόμου.

Για να αντιμετωπίσουν αυτές τις προκλήσεις, οι ερευνητές/-τριες οικονομικού εγκλήματος βασίζονται όλο και περισσότερο στη **συνεργασία με εμπειρογνώμονες ψηφιακής εγκληματολογίας**. Η ψηφιακή εγκληματολογία επιτρέπει στους/στις ερευνητές/-τριες να εξάγουν και να αναλύουν ηλεκτρονικά αποδεικτικά στοιχεία,

όπως κρυπτογραφημένες επικοινωνίες, διευθύνσεις IP και μεταδεδομένα συναλλαγών. Αυτή η διεπιστημονική προσέγγιση είναι ζωτικής σημασίας για την αποκάλυψη κρυφών χρηματοοικονομικών δικτύων και τον εντοπισμό παράνομων χρηματοοικονομικών ροών πέρα από τα σύνορα. Δεδομένης της διακρατικής φύσης των οικονομικών εγκλημάτων, η συνεργασία μεταξύ χρηματοπιστωτικών ιδρυμάτων, ρυθμιστικών αρχών και διεθνών οργανισμών είναι απαραίτητη για την αποτελεσματική διεξαγωγή οικονομικών ερευνών. «Οι καινοτόμοι τρόποι μεταφοράς χρημάτων, σε συνδυασμό με την αυξανόμενη συνειδητοποίηση των επαγγελματιών που καταπολεμούν τα οικονομικά εγκλήματα ότι οι διακινητές μετακινούνται από ίδρυμα σε ίδρυμα, από τράπεζα σε τράπεζα, τους οδήγησε στη συνεργασία» (OSCE, 2019, σ. 43).

9.5.6 Τεχνολογικές εξελίξεις και τάσεις

Οι πρόσφατες τεχνολογικές εξελίξεις έχουν επηρεάσει σημαντικά το χρηματοοικονομικό έγκλημα διαμορφώνοντας νέες μεθόδους παράνομης δραστηριότητας, ενώ παράλληλα παρέχουν βελτιωμένα εργαλεία για χρηματοοικονομικές έρευνες. Για παράδειγμα, η άνοδος των κρυπτονομισμάτων και της τεχνολογίας blockchain, έχει διευκολύνει διάφορες μορφές οικονομικού εγκλήματος, όπως το ξέπλυμα χρήματος, η απάτη και ακόμη και η εμπορία ανθρώπων. Η αυξημένη χρήση **ψηφιακών περιουσιακών στοιχείων** επιτρέπει στους εγκληματίες να μεταφέρουν κεφάλαια εντός και εκτός συνόρων με μεγαλύτερη ανωνυμία παρακάμπτοντας τα παραδοσιακά χρηματοπιστωτικά ιδρύματα και τους ρυθμιστικούς ελέγχους. Αν και το **Bitcoin** εξακολουθεί να είναι το πιο γνωστό κρυπτονόμισμα, παρατηρείται μια αυξανόμενη στροφή προς εναλλακτικές λύσεις που εστιάζουν

περισσότερο στην προστασία του απορρήτου, όπως το **Monero** και το **Zcash**, οι οποίες περιπλέκουν περαιτέρω τις προσπάθειες των αρχών επιβολής του νόμου.

Μια σημαντική τάση είναι η χρήση **τεχνικών συσκότισης** που έχουν σχεδιαστεί ειδικά για ψηφιακά περιουσιακά στοιχεία. Οι εγκληματίες βασίζονται όλο και περισσότερο σε εργαλεία όπως **mixer**, **tumbler** και **πορτοφόλια απορρήτου (privacy wallets)** για να συγκαλύψουν τα ίχνη των συναλλαγών και να αποφύγουν τον εντοπισμό. Αυτές οι μέθοδοι καθιστούν δύσκολη για τις αρχές την παρακολούθηση των παράνομων χρηματοοικονομικών ροών, ιδίως σε περιπτώσεις που σχετίζονται με την εμπορία ανθρώπων, καθώς οι διακινητές χρησιμοποιούν ψηφιακά νομίσματα για να εισπράττουν πληρωμές και να ξεπλένουν τα έσοδα. Η αποκεντρωμένη και ψευδώνυμη φύση των συναλλαγών που βασίζονται σε blockchain έχει δημιουργήσει ένα περιβάλλον στο οποίο το οικονομικό έγκλημα μπορεί να ευδοκιμήσει εκτός αν αντιμετωπιστεί με προηγμένες τεχνικές έρευνας.

Παράλληλα, τα άτομα που διαπράττουν οικονομικά εγκλήματα γίνονται ολοένα και πιο **αυτοδύναμα** απομακρύνοντας την εξάρτησή τους από εξωτερικούς χορηγούς ή μεσάζοντες. Αυτή η τάση είναι εμφανής στην αύξηση των ηλεκτρονικών απάτων, των επιθέσεων ransomware και των διαδικτυακών απάτων, οι οποίες δημιουργούν κεφάλαια για δίκτυα οργανωμένου εγκλήματος, συμπεριλαμβανομένων εκείνων που ασχολούνται με την εμπορία ανθρώπων. Η αυξανόμενη χρήση ψευδών διαδικτυακών αγορών, ψευδών εκστρατειών συγκέντρωσης κεφαλαίων και παραπλανητικών πλατφορμών ηλεκτρονικού εμπορίου έχει διευρύνει περαιτέρω τις ευκαιρίες για οικονομικό έγκλημα.

Παρά τις προκλήσεις αυτές, οι τεχνολογικές εξελίξεις φέρνουν στο φως νέα εργαλεία για την καταπολέμηση του οικονομικού εγκλήματος. **Η ανάλυση blockchain**

και **η Τεχνητή Νοημοσύνη** διαδραματίζουν καθοριστικό ρόλο στις οικονομικές έρευνες, καθώς βοηθούν τις αρχές να εντοπίζουν παράνομες συναλλαγές και να αναγνωρίζουν ύποπτα μοτίβα. Τα συστήματα παρακολούθησης συναλλαγών που βασίζονται στην Τεχνητή Νοημοσύνη μπορούν να αναλύουν τεράστιες ποσότητες δεδομένων σε πραγματικό χρόνο επισημαίνοντας ανωμαλίες που μπορεί να υποδηλώνουν δραστηριότητες σχετικές με το ξέπλυμα χρήματος ή την εμπορία ανθρώπων. Τέλος, τα εργαλεία εγκληματολογικής ανάλυσης blockchain επιτρέπουν στους/στις ερευνητές/-τριες να παρακολουθούν τις κινήσεις των κρυπτονομισμάτων και να αποκαλύπτουν κρυφές συνδέσεις μεταξύ εγκληματικών οντοτήτων.

9.5.7 Συστάσεις

Για την αποτελεσματική διεξαγωγή χρηματοοικονομικών ερευνών είναι απαραίτητο ένα ισχυρό νομικό πλαίσιο για τη δίωξη οικονομικών αδικημάτων. Τα διεθνή πρότυπα, όπως για παράδειγμα οι συστάσεις της **Ομάδας Χρηματοοικονομικής Δράσης (FATF)**, παρέχουν τη βάση για τα μέτρα AML/CFT. Οι εν λόγω κανονισμοί απαιτούν από τις αρχές επιβολής του νόμου να διεξάγουν χρηματοοικονομικές έρευνες, να διευκολύνουν τη διασυνοριακή συνεργασία και να εφαρμόζουν διαδικασίες κατάσχεσης περιουσιακών στοιχείων. Η Σύσταση 30 της FATF, για παράδειγμα, υπογραμμίζει τη σημασία του διορισμού αρμόδιων αρχών με εξουσία να διερευνούν αδικήματα νομιμοποίησης εσόδων από παράνομες δραστηριότητες και χρηματοδότησης της τρομοκρατίας.

Λόγω του πολέμου στην Ουκρανία, οι εκτοπισμένοι άνθρωποι αντιμετωπίζουν αυξημένο κίνδυνο εμπορίας ανθρώπων. Σε απάντηση σε αυτή την αυξημένη ευαλωτότητα, οργανισμοί όπως ο Οργανισμός για την Ασφάλεια και τη Συνεργασία

στην Ευρώπη (ΟΑΣΕ) έχουν αναπτύξει στοχευμένους πόρους για την υποστήριξη των πρώτων ανταποκριτών. Για παράδειγμα, ο ΟΑΣΕ προσφέρει *ένα Συνοπτικό Εγχειρίδιο Εκπαιδευτικών Μαθημάτων κατά της Εμπορίας Ανθρώπων για τους Πρώτους Ανταποκριτές*, το οποίο περιλαμβάνει εξειδικευμένη εκπαίδευση σε διάφορες πτυχές των προσπαθειών καταπολέμησης της εμπορίας ανθρώπων. Μεταξύ αυτών, συγκεκριμένα μαθήματα εστιάζουν στις χρηματοοικονομικές έρευνες εφοδιάζοντας τους/τις επαγγελματίες με τα απαραίτητα εργαλεία για τον εντοπισμό και την καταπολέμηση των παράνομων χρηματοοικονομικών ροών που συνδέονται με την εμπορία ανθρώπων. Σύνδεσμος προς την επισκόπηση του μαθήματος: https://www.osce.org/cthb/562572.

9.6 Προτεινόμενες δραστηριότητες για το κεφάλαιο

Πίνακας 1 . Δραστηριότητα για ψηφιακή εγκληματολογία και χρηματοοικονομικές έρευνες

Τίτλος Δραστηριότητας	**Δραστηριότητα για ψηφιακή εγκληματολογία**
Τύπος Δραστηριότητας	Ομαδική εργασία (π.χ. ομάδες 3-6 ατόμων)
Διάρκεια	15-35 λεπτά
Μαθησιακοί Στόχοι	Προσδιορισμός βασικών ψηφιακών ιχνών και επόμενων βημάτων που πρέπει να ληφθούν.
Απαιτούμενα Υλικά	Παράδειγμα περίπτωσης με επαρκές ιστορικό (π.χ. έντυπη έκδοση) • Thomas, Day & Jackson (2019) στις σελίδες 31-38 και 38-42 στο https://airewb.org/wp-content/uploads/PUBLICATIONS/AR_EN_handbook_tools_best_practices.pdf

	• Crates (2022) στις σελίδες 9-14 στο https://www.antislaverycommissioner.co.uk/media/h4ggz4c2/iasc-construction-report-april-2022.pdf • Blog του Υπουργείου Εργασίας των ΗΠΑ (2022) στη διεύθυνση https://blog.dol.gov/2022/01/11/fighting-human-trafficking-the-legacy-of-the-el-monte-sweatshop • Lam & Skivankova (2009) στη σελίδα 5 στη διεύθυνση https://www.antislavery.org/wp-content/uploads/2017/01/trafficking_and_compensation2009.pdf • KOK Γερμανικό Δίκτυο ΜΚΟ κατά της Εμπορίας Ανθρώπων (χ.χ.) στη διεύθυνση https://www.kok-gegen-menschenhandel.de/menschenhandel/was-ist-menschenhandel/fallbeispiele (*χρησιμοποιήστε την αυτόματη μετάφραση για τον ιστότοπο και επιλέξτε την υποενότητα «Εμπορία Ανθρώπων για Εργασιακή Εκμετάλλευση»*) • 8ο Κεφάλαιο της Εκπαίδευσης
Οδηγίες για τον/τη Συντονιστή/-στρια	Τα συμμετέχοντα άτομα θα χωριστούν σε μικρότερες ομάδες. Θα τους δοθεί μια μελέτη περίπτωσης την οποία θα διαβάσουν (3-4 λεπτά). Στη συνέχεια, θα αρχίσουν να συζητούν στην ομάδα τους και θα προσπαθήσουν να προσδιορίσουν ποια ψηφιακά αποδεικτικά

	στοιχεία θα ήταν τα καταλληλότερα για μια επιτυχημένη ψηφιακή εγκληματολογική έρευνα. Επιπλέον, θα συζητήσουν ποιοι παράγοντες θα εμπλακούν και σε ποιο σημείο της ερευνητικής διαδικασίας (10-15 λεπτά). • Ποια ψηφιακά αποδεικτικά στοιχεία είναι σχετικά; Ποια ψηφιακά αποδεικτικά στοιχεία είναι πιο χρήσιμα και γιατί; • Πώς μπορούν οι εγκληματολόγοι να εξαγάγουν και να αναλύσουν αυτά τα ψηφιακά ίχνη; • Πώς μπορούν να βοηθήσουν στον εντοπισμό θυμάτων, διακινητών και μοτίβων; • Ποια μοτίβα ή προειδοποιητικά σημάδια (red flags) υποδηλώνουν εμπορία ανθρώπων; • Ποια είναι τα επόμενα βήματα που πρέπει να ακολουθήσουν οι ερευνητές/-τριες; • Πώς μπορούν να χρησιμοποιηθούν αυτά τα αποδεικτικά στοιχεία για την υποστήριξη των θυμάτων; Στη συνέχεια, κάθε ομάδα θα παρουσιάσει τα ευρήματά της (5-10 λεπτά).
Ανασκόπηση	Ο/Η συντονιστής/-στρια διευθύνει την παρουσίαση μετά την ομαδική εργασία.

Συμβουλές για τον/τη Συντονιστή/-στρια	Αν έχετε περισσότερο χρόνο, μπορείτε να χρησιμοποιήσετε διαφορετικά σενάρια περιπτώσεων. Κάθε ομάδα θα παρουσιάσει εν συντομία την περίπτωση και στη συνέχεια τα αποτελέσματα της συζήτησής της (αντί να εργάζεται κάθε ομάδα στην ίδια περίπτωση).
Φυλλάδια	Για παράδειγμα, μελέτες περίπτωσης που πρέπει να εκτυπωθούν και να δοθούν στα συμμετέχοντα άτομα, ενδεχομένως συμπληρωμένες με υλικό που περιλαμβάνει αποσπάσματα από: • Συνομιλίες WhatsApp μεταξύ του θύματος και του διακινητή με μηνύματα όπως «Μην ανησυχείς για τα χαρτιά, θα τα τακτοποιήσουμε εμείς για σένα», «Θα έχεις δωρεάν στέγαση και μεταφορά» ή «Συνάντησέ με στον σταθμό των λεωφορείων. Σβήσε αυτά τα μηνύματα». • Διαφημίσεις από την πλατφόρμα πρόσληψης. • Αρχεία τραπεζικών συναλλαγών. • Μεταδεδομένα από μια φωτογραφία που στάλθηκε στο θύμα με δεδομένα γεωγραφικής θέσης.
Παραλλαγές για Υλοποίηση μέσω του Διαδικτύου	Η υλοποίηση της δραστηριότητας μπορεί να γίνει διαδικτυακά. Δημιουργήστε συνεδρίες με δωμάτια επιμέρους συνομιλιών (breakout rooms) για την ομαδική εργασία.

Τίτλος Δραστηριότητας	**Δραστηριότητα για χρηματοοικονομικές έρευνες**
Τύπος Δραστηριότητας	Ομαδική εργασία (π.χ. ομάδες 3-6 ατόμων)
Διάρκεια	15-35 λεπτά
Μαθησιακοί Στόχοι	Εσωτερικοποίηση των βημάτων για τις χρηματοοικονομικές έρευνες και αναστοχασμός σχετικά με τις πιθανές προκλήσεις που προκύπτουν στον τομέα της εμπορίας ανθρώπων.
Απαιτούμενα Υλικά	Για παράδειγμα, μελέτες περίπτωσης που πρέπει να εκτυπωθούν και να διανεμηθούν στα συμμετέχοντα άτομα, ενδεχομένως συμπληρωμένες με υλικό που περιλαμβάνει αποσπάσματα από: • Αρχεία τραπεζικών συναλλαγών και τραπεζικά εκκαθαριστικά (μπορεί επίσης να είναι ένας πίνακας με τις στήλες: ημερομηνία, περιγραφή, χρέωση (EUR), πίστωση (EUR) και υπόλοιπο (EUR), που δείχνει πότε ένα άτομο πραγματοποίησε συναλλαγή (και σε ποια εταιρεία/πρόσωπο). • Αρχεία μισθοδοσίας.

	• Τιμολόγια.
Οδηγίες για τον/τη Συντονιστή/-στρια	Τα συμμετέχοντα άτομα θα χωριστούν σε μικρότερες ομάδες. Θα τους δοθεί μια μελέτη περίπτωσης την οποία θα διαβάσουν (3-4 λεπτά). Στη συνέχεια, θα ξεκινήσουν να συζητούν στην ομάδα τους και θα προσπαθήσουν να προσδιορίσουν τα βήματα για τις χρηματοοικονομικές έρευνες (π.χ. εξετάζοντας κάθε βήμα που έμαθαν προηγουμένως). Επιπλέον, θα συζητήσουν ποιοι παράγοντες θα εμπλακούν και σε ποιο σημείο της ερευνητικής διαδικασίας (10-15 λεπτά). • Ποιες τεχνικές χρηματοοικονομικής έρευνας πρέπει να χρησιμοποιηθούν; • Πώς μπορούν να συνεργαστούν οι αρχές επιβολής του νόμου με τις ΜΧΠ σε αυτό το θέμα; • Ποια νομικά εργαλεία πρέπει να εφαρμοστούν; • Ποιες προκλήσεις μπορούν να προσδιοριστούν; Στη συνέχεια, κάθε ομάδα θα παρουσιάσει τα ευρήματά της.
Ανασκόπηση	Ο/Η συντονιστής/-στρια διευθύνει την παρουσίαση μετά την ομαδική εργασία.

Συμβουλές για τον/τη Συντονιστή/-στρια	Αν έχετε περισσότερο χρόνο, μπορείτε να χρησιμοποιήσετε διαφορετικά σενάρια περιπτώσεων. Κάθε ομάδα θα παρουσιάσει εν συντομία την περίπτωση και στη συνέχεια τα αποτελέσματα της συζήτησής της (αντί να εργάζεται κάθε ομάδα στην ίδια περίπτωση).
Φυλλάδια	*Θα πρέπει να εκτυπωθεί μια μελέτη περίπτωσης και να δοθεί στα συμμετέχοντα άτομα.* • Thomas, Day & Jackson (2019) στις σελίδες 31-38 και 38-42 στο https://airewb.org/wp-content/uploads/PUBLICATIONS/AR_EN_handbook_tools_best_practices.pdf • Μελέτη περίπτωσης της Top Glove (Μαλαισία). Περισσότερες λεπτομέρειες είναι διαθέσιμες στο https://sevenpillarsinstitute.org/labor-exploitation-case-study-of-top-glove/#:~:text=This%20case%20study%20examines%20the%20allegations%20of%20forced,serves%20as%20the%20home%20of%20this%20multinational%20corporation. και Malaysia: Hidden cameras reveal poor working & living conditions at Top Glove factory, fuelling forced labour concerns in glove industry; incl. company comments - Business & Human Rights Resource Centre

Παραλλαγές για Υλοποίηση μέσω του Διαδικτύου	Η υλοποίηση της δραστηριότητας μπορεί να γίνει διαδικτυακά. Δημιουργήστε συνεδρίες με δωμάτια επιμέρους συνομιλιών (breakout rooms) για την ομαδική εργασία.

9.7 Αναφορές

Aronowitz, Alexis & Theuermann, Gerda & Tyurykanova, Elena. (2010). OSCE. *Analysing the Business Model of Trafficking in Human Beings to Better Prevent the Crime*. https://www.osce.org/files/f/documents/c/f/69028.pdf

Belser, P. (2005). *Forced labour and human trafficking: Estimating the profits*. Geneva: International Labour Office. https://ecommons.cornell.edu/bitstream/1813/99623/1/Forced_labor_no__17_Forced_labour_and_human.pdf

Cellebrite. (2024, November 15). *How Law Enforcement Can Turn the Tide Against Human Trafficking with Digital Evidence*. https://cellebrite.com/en/how-law-enforcement-can-turn-the-tide-against-human-trafficking-with-digital-evidence/

Dubey, H., Bhatt, S., & Negi, L. (2023). *Digital forensics techniques and trends: a review* The International Arab Journal of Information Technology, *20*(4), 644-654.

European Commission. (n.d.). *Financial investigations*. https://home-affairs.ec.europa.eu/policies/internal-security/organised-crime-and-human-trafficking/financial-investigations_en

Europol. (2020). *The challenges of countering human trafficking in the digital era*. https://www.europol.europa.eu/cms/sites/default/files/documents/the_challenges_of_countering_human_trafficking_in_the_digital_era.pdf

Europol. (2024, July). *Tackling threats, addressing challenges. Europol's response to migrant smuggling and trafficking in human beings in 2023 and onwards*. European

Migrant Smuggling Centre (EMSC). https://www.europol.europa.eu/cms/sites/default/files/documents/Tackling_threats__addressing_challenges_-_Europol%E2%80%99s_response_to_migrant_smuggling_and_trafficking_in_human_beings_in_2023_and_onwards.pdf

Francavilla, F., Lyon, S., & De Cock, M. (2024). *Profits and poverty: The economics of forced labour*. ILO. https://www.ilo.org/sites/default/files/2024-10/Profits%20and%20poverty%20-%20The%20economics%20of%20forced%20labour_WEB_20241017.pdf

Fraser, C. (2016). An analysis of the emerging role of social media in human trafficking: Examples from labour and human organ trading. *International Journal of Development Issues*, *15*(2), 98-112.

Gorenc, M. (2019). Benford's Law As a Useful Tool to Determine Fraud in Financial Statements. *Management, 14*(1). 19-31. 10.26493/1854-4231.14.19-31.

International Labour Organization. (2018). *Investigating Human Trafficking Cases Using a Victim-centred Approach*. International Organization for Migration. https://publications.iom.int/system/files/pdf/investigating_human_trafficking.pdf

International Labour Organization. (2023, July 30). H*uman Trafficking Evidence Gap Map*. https://rtaproject.org/human-trafficking-egm/#:~:text=The%20Evidence%20Gap%20Maps%20are%20a%20visual%20tool,the%20areas%20where%20evidence%20is%20limited%20or%20non-existent.

Kunz, R., Baughman, M., Yarnell, R., & Williamson, C. (2018). *Social media and sex trafficking process: From connection and recruitment, to sales*. Ohio: University of Toledo. https://www.utoledo.edu/hhs/htsji/pdfs/smr.pdf

Lugo-Graulich, K., Meyer, L. F., Souza, K., Tapp, S. N., Maryfield, B., & Bostwick, L. (2024). Improving sex trafficking victim identification: Indicators of trafficking in Online Escort Ads. *Journal of Human Trafficking*, 1-22.

Maras, M.-H. (2014). *Computer Forensics: Cybercriminals, Laws and* Evidence (2nd edition). Jones and Bartlett.

Mattmann, C., Yan G. H., Manjunatha, H., Gowda N, T., Zhou, A. J., Luo, J., & McGibbney, L. J. (2016). *Multimedia metadata-based forensics in human trafficking web data*. In: Murdock, V., Clarke, C. L. A., Kamps, J. & J. Karlgren. *Search an Exploration of X-rated Information*. p. 10-13.

OSCE. (2019, November 7). *Following the Money: Compendium of Resources and Step-by-Step Guide to Financial Investigations Related to Trafficking in Human Beings*. https://www.osce.org/files/f/documents/f/5/438323_0.pdf

Perez, A. R., & Rivas, P. (2023). Combatting human trafficking in the cyberspace: A natural language processing-based methodology to analyze the language in online advertisements. *arXiv preprint arXiv:2311.13118*.

Pizzuro, J. (2022, March 11). *Leveraging Magnet Forensics Software for Human Trafficking Investigations.* MAGNET FORENSICS. https://www.magnetforensics.com/blog/leveraging-magnet-forensics-software-for-human-trafficking-investigations/

Siavoshi, M. (2025, February 25). *Unraveling the Mystery of Benford's Law: Applications in Fraud Detection*. Statology. https://www.statology.org/unraveling-the-mystery-of-benfords-law-applications-in-fraud-detection/

Thomson Reuters. (2025, January 2). *Technology and human trafficking: Fighting the good fight.* https://legal.thomsonreuters.com/blog/technology-and-human-trafficking/#:~:text=How%20technology%20can%20fight%20human%20trafficking%201%20Prevention,in%20several%20ways%20that%20incorporate%20digital%20technology.%20

UNODC. (2019a, May). *Technology facilitating trafficking in persons*. https://www.unodc.org/e4j/en/tip-and-som/module-14/key-issues/technology-facilitating-trafficking-in-persons.html

UNODC. (2019b, March). *Module 6: Practical Aspects of Cybercrime Investigations and Digital Forensics. Handling of digital evidence*. https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/handling-of-digital-evidence.html

UNODC. (2020). *Global report on trafficking in persons 2020*. https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP_2020_15jan_web.pdf

Volodko, A., Cockbain, E., & Kleinberg, B. (2020). 'Spotting the signs' of trafficking recruitment online: exploring the characteristics of advertisements targeted at migrant job-seekers. *Trends in Organized Crime*, *23*, 7-35.

www.eradicating2project.eu

Co-funded by the European Union