Capitolul 9. Criminalistică digitală și investigații financiare

Coordonator de capitol:

BayHfoD

Co-funded by
the European Union

9. Capitolul 9. Criminalistică digitală și investigații financiare

9.1 Introducere

În lumea digitală de astăzi, granițele dintre viața virtuală și cea reală sunt adesea neclare, iar acest lucru este valabil și pentru dinamicile infracționale ale traficului de persoane în scopul exploatării prin muncă (pe scurt: exploatare prin muncă sau trafic de persoane). Capitolul de instruire „Criminalistică digitală și investigații financiare" evidențiază rolul crucial al acestor două discipline în detectarea și combaterea exploatării prin muncă. Criminalistica digitală se concentrează pe analiza datelor electronice pentru a colecta dovezi digitale ale activității infracționale legate de exploatarea prin muncă, în timp ce investigațiile financiare vizează urmărirea fluxurilor de bani și descoperirea rețelelor financiare din spatele acestor infracțiuni. Prin combinarea acestor două abordări, anchetatorii nu numai că pot identifica autorii, ci și pot descoperi legăturile adesea complexe dintre urmele digitale și tranzacțiile financiare care permit exploatarea prin muncă. În acest context, sunt prezentate proceduri, cele mai bune practici, metode și instrumente posibile care permit profesioniștilor să utilizeze interacțiunile dinamice dintre comunicarea digitală și fluxurile monetare pentru a ajuta victimele traficului de persoane și a lua măsuri legale împotriva autorilor.

Capitolul de instruire începe cu obiectivele de învățare pentru participanții la instruire (Secțiunea 2). Acestea sunt enumerate separat pentru „criminalistică digitală" și „investigații financiare". Aceasta este urmată de definițiile celor mai importanți termeni pentru acest capitol (Secțiunea 3). Secțiunea 4, nucleul capitolului de instruire, conține contextul teoretic și informativ al subiectelor. Aceasta este urmată de o activitate practică pentru capitolul de instruire, care permite participantului să lucreze cu informațiile

teoretice învățate în prealabil și să le proceseze mai profund (Secțiunea 5). Capitolul se încheie cu surse (Secțiunea 6).

9.2 Obiective de învățare

Acest capitol de instruire oferă participanților cunoștințele necesare pentru criminalistica digitală și investigațiile financiare legate de traficul de persoane și exploatarea prin muncă. Până la sfârșitul acestui capitol, participantul va fi capabil…

Criminalistică digitală

- să înțeleagă principiile criminalisticii digitale, inclusiv colectarea, conservarea și analiza datelor, asigurând în același timp integritatea lanțului de custodie
- să dețină competențele necesare pentru efectuarea achizițiilor criminalistice (imagine și copii logice)
- să știe unde să caute urme și dovezi digitale lăsate de traficanți și ce poate fi derivat din diferite surse de dovezi digitale
- înțelegerea cadrului legal privind dovezile digitale și asigurarea respectării cerințelor procedurale

Investigații financiare

- să identifice activitățile financiare suspecte care ar putea indica trafic de persoane
- să aplice o metodologie pas cu pas pentru efectuarea investigațiilor financiare legate de traficul de persoane
- să înțeleagă factorii economici ai traficului

- să fie conștient de provocările din investigațiile financiare, inclusiv utilizarea criptomonedelor, a conturilor offshore și a tehnicilor de anonimizare digitală
- să înțeleagă rolul parteneriatului public-privat (PPP) în investigațiile financiare și cooperarea internațională în combaterea traficului de persoane

9.3 Definiții

În cele ce urmează, vor fi prezentate pe scurt definițiile importante ale ambelor subiecte.

9.3.1 Definiții cheie în domeniul criminalisticii digitale

Criminalistică digitală

Criminalistica digitală implică identificarea, conservarea și examinarea probelor digitale pentru a susține investigațiile penale. Aceasta include metode de obținere, analiză și documentare a datelor pentru a urmări amprentele digitale ale activităților criminale.

Achiziție criminalistică

Crearea de copii fidele ale suporturilor de stocare digitale, menținând în același timp integritatea și trasabilitatea datelor (Lanțul de custodie). Aceasta include achiziții fizice (RAW, E01) și achiziții logice (L01, AD1).

Lanțul de custodie

O documentație continuă și cronologică a manipulării probelor digitale pentru a asigura autenticitatea și integritatea acestora în cadrul procedurilor judiciare.

Anti-criminalistică

Măsuri luate de un utilizator pentru a îngreuna evaluarea urmelor digitale sau chiar a o preveni: Criptare (FDE, container, ...); TOR/navigare privată, virtualizare → ștergerea mașinii virtuale (VM); programe pentru ștergere, curățare, schimbarea timestamp-ului etc.; ascunderea datelor, de exemplu, steganografie; împachetare multiplă.

eDiscovery

Utilizarea specifică a criminalisticii digitale pentru a analiza volume mari de date în scopul extragerii de informații relevante pentru investigații sau proceduri judiciare. Cu alte cuvinte, eDiscovery (electronic discovery) este analiza datelor pentru cazuri specifice (de exemplu, pentru crimă organizată; criminalitate economică, infracțiuni legate de securitatea statului). Pentru a efectua eDiscovery, sunt necesare cunoștințe specifice despre infracțiuni și despre cazul specific. În plus, deoarece datele sunt în continuă creștere, rapoartele criminalistice necesită extrase de date. Ceea ce ar putea ajuta la facilitarea eDiscovery este Modelul de referință pentru descoperirea electronică EDRM, un cadru care include standardele de descoperire și recuperare a datelor digitale, de exemplu:

- Noțiuni de bază despre hardware
- Noțiuni de bază ale criminalisticii digitale
- Structura suporturilor de date și a sistemelor de fișiere
- Scurtă introducere în instrumentele criminalistice
- Activități criminalistice de bază
- Structura și funcționalitatea sistemului de operare Windows
- Artefacte criminalistice din sistemele Windows

Medii de bootare criminalistice

Sisteme de operare specializate (de exemplu, sisteme bazate pe Linux sau Windows) utilizate pentru pornirea dispozitivelor digitale și efectuarea de analize criminalistice fără a modifica datele originale.

Matrice redundantă de discuri independente (RAID)

Un sistem care combină mai multe hard disk-uri pentru a îmbunătăți securitatea și performanța datelor, necesitând tehnici criminalistice specializate pentru obținerea de date.

9.3.2Cuvinte cheie legate de investigațiile financiare

Investigații financiare

Examinarea tranzacțiilor financiare pentru a descoperi activități ilegale precum spălarea de bani, finanțarea terorismului sau traficul de persoane și pentru a identifica autorii..

Spălare de bani (ML)

Procesul de deghizare a originii ilicite a fondurilor printr-o serie de tranzacții financiare pentru a le face să pară legitime. (Opus: Combaterea spălării banilor)

Cunoașterea clientelei (KYC)

O cerință de reglementare pentru instituțiile financiare de a verifica identitatea și antecedentele financiare ale clienților lor pentru a preveni spălarea banilor și finanțarea terorismului.

Rapoarte de tranzacții suspecte (STR-uri)

Rapoarte pe care instituțiile financiare trebuie să le depună atunci când o tranzacție este considerată potențial suspectă sau legată de spălarea banilor sau finanțarea terorismului.

Analiza blockchain-ului

Investigarea tranzacțiilor cu criptomonede pentru a identifica activități ilegale precum spălarea de bani, frauda sau finanțarea terorismului și pentru a urmări rețelele de infractori.

Criptomonede și tehnici de anonimizare

Monede digitale (de exemplu, Bitcoin, Monero) și metode precum mixere, tumblere sau lanțuri de tranzacții utilizate pentru a ascunde tranzacțiile financiare.

9.4 Partea teoretică / informativă

9.4.1 Criminalistică digitală

Această secțiune oferă o prezentare generală a criminalisticii digitale în Secțiunea 9.6.2, oferind informații generale despre ce este aceasta, cum poate fi clasificată și cum arată un proces tipic de criminalistică digitală. În plus, secțiunea descrie principiile de bază pe care un expert în criminalistică digitală ar trebui să le ia în considerare. Ulterior, Secțiunea 9.6.2 tratează cunoștințele de bază despre achizițiile criminalistice, deoarece acestea pun bazele unui proces de criminalistică digitală solid și de succes. Cu toate acestea, o introducere tehnică de bază suplimentară în criminalistica digitală (prin intermediul acestui prim pas al achiziției criminalistice) ar merge prea departe în acest moment - mai ales că, de exemplu, metodele de analiză sunt prea diverse pentru a fi acoperite aici. Prin urmare, nu este oportun, mai ales că aplicația se află în contextul traficului de persoane și al exploatării prin muncă, să se intre în pași suplimentari. În

consecință, Secțiunea 4.1.3 tratează criminalistica digitală în contextul traficului de persoane.

9.4.2Prezentare generală

Criminalistica este aplicarea metodelor științifice pentru analizarea și urmărirea penală a infracțiunilor. Criminalistica digitală, în special, se ocupă de întrebări precum:

- Unde sunt create urmele digitale?
- Cum pot fi recunoscute și evaluate urmele digitale?
- Cum pot fi securizate și utilizate urmele digitale?

Chiar dacă criminalistica digitală a fost deja definită în Secțiunea 3, merită să intrăm mai în detaliu. Criminalistica digitală cuprinde (1) căutarea, identificarea, (2) descrierea și (3) examinarea probelor digitale, inclusiv pentru a evalua fiabilitatea, validitatea și relevanța acestora pentru cazul specific. Ca ultimă etapă, (4) criminalistica digitală implică și raportarea acestor probe (Maras, 2014). Aceasta include metode de obținere, analiză și documentare a datelor pentru a urmări amprentele digitale ale activităților criminale, urme pe dispozitive digitale care pot și trebuie analizate în scopul urmăririi penale.

În mod normal, există **unități specializate** în criminalistică digitală în cadrul autorităților de aplicare a legii (LEA), motiv pentru care unitățile THB colaborează în principal cu unitățile de criminalistică digitală și nu lucrează de obicei doar pe probleme de criminalistică digitală. Prin urmare, este cel mai bine să se stabilească și să se asigure cooperarea cu această unitate. Mai mult, este recomandabil să se cunoască diferitele poziții profesionale din cadrul agenției, de exemplu, există un ofițer/agent de poliție specializat în IT? Ofițer/agent de poliție specializat în criminalitate cibernetică? Serviciu tehnic de investigații criminale? Specialist în criminalistică digitală? Cine este responsabil pentru ce și când pot contacta pe cine?

Criminalistica digitală cuprinde identificarea, securizarea și investigarea probelor digitale, luând în considerare și (1) circumstanțele juridice și condițiile-cadru (pentru a asigura utilizabilitatea în instanță) și (2) conservarea și documentarea lanțului de custodie și a integrității datelor. Prin urmare, esențială pentru criminalistica digitală este ca fiecare efort și fiecare pas să fie valabil în instanță și utilizabil în documentația judiciară.

Sarcinile tipice ale specialiștilor în criminalistică digitală includ: achiziția datelor de pe computere, suporturi de date, dispozitive mobile și spații de stocare online; pregătirea și evaluarea probelor computerizate; consiliere și asistență în timpul percheziților.

În plus, criminalistica digitală poate fi împărțită și clasificată în diferite domenii. Figura 11 oferă o imagine de ansamblu asupra posibilelor ramuri ale criminalisticii digitale. Criminalistica digitală se concentrează pe recuperarea, analizarea și conservarea dovezilor digitale de pe computere, inclusiv hard disk-uri, sisteme de fișiere, sisteme de operare și date de aplicații. Tehnicile cheie sunt imagistica discului, recuperarea fișierelor și analiza registrelor (vezi de exemplu, Casey, 2011). Criminalistica bazelor de date (uneori enumerată separat) se ocupă de examinarea bazelor de date (inclusiv bazele de date SQL și NoSQL) și a metadatelor acestora și, de exemplu, implică marcarea temporală a unei baze de date și analiza în timp real (vezi de exemplu, Dubey, Bhatt & Negi, 2023) pentru a descoperi manipularea datelor, accesul neautorizat sau alterarea. Dar criminalistica bazelor de date poate fi considerată și un subdomeniu al criminalisticii digitale, deoarece bazele de date sunt stocate în principal pe sisteme de calcul tradiționale, cum ar fi serverele. Criminalistica mobilă, sau uneori numită criminalistică a dispozitivelor mobile, se ocupă de extragerea și analiza datelor stocate pe dispozitive mobile, cum ar fi smartphone-uri, tablete și sisteme GPS (Dubey, Bhatt & Negi, 2023). Criminalistica rețelelor include analiza traficului de rețea pentru a obține informații, a detecta intruziuni și a obține probe criminalistice. În subdomeniul criminalisticii firewall-urilor, toate jurnalele firewall-urilor sunt examinate pentru a găsi dovezi valoroase.

Criminalistica cloud investighează dovezile stocate în medii cloud, abordând provocările legate de stocarea datelor multi-jurisdicționale, restricțiile de acces și cooperarea furnizorilor. Prin urmare, necesită considerații juridice și tehnice specializate. Criminalistica IoT examinează urmele digitale de pe dispozitivele Internet of Things (IoT), cum ar fi electrocasnicele inteligente, dispozitivele portabile, senzorii industriali și sistemele auto. Adesea implică o combinație de analiză a sistemelor încorporate, criminalistică a rețelelor și criminalistică tradițională a dispozitivelor. Criminalistica memoriei (RAM) se concentrează pe extragerea și analizarea memoriei volatile (RAM) pentru a descoperi procesele care rulează, cheile de criptare, programele malware și activitatea sistemului în timp real. Criminalistica malware implică analizarea software-ului malware pentru a înțelege comportamentul acestuia, a identifica originea acestuia și a atenua impactul acestuia (de exemplu, prin analiza statică și dinamică a programelor malware, sandboxing, inginerie inversă). Criminalistica dronelor se ocupă de extragerea datelor din vehiculele aeriene fără pilot (UAV), inclusiv jurnalele de zbor, stocarea la bord, urmărirea GPS și sistemele de comunicații. Criminalistica dark web și a criptomonedelor se concentrează pe activitățile ilicite de pe dark web, inclusiv traficul de persoane, comerțul cu droguri și criminalitatea cibernetică. Tehnicile criminalistice ale criptomonedelor ajută la urmărirea tranzacțiilor în Bitcoin sau alte monede digitale pentru a identifica actorii infracționali.

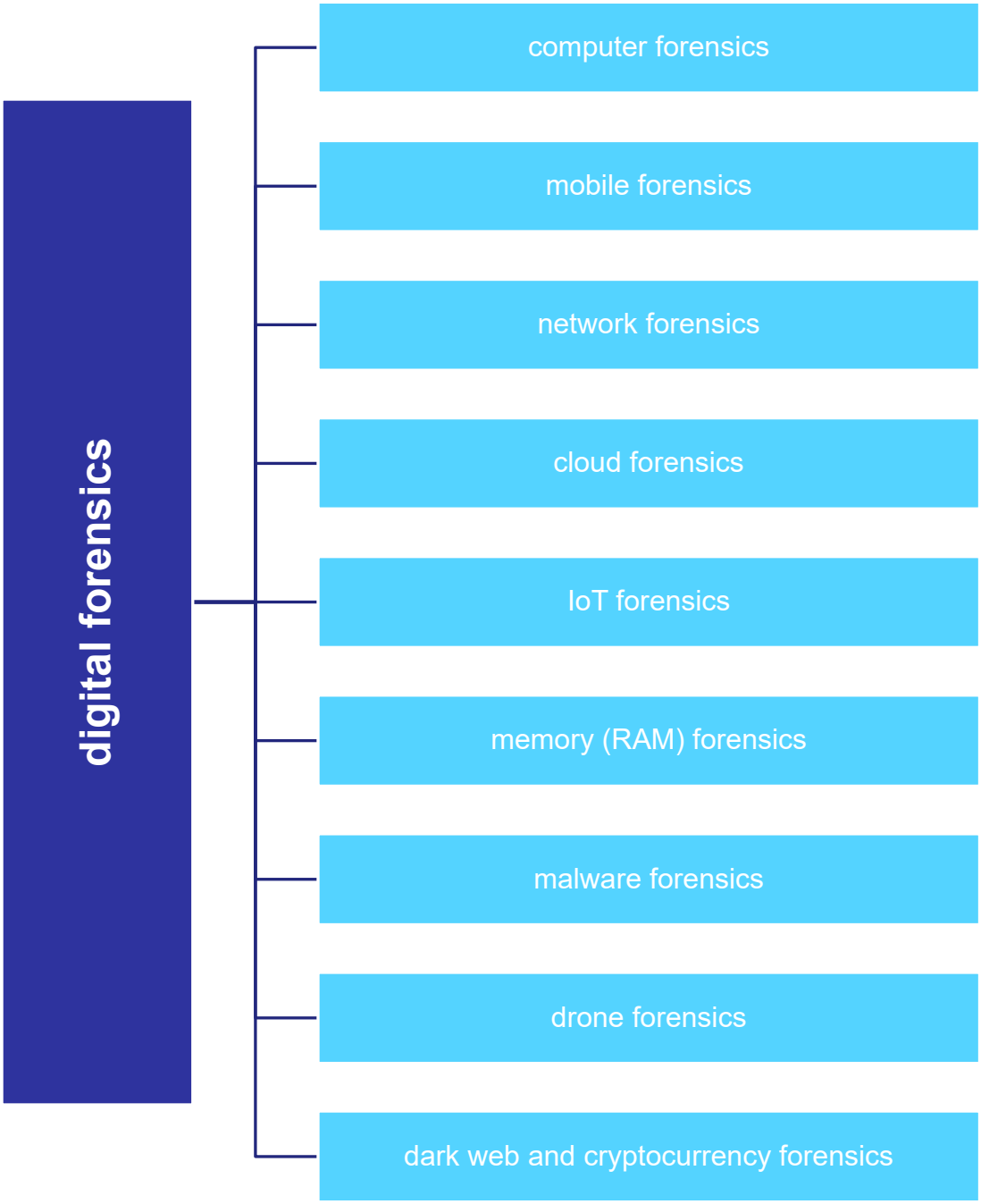

Figura1Posibile ramuri ale criminalisticii digitale

În plus, legătura dintre diferitele ramuri ale criminalisticii digitale și mediul tehnologiei informației este crucială, deoarece tipul de infrastructură determină unde sunt stocate dovezile digitale, cum pot fi accesate și cu ce provocări criminalistice se confruntă anchetatorii:

Criminalistica digitală „clasică" vs. criminalistica online

- IT tradițional→Compania își gestionează întreaga infrastructură IT locală, serverele, rețelele, stocarea, sistemele de operare și software-ul fiind operate fizic în propriile facilități ale companiei. Aceasta implică criminalistica computerizată clasică, criminalistica rețelelor și criminalistica bazelor de date aplicate mașinilor fizice, serverelor locale și rețelelor interne. Sursele comune de dovezi sunt hard disk-urile (HDD, SSD), bazele de date locale și jurnalele de sistem. Necesită acces fizic, dar controlul deplin asupra hardware-ului poate simplifica imagistica și analiza criminalistică.

- IaaS→Infrastructură ca serviciu; IaaS oferă resurse IT de bază, cum ar fi servere virtuale, stocare și rețele prin internet. Companiile închiriază această infrastructură de la un furnizor de cloud. Ramurile relevante ale criminalisticii sunt criminalistica cloud și criminalistica rețelelor. Principalele surse de date sunt mașinile virtuale, spațiile de stocare cloud și jurnalele de trafic de rețea.

- PaaS→Platformă ca serviciu (PaaS) oferă o platformă unde dezvoltatorii pot dezvolta, testa și implementa aplicații. Infrastructura și middleware-ul subiacente sunt gestionate de furnizor. Ramurile dominante sunt criminalistica bazelor de date și criminalistica cloud. Sursele de date sunt în principal jurnalele aplicațiilor, instantaneele bazelor de date și jurnalele API.

- SaaS→Software ca serviciu (SaaS) oferă software complet funcțional prin internet. Utilizatorii accesează software-ul prin intermediul browserelor web sau al aplicațiilor

fără a fi nevoiți să își facă griji cu privire la instalare, administrare sau întreținere. Nu este necesară nicio instalare.→Microsoft 365, de exemplu. Criminalistica în cloud și criminalistica în rețea sunt ramurile criminalistice predominante aici. Sursele de date importante includ jurnalele de audit, istoricul versiunilor și înregistrările activității utilizatorilor.

Figura 11 prezintă o imagine de ansamblu asupra diferitelor medii ale tehnologiei informației.

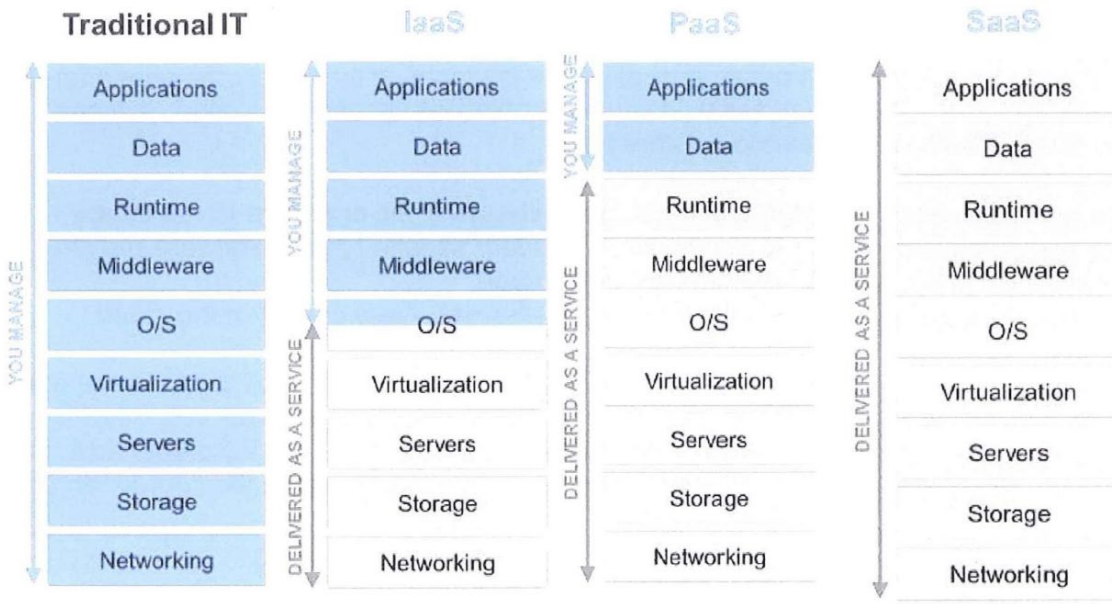

Figura2Mediu diferit al tehnologiei informației[1]

Chiar dacă există ramuri separate și trebuie luat în considerare tipul de infrastructură, structura unui proces de investigație criminalistică digitală rămâne în mare parte aceeași.

[1]Sursa: Poliția Bavareză. Distribuirea fără permis nu este permisă.

Pașii pot fi rezumați pe scurt ca fiind (1) obținerea de probe digitale, (2) analiza acestora, inclusiv interpretarea, și (3) prezentarea acestora (de exemplu, anchetatorilor principali ai cazurilor, instanței), conform lui Dubey, Bhatt & Negi (2023). Un alt model de proces influent este modelul de proces de investigație criminalistică digitală multidisciplinară din Lutui (2016), prezentat în Figura 12.

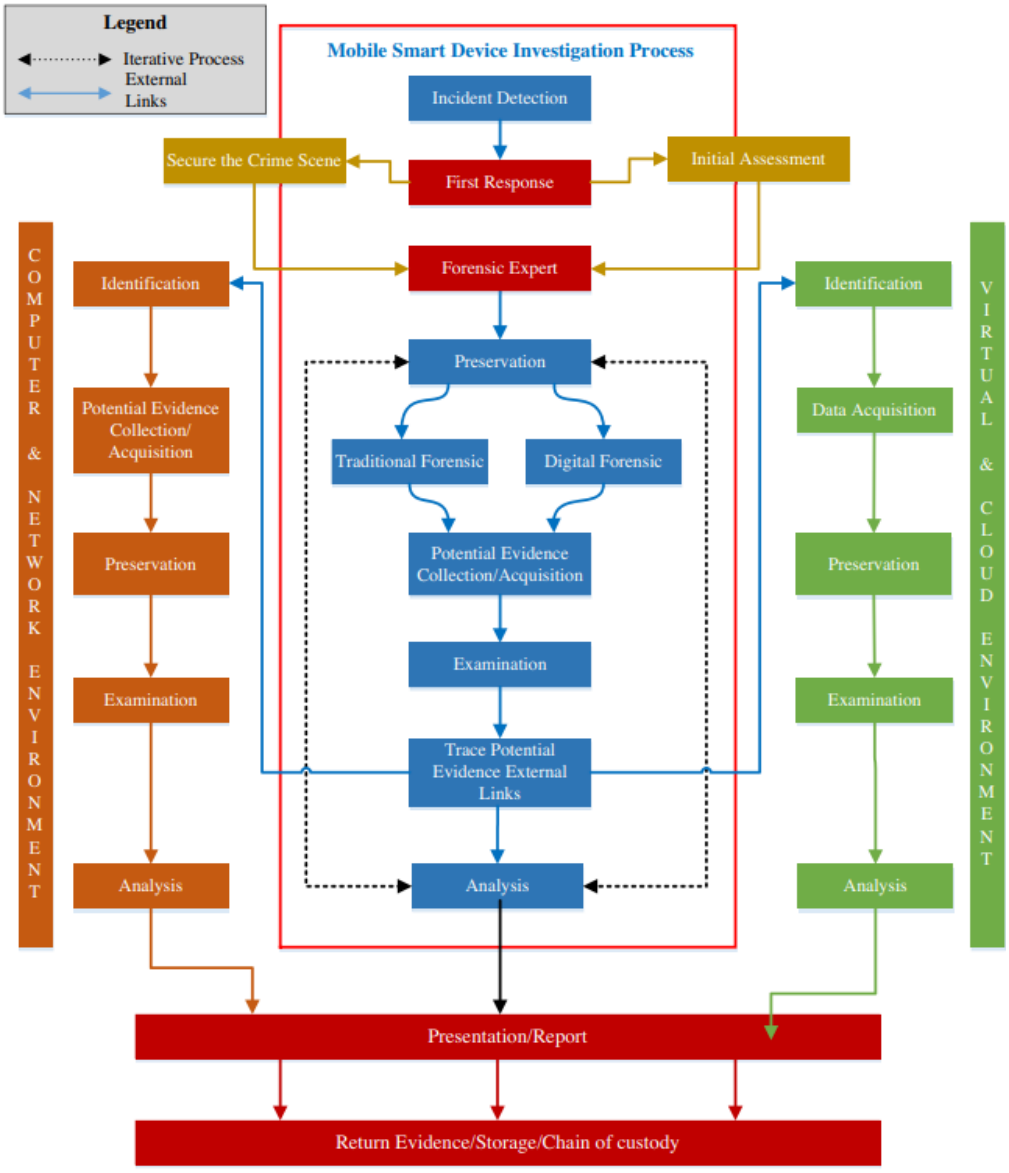

Figura3Prezentare generală a procesului de criminalistică digitală[2]

[2]Sursă: Reprezentarea originală a lui Lutui (2016), p. 601

Mai mult, pentru practician, un alt ghid pas cu pas poate ajuta la structurarea procesului de criminalistică digitală, care conține elemente mai practice decât cele două modele de proces prezentate anterior:

Nouă elemente practice ale procesului de criminalistică digitală

1. **Înregistrare**: primește dispozitivul ca probă, primește cererea de examinare
2. **Identificare**: identificarea specificațiilor și capacităților dispozitivului, identificarea obiectivelor examinării, identificarea autorității legale pentru examinare
3. **Pregătire**: pregătirea metodelor și instrumentelor care vor fi utilizate, pregătirea suporturilor media și a stației de lucru criminalistice pentru examen
4. **Izolare**: protejarea dovezilor, prevenirea distrugerii datelor la distanță, izolarea de rețea, Bluetooth, Wi-Fi
5. **Prelucrare**: efectuarea de imagini criminalistice, efectuarea de analize criminalistice, scanarea pentru programe malware
6. **Verificare**: validați imaginea, validați descoperirile criminalistice
7. **Documentare**/Raportare: păstrați notițe despre constatările și procesele dvs., redactați și finalizați rapoartele criminalistice
8. **Prezentare**pregătiți expoziții, prezentați descoperirile
9. **Arhivare**Păstrați o copie a datelor într-un loc sigur, păstrați datele în formate comune pentru viitor

Pentru specialistul/practicianul în criminalistică digitală, este important, de asemenea, să aibă în vedere întreaga procedură a unei investigații criminalistice:

Procedura unei investigații criminalistice

1. Probele ridicate au fost predate unui specialist în criminalistică digitală
2. Conservarea (stocarea înregistrată) a datelor și a suporturilor de date (]nregistrarea în borderoul de probe, aplicarea etichetelor de sigilare, etc)
3. Realizarea imaginilor de date: imagini fizice (bit-cu-bit), achiziții logice
4. Stocarea securizată a probelor originale
5. Documentarea lanțului de custodie

În plus, ar trebui aplicate întotdeauna câteva principii de bază ale criminalisticii digitale:

Principiile de bază ale criminalisticii digitale

- Realizarea copiilor de date (există diferite tipuri care trebuie diferențiate):
  - copii fidele (unu-la-unu) ale probelor informatice
  - imagini fizice (format de fișier imagine E01 sau RAW)
  - achiziții logice (L01, AD1 sau CTR)
- Examinarea copiilor sau a imaginilor de date (analiză post-mortem)
- Integritatea datelor securizate: Nicio modificare a datelor asigurate ca probă.
- Documentarea precisă a tuturor intervențiilor (cine, ce acțiune și când a efectuat asupra imaginilor de date) pentru a asigura respectarea lanțului de custodie. Acesta din urmă necesită (1) documentație cronologică și (2) trasabilitate pentru securizarea transferului, evaluării și depunerii corpurilor delicte (probelor). Se respectă principiul

utilizării metodelor recunoscute științific, iar specialistul în criminalistică digitală pregătește o documentație completă.

- Realizarea de copii fidele (unu-la-unu) ale probelor informatice, având în vedere:a
    - asigurarea integrității și autenticității probelor
    - utilizarea dispozitivelor de protecție la scriere
    - verificarea (prin calcularea valorilor de tip hash).
- Interdicția modificării intenționate : orice modificare poate surveni rapid, de exemplu, prin simpla pornire a sistemului sau prin montarea (mounting) unui hard disk
- **Trasabilitatea:** Orice acțiune trebuie să fie trasabilă, permanent și în orice etapă (prin documentare riguroasă!).

În plus, este esețială cunoașterea aspectele juridice pentru a garanta legalitatea percheziției și a ridicării de obiecte. Mai mult, în calitate de specialist criminalist, în general nu trebuie să vă preocupați de inadmisibilitatea probelor (aceasta fiind responsabilitatea ofițerului de caz și, în cele din urmă, a procurorului). Nu în ultimul rând, este recomandabil să consultați anchetatorii în cazul unor descoperiri incidentale.

9.4.3Copie criminalistică

În criminalistica digitală, realizarea copiilor criminalistice este un pas fundamental în conservarea și analizarea probelor digitale. Asigurarea integrității și disponibilității datelor este esențială pentru investigații, proceduri judiciare și răspunsul la incidentele de securitate cibernetică. O achiziție criminalistică adecvată permite anchetatorilor să lucreze cu o copie exactă, nealterată, a datelor originale, reducând la minimum riscul de contaminare sau pierdere a probelor.

Această secțiune explorează aspectele cheie ale achiziției datelor în domeniul criminalistic, începând cu principiile sale de bază (Secțiunea 9.6.3.1), inclusiv integritatea datelor, autenticitatea și lanțul de custodie. Apoi, oferă o prezentare generală a formatelor de imagine criminalistică și a structurii acestora (Secțiunea 9.6.3.2), urmată de o examinare a mecanismelor de protecție la scriere bazate pe software pentru a preveni modificarea datelor (Secțiunea 9.6.3.3). De asemenea, sunt discutate diferite tipuri de suporturi de date și rolul acestora în investigațiile criminalistice (Secțiunea 9.6.3.4), alături de o analiză a soluțiilor software și hardware specializate pentru captura criminalistică a datelor (Secțiunea 9.6.3.5). În plus, secțiunea acoperă crearea și utilizarea mediilor de bootare criminalistice (Secțiunea 9.6.3.6), care facilitează extragerea de date din sisteme live și offline. Sunt explorate și metodele de achiziție criminalistică prin rețea, inclusiv tehnicile de extragere la distanță (Secțiunea 9.6.3.7). În cele din urmă, sunt discutate considerații speciale pentru gestionarea sistemelor complexe de stocare, cum ar fi matricele RAID și dispozitivele NAS (Secțiunea 9.6.3.8), evidențiind pe scurt provocările și cele mai bune practici în conservarea unor astfel de structuri de date.

Prin înțelegerea acestor concepte, specialiștii și practicienii în criminalistică pot asigura imagini de date fiabile, verificabile și admisibile în instanță, formând fundamentul unei investigații criminalistice solide.

9.4.3.1 Principiile achiziției datelor în criminalistica digitală

Există principii esențiale care trebuie respectate în ceea ce privește achiziția datelor:

- **Realizarea copiilor criminalistice și protecția la scriere**:
    - Lucrul se efectuează exclusiv pe copii criminalistice, nu pe suporturile originale

- Realizarea copiilor sub formă de imagini bitstream (imagini fizice) sau achiziții logice
- Prevenirea modificărilor asupra datelor sau suporturilor originale în timpul proceselor de achiziție, investigare și examinare
- Acces exclusiv pentru citire în timpul procesului de achiziție (protecție la scriere)

- **Asigurarea integrității imaginilor criminalistice**:
  - Asigurarea faptului că datele achiziționate rămân adecvate pentru analiză
  - Interdicția modificării datelor copiate (utilizarea unei a doua copii de lucru, dacă este necesar)
  - Utilizarea suporturilor de stocare curățate (pentru a invoca riscul de contaminare încrucișată cu date de la alte cazuri)
  - Verificarea imaginilor de date (compararea valorilor hash între original și copie, imediat după finalizarea procesului de achiziție)
- **Documentația lanțului de custodie** Documentarea precisă a tuturor interacțiunilor cu probele și imaginile de date (menținerea „lanțului de custodie")

9.4.3.2Prezentare generală și structura formatelor comune de imagine criminalistică

Domeniul de aplicare al achiziției datelor în criminalistica digitală include hard disk-uri magnetice și SSD de pe computere, dispozitive de stocare portabile, cum ar fi unități USB sau memorie flash, și suporturi optice. Acestea pot fi asigurate folosind două metode principale: imagini fizice, care creează copii complete, sector cu sector, sau achiziții logice, care se concentrează pe fișiere și directoare specifice. Ambele metode sunt

integrate în instrumente specializate precum X-Ways, EnCase, FTK, NUIX Imager și Magnet Acquire.

Imaginile criminalistice O imagine criminalistică este o copie bit cu bit a unui dispozitiv de stocare, capturând toate datele, inclusiv fișiere, foldere și spații de stocare nealocate, libere și marcate pentru ștergere.

Imaginea diferă de o clonă prin faptul că procesul de realizare a imaginii creează un fișier comprimat (imagine) care conține datele unui disc, partiție sau ale unui întreg sistem. Fișierul imagine trebuie procesat sau montat într-un mediu virtual înainte de a putea fi analizat. În criminalistica digitală, imaginilesunt realizate, de exemplu, de pe hard disk-ul unui suspect pentru analiza post-mortem. In schimb, clonarea presupune copierea directă de pe un suport pe altul pentru a crea configurații identice (de exemplu, clonarea unui HDD vechi pe SSD fără a reinstala sistemul de operare). Deși clonarea este mai rar utilizată în scopuri criminalistice,discul clonat este imediat bootabil și utilizabil.

Există mai multe formate de imagini criminalistice utilizate în mod obișnuit:

- **Format RAW:**O copie directă, în flux de biți, a mediului de stocare. În funcție de software-ul utilizat, se generează valori hash MD5 ale imaginii complete sau ale unor segmente ale acesteia.
- **Formatul Expert Witness (EWF-E01)** Format imuabil conceput special pentru utilizare criminalistică. Antetul EVF include metadate precum numărul de blocuri și dimensiunile sectoarelor. Include verificări de redundanță ciclică (CRC) pentru verificarea blocurilor individuale și o structură segmentată cu anteturi, date și tabele de sectoare.
- **Formatul EnCase Evidence File (Ex01):**Dezvoltat de Guidance/OpenText, acesta este succesorulformatului E01. Este mai eficient și mai performant în comparație cu E01 și este suportat în principal de EnCase și NUIX.

- **Advanced Forensic Format (AFF):** Format open-source, independent de producător, gestionat de o comunitate online. Acceptă variantele AFF4 și AFF4-L. Este compatibil cu instrumente precum FTK Imager și Magnet AXIOM.

Criminalistica digitală utilizează și achiziții logice. O achiziție logică este o copie a datelor active de pe un dispozitiv de stocare sau o partiție, capturând doar fișierele și folderele prezente în sistemul de fișiere, fără a prelua și zonele nealocate sau datele șterse. Achizițiile logice sunt utilizate frecvent la fața locului sau în timpul percheziților pentru colectarea datelor din sistemele NAS.

9.4.3.3 Verificarea protecției la scriere

Protecția la scriere se referă la instrumente software care împiedică modificarea datelor de pe un suport prin impunerea accesului exclusiv pentru citire. Există diferite programe software care garantează că nicio dată nu este modificată sau ștearsă accidental în timpul investigațiilor criminalistice.

- **X-Ways Forensics:** Protejează discuri întregi sau partiții specifice. Este eficient doar după ce Windows a recunoscut și a accesat discul.
- **Discpart:** Utilitar de sistem folosit pentru a activa sau dezactiva atributul de protecție la scriere pe discuri sau volume. Devine activ numai după ce dispozitivul este recunoscut de Windows.
- **FastBloc SE:** Soluție software de blocare a scrierii care permite realizarea imaginilor criminalistice pe interfețe IDE, SATA, SCSI, FireWire și USB fără a necesita dispozitive hardware de tip write-blocker.

- **Protecție prin registru (Windows Registry):** activează protecția la scriere pentru dispozitivele de stocare prin modificarea cheilor de sistem, restricționând drepturile de scriere la nivel de sistem de operare.
- **Porturi USB:** Protecție la scriere prin diskpart (metodă considerată nesigură în criminalistică) sau modificări în regiștrii Windows (WriteProtect), aplicând restricția asupra dispozitivelor conectate prin USB..

9.4.3.4Suporturi de date

Suporturi magnetice de date, cum ar fi unitățile de hard disk, stochează datele prin magnetizare pe platouri rotative divizate în sectoare. Aceste sectoare au, de obicei, o dimensiune fizică de 512 octeți sau 4096 octeți în unitățile moderne, iar datele sunt citite mecanic folosind un cap de citire/scriere.

Suporturi de date flash Memoria flash, regăsită în SSD-uri și unitățile USB, stochează datele electronic în celule de memorie organizate în pagini și blocuri. Spre deosebire de unitățile magnetice, acestea nu au componente mobile. Memoria flash utilizează controlere pentru a emula structura tradițională bazată pe sectoare, pentru compatibilitate cu sistemele de operare existente. Este rezistentă la șocuri, are dimensiuni compacte, oferind în același timp capacități mari de stocare și consumă mai puțină energie. Cu toate acestea, are și unele dezavantaje. Un dezavantaj semnificativ este durata sa de viață limitată. Există în principal două tipuri de memorie flash: NAND și NOR. Memoria flash NAND este mai accesibilă ca preț și oferă capacități de stocare mai mari. Funcționează similar cu un dispozitiv de tip bloc, precum un HDD, permițând organizarea datelor într-un sistem de fișiere care poate fi partiționat.

Unitățile SSD (Solid-State Drives) utilizează exclusiv memorie flash NAND și sunt concepute pentru a înlocui hard disk-urile tradiționale, oferind performanțe superioare,

precum viteze mult mai mari de citire și scriere.. O soluție de stocare hibridă, cunoscută sub numele de Hybrid Solid State Drives (SSHD), combină un hard disk magnetic tradițional cu o memorie flash de capacitate mică utilizată pentru stocarea în cache. Datele accesate frecvent sunt stocate în memoria flash, ceea ce accelerează performanța generală a sistemului prin recuperarea rapidă a informațiilor.

9.4.3.5Software și hardware pentru achiziția criminalistică

Realizarea unei achiziții criminalistice implică utilizarea unei combinații de software specializat și instrumente hardware. Printre cele mai utilizate instrumente software dedicate realizării imaginilor (imaging) se numără:

- **FTK Imager:** Disponibil în versiuni portabile și instalabile. Permite previzualizarea unităților locale, a partajărilor de rețea și a imaginilor criminalistice. Creează imagini bitstream în format RAW, E01 și SMART. Permite calcularea valorilor hash, exportarea fișierelor, segmentarea sau îmbinarea imaginilor și achiziția logică (format AD1). Este compatibil multiplatformă (Windows, Linux, macOS).
- **EnCase Imager:** Instrument de achiziție cu funcții avansate.
- **Magnet Acquire:** Instrument simplificat pentru realizarea imaginilor criminalistice de pe dispozitive mobile și calculatoare.
- **NUIX Imager:** permite achiziția securizată a unităților fizice și mediilor cloud. Acceptă formate logice specifice (*.nli) cu verificarea metadatelor și a valorilor hash.

În plus, suitele complete de analiză criminalistică oferă un set extins de funcționalități pentru investigații, cum ar fi:

- **X-Ways Forensics:** Permite crearea de imagini pentru unități fizice și logice. Oferă diverse moduri de achiziție (complet, minim, curățat). Permite crearea de containere de fișiere, conversia formatului și compresia de tip sparse.
- **EnCase Forensics:** Suită completă pentru achiziție și analiză
- **Magnet IEF/AXIOM:** Se concentrează pe analiza și achiziția probelor digitale

Pentru o prezentare generală specifică a instrumentelor de criminalistică digitală dedicate investigării traficului de persoane, vă rugăm să consultați Secțiunea 9.6.4.3. Captura de datenecesită, de asemenea, echipamente hardware specifice:

- **Duplicatoare de discuri cu protecție la scriere:** sunt utilizate pentru a crea copii fidele, bit cu bit, prevenind orice modificare a suportului original. Exemplele include dispozitivele Logicube și VOOM Hardcopy. De asemenea, există stații criminalistice portabile, concepute pentru achiziția rapidă în teren și sunt adesea utilizate cu laptopuri sau unități externe.
- **Instrumente suplimentare:** includ soluții pentru transferul securizat al imaginilor, precum NUIX Evidence Mover și utilitare pentru verificarea integrității prin valori hash, cum ar fi HashMyFiles, HashCalc și MD5.exe. Acestea sunt utilizate adesea împreună cu software-ul principal precum EnCase și X-Ways pentru a valida integritatea fișierelor de imagine E01.

Pentru dezasamblarea unităților de stocare din sistemele compacte, resurse precum iFixit, tutoriale YouTube și portaluri oficiale (de exemplu, TeSIT) oferă îndrumări valoroase. În cazurile în care unitățile de stocare nu pot fi accesate fizic, se recomandă utilizarea unui mediu de bootare criminalistic pentru a facilita captura de date.

9.4.3.6Crearea și utilizarea mediilor de bootare criminalistice

Mediile de bootare criminalistice sunt instrumente esențiale atunci când extragerea sau accesarea directă a unui dispozitiv de stocare nu este posibilă ori când nu este disponibil un dispozitiv hardware de protecție la scriere (write-blocker).

Arhitecturi de sistem pentru procesul de bootare:

- BIOS (Basic Input-Output System)): Interfață tradițională între hardware-ul computerului și sistemul de operare. Acceptă pornirea a până la patru sisteme de operare pe o singură unitate. Se activează imediat după pornirea computerului. Conceput pentru suporturi de date bazate pe MBR (Master Boot Record).
- „Extensible Firmware Interface” (EFI): Succesorul BIOS-ului, cu suport pentru până la 128 de sisteme de operare pe un singur disc. Variantele includ: UEFI (Unified Extensible Firmware Interface) pentru Windows/Linux și EFI pentru macOS. Esențial pentru discurile bazate pe GPT. Folosit pentru pornirea sistemului de operare pe suporturi de date GPT (GUID Partition Table). Acceptat de toate sistemele de operare actuale. Oferă securitate și funcționalitate îmbunătățite:
    - CSM (Compatibility Support Module): simulează un BIOS pentru hardware și sistemul de operare pentru compatibilitate (Legacy mode).
    - Secure Boot: Previne încărcarea programelor malware înainte de pornirea sistemului
    - Trusted Boot: verifică semnătura digitală a nucleului (kernel) din Windows 10 pentru a exclude programele malware
- Secvența de pornire

- BIOS: verifică unitățile specificate una după alta pentru sisteme de operare bootabile și transferă procesul de bootare
- UEFI: Include un manager de boot încorporat care permite selectarea directă a unității.

Linux-Boot-Media

Mediile de boot Linux sunt echipate cu o gamă largă de instrumente criminalistice gratuite pentru sarcini precum achiziția, analiza și recuperarea datelor. Exemple ale acestor instrumente includ: Achiziție (`Guymager`,`dcfldd`, `ddrescue`); Analiză (`Sleuth Kit`, `Autopsy`) și Recuperare (`Foremost`, `TestDisk`).

Distribuții Linux populare sunt Knoppix, Helox, CAINE (Computer Aided INvestigative Environment), DEFT¸ Grml, Kali Linux.

Realizarea imaginilor în Linux Sistemele Linux sunt stocate în containere Casper formatate în FAT32, fișierele generate de utilizatori fiind stocate extern. Mediile de boot pot fi create folosind instrumente precum YUMI, Rufus sau Linux Live USB-Creator. Dispozitive precum Zalman sau IODD pot servi ca hardware de backup/boot.

De obicei, se utilizează imagini RAW. „dd” este de obicei disponibil pe fiecare sistem Linux. Sintaxă: dd if=/dev/sdX of=/media/image.dd. Împărțirea imaginilor mari. Monitorizarea progresului se face prin utilitare precum Pipe Viewer (pv). Verificarea integrității se realizează prin algoritmi hash (md5sum, sha256sum).

Programe alternative de backup pentru Linux sunt Guymager, dcfldd, dc3dd, ddrescue. O achiziție logică este creată folosind tar (Tape Archiver), care este acum integrat în Windows.

Medii de bootare bazate pe Windows

Mediul de bootare Windows oferă funcționalități alternative sau suplimentare față de mediul de bootare Linux.

- WinPE (Windows Preinstallation Environment):: Un sistem de operare (OS) minimalist, independent de sistemul instalat pe dispozitiv. Permite analiza și crearea de imagini de sistem fără a afecta datele sistemului de operare instalat.
- WinFE (Windows Forensic Environment): WinPE personalizat, configurat special pentru utilizare în domeniul criminalistic. Aplicații:
    - Imagini criminalistice folosind X-Ways Forensics sau FTK Imager
    - Triaj și previzualizarea probelor
    - Ocolirea privilegiilor de administrator pe sistemele țintă
- Format imagine Windows (WIM): Stochează imagini de bază ale sistemului Windows (de exemplu, Pro, Home, Education). Folosit pentru pornirea Windows PE („boot.wim”). Pentru instalare, WinPE este pornit, iar fișierul „install.wim” este scris pe hard disk. Compatibil cu instrumente precum`7zip`pentru inspecția imaginilor. Poate fi livrat și în format comprimat ESD (Electronic Software Distribution).

Opțiuni avansate pentru suportul de bootare

- Ventoy: instrument software pentru bootarea imaginilor ISO direct de pe o unitate USB. Printre caracteristici se numără compatibilitatea cu Secure Boot și suport pentru partiții GPT. Creează două partiții (FAT pentru managerul de boot și exFAT pentru stocarea ISO).
- Mediu de bootare Macintosh:

- **Target Disk Mode (TDM):** Permite Mac-urilor să funcționeze ca unități externe prin Thunderbolt sau FireWire
- **Mod de recuperare:** Oferă acces la instrumente precum Disk Utility și Terminal pentru crearea de imagini
- **Decriptarea FileVault:** Necesită parole sau chei de recuperare pentru acces
- **Considerații privind cipurile de securitate T2:** Limitează bootarea externă și necesită parolele specifice dispozitivului pentru achiziția de imagini

- Medii de bootare multiplă: Instrumente precum YUMI creează unități USB bootabile cu mai multe opțiuni de sistem de operare (Linux, Windows, macOS). Asigură compatibilitatea cu diverse sisteme (BIOS/UEFI, macOS System Integrity Protection).

Considerații speciale pentru macOS

- **FileVault și cip de securitate T2:** Criptarea necesită acreditări cunoscute. Cipul T2 integrează Secure Boot și restricții de bootare externă.
- **Unități de fuziune:** Hibrid între HDD și SSD, necesitând imagistica separată a fiecărei componente și reconstrucție.

9.4.3.7Achiziția datelor prin rețea

Achiziția datelor prin rețea oferă o metodă eficientă pentru crearea de imagini și transferul de date între sisteme.

EnCase și LinEn oferă un cadru robust pentru imagini prin rețea, permițând investigatorilor să acceseze și să creeze imagini ale sistemelor la distanță în siguranță.

- **Proces:**
  - Porniți computerul țintă folosind o distribuție Linux forensică, cum ar fi Deft
  - Pe PC-ul de rezervă, lansați EnCase Imager.
  - Stabiliți o conexiune fizică între cele două computere folosind un cablu crossover.
  - Atribuiți adrese IP statice ambelor sisteme: Windows: Configurați prin intermediul „Centrului de rețea și partajare” din „Setări adaptor”. Linux: Folosiți comenzile de sistem pentru a seta adresa IP.
  - Verificați conexiunea efectuând un test ping.
  - Copiați programul LinEn pe un dispozitiv de stocare extern și montați-l pe sistemul țintă.
  - Navigați la locația LinEn pe sistemul țintă și executați comanda. Alegeți opțiunea „Server” din interfața LinEn.
  - Pe PC-ul de rezervă, utilizați EnCase pentru a iniția procesul de realizare a imaginii prin intermediul opțiunilor „Adăugare dovezi” și „Previzualizare crossover”.
- **Avantaje:** Previne accesul automat la scriere pe dispozitivele de stocare conectate. Sistemele Linux pot recunoaște configurații hardware complexe, cum ar fi controlerele RAID.

Instrumente Unix iar mediile de bootare criminalistice bazate pe Linux oferă flexibilitate și control în timpul operațiunilor de realizare a imaginii prin rețea.

- **Proces:**
    - Conectați ambele sisteme folosind fie un cablu crossover, fie un cablu patch standard. Utilizați un hub sau un switch de rețea, dacă este necesar.
    - Atribuiți adrese IP statice fiecărui computer:

      Ferestre Configurați prin intermediul „Centrului de rețea și partajare”

      Linux Setați IP-ul folosind instrumente precum ifconfig (de exemplu, ifconfig eth0 192.168.100.1).
    - Testați conectivitatea folosind o comandă ping pentru a vă asigura că ambele dispozitive comunică.

Combinația dintre dd și Netcat permite transferuri de date simple și eficiente prin rețea.

- **Proces:**
    - **Pregătiți computerul de destinație:** se configurează Netcat să „asculte” pe un anumit port și să redirecționeze datele primite într-un fișier imagine.. exemplu: Salvați datele direct într-un fișier sau transmiteți-le către dd pentru scriere.
    - **Pregătiți computerul sursă:** Transmiteți datele de pe disc către destinație: Pe Linux: Folosiți dd pentru a citi datele și a le transmite către Netcat. Pe Windows: Folosiți un fișier dd.exe compatibil pentru a efectua sarcini similare.

- Considerații suplimentare**:** Dezactivați temporar firewall-urile și software-ul antivirus pentru a evita interferențele. Netcat poate declanșa alerte de securitate, deoarece este adesea clasificat drept „program potențial nedorit”.

Utilizarea SSH asigură transferuri de date securizate, în special atunci când se lucrează cu sisteme Linux sau macOS.

- **Proces:**
  - Folosește dd pentru a crea o copie bitstream a discului sursă.
  - Transmiteți ieșirea printr-o conexiune SSH către sistemul de destinație, unde este salvată ca imagine.
- **Caracteristici suplimentare**
  - **Urmărirea progresului** Folosiți utilitare precum Pipe Viewer (pv) pentru a monitoriza transferul de date în timp real.
  - **Comprimare:** Transmiteți date în flux prin instrumente de compresie precum Gzip pentru a reduce cerințele de stocare.

9.4.3.8 Particularități ale sistemelor RAID și NAS

RAID Sistemele de tip (Redundant Array of Independent Disks) sunt concepute pentru a îmbunătăți performanța și fiabilitatea prin distribuirea datelor pe mai multe hard disk-uri.

- **Tipuri de RIAD-uri:**
  - **RAID hardware:** Gestionat cu ajutorul unei plăci de controler RAID dedicate, oferind performanță robustă și fiabilitate
  - **RAID software:** Controlat de sistemul de operare, de obicei mai puțin costisitor, dar dependent de resursele sistemului
- **Niveluri RAID:**

- **JBOD:** toate HDD-urile sunt combinate într-un singur spațiu de stocare mare; rețeaua de stocare este un sistem de fișiere mare în care sunt stocate datele
- **RAID0:** Toate HDD-urile sunt combinate într-un singur sistem de stocare mare; logica de stocare a datelor asigură că datele sunt stocate în blocuri pe HDD-uri
- **RAID10:** Două sau mai multe HDD-uri sunt combinate pentru a forma o singură zonă de stocare combinată (RAID0); zona de stocare este oglindită (RAID1 Mirroring)
- **RAID5 sau RAID6:** Cel puțin 3 (RAID5) sau cel puțin 4 (RAID6) HDD-uri sunt combinate într-o singură zonă de stocare; Informațiile de paritate sunt distribuite pe discuri. Dacă unul (RAID5) sau două (RAID6) HDD-uri se defectează, conținutul lor poate fi restaurat de pe suporturile de date rămase; În funcție de controler/producător, informațiile de paritate pot fi rotite „înainte” sau „înapoi” către hard disk-urile individuale.
- **Synology Hybrid RAID (SHR):** O variantă de RAID care utilizează software-ul RAID pentru Linux (MD RAID și LVM2)

- **Cele mai bune practici pentru backup-ul RAID**:
  - Documentație precisă a configurațiilor RAID (de exemplu, setări BIOS, tipul de controler RAID, nivelul RAID, dimensiunea stripe-ului).
  - Achiziția prin intermediul controllerului RAID; de exemplu, prin bootarea unui sistem tip Linux Live CD sau WinFE, capabil să recunoască controllerul RAID hardware.
  - Achiziția logică a datelor selectate (de exemplu, utilizând opțiunea „Custom Content Image” din FTK Imager), atunci când situația o impune.

NAS (Network Attached Storage) sunt servere compacte, autonome, care utilizează sisteme de operare personalizate, de obicei versiuni personalizate de Linux. Suportul de date intern constă de obicei din hard disk-uri SATA. Primul pas este creareaimaginilor. Atunci când scoateți unități din sistem, este important să etichetați ce unitate se afla în ce slot. Sistemele NAS dispun de o interfață bazată pe browser (Web GUI). Pentru a accesa această interfață, NAS-ul trebuie să fie conectat la rețeaua de investigare.

9.4.4Criminalistica digitală în contextul traficului de persoane și al exploatării prin muncă

Traficul de persoane, inclusiv exploatarea prin muncă, se bazează din ce în ce mai mult pe comunicarea digitală, tranzacțiile financiare și recrutarea online (Europol, 2020; 2024). Prin urmare, criminalistica digitală joacă un rol crucial în identificarea autorilor, descoperirea modelelor de exploatare a victimelor și obținerea probelor pentru urmărire penală. Această subsecțiune explorează modul în care metodologiile criminalistice digitale pot fi aplicate cazurilor de trafic, abordând atât considerații tehnice, cât și etice. Această secțiune începe cu surse cheie de probe digitale în domeniul traficului de persoane (și, ori de câte ori este posibil, pentru a colecta informații, în special pentru exploatarea prin muncă, Secțiunea 9.6.4.1). Ulterior, Secțiunea 9.6.4.2 tratează analiza probelor digitale tipice traficului de persoane (de exemplu, ce caută anchetatorii?). Aceasta este urmată de Secțiunea 9.6.4.3, care prezintă câteva instrumente posibile de criminalistică digitală pentru utilizarea de către autoritățile de aplicare a legii. Apoi, sunt discutate principalele provocări care sunt relevante pentru procesul de criminalistică digitală în timpul investigațiilor privind traficul de persoane (Secțiunea 9.6.4.4). Secțiunea se încheie cu aspecte juridice și etice de luat în considerare (Secțiunea 9.6.4.5). O prezentare generală suplimentară a tehnologiei utilizate pentru prevenirea și combaterea

traficului de persoane a fost întocmită de UNODC –Modulul 14: Legăturile dintre criminalitatea cibernetică, traficul de persoane și traficul de migranți.

9.4.4.1Surse cheie de dovezi digitale

Traficanții și exploatatorii folosesc diverse platforme și tehnologii digitale, lăsând în urmă urme criminalistice critice, iar autoritățile de aplicare a legii pot folosi dovezi digitale pentru a identifica traficul de persoane și autorii și pentru a găsi dovezi legale pentru a-i acuza de această infracțiune (Cellebrite, 2024). Sursele comune de probe includ:

Dispozitive digitale personale

În contextul investigațiilor privind exploatarea prin muncă, dispozitivele digitale personale, cum ar fi telefoanele mobile și computerele, pot servi drept surse esențiale de probe. Aceste dispozitive conțin adesea comunicații, contacte, tranzacții financiare și date de localizare care pot dezvălui practici de exploatare.

- **Dispozitive mobile** Traficanții utilizează frecvent dispozitive mobile pentru a coordona activități ilegale. Dovezile provenite de pe aceste dispozitive pot include: (1) jurnale de apeluri și liste de contacte care dezvăluie comunicare (2) modele și rețele, (2) mesaje text și istoricul chat-urilor care conțin detalii despre activitățile de recrutare, coordonare și exploatare, (3) fișiere multimedia precum fotografii și videoclipuri care pot documenta victime, locații sau acte ilicite și (4) date de localizare (informațiile GPS pot urmări mișcările și identifica locații cheie).
- **Calculatoare:** Mai multe tipuri de date stocate sau accesibile prin intermediul computerului pot prezenta un interes special pentru investigarea traficului (suprapunerea cu datele de pe dispozitivele mobile este posibilă): (1) înregistrări de comunicare, cum ar fi e-mailuri și mesaje text, activități pe rețelele de socializare sau reclame online sau anunțuri de locuri de muncă, (2) date financiare,

cum ar fi tranzacții bancare și înregistrări de plăți sau înregistrări de criptomonede, (3) date de identificare personală, cum ar fi copii digitale ale documentelor de identitate sau date de localizare, (4) înregistrări ale condițiilor de angajare și de muncă, cum ar fi contracte de muncă, programe de muncă ilegale, sisteme de pontaj și prezență (de exemplu, pentru detectarea orelor de lucru excesive), (5) date de călătorie, cum ar fi informații despre rezervările de călătorie de la companiile aeriene sau agențiile de turism sau achiziții de bilete și itinerarii, (6) istoricul activităților pe web-ul (dark web sau surface web), (7) dosare medicale și de sănătate care sunt stocate, de exemplu, din vizitele la medic ale victimelor după atacuri fizice sau (8) date de la camerele de supraveghere sau sistemele de securitate de la locurile de muncă sau proprietăți private, care arată condițiile de viață și de muncă ale victimelor.

Stocare în cloud

Stocarea în cloud poate fi utilizată de către traficanți datorită confortului său, accesului la distanță și capacității de a stoca cantități mari de date, ceea ce o face o sursă importantă de dovezi digitale în astfel de cazuri. Datele colectate din stocarea în cloud pot fi similare cu lista prezentată mai sus pentru dispozitive mobile și computere. Mai mult, datele speciale care pot fi găsite mai des în stocările în cloud sunt calendarele digitale care pot dezvălui întâlniri organizate sau planificate, mișcările de călătorie ale victimelor sau alte informații logistice privind operațiunile care au fost partajate în rețeaua de trafic. Prin urmare, stocările în cloud pot oferi o probabilitate mai mare de a dezvălui structurile rețelei de trafic sau victimele care suferă de pe urma exploatării prin muncă forțată. Accesarea și analizarea datelor stocate în cloud necesită, însă, procese legale și expertiză tehnică specială pentru a asigura integritatea probelor (dacă nu se cunosc acreditările utilizatorului). Modalitățile tehnice de acces (cel puțin parțial) sunt, de exemplu, cooperarea cu furnizorul de servicii cloud, utilizarea instrumentelor de extragere

a datelor din cloud, utilizarea API-urilor serviciilor cloud, obținerea accesului prin intermediul dispozitivelor ridicate ca probă (autentificarea cu datele de acces ale utilizatorului, analiza imaginilor de tip backup ale dispozitivului și verificarea sincronizării datelor cu serviciile Cloud), efectuarea analizei metadatelor cu fișierele stocate în cloud, aplicarea analizei criminalistice a traficului de rețea (Secțiunea 4.1.1) sau accesarea jurnalelor de evenimente (log-urilor) furnizate de serviciile cloud, de exemplu, obținerea istoricului de autentificare sau a istoricului de descărcare a fișierelor.

Platforme de comunicare și recrutare

Internetul oferă traficanților acces la potențiale victime prin diverse canale digitale, inclusiv rețele de socializare și site-uri web de recrutare (UNODC, 2019a). Fraser (2016) a detaliat modul în care procesele dintre traficanții de persoane și victime se schimbă odată cu trecerea de la rețelele geografice la cele online. Fraser subliniază faptul că, în zilele noastre, traficanții știu cum să utilizeze rețelele de socializare online și dark web-ul. Lucrarea descrie, de asemenea, modul în care aceste rețele afectează dezechilibrul de putere în trafic și modelează experiențele victimelor (Fraser, 2016). Dovezile digitale de pe aceste platforme cuprind (1) profiluri și postări care pot conține tentative de recrutare, oferte de muncă înșelătoare sau reclame pentru servicii ilicite, (2) mesaje directe (care facilitează comunicarea privată între traficanți și victime) și (3) apartenența la grupuri care indică implicarea în rețele sau forumuri de trafic. Analiza acestor elemente poate dezvălui, de exemplu, strategii de recrutare și poate identifica atât victimele, cât și autorii.

- **Platforme de socializare** Un raport al lui Kunz și colab. (2018) prezintă pe scurt site-urile web utilizate în scopuri de exploatare sexuală. Printre acestea se numără (1) site-uri pentru vizualizare și comentarii precum Facebook, Instagram și Snapchat, dar și YikYak și Wispher, (2) site-uri web pentru conversații precum Tinder, Blendr, WhatsApp și KIK, dar și Yellow și #1 Chat Avenue ca site-uri mai puțin comune, (3) site-uri de webcam, inclusiv Chatroulette, Omegle și Monkey, și

(4) site-uri pentru publicitate și vânzări precum Cityxguide, skipthegames, bedpage, seekingarrangement.com sau sugar-babies.com. În ceea ce privește exploatarea prin muncă, nu s-a putut găsi o astfel de imagine de ansamblu. Cu toate acestea, se știe că platformele de socializare tradiționale sunt utilizate pentru recrutarea în scopul exploatării prin muncă, alături de portalurile de locuri de muncă online și site-urile de mică publicitate (a se vedea, de exemplu, Europol, 2024).

- **Site-uri de recrutare online** Chiar dacă aceste portaluri și site-uri web de mica publicitate ar putea fi legitime, traficanții pot posta oferte de muncă înșelătoare, vizând categorii vulnerabile care caută un loc de muncă. Ca a doua etapă, aplicațiile de mesagerie instantanee sunt utilizate de către traficanți pentru schimbul de detalii operaționale, deoarece acestea oferă un mediu mai sigur (Europol, 2024).
- **Reclame online** Spre deosebire de platformele de social media, aplicațiile de mesagerie instantanee și site-urile de recrutare online, anunțurile publicitare online pot fi considerate o formă de comunicare unidirecțională, în timp ce restul surselor vizează, de regulă, comunicarea bidirecțională între persoane (de exemplu, între potențiala victimă și suspectul de trafic). Caracteristicile anunțurilor online folosite în scopul traficului prin exploatare prin muncă includ::
    - **Lipsa de specificitate** Anunțurile oferă adesea descrieri vagi ale posturilor, cu detalii minime despre rol, responsabilități sau condiții de muncă. Această ambiguitate servește la atragerea unei game mai largi de candidați, fără a dezvălui potențiale situații de exploatare (Volodko, Cockbain și Kleinberg, 2020).
    - **Promisiuni nerealiste** Ofertele pot include salarii neobișnuit de mari, procesare accelerată a vizelor sau alte beneficii care par prea bune ca să

fie adevărate, cu scopul de a atrage persoane care caută oportunități mai bune (vezi, de exemplu, Fraser, 2016).

- **Grupuri demografice vizate** Eforturile de recrutare se concentrează adesea pe anumite populații, cum ar fi migranții sau persoanele provenite din medii defavorizate din punct de vedere economic, care sunt mai susceptibile la exploatare (Volodko, Cockbain și Kleinberg, 2020).
- Deși au existat eforturi de investigare a anunțurilor online pentru exploatare sexuală folosind metode tehnologice moderne, cum ar fi Prelucrarea Limbajului Natural (NLP) (de exemplu, Perez & Rivas, 2023; Lugo-Graulich et al., 2024), infracțiunea de exploatare prin muncă, precum și alte forme de trafic de persoane, încă nu fac obiectul unor cercetări științifice în acest domeniu.

- **Dark Web vs. Surface Web** Găzduite în rețele criptate care necesită software specializat pentru acces,anunțurile și ofertele de pe Dark Web asigură un grad mai mare de anonimat. Această natură clandestină generează provocări semnificative pentru autoritățile de aplicare a legii (LEA), deoarece aceste platforme implementează adesea măsuri tehnice avansate pentru a proteja identitatea utilizatorilor. Dimpotrivă, anunțurile și ofertele de pe Surface Web sunt accesibile publicului și se găsesc adesea pe platforme mainstream, cum ar fi rețelele de socializare și site-urile de mică publicitate. Deși pot folosi limbaj și imagini codificate pentru a evita detectarea, natura lor publică permite o monitorizare mai simplă de către forțele de ordine. Traficanții utilizează atât platformele de pe Surface Web, cât și pe cele de pe Dark Web pentru a face publicitate serviciilor sau oportunităților de exploatare. Probele digitale relevante de pe Dark Web cuprind, de exemplu, (1) anunțuri și oferte care pot viza servicii ilicite sau oportunități de angajare înșelătoare și (2) postări pe forumuri și canale de comunicăre în care se discută metode de operare, se partajează informații sau se

negociază tranzacții (de exemplu, o postare pe forum care menționează „ disponibilitate forță de muncă ieftină") sau (3) documente falsificate care au fost achiziționate de pe piețele Dark Web, cum ar fi vize și permisele de muncă false pentru migranții aflați în ședere nereglementată.

Supraveghere și urmărire

Datele de supraveghere și urmărire se referă la orice date care pot dezvălui locația, mișcările sau acțiunile indivizilor, adesea colectate prin mijloace electronice, motiv pentru care intervine criminalistica digitală. Mediile moderne echipate cu sisteme de supraveghere și dispozitive IoT pot surprinde în mod accidental activitățile de trafic. Investigațiile ar putea permite, de asemenea (dacă sunt confirmate legal) urmărirea și monitorizarea suspecților.

Supraveghere inițiată de forțele de ordine (de obicei, necesită o hotărâre judecătorească)

- **Urmărire GPS, de exemplu, urmărirea vehiculelor:** pot fi utilizate de către autoritățile de aplicare a legii (LEA) pentru a monitoriza mișcările. Autoritățile pot, de exemplu, urmări mișcarea mașinii unui suspect care transportă în mod regulat victimele către și de la diverse locuri de muncă. Modelele din datele de localizare ale vehiculului ar putea ajuta autoritățile să localizeze centrele de trafic sau să identifice rutele de călătorie sau orele de lucru ale victimei.
- **Camere de supraveghere:** Imaginile CCTV de la camerele de supraveghere publice sau private pot fi folosite pentru a urmări mișcările traficanților sau ale victimelor în anumite locații (de exemplu, la locurile de muncă, în apropierea granițelor).
- **Interceptarea comunicațiilor (interceptări telefonice):** Interceptările telefonice (de exemplu, apeluri telefonice, e-mailuri, mesaje) pot oferi informații despre

activitățile de trafic. Interceptările pot ajuta autoritățile să asculte traficanții care aranjează călătorii, plăți, amenință victimele etc.

- **Dispozitive de urmărire pe telefoanele mobile:** Triangulația celulară și datele GPS de la telefoanele mobile pot fi utilizate pentru a identifica cu precizie locația victimei sau a traficantului și, de exemplu, pentru a cartografia locațiile acestora în timp.
- **Dronele sau supravegherea aeriană:** Dronele echipate cu camere pot fi utilizate pentru urmărirea mișcărilor pe zone mai mari (în special în locuri rurale sau greu accesibile, unde supravegherea umană poate fi dificilă).

Supraveghere inițiată de traficanți (date colectate de traficanți)

- **Urmărirea dispozitivelor mobile de către traficanți** Traficanții pot folosi telefoanele victimelor sau propriile dispozitive pentru a le urmări. Aceasta poate include utilizarea aplicațiilor de urmărire GPS sau chiar instalarea de programe spyware (de exemplu, mSpy, FlexiSPY) pentru a monitoriza locația și comunicațiile victimei.
- **Date de locație de la dispozitivele IoT** Dispozitivele IoT, cum ar fi ceasurile inteligente sau chiar vehiculele conectate, pot fi utilizate de către traficanți pentru a monitoriza locația victimelor. Jurnalele de pe aceste dispozitive pot fi analizate, de exemplu, pentru a găsi momente de acces neobișnuite sau schimbări de mediu.
- **Monitorizare online** Traficanții monitorizează frecvent conturile de socializare ale victimelor lor pentru a le controla comunicarea sau chiar pentru a le uzurpa identitatea, pentru a le controla profilul online și, de exemplu, pentru a le împiedica să ceară ajutor. Prin urmare, autoritățile de aplicare a legii ar putea verifica dacă traficantul avea datele de autentificare ale victimei (victimelor) pentru a se conecta la diferite rețele de socializare sau alte platforme.

- **Supraveghere video și audio** Traficanții pot amplasa camere ascunse sau dispozitive de înregistrare audio în camere sau la locul de muncă pentru a monitoriza victimele în mod continuu, de exemplu, asigurându-se că acestea îndeplinesc sarcinile. Autoritățile de aplicare a legii s-ar putea concentra pe detectarea unor astfel de dispozitive și ar putea apoi evalua datele lor pentru a defini amploarea exploatării prin muncă și pentru a putea prezenta dovezi fiabile în instanță.

Tranzacții financiare și metode de plată

Tranzacții financiare și criptomonede (intern și internațional): Traficanții exploatează adesea sistemele financiare digitale [sau activele virtuale] pentru a spăla bani și a-și ascunde profiturile. Dovezile digitale cheie includ (1) extrase de cont bancar și istoricul tranzacțiilor care evidențiază modele neobișnuite care indică activități ilicite, (2) portofele și tranzacții cu criptomonede utilizate pentru a ascunde urmele financiare, necesitând analize criminalistice specializate. Analiza financiară (a se vedea secțiunea 9.2) este crucială în urmărirea fluxului de bani, destructurarea operațiunilor de trafic și urmărirea penală a infractorilor (Thomson Reuters, 2025).

- **Tranzacții bancare tradiționale**
- **Tranzacții cu criptomonede**
- **Sisteme de plată preplătite și digitale**

9.4.4.2Analiza și corelarea dovezilor

După ridicarea și conservarea probelor digitale (de exemplu, ridicarea telefoanelor mobile, computerelor, driverelor USB, conturilor cloud, datelor de pe rețelele sociale), datele trebuie extrase din aceste dispozitive sau spații de stocare, aplicând diferite tipuri

de analize criminalistice descrise în Secțiunea 9.1.1 (de exemplu, analize criminalistice în cloud; extragerea datelor la nivel hardware, cum ar fi extragerea cipurilor sau metode precum spargerea/decriptarea parolelor). Apoi, anchetatorii pot analiza și corela probele digitale. Procedurile și principiile criminalistice digitale prezentate mai jos pot fi doar exemplificative, pe de o parte, iar pe de altă parte, nu sunt în întregime unice pentru traficul de persoane: multe tehnici se suprapun cu investigațiile privind criminalitatea cibernetică, crima organizată și frauda. Cu toate acestea, unele aspecte fac ca traficul de persoane să fie unic în acest context, cum ar fi accentul pus pe rețelele de socializare și anunțurile de recrutare (spre deosebire de infracțiunile financiare, cazurile de trafic de persoane se bazează în mare măsură pe înșelăciunea online și urmărirea comunicărilor). În plus, o cantitate mare de probe (pe care echipele de criminalistică digitală le reconstituie) sunt centrate pe victimă, deoarece traficanții mențin controlul asupra victimei (victimelor) lor, de exemplu, prin mesaje de amenințare, șantaj sau urmărire GPS. Mai mult, victimele traficului de persoane adesea nu dețin propriile computere sau laptopuri, ci smartphone-uri și conturi cloud. Acest lucru face ca investigațiile privind traficul de persoane să depindă mai mult de investigațiile criminalistice mobile și cloud (a se vedea secțiunea 9.1.1).

În cazurile de trafic de persoane, experții în criminalistică digitală pot căuta în mod specific:

- **Modele de comunicare** Adesea, traficanții folosesc un limbaj codificat sau argou în texte și, prin urmare, caută diferite cuvinte cheie precum „loc de muncă ușor”, „plată în numerar”, „călătorie gratuită” în contextul exploatării prin muncă sau „modeling” și „escortă” în contextul exploatării sexuale. Adesea, acele cuvinte cheie specifice legate de muncă, cazare și salarii sunt utilizate în mod repetat. Tong și colab. (2017), de exemplu, au descoperit că traficanții din SUA și Canada își modifică limbajul pentru a evita detectarea de către autoritățile de aplicare a

legii. Mai mult, schimbă terminologia, ceea ce face dificilă elaborarea unor liste de cuvinte cheie pentru urmărirea anunțurilor legate de trafic. Acest lucru creează un lexicon în continuă evoluție. De exemplu, în loc să menționeze explicit „tânără fată", traficanții folosesc text ofuscat, emoji-uri sau argou. (de exemplu, „Y"🖤ng G!rl'). Multe reclame nu au, în plus, structuri gramaticale adecvate, ceea ce face ca tehnicile tradiționale NLP să fie mai puțin eficiente. Anunțurile conțin frecvent simboluri, emoji-uri și caractere nestandard. Ordinea cuvintelor este adesea inconsistentă, asemănându-se cu scrierea pe rețelele de socializare sau a mesajelor text, mai degrabă decât cu structurile de scriere (de exemplu, „@" în loc de „at" sau „m33t" în loc de „meet"). Complexitatea unigramelor, bigramelor și trigramelor este ridicată. Variabilitatea ridicată a cuvintelor rezultă din faptul că traficanții modifică intenționat cuvintele pentru a evita detectarea automată (combinații neobișnuite de cuvinte, cuvinte rare, sintagme modificate). Reclamele sunt de obicei scurte (media de 133 de cuvinte) și nu au descrieri ample. Tong și colab. (2017) concluzionează că traficanții își adaptează constant limbajul, necesitând modele de detectare flexibile. Listele de cuvinte cheie singure sunt insuficiente, anchetatorii vor avea nevoie de modele de inteligență artificială conștiente de context.

O altă modalitate de a înțelege și de a urmări modele specifice de comunicare pentru criminalistica digitală este reprezentată de strategiile de recrutare aplicate de traficanți. Acestea pot fi clasificate în metode active și pasive (Europol, 2020): Recrutarea activă este similară cu „pescuitul cu cârligul", în care infractorii postează anunțuri de locuri de muncă false pe portaluri de locuri de muncă și pe platforme de socializare de încredere. Aceștia pot chiar crea site-uri web de recrutare false care par profesionale, uneori cu chat live pentru a le face să pară legitime. UNODC numește acest fenomen și „strategia de vânătoare" (UNODC, 2020). Recrutarea activă include în mare parte mesaje directe și chat-uri care

vizează persoane vulnerabile. Poate conține modele de constrângere, manipulare și oferte de muncă frauduloase. De asemenea, nu este neobișnuită ștergerea bruscă a mesajelor sau a conturilor după contactul inițial (de exemplu, atunci când traficantul observă că persoana care urmează să fie traficată nu este accesibilă pentru oferta/ofertele de muncă). Recrutarea pasivă este mai discretă și mai greu de detectat de către autoritățile de aplicare a legii. Funcționează ca „pescuitul cu plasă" (sau „strategia de pescuit", UNODC, 2020), în care traficanții monitorizează anunțurile online ale persoanelor aflate în căutarea unui loc de muncă și îi contactează direct. Aceștia promit oportunități de angajare în străinătate, cerând un comision pentru a asigura locul de muncă și pentru a acoperi costurile de călătorie sau de plasare. Victimele își dau seama că au fost înșelate abia atunci când ajung în țara străină (Europol, 2020).

Nu în ultimul rând, dovezile științifice fiabile despre tehnicile de investigare a modelelor de comunicare sunt foarte rare (vezi, de exemplu, Harta lacunelor de dovezi a Organizației Internaționale a Muncii, 2023, pentru posibile actualizări ale elaborărilor științifice).

- **Urmărirea geolocalizării** Mai mult, similar cu înțelegerea modelelor de comunicare, aceasta poate ajuta la adoptarea perspectivei făptuitorului: Dispozitivele care permit urmărirea geolocalizării ar fi putut fi utilizate pentru monitorizarea în timp real a victimei (victimelor), de exemplu, prin GPS, camere încorporate în smartphone-uri, aplicații de partajare a locației (Europol, 2020). Posibilitatea controlului de la distanță scade pragul de inhibiție al făptuitorilor pentru exploatare și complică, de asemenea, eforturile de identificare de către autoritățile de aplicare a legii, așa cum a afirmat Europol (2020, p. 3):

  > „[Deși] din punct de vedere istoric, grupurile de crimă organizată ar fi trebuit să exercite control fizic și monopol asupra anumitor cartiere ale orașului și ar fi fost, în general, formate dintr-o rețea extinsă de membri, noii veniți în domeniul traficului de

persoane pot acum gestiona eficient o afacere online fără a fi nevoie de o infrastructură infracțională fizică și cu o forță de muncă redusă. Prin urmare, stăpânirea tehnologiei poate face ca un grup criminal să fie mai amenințător, dar totodată mai puțin identificabil de către autoritățile de aplicare a legii."

Mai multe despre urmărirea geolocației pot fi găsite în Secțiunea anterioară 9.1.3.1.

- **Analiză financiară** Analiza financiară și criminalistica digitală pot merge mână în mână, în special în ceea ce privește tranzacțiile financiare efectuate de traficanți pentru a încărca anunțuri online (Europol, 2020). Mai mult, victimele efectuează adesea transferuri bancare către traficanți. O perspectivă mai detaliată asupra finanțelor, tranzacțiilor financiare și investigațiilor financiare poate fi găsită în Secțiunea 9.2.
- **Identificarea victimei** Pentru identificarea victimelor, oamenii de știință și practicienii din domeniul criminalisticii digitale pot aplica recunoașterea facială pentru a le găsi, de exemplu, în anunțuri sau postări pe rețelele de socializare. În plus, căutarea inversă de imagini poate dezvălui dacă victimele au fost promovate pe site-uri pentru adulți sau pe platforme de pe piața neagră.
- **Analiza web-ului profund și dark web** Utilizarea forumurilor darknet nu este neobișnuită pentru traficanți. Anchetatorii pot folosi instrumente criminalistice TOR și de monitorizare a dark web-ului, de exemplu, pentru a găsi mesaje de recrutare, conținut de exploatare a victimelor sau tranzacții ilicite.

9.4.4.3Abordări și instrumente de criminalistică digitală

Pentru a colecta și analiza eficient probele în cazurile de trafic de persoane și exploatare prin muncă, criminalistica digitală se bazează în mare măsură pe:

- Criminalistică mobilă
- Criminalistică de rețea și cloud
- Analiză financiară și a criptomonedelor
- Investigații pe dark web

Pentru a continua cronologic, iată principiile relevante pentru criminalistica digitală care trebuie luate în considerare în mod practic, inclusiv în contextul traficului de persoane: În prima fază de identificare și conservare, primii respondenți trebuie să identifice și să securizeze prompt dispozitivele digitale pentru a preveni modificarea sau pierderea datelor (de exemplu, izolarea de rețele; UNODC, 2019b). Apoi, pentru gestionarea probelor digitale, este important să se realizeze înregistrări detaliate ale stării fiecărui dispozitiv, inclusiv starea de funcționare (pornit, oprit, standby), modelul, orice daune vizibile. Fotografiile și notițele scrise ajută la menținerea lanțului de custodie și susțin integritatea probelor (UNODC, 2019b). Extragerea datelor se poate face apoi cu instrumente criminalistice specializate pentru a recupera datele fără a altera conținutul original (a se vedea Secțiunea 9.6.2 pentru o prezentare generală). Pentru unele dispozitive, acest lucru poate implica depășirea caracteristicilor de securitate precum criptarea sau parolele. În mod specific, în contextul traficului de persoane/(exploatării prin muncă), autoritățile de aplicare a legii utilizează instrumente de criminalistică digitală care facilitează investigarea acestei infracțiuni.

O imagine de ansamblu completă asupra instrumentelor de criminalistică digitală care ar putea fi și sunt utilizate în aplicarea legii nu poate fi oferită aici din cauza (1) diversității instrumentelor utilizate de diferitele autorități de aplicare a legii (LEA) din Europa (criminalistica digitală în ansamblu, iar criminalistica digitală pentru investigarea traficului de persoane fiind o ramură a acesteia), (2) utilizării interconectate a diferitelor tehnici și instrumente care depind de fiecare caz în parte și (3) accesibilității nepublice a

modului în care autoritățile de aplicare a legii funcționează în acest sens, pentru a numi doar câteva motive. Cu toate acestea, unele instrumente și companii de criminalistică digitală care oferă soluții software pentru investigarea cazurilor de trafic de persoane pot fi prezentate superficial:

- **Cellebrite Pathfinder**: un instrument criminalistic mobil care extrage, analizează și decodează date de pe smartphone-uri, tablete și surse cloud. Poate recupera mesaje șterse, jurnalele de apeluri și locațiile GPS.

  ***Aplicare potențială într-un caz de trafic de persoane/exploatare prin muncă**:*

  ➔ extrage, de exemplu, mesaje WhatsApp, Telegram între traficanți și victime

  ➔ recuperează conversațiile șterse în care victimelor li s-au promis locuri de muncă false

  ➔ identifică locațiile GPS de pe telefonul victimei pentru a-i identifica modelele de mișcare

- **MAGNET ACQUIRE** Compania oferă mai multe soluții software pentru siguranță publică, armată și informații etc.

  MAGNET AXIOM este relevant în special pentru traficul de persoane: Instrumentul este specializat în criminalistică informatică și în cloud, analizând date de pe hard disk-uri, rețele de socializare, e-mailuri și fișiere criptate.

  ***Aplicare potențială într-un caz de trafic de persoane/exploatare prin muncă**:*

  ➔ investighează postările pe rețelele de socializare și activitatea portalurilor de locuri de muncă unde traficanții postează anunțuri de locuri de muncă false

  ➔ extrage fișiere ascunse (de exemplu, contracte ale victimelor, bilete de avion, permise de muncă) de pe computerele traficanților

➔ analizează jurnalele de comunicare dintre mai mulți suspecți din diferite țări

MAGNET OUTRIDERDe asemenea, poate sprijini în mod pozitiv procesul de investigație criminalistică digitală, deoarece scanează dispozitivele mobile iOS și Android și descoperă, de exemplu, aplicații ilicite, liste de contacte, mesaje SMS și aplicații utilizate recent.

Aplicare potențială într-un caz de trafic de persoane/exploatare prin muncă:

➔ dezvăluie activități online ascunse și descoperă traficanți care utilizează forumuri dark web sau conturi false de socializare

➔ poate detecta contracte de muncă false, anunțuri de angajare și înregistrări financiare false

MAGNET GRAYKEY, specializat în spargerea dispozitivelor mobile criptate, poate contribui și el. Ocolește blocările ecranului și extrage datele sistemului de fișiere.

Aplicare potențială într-un caz de trafic de persoane/exploatare prin muncă:

➔ Deblochează telefoanele traficanților confiscați și ajută la recuperarea conversațiilor de pe WhatsApp, Telegram, Signal, Viber etc.

De asemenea, alte programe software MAGNET ar putea fi utile (vezi Pizzuro, 2022).

- MSAB XRYun instrument criminalistic mobil utilizat de autoritățile locale de poliție (LEA) pentru a extrage, analiza și decodifica date de pe telefoane mobile, tablete, dispozitive GPS și drone.

Aplicare potențială într-un caz de trafic de persoane/exploatare prin muncă

➔ extrage comunicații mobile, dezvăluind potențial dovezi digitale relevante pentru traficul de persoane

➔ analizează rețelele de socializare și platformele de angajare

➔ recuperează fișierele și fotografiile șterse

- **Maltego** Compania oferă instrumente folosite pentru cartografierea relațiilor dintre persoane, companii, conturi de socializare și site-uri web (GRAFIC), pentru căutări OSINTasupra suspecților infractori (SEARCH), monitorizarea rețelelor de socializare în timp real (MONITOR) și efectuarea analizei rețelelor de socializare (DOVEZI).

  ***Aplicare potențială într-un caz de trafic de persoane/exploatare prin muncă**:*

  ➔ descoperă site-uri web de recrutare false și le leagă de traficanți cunoscuți

  ➔ mapează conexiunile dintre diferite profiluri de social media utilizate pentru recrutare

  ➔ identifică portofelele cripto și tranzacțiile financiare legate de traficanți

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

- **Autopsy**: un instrument gratuit, open-source, de investigare digitală criminalistică, care oferă o platformă pentru investigarea hard disk-urilor.

  ***Aplicare potențială într-un caz de trafic de persoane/exploatare prin muncă**:*

  ➔ recuperează contracte de muncă șterse sau documente de viză false

  ➔ urmărește istoricul browserului (de exemplu, vizite pe site-uri web false de locuri de muncă sau platforme de chat criptate)

  ➔ extrage istoricul dispozitivelor USB pentru a vedea dacă au fost folosite unități externe pentru stocarea, de exemplu, a datelor victimei

- **ADF PRO**: este un software de criminalistică digitală și triaj conceput pentru analiza rapidă a computerelor, unităților externe și dispozitivelor mobile.

Aplicare potențială într-un caz de trafic de persoane/exploatare prin muncă:

- ➔ Ridicarea rapidă a probelor digitale la percheziții (de exemplu, scanarea rețelelor de socializare, a laptopurilor și a telefoanelor suspecților)
- ➔ Recunoaștere facială: identificare și potrivire rapidă a fețelor din imagini și videoclipuri (aplicabilă pentru identificarea victimei și a agresorului)

- **Instrumente de analiză Blockchain** (de exemplu, Chainalysis,,Elliptic, CipherTrace)

  Aceste instrumente sunt specializate în urmărirea tranzacțiilor cu criptomonede, fiind adesea folosite de traficanți pentru a primi plăți pentru comisioane de recrutare sau exploatarea victimelor.

  Aplicare potențială într-un caz de trafic de persoane/exploatare prin muncă:

  - ➔ urmărește tranzacțiile Bitcoin sau cripto efectuate de victime până la recrutorul(ii) exploatator(i)
  - ➔ conectează adresele portofelului la rețele cunoscute de trafic de persoane
  - ➔ identifică tehnicile de spălare a banilor folosite pentru a ascunde profiturile ilicite

Pentru procesele de criminalistică digitală de combatere a traficului de persoane, sunt introduse și descrise pe scurt încă două abordări potențiale. Într-o oarecare măsură, acestea se pot suprapune și cu instrumentele sau ramurile criminalistice digitale deja descrise.

Prima abordare este utilizarea metadatelor din imagini și videoclipuri din traficul de persoane pentru investigații criminalistice (digitale). În loc să se bazeze exclusiv pe tehnici de viziune computerizată costisitoare din punct de vedere computațional, metadatele imaginilor și videoclipurilor ar putea ajuta autoritățile de aplicare a legii în

identificarea victimelor și a traficanților (Mattmann și colab., 2016). Traficul de persoane conține adesea semne textuale, cum ar fi caracteristicile fizice ale victimei, locația și elemente multimedia (de exemplu, imagini, videoclipuri pe diferite platforme). Mattmann și colab. (2016) au dezvoltat un set de instrumente de metadate criminalistice pentru multimedia, care cuprinde ImageCat (catalog de imagini) și ImageSpace. ImageCat este un sistem de extragere, transformare și încărcare (ETL) conceput pentru a procesa și cataloga metadatele multimedia, în special în domeniul investigațiilor privind traficul de persoane. Poate lega mai multe reclame cu metadate comune (de exemplu, aceeași cameră utilizată pentru victime diferite; analiza similarității) și permite căutarea și recuperarea rapidă a probelor multimedia. Prin urmare, poate ajuta autoritățile de aplicare a legii (LEA) să identifice atât victimele, cât și traficanții (Mattmann și colab., 2016). În plus, ImageSpace (construit pe ImageCat) extrage metadate multimedia (de exemplu, spațiul de culoare RGB, modelul camerei, geolocația, marcajele temporale). Poate căuta și interoga baze de date multimedia mari, ceea ce permite autorităților de aplicare a legii (LEA) să caute imagini și videoclipuri folosind text, metadate sau similaritatea imaginilor. Mai mult, răsfoirea și vizualizarea interactivă a imaginilor ajută autoritățile de aplicare a legii să afișeze aceste dovezi într-o galerie organizată pentru examinare criminalistică și oferă histograme și grafice de densitate interactive. ImageSpace permite, de asemenea, potrivirea similarității între imagini și videoclipuri pentru a grupa fișiere corelate, ajutând anchetatorii să urmărească, de exemplu, victimele pe diferite reclame și platforme. În plus, își poate optimiza rezultatele căutării în timp și acceptă recunoașterea optică a caracterelor și extragerea textului (adică extragerea numerelor de telefon, a e-mailurilor, a adreselor) din imagini și videoclipuri. Această abordare multimedia specifică oferă o metodă alternativă de a lega reclamele, victimele și traficanții prin analizarea modelelor de metadate în loc de conținutul exclusiv al imaginilor sau videoclipurilor.

O altă abordare care este parțial încorporată în instrumentele prezentate anterior și rezonează în multe dintre elaborările de până acum privind investigațiile privind traficul

de persoane și criminalistica digitală este cercetarea în domeniul informațiilor open-source (OSINT). Cercetarea OSINT se referă la colectarea și analizarea datelor disponibile publicului pentru a sprijini investigațiile. Aceasta joacă un rol esențial în criminalistica digitală pentru investigațiile privind traficul de persoane prin identificarea tiparelor, urmărirea amprentelor digitale și conectarea suspecților la activități criminale. Deoarece elemente OSINT deosebit de utile au fost menționate anterior, această scurtă secțiune despre aceasta servește doar la sublinierea importanței și a marelui potențial al acesteia. OSINT este esențial pentru identificarea tiparelor de recrutare și comunicare, deoarece ajută la descoperirea platformelor cheie, a tiparelor lingvistice și a strategiilor de recrutare utilizate în metodele de recrutare activă (vânătoare) și pasaj (pescuit). OSINT, care poate fi împărțit în informații despre rețelele de socializare (SOCMINT), informații geospațiale (GEOINT) și informații umane (HUMINT), implică, de exemplu, monitorizarea rețelelor de socializare și a anunțurilor de locuri de muncă, analizarea discuțiilor pe forumuri, a activităților de pe dark web și căutarea inversă de imagini și videoclipuri. Aceasta servește la conectarea anunțurilor online la rețelele de trafic prin accesarea cu crawlere și analiza anunțurilor de locuri de muncă, urmărirea criptomonedelor și a plăților și analiza domeniilor și site-urilor web. Poate fi important pentru geolocalizarea victimelor și a traficanților prin analizarea imaginilor și videoclipurilor (și a metadatelor acestora) sau prin utilizarea geolocalizării crowdsourcing (de exemplu, Google Street View, imagini din satelit). În plus, OSINT poate ajuta, de asemenea, la demascarea identităților și rețelelor false prin corelarea datelor de pe rețelele de socializare (sau, de asemenea, din dark web), prin analizarea amprentelor digitale și verificarea datelor personale (a se vedea, de exemplu, https://epieos.com/ pentru căutarea inversă dacă o adresă de e-mail sau un număr de telefon este asociat cu conturi specifice, cum ar fi un cont Google), sau prin analiza comportamentală (de exemplu, comportamente de postare, tipare lingvistice, momentul activităților online).

9.4.4.4Provocări în investigațiile criminalistice digitale

Investigațiile privind traficul de persoane prezintă obstacole unice pentru criminalistica digitală, cum ar fi:

- Comunicare criptată și autodistructivă
- Ștergerea și ascunderea datelor
- Probleme legate de datele transfrontaliere
- Protecția victimelor și intimitatea

Pentru a avea o imagine de ansamblu mai sistematică a provocărilor, le putem împărți în provocări legate de materie și provocări structurale.

Provocări legate de materie

Provocările legate de materie sunt provocări care decurg din domeniul criminalisticii digitale și al investigațiilor privind traficul de ființe umane. Prin urmare, acestea sunt imanente infracțiunii în sine. De exemplu, se poate face o diferențiere între investigațiile proactive și cele reactive. Investigațiile proactive sunt mult mai complexe de început, deoarece autoritățile de aplicare a legii trebuie să identifice semne de exploatare care ar putea indica exploatarea. Este dificil să se filtreze aceste referințe din numărul mare de anunțuri online disponibile, de exemplu (Europol, 2020). Prin urmare, „investigațiile reactive sunt mai ușoare deoarece au un punct de plecare, cum ar fi mărturia unei victime identificate și/sau contul sau site-ul web utilizat în scopuri de recrutare sau exploatare” (Europol, 2020, p. 5).

În plus, dovezile digitale în sine cu care anchetatorii se ocupă predominant în cazurile de trafic de persoane prezintă provocări. Întrucât mulți traficanți utilizează aplicații de mesagerie instantanee precum WhatsApp, Signal sau Telegram, criptarea end-to-end

încorporată (E2EE) îngreunează recuperarea mesajelor. Un alt aspect este că traficanții șterg adesea dovezile digitale (ei înșiși sau utilizează funcții de auto-ștergere, de exemplu, în chat-urile WhatsApp). Posibilitatea de recuperare a datelor șterse este limitată; prin urmare, anchetatorii se pot concentra pe analiza imaginilor de backup create anterior. În plus, traficanții ar putea opera pe servicii ascunse Tor (dark web, utilizare VPN), ceea ce îngreunează urmărirea. Mai mult, traficanții încearcă să estompeze urmele printr-o diversificare extremă a prezenței lor digitale - de exemplu, utilizând mai multe cartele SIM și telefoane mobile, diverse conturi (inclusiv conturi false) etc. Această dificultate exemplifică o altă provocare: anchetatorul implicat în caz trebuie adesea să stăpânească o cantitate vastă de date (în special digitale), să analizeze aceste date, să le clasifice drept relevante sau irelevante pentru infracțiunea sau infracțiunile care urmează a fi acuzate, să mențină o imagine de ansamblu și să planifice pași strategici suplimentari. De asemenea, legat de această provocare este un alt aspect juridic care poate deveni problematic: un caz poate deveni incredibil de complex, deoarece adesea nu numai traficul de persoane/exploatarea prin muncă poate fi acuzat, ci și, de exemplu, evaziunea fiscală; încălcarea legislației muncii și a obligațiilor de securitate socială; munca forțată; agresiunea; frauda; falsificarea documentelor; sau încălcarea drepturilor omului. Acest lucru poate afecta, de exemplu, criminalistica digitală, deoarece un caz mai complex necesită un schimb mai amplu și consecvent de informații între investigatorul principal al cazului și specialistul în criminalistică digitală.

Provocări structurale

Provocările pot fi văzute ca fiind structurale atunci când decurg din sistem (de exemplu, din organizarea aplicării legii într-o țară, circumstanțe legislative). De exemplu, tehnologiile digitale aplicate de traficanți sunt în continuă dezvoltare, motiv pentru care aplicarea legii trebuie să se adapteze la aceste (cele mai recente) evoluții tehnice care sunt aplicate de autori (Europol, 2020). În plus, autoritățile de aplicare a legii trebuie să

obțină resurse umane adecvate pentru aceste investigații. Acest lucru nu se aplică doar anchetatorilor specializați în traficul de persoane și specialiștilor și practicienilor în criminalistică digitală, ci și altor tipuri de personal necesare rapid pentru investigarea cazurilor de trafic de persoane, cum ar fi interpreții (pentru traducerea datelor de supraveghere a telecomunicațiilor, de exemplu). De asemenea, instrumentele legislative trebuie îmbunătățite pentru a asigura urmărirea penală și condamnarea (Europol, 2020).

Extinderea posibilităților legislative este, de asemenea, deosebit de relevantă, deoarece victimele sunt adesea reticente în a face mărturisiri și declarații majore, deoarece sunt deja supuse unui stres psihologic mare - amenințări, șantaj, precum și riscul inerent de a fi puse în situația de a fi puse în dificultate în public prin intermediul rețelelor de socializare (de exemplu, prin publicarea exploatării lor). Prin urmare, accesul mai ușor la seturile de date disponibile pentru criminalistica digitală este important pentru a impulsiona investigațiile și, în cele din urmă, pentru a sprijini sau chiar a permite urmărirea penală (Europol, 2020).

În ceea ce privește aspectele juridice, trebuie menționat și faptul că eforturile de colaborare transfrontalieră pot fi afectate dacă cooperarea judiciară și normele aplicabile nu sunt clare. Acest lucru poate împiedica, de exemplu, schimbul de probe între țări. Având în vedere lipsa unei cooperări internaționale standardizate, nu există încă o bază de date centralizată globală privind traficul de persoane care să urmărească activitatea online a traficanților la nivel global.

9.4.4.5Considerații juridice și etice

Datorită naturii sensibile a cazurilor de trafic de persoane, investigațiile criminalistice trebuie să respecte standarde etice și legale stricte, dintre care unele au fost deja prezentate anterior. Prin integrarea acestor considerații, profesioniștii în criminalistică digitală pot naviga în peisajul complex al investigațiilor privind traficul de persoane și

exploatarea prin muncă în mod etic, legal și eficient, asigurându-se că urmărirea justiției se aliniază cu protejarea drepturilor individuale și a valorilor societale.

Abordarea centrată pe victimă

O abordare centrată pe victimă prioritizează drepturile, nevoile și bunăstarea victimelor pe tot parcursul procesului de investigație. Această metodologie pune accent pe tratarea victimelor cu respect și sensibilitate, asigurându-se că acestea sunt informate și sprijinite și implicându-le activ în deciziile care le afectează viața. Concentrându-se pe experiența victimei, anchetatorii pot construi încredere, ceea ce este crucial nu numai pentru colectarea de informații exacte, ci și pentru furnizarea de servicii de sprijin adecvate victimei. Această abordare nu numai că ajută la recuperarea victimelor, dar consolidează și integritatea generală a investigației (Organizația Internațională a Muncii, 2018). „Siguranța victimelor, a familiilor și a celor dragi acestora este primordială în orice moment și este o responsabilitate a anchetatorului și a procurorului” (Organizația Internațională a Muncii, 2018, p. 47). Acest lucru subliniază, de asemenea, necesitatea de a ne concentra nu doar asupra victimei ca individ, ci și asupra familiilor/rudelor, deoarece posibilitatea represaliilor împotriva membrilor familiei de către traficanți este iminentă. (Organizația Internațională a Muncii, 2018).

Mai mult, în special în ceea ce privește criminalistica digitală, se recomandă minimizarea supravegherii digitale intruzive, concentrându-se pe traficanți în această privință, nu pe victimă/victime. Confidențialitatea datelor victimelor ar trebui asigurată în orice moment pentru a preveni represaliile sau expunerea publică. Investigatorul ar trebui să evite să facă presiuni asupra victimelor pentru a relata interacțiunile digitale de mai multe ori (și să utilizeze în schimb instrumente criminalistice), acesta ar trebui să respecte consimțământul victimei înainte de a accesa dispozitivele personale. Trebuie evitate tehnicile de interogare agresive bazate pe descoperiri digitale (de exemplu, confruntarea unei victime cu jurnalele sale de chat într-un mod care declanșează stres). O altă

provocare majoră în urmărirea penală a traficanților poate fi dependența de mărturiile victimelor, care poate fi traumatizantă pentru victimă, dar potențial și nesigură din cauza fricii. În acest sens, criminalistica digitală poate consolida cazurile și reduce dependența victimelor în instanță, ceea ce, la rândul său, poate reduce povara asupra victimelor. Experții în criminalistică digitală pot, de asemenea, preveni represaliile și retraficarea victimelor prin scanarea dispozitivelor acestora, dacă se convine/se dorește, pentru spyware și prin eliminarea ulterioară a instrumentelor de urmărire.

Protecția datelor

În timpul procesului de investigație: Protejarea persoanelor care demască activități de trafic este vitală pentru încurajarea raportării infracțiunilor. De asemenea, protecția denunțătorilor asigură că cei care demască informații nu se confruntă cu represalii, promovând un mediu în care informațiile pot fi partajate în siguranță. În plus, raportarea etică de către mass-media și autorități garantează că victimele nu sunt revictimizate prin expunere și că informațiile diseminate servesc interesului public fără a provoca prejudicii.

UNODC a întocmit o prezentare generală a confidențialității și protecției datelor în Modulul 10 despre confidențialitate și protecția datelor care ia în considerare pentru chestiuni legate de securitatea cibernetică.

- **Probe ridicate:** Asigurarea integrității și confidențialității probelor digitale este esențială. Trebuie implementate măsuri adecvate de protecție a datelor pentru a preveni accesul neautorizat, manipularea sau pierderea probelor. Menținerea unui lanț clar de custodie este esențială pentru admisibilitatea probelor în instanță, deoarece documentează gestionarea probelor de la colectare până la prezentare. Respectarea standardelor și protocoalelor legale protejează drepturile tuturor părților implicate și menține credibilitatea procesului de investigație.

Cooperare internațională

Traficul de persoane și exploatarea prin muncă sunt adesea infracțiuni transnaționale, necesitând colaborare transfrontalieră. Cooperarea internațională implică alinierea cadrelor juridice, schimbul de informații și coordonarea eforturilor între diverse jurisdicții. Această abordare colectivă sporește capacitatea de a urmări autorii, de a proteja victimele și de a demonta eficient rețelele de trafic. Modulul 11 – Cooperarea internațională pentru combaterea criminalității organizate transnaționale de la UNODC poate ajuta la obținerea unei perspective de ansamblu asupra cadrului juridic aplicabil în acest domeniu.

Proporționalitate și necesitate

Investigațiile ar trebui să echilibreze nevoia de informații cu respectarea vieții private individuale. Colectarea probelor digitale trebuie să fie proporțională cu gravitatea infracțiunii și necesară pentru investigație. Acest principiu garantează că măsurile de investigație nu depășesc și nu încalcă drepturile fundamentale, menținând standardele etice în timp ce se urmărește justiția.

Integrarea inteligenței artificiale

Integrarea inteligenței artificiale în criminalistica digitală oferă eficiență, dar ridică și îngrijorări cu privire la acuratețe și părtinire. Instrumentele automate trebuie proiectate cu atenție și evaluate periodic pentru a preveni părtinirile care ar putea duce la acuzații nefondate sau ar putea trece cu vederea anumite profiluri ale victimelor. Supravegherea umană rămâne crucială pentru interpretarea datelor generate de inteligența artificială în contextul legal și etic adecvat. În special în punctele relevante sau chiar cheie ale procesului de investigație, utilizarea inteligenței artificiale nu trebuie să înlocuiască judecata umană.

Utilizarea etică a OSINT și a monitorizării dark web

Deși monitorizarea OSINT și a dark web-ului sunt valoroase în descoperirea activităților ilicite, acestea trebuie efectuate în limitele legale. Anchetatorii ar trebui să evite accesul neautorizat sau practicile înșelătoare care ar putea compromite integritatea investigației sau ar putea încălca standardele etice. Respectarea vieții private și obținerea informațiilor în mod legal sunt fundamentale pentru menținerea încrederii publice și respectarea statului de drept.

9.5 Investigații financiare

Investigațiile financiare sunt un instrument esențial în combaterea infracțiunilor financiare, cum ar fi spălarea banilor (ML), finanțarea terorismului (FT) și traficul de persoane. Aceste investigații se concentrează pe analizarea tranzacțiilor financiare pentru a detecta activități ilicite, a urmări fondurile ilegale și a identifica autorii și rețelele acestora. Conceptele și obiectivele de bază ale investigațiilor financiare se învârt în jurul urmăririi pistei banilor pentru a descoperi și documenta infracțiunile financiare. Obiectivele principale includ identificarea rețelelor criminale, urmărirea fondurilor ilicite și colectarea de probe care pot fi utilizate în urmărirea penală. O investigație financiară bine condusă consolidează eforturile de aplicare a legii prin privarea infractorilor de resursele lor financiare și prin demontarea infrastructurii financiare care susține crima organizată.

Relevanța analizelor financiare în contextul traficului de persoane este deosebit de semnificativă, deoarece traficanții depind de tranzacțiile financiare pentru a muta, stoca și spăla veniturile lor ilegale. Prin examinarea atentă a înregistrărilor tranzacțiilor, a extraselor de cont bancar și a metodelor de plată digitale, anchetatorii pot descoperi legături financiare între traficanți și asociații acestora. Acest lucru nu numai că ajută la urmărirea penală a infractorilor, dar ajută și la identificarea victimelor prin detectarea tiparelor financiare care indică exploatarea. Prin urmare, investigațiile financiare joacă un

rol crucial în destructurarea rețelelor de trafic de persoane, vizând resursele financiare vitale care le susțin. „Cu toate acestea, recunoașterea, implementarea și armonizarea pe scară largă a strategiilor și tacticilor de investigare care vizează în mod specific finanțele traficului de persoane sunt încă în curs de desfășurare" (OSCE, 2019, p. 37).

Secțiunea 9.7.1 prezintă elementele generale de bază ale investigației financiare, urmată de o introducere despre structurile afacerilor de trafic pentru a evidenția relevanța investigației financiare în domeniul traficului de persoane și al exploatării prin muncă (Secțiunea 9.7.2). Secțiunea 9.7.3 ilustrează pas cu pas modul de desfășurare a unei investigații financiare în cazurile de trafic. Secțiunea 9.7.4 prezintă indicatori tranzacționali care indică activități financiare suspecte în domeniul traficului de persoane și în special al exploatării prin muncă. Secțiunea 9.7.5 descrie provocările din cadrul investigațiilor financiare, în timp ce secțiunea 9.7.6 analizează inovațiile și tendințele tehnice. Secțiunea 9.7.7 se încheie cu câteva recomandări suplimentare.

9.5.1 Prezentare generală

Investigațiile financiare joacă un rol crucial în aplicarea legii și în urmărirea penală, în special în cazurile care implică spălarea banilor, finanțarea terorismului și crimă organizată (FATF, 2012). Ghidul Grupului de Acțiune Financiară Internațională (GAFI) privind Investigațiile Financiare prezintă principiile, instrumentele și strategiile esențiale necesare pentru desfășurarea unor anchete financiare eficiente. Scopul principal al unei investigații financiare este de a urmări și documenta mișcarea fondurilor ilicite, ajutând la identificarea rețelelor criminale, descoperirea structurilor financiare și construirea unor rechizitorii solide (FATF, 2012). Prin examinarea aspectelor financiare ale activităților criminale, anchetatorii pot descoperi noi piste, pot cartografia rețele criminale întregi - inclusiv conexiunile lor transnaționale - și pot aduna probe pentru a urmări penal suspecții și a confisca activele ilicite.

9.5.1.1 Aspecte esențiale ale investigațiilor financiare

O componentă esențială a investigațiilor financiare o reprezintă investigațiile paralele, în care anchetele financiare se desfășoară alături de anchetele penale. Această abordare asigură că, în timp ce autoritățile de aplicare a legii se concentrează pe infracțiuni precum traficul de persoane, corupția sau traficul de droguri, o investigație financiară simultană urmărește fluxul de bani generat de aceste activități (FATF, 2012). Investigațiile paralele ajută la urmărirea activelor ilicite, la identificarea suspecților suplimentari și la sprijinirea confiscării produselor infracțiunii. Pentru a spori eficacitatea, se înființează adesea grupuri operative multidisciplinare, care reunesc analiști financiari, contabili judiciari, experți în criminalistică digitală și procurori. Aceste echipe îmbunătățesc schimbul de informații, reduc duplicarea eforturilor și asigură o abordare cuprinzătoare a criminalității financiare (FATF, 2012).

Un obiectiv esențial al investigațiilor financiare este recuperarea și confiscarea activelor (a se vedea capitolul 10 din secțiunea Instruire). Infractorii se bazează pe câștigurile financiare ca factor motivațional cheie, iar privarea lor de veniturile ilicite le slăbește operațiunile. Autoritățile de aplicare a legii trebuie să urmărească, să îndisponibilizeze și să confiște activele ilicite folosind tehnici avansate de criminalistică financiară. Confiscarea fără condamnare este, de asemenea, recomandată ca un instrument juridic eficient, permițând autorităților să confiște activele provenite din infracțiuni chiar și în cazurile în care o condamnare nu este posibilă. Înființarea de unități specializate de recuperare a activelor și a unor baze de date centralizate de informații financiare consolidează semnificativ investigațiile financiare prin îmbunătățirea eficienței și a coordonării.

O investigație financiară reușită se bazează pe multiple surse de informații. Autoritățile de aplicare a legii trebuie să aibă acces la rapoarte de informații financiare,

inclusiv STR (Rapoarte de tranzacții suspecte), rapoarte de tranzacții valutare și declarații transfrontaliere de numerar. În plus, înregistrările bancare și financiare, registrele companiilor, declarațiile fiscale, datele vamale și OSINT (Informații open-source) oferă indicii cruciale. Este esențial ca ofițerii de aplicare a legii să aibă autoritatea legală de a accesa și analiza aceste înregistrări, asigurând în același timp respectarea legilor privind protecția datelor.

Tehnici de investigație

În investigațiile financiare se utilizează o varietate de tehnici de investigație (tehnicile enumerate, a se vedea FATF, 2012, dacă nu este indicată nicio altă sursă).

- **Supraveghere fizică** Această tehnică implică monitorizarea suspecților pentru a le înțelege activitățile financiare, cum ar fi mișcările de numerar în cantități mari sau interacțiunile cu intermediarii financiari. Este utilă în special în cazurile de spălare de bani și finanțare a terorismului.
- **Analiza resturilor** Anchetatorii pot colecta și analiza în mod legal înregistrări financiare aruncate și alte documente care ar putea dezvălui active ascunse sau tranzacții ilicite.
- **Măsuri obligatorii** Acestea includ mandate de percheziție, citații și ordine de prezentare pentru obținerea de documente financiare critice, cum ar fi extrase de cont bancare, declarații fiscale și registre comerciale. Procedurile de percheziție și ridicare executate corespunzător asigură că probele digitale și fizice sunt colectate legal și păstrate sub un lanț de custodie.
- **Interceptarea comunicațiilor** Forțele de ordine pot efectua interceptări telefonice, monitorizare a e-mailurilor și alte forme de supraveghere electronică pentru a urmări tranzacțiile financiare și a identifica complicii. Această metodă este extrem

de eficientă, dar trebuie să respecte cadrul legal pentru a evita încălcarea confidențialității.

- **Operațiuni sub acoperire** În unele cazuri, anchetatorii pot prelua identități false pentru a se infiltra în organizațiile criminale și a aduna dovezi directe ale abaterilor financiare. Această tehnică necesită resurse intensive și o instruire extinsă.
- **Livrări supravegheate** Această metodă implică urmărirea mișcării fondurilor ilicite, fie în numerar, fie prin transferuri digitale, sub supravegherea forțelor de ordine. Aceasta ajută la identificarea actorilor cheie din rețelele de spălare a banilor sau de fraudă.
- **Contabilitate judiciară** Contabilitatea judiciară este o practică specializată care combină abilități de contabilitate, audit și investigație pentru a examina înregistrările financiare pentru a depista semne de abateri contabile. Contabilii judiciari pot descoperi discrepanțe în registre, pot detecta fraude și pot urmări activități financiare ilicite prin intermediul situațiilor financiare detaliate. Aceștia aplică atât metode cantitative, cum ar fi analiza datelor și modelarea statistică, cât și abordări calitative, inclusiv evaluarea modelelor comportamentale și a culturii organizaționale, pentru a detecta anomalii. Legea lui Benford prezice distribuția frecvenței cifrelor în seturile de date care apar în mod natural. Contabilii judiciari utilizează acest principiu pentru a identifica nereguli în datele financiare. Abaterile de la distribuția așteptată pot semnala o potențială manipulare sau fraudă. Mark Nigrini, un pionier în acest domeniu, a cercetat pe larg și a aplicat Legea lui Benford pentru a detecta anomalii în datele contabile (vezi, de exemplu, Gorenc, 2019; Siavoshi, 2025).
- **Metode de dovedire a veniturilor** Anchetatorii folosesc metode directe și indirecte pentru a stabili surse ilegale de venit. Metoda fluxurilor de patrimoniu compară activele unei persoane în două momente pentru a determina veniturile

neraportate. Metoda depozitelor bancare analizează intrările inexplicabile din conturile bancare. Metoda cheltuielilor compară modelele de cheltuieli cu sursele legale de venit cunoscute.

- **Partajarea informațiilor financiare** Autoritățile de aplicare a legii colaborează cu unitățile de informații financiare (FIU), băncile și omologii internaționali pentru a obține rapoarte de tranzacții suspecte (STR) și alte date financiare relevante.
- **Revizuirea tranzacțiilor financiare** ajută anchetatorii să identifice tipare bancare suspecte, tehnici de stratificare și metode de integrare a activelor.
- **Criminalistică digitală**(a se vedea secțiunea 9.6.1) joacă un rol cheie în urmărirea transferurilor de bani online, analizarea tranzacțiilor cu criptomonede și interceptarea comunicațiilor financiare ilicite.

Utilizarea sinergiilor de colaborare

Unitățile de informații financiare (FIU) joacă un rol esențial în investigațiile financiare prin colectarea, analizarea și diseminarea informațiilor financiare către autoritățile de aplicare a legii. FIU-urile primesc dezvăluiri privind combaterea spălării banilor și combaterea terorismului (AML/CFT), rapoarte de tranzacții suspecte (STR) și rapoarte de tranzacții transfrontaliere, care pot oferi avertizări timpurii cu privire la activitățile financiare infracționale. O colaborare națională puternică între FIU-uri și anchetatori asigură accesul autorităților de aplicare a legii la informații concrete și corecte, în timp real. Pentru a spori eficiența, FIU-urile și autorităților de aplicare a legii ar trebui să stabilească platforme securizate, în timp real, pentru partajarea datelor și să dezvolte protocoale pentru analizarea informațiilor financiare.

Întrucât criminalitatea financiară este adesea transnațională, și cooperarea internațională este vitală. Infractorii exploatează sistemele bancare internaționale și centrele financiare offshore pentru a ascunde fonduri ilicite. Autoritățile de aplicare a legii

trebuie să utilizeze Tratatele de asistență juridică reciprocă (MLAT), Interpol, Europol și rețelele GAFI pentru a facilita investigațiile transfrontaliere. Înființarea de echipe comune de anchetă (JIT) și eficientizarea cadrelor juridice pentru schimbul de informații consolidează lupta globală împotriva criminalității financiare (GAFI, 2012).

Pentru a îmbunătăți investigațiile financiare, autoritățile de aplicare a legii și organele de urmărire penală ar trebui să integreze criminalistica financiară în toate investigațiile majore privind infracțiunile, să utilizeze sistemele de informații financiare pentru analize în timp real și să consolideze colaborarea internațională privind recuperarea activelor și schimbul de informații. Prin adoptarea acestor bune practici, investigațiile financiare pot servi drept un instrument puternic în dezmembrarea întreprinderilor criminale și în asigurarea faptului că infracțiunile nu sunt rentabile.

9.5.1.2Eforturile Uniunii Europene

Recunoscând amenințarea tot mai mare a criminalității organizate care se infiltrează în economia legală, Uniunea Europeană a subliniat necesitatea consolidării capacităților de investigare financiară. Strategia UE din 2021 de combatere a criminalității organizate a subliniat importanța promovării investigațiilor financiare timpurii în toate țările UE. Această abordare își propune să demonteze infrastructura financiară a organizațiilor criminale, să elimine profiturile acestora și să prevină integrarea lor în economia și societatea legală (Comisia Europeană). Pentru a sprijini aceste eforturi, Platforma europeană multidisciplinară împotriva amenințărilor infracționale (EMPACT) a prioritizat investigațiile financiare în agenda sa. EMPACT facilitează colaborarea dintre statele membre ale UE pentru a aborda diverse amenințări infracționale, inclusiv traficul de droguri și traficul de persoane, prin integrarea investigațiilor financiare ca obiectiv comun în toate prioritățile.

În plus, Comisia Europeană oferă sprijin financiar Rețelei Operaționale de Combatere a Spălării Banilor (AMON), o rețea globală de anchetatori în domeniul combaterii spălării banilor înființată în 2012. AMON facilitează schimbul de cunoștințe între autoritățile de aplicare a legii și sprijină cooperarea operațională rapidă în investigațiile privind spălarea banilor, reflectând natura transfrontalieră a acestor infracțiuni.

Europol și-a intensificat, de asemenea, eforturile prin înființarea Centrului European pentru Criminalitate Financiară și Economică (EFECC) în 2020. EFECC oferă sprijin operațional statelor membre ale UE în cazurile care implică infracțiuni fiscale, fraudă, corupție, spălare de bani, recuperarea activelor, falsificarea monedei euro și infracțiuni împotriva proprietății intelectuale. Această inițiativă își propune să combată cazurile extrem de sofisticate de criminalitate financiară care vizează persoane fizice, companii și sectorul public.

În plus, Agenția Europeană pentru Formare Profesională în Aplicarea Legii (CEPOL) oferă periodic cursuri de formare ofițerilor de aplicare a legii pentru a le îmbunătăți înțelegerea schemelor de spălare a banilor și a tehnicilor transnaționale de investigare financiară. Această formare își propune să consolideze capacitatea anchetatorilor de a aborda în mod eficient dimensiunile financiare ale criminalității organizate (Comisia Europeană, fără dată).

În concluzie, abordarea cuprinzătoare a Uniunii Europene în ceea ce privește investigațiile financiare subliniază rolul esențial al acestora în desființarea activităților criminale, protejarea economiei legale și sporirea eficacității aplicării legii în statele membre.

9.5.2Traficul de persoane ca afacere

Traficul de persoane funcționează ca o afacere axată pe profit, la fel ca afacerile legitime, și merită să analizăm această perspectivă pentru a (1) înțelege principalii factori ai traficului și (2) necesitatea efectuării unor investigații financiare. Teoriile economice ale criminalității sugerează că autorii fac alegeri raționale bazate pe profiturile, riscurile și oportunitățile potențiale (vezi, de exemplu, Belser, 2005). Aceste oportunități apar datorită faptului că persoanele caută condiții economice mai bune, fie prin migrația din zonele rurale sărace către centre urbane mai bogate, fie peste granițele internaționale. Rețelele criminale exploatează aceste vulnerabilități oferind promisiuni false de angajare, dragoste sau securitate, conducând victimele către exploatarea prin muncă sau sexuală sau alte forme de trafic (de exemplu, prelevarea de organe). Modelul de afaceri pentru exploatarea specifică prin muncă este simplu: victimele lucrează sub constrângere sau fără a fi conștiente de situația de exploatare, generând profituri mari, suportând în același timp costuri minime pentru traficanți. Sectoare precum agricultura, construcțiile, munca domestică și ospitalitatea oferă acoperire pentru traficul de persoane prin muncă, în timp ce exploatarea sexuală rămâne una dintre cele mai profitabile piețe pentru traficanți (vezi, de exemplu,Aronowitz, Theuermann și Tyurykanova, 2010).

În ciuda profitabilității ridicate, riscurile pentru traficanți rămân scăzute. Multe victime se tem de aplicarea legii din cauza statutului lor juridic, a stigmatului social sau a amenințărilor din partea exploatatorilor lor. În țările în care prostituția este ilegală, victimele sunt mai predispuse să fie arestate decât să primească protecție. În plus, ratele de detectare și urmărire penală a traficanților rămân scăzute, consolidând sustenabilitatea modelului de afaceri. Forțele pieței joacă, de asemenea, un rol semnificativ în modelarea operațiunilor de trafic. Nu doar cererea consumatorilor determină traficul de persoane, ci mai degrabă existența unei oferte mari de persoane vulnerabile. Organizațiile criminale își adaptează metodele pe baza cadrelor juridice, a condițiilor economice și a mecanismelor de aplicare a legii, la fel cum întreprinderile legitime răspund la schimbările pieței (Aronowitz, Theuermann și Tyurykanova, 2010).

Investigațiile financiare privind traficul de persoane trebuie să ia în considerare acești factori economici. Prin analizarea tranzacțiilor financiare, a marjelor de profit și a fluxurilor de numerar ilicite, autoritățile de aplicare a legii pot identifica modele de exploatare, pot perturba rețelele și pot slăbi stimulentele financiare din spatele operațiunilor de trafic. Înțelegerea traficului de persoane ca întreprindere economică este crucială pentru dezvoltarea unor contramăsuri eficiente, inclusiv cadre de reglementare, supraveghere financiară și intervenții specifice. Următoarea secțiune prezintă cadrul general al investigațiilor financiare în cazurile de trafic de persoane și ce măsuri specifice ar trebui luate.

9.5.3Ghid pas cu pas pentru investigațiile financiare legate de traficul de persoane

Această secțiune prezintă unsprezece etape cheie pentru desfășurarea unor investigații financiare eficiente în cazurile de trafic de persoane. Acești pași sunt clasificați în trei domenii: fundamental, operațional și comunitar.

Etapele fundamentale sunt de obicei întreprinse o singură dată în timpul stabilirii cadrului de investigație și se aplică pe scară largă atât în sectorul public, cât și în cel privat. Etapele operaționale sunt aplicate mai frecvent datorită relevanței lor pentru investigațiile individuale, deși implementarea lor variază între entitățile publice și cele private. De exemplu, Etapele 7 și 8 privesc în principal entitățile raportoare din sectorul privat. În cele din urmă, etapele comune sunt împărțite în ceea ce privește aplicabilitatea: ambele sectoare au un interes comun pentru Etapa 10, în timp ce furnizorii de servicii financiare poartă o responsabilitate mai mare pentru Etapa 11.

Figura 14 prezintă schematic acest proces pas cu pas între autoritățile de ordine publică și unitățile de informații financiare. Această figură este preluată de la OSCE (2020).

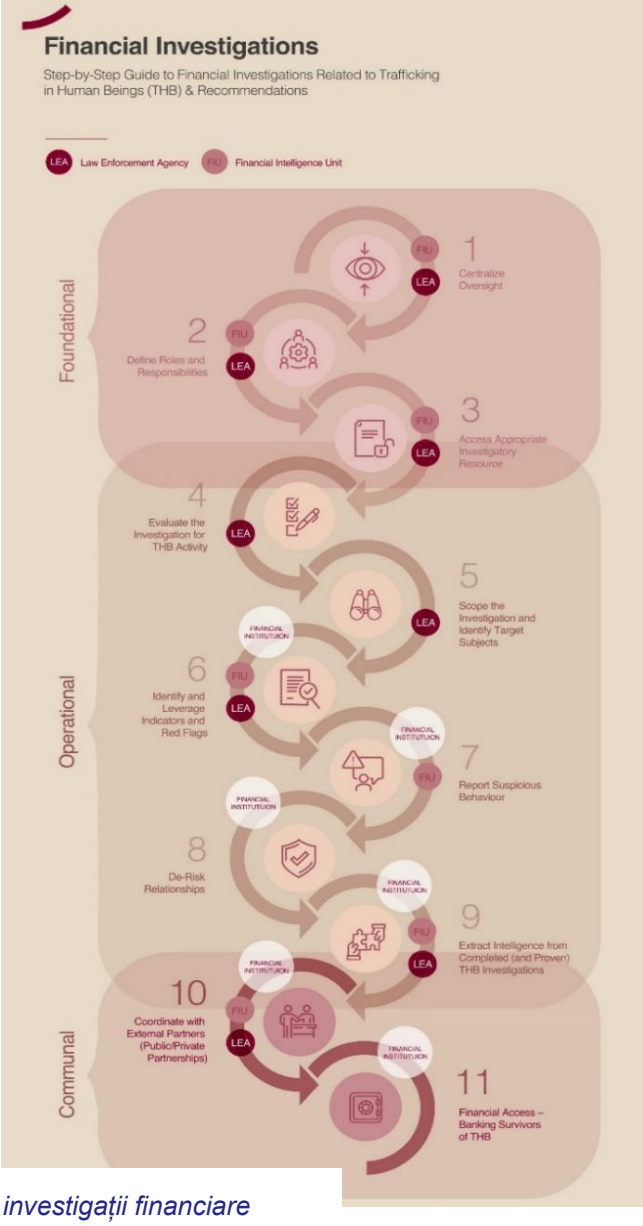

Figura4Etapele unei investigații financiare

Pasul 1: Primul pas într-o investigație financiară de succes privind traficul de persoane este stabilirea unui mecanism centralizat de supraveghere. Aceasta asigură un răspuns coordonat și cuprinzător la fiecare caz suspect, deși structura sa poate varia în funcție de dimensiunea și mandatul unei instituții. Aautoritățile de aplicare a legii integrează adesea investigațiile privind traficul de persoane în unități specializate. De exemplu, Departamentul de Poliție din New York (NYPD) și Serviciul de Poliție Metropolitană din Londra (MPS) au echipe dedicate, în timp ce Serviciul de Poliție din Toronto (TPS) se ocupă de cazurile de trafic în cadrul Unității sale pentru Infracțiuni Sexuale, recunoscând distincția acestora față de infracțiunile legate de vicii. Agențiile federale precum FBI și Interpol centralizează, de asemenea, expertiza, la fel ca și FIU-urile, deși acestea din urmă operează adesea cu mai puțină vizibilitate publică.

În sectorul privat, în special în bănci, supravegherea este mai puțin structurată din cauza volumului mare de tranzacții și a cerințelor de reglementare. Cu toate acestea, multe instituții mențin echipe speciale de investigație pentru a aborda infracțiunile financiare, inclusiv traficul de persoane. Centralizarea eforturilor de investigație oferă mai multe beneficii, inclusiv reducerea duplicării, îmbunătățirea eficienței, sporirea expertizei și permiterea unei analize cuprinzătoare a datelor. Cu toate acestea, aceasta prezintă și riscuri, cum ar fi limitarea cunoștințelor la un grup select și potențiale întârzieri în investigații. Pentru a atenua aceste riscuri, instituțiile ar trebui să promoveze inițiative de partajare a cunoștințelor și să permită flexibilitate în responsabilitățile investigative pentru a preveni blocajele. În cele din urmă, atâta timp cât cazurile sunt înregistrate și gestionate corespunzător, investigațiile pot fi efectuate de echipe diferite, în beneficiul atât al părților interesate interne, cât și al celor externe.

Pasul 2: Odată ce este stabilit un cadru de supraveghere pentru investigațiile privind traficul de persoane, este esențial să se definească clar rolurile și responsabilitățile celor

implicați. Deși aceasta este o practică standard în multe instituții publice și private, uneori este trecută cu vederea. Definirea clară a responsabilităților ajută la prevenirea duplicării eforturilor, sporește eficiența operațională și aduce beneficii suplimentare, cum ar fi o planificare mai fluidă a succesiunii, o triere mai eficientă a cazurilor, o mai bună prioritizare a investigațiilor și o comunicare consecventă în cadrul și în afara echipei. Documentarea rolurilor asigură desfășurarea investigațiilor mai eficientă și în timp util. În cele din urmă, această abordare urmează principiul „dezbină și cucerește" - atunci când toată lumea își înțelege rolul, se poate concentra pe execuție. Fără responsabilități clare, chiar și eforturile bine intenționate pot duce la un proces de investigație inconsistent și ineficient.

Pasul 3:O anchetă reușită necesită acces la resursele potrivite, care pot varia în funcție de natura anchetei. Anchetele financiare, în special cele axate pe spălarea banilor și traficul de persoane, necesită instrumente specializate diferite de cele utilizate în operațiunile de teren. Având în vedere complexitatea urmăririi fluxurilor financiare, anchetatorii trebuie să fie dotați cu resurse adecvate pentru a analiza eficient tranzacțiile, a conecta cazurile conexe și a se adapta la tacticile criminale în continuă evoluție.

Furnizarea instrumentelor necesare anchetatorilor sporește eficiența, îmbunătățește calitatea investigațiilor și crește probabilitatea unor arestări și condamnări reușite. Printre resursele cheie se numără:

- **Sisteme digitale de gestionare a cazurilor:**O bază de date centralizată pentru stocarea notelor de caz și a probelor permite o mai bună urmărire a cazurilor și conectarea investigațiilor
- **Acces nerestricționat la internet:**Anchetatorii pot avea nevoie de acces la site-uri restricționate, cum ar fi platformele de conținut pentru adulți, atunci când

urmăresc activitatea de trafic de persoane, cu condiția să primească instruirea adecvată pentru a preveni utilizarea abuzivă.

- **Training OSINT:**Instruirea specializată în investigațiile online ajută la descoperirea informațiilor critice și la protejarea identităților anchetatorilor.
- **Accesul la datele interne:**Disponibilitatea imediată a datelor instituționale relevante, cum ar fi înregistrările tranzacțiilor sau dosarele cazurilor anterioare, este esențială. Depășirea barierelor tehnologice, juridice și birocratice în calea accesului la date îmbunătățește eficiența investigațiilor.
- **Consultanță juridică de specialitate:**Infracțiunile financiare implică adesea impozitarea, valorile mobiliare și proprietățile imobiliare, necesitând contribuția specialiștilor. Identificarea experților juridici și financiari din timp consolidează rezultatele investigațiilor.

Deși accesul la resurse este vital, instituțiile trebuie să echilibreze eficiența cu considerațiile legale și etice, asigurându-se că anchetatorii operează în limitele reglementărilor, maximizând în același timp capacitățile lor de investigare.

Pasul 4: Una dintre principalele provocări în investigațiile financiare legate de traficul de persoane este riscul de identificare greșită a infracțiunilor - fie confundând o altă infracțiune cu traficul de persoane, fie trecând cu vederea indicatorii traficului de persoane. Acest lucru poate proveni din lipsa de cunoștințe juridice sau din caracteristicile suprapuse ale unor infracțiuni precum traficul de persoane sau încălcările legislației muncii. Încadrarea juridică a acestor infracțiuni este crucială, în special pentru anchetatorii atât din sectorul public, cât și din cel privat. Instituțiile private ar trebui, de asemenea, să definească ce infracțiuni predicat vor examina echipele lor specializate, deoarece unitățile exclusive în domeniul traficului de persoane sunt rare din cauza constrângerilor de resurse. Odată ce se stabilește o înțelegere fundamentală a legilor

legate de traficul de persoane și a responsabilităților de investigare, anchetatorii își pot rafina abordarea în gestionarea sesizărilor. Agențiile din sectorul public primesc de obicei un volum mai mare de sesizări legate de traficul de persoane datorită mandatelor lor mai largi, în timp ce echipele din sectorul privat pot avea mai puține cazuri, dar oportunități mai mari pentru investigații proactive. Strategiile proactive includ:

- **Revizuirea cazurilor închise anterior:**Cazurile mai vechi, etichetate eronat drept prostituție sau contrabandă, ar putea conține dovezi trecute cu vederea despre traficul de persoane.
- **Efectuarea căutărilor media negative din trecut:**Revizuirea știrilor despre suspecții de trafic poate dezvălui legături sau tipare financiare în conturile unei instituții.
- **Analizarea STR-urilor:**Extragerea datelor istorice STR poate ajuta la identificarea semnalelor de alarmă legate de traficul de persoane trecute cu vederea
- **Monitorizarea sectoarelor de afaceri cu risc ridicat:**Industrii precum saloanele de masaj, cluburile de striptease și pornografia au fost asociate cu traficul de persoane și merită o analiză mai atentă.

Investigațiile financiare eficiente necesită atât măsuri reactive, cât și proactive. Cu toate acestea, succesul lor depinde de calitatea informațiilor partajate — asigurându-se că rapoartele de tranzacții suspecte (STR) bine documentate ajung la autoritățile de aplicare a legii și determină acțiuni semnificative.

Pasul 5:O arie de investigație bine definită este crucială pentru a preveni ca cazurile să devină prea ample pentru a fi gestionate și pentru a evita asocierea eronată a unor persoane nevinovate cu activități infracționale. În investigațiile privind traficul de persoane, traficanții exploatează frecvent conturile bancare ale victimelor lor în scopuri

personale, ceea ce face esențial ca organizațiile să aibă politici care să prevină victimizarea ulterioară. Distincția clară între traficanți și victime este o prioritate, urmată de identificarea autorilor cheie înainte de identificarea facilitatorilor secundari. Această abordare bazată pe risc optimizează resursele și asigură eficiența investigațiilor.

Pentru a defini cu exactitate amploarea unei investigații, aceasta trebuie să fie cât mai cuprinzătoare posibil de la bun început. Modelul 360, de exemplu, dezvoltat de Peter Warrack, oferă o metodă structurată pentru evaluarea activității financiare pentru o potențială spălare de bani și poate fi aplicat atât în instituțiile financiare private, cât și în autoritățile de aplicare a legii. Modelul constă în șase etape:

1. **Eveniment declanșator**– Investigația începe cu o alertă, cum ar fi un raport de tranzacții suspecte (STR), un semnalizator automat de monitorizare a tranzacțiilor, media adversă, o sesizare internă sau o solicitare din partea organelor de drept.
2. **Înțelegeți clientul**– Anchetatorii adună informații contextuale despre subiect, inclusiv angajarea, statutul financiar și profilul general al acestora.
3. **Înțelegerea activității financiare**– Comportamentul financiar al clientului este evaluat în raport cu antecedentele sale cunoscute pentru a determina dacă acesta corespunde așteptărilor.
4. **Eliminați normalul**– Tranzacțiile care par normale pentru client sunt filtrate, permițând anchetatorilor să se concentreze asupra activităților cu adevărat suspecte.
5. **Analizați activitatea financiară rămasă**– Ancheta se concentrează asupra activității care a declanșat suspiciunea inițială, analizând tiparele și potențialele legături cu comportamente ilicite.

6. **Raportați și luați în considerare terminarea relației de afaceri**– Dacă ancheta confirmă suspiciunile, se depune un raport de tranzacții suspecte (STR) la FIU-ul local, iar în cazurile de aplicare a legii, se poate solicita un mandat de arestare.

Această abordare structurată asigură că resursele de investigație sunt concentrate pe amenințări legitime, reducând la minimum rezultatele fals pozitive și sporind eficacitatea generală.

Pasul 6:Înțelegerea a ceea ce constituie o activitate financiară suspectă în contextul traficului de persoane necesită atât cunoștințe generale despre practicile bancare, cât și o conștientizare aprofundată a metodelor traficanților. Deși cunoștințele bancare fundamentale sunt relativ ușor de dobândit, recunoașterea anomaliilor necesită adesea acces la date substanțiale și experiență practică de investigare. Cu toate acestea, având în vedere documentația extinsă disponibilă privind comportamentele financiare ale traficanților, cercetarea poate compensa lipsa experienței directe.

La nivel macro, indicatorii traficului de ființe umane pot fi clasificați în trei categorii:

1. **Indicatori comportamentali**– Acestea implică indicii vizuale în persoană care pot sugera că o persoană este prinsă în trafic sau că cineva este traficant.
2. **Indicatori de cunoaștere a clientului (KYC)**– Semnale de alarmă bazate pe informațiile furnizate de client, cum ar fi inconsecvențele în identificarea sau adresele.
3. **Indicatori tranzacționali**– Modele financiare suspecte care pot apărea oricând după deschiderea unui cont, adesea fără interacțiune față în față, în special odată cu creșterea serviciilor bancare digitale.

Acești indicatori se pot manifesta independent sau în combinație și pot fi detectați de diferite echipe din cadrul unei organizații - personalul din prima linie identifică semnele

comportamentale, echipele de colectare a datelor observă semnalele de alarmă KYC și echipele de monitorizare a tranzacțiilor recunosc anomaliile financiare. Protocoalele clare de comunicare și sesizare sunt esențiale pentru a se asigura că activitățile potențial suspecte sunt investigate temeinic. Segmentarea indicatorilor în aceste trei categorii se aliniază cu cadrele dezvoltate de Thomson Reuters și Banks Alliance în Europa, Asia și Statele Unite. Seturile lor de instrumente oferă informații suplimentare, inclusiv puterea relativă a fiecărui indicator și legătura sa cu forme specifice de trafic de persoane, cum ar fi exploatarea prin muncă.

Este important să recunoaștem că anumiți indicatori, cum ar fi achizițiile frecvente din farmacii, pot să nu fie suspecti în mod izolat. Prin urmare, analiștii trebuie să ia în considerare mai mulți factori împreună pentru a stabili motive rezonabile de suspiciune. Acest lucru este în concordanță cu îndrumările agențiilor de informații financiare, inclusiv:

- **FINTRAC** (Canada, 2016): „O singură tranzacție, considerată izolat, poate duce la o presupunere falsă de normalitate. Luarea în considerare a tuturor indicatorilor poate dezvălui legături necunoscute care, luate împreună, ar putea duce la motive întemeiate de a suspecta traficul de persoane.”
- **FinCEN**(SUA, 2014): „Niciun semnal de alarmă tranzacțional singular nu este un indicator clar al activității legate de contrabandă sau trafic de persoane. Ar trebui luați în considerare și factori suplimentari, cum ar fi activitatea financiară preconizată a unui client.”

Atât FINTRAC, cât și FinCEN subliniază importanța unei abordări structurate de investigare, cum ar fi modelul 360 al lui Warrack, pentru a asigura evaluarea semnalelor de alarmă financiare în context, mai degrabă decât izolat. Pentru o listă completă a indicatorilor sintetizați, consultați anexele din documentul OSCE - **Compendiu de**

resurse și ghid pas cu pas privind investigațiile financiare legate de traficul de ființe umane(OSCE, 2019).

Pasul 7: Rapoartele STR joacă un rol esențial în investigațiile financiare atât în sectorul public, cât și în cel privat. În mod tradițional, un STR marchează sfârșitul investigației unei instituții private, de obicei o instituție financiară precum o bancă, care apoi transmite raportul către unitatea sa de informații financiare. Din punct de vedere legal, un STR poate declanșa începerea unei investigații de aplicare a legii. Cu toate acestea, pentru a-și maximiza potențialul, STR-urile ar trebui considerate instrumente valoroase pe tot parcursul procesului de investigație, nu doar ca un pas final sau o inițiere a anchetelor publice. Acestea pot oferi informații utile în diferite etape, fie prin contribuția la investigațiile în curs, fie prin oferirea de context pentru investigațiile interne din cadrul instituțiilor private.

În sectorul privat, se recomandă utilizarea unor soluții tehnice pentru a ușura sarcina administrativă a introducerii datelor de rutină, permițând anchetatorilor să se concentreze asupra aspectelor detaliate ale activităților suspecte. În plus, datele din rapoartele STR anterioare ar trebui să fie ușor accesibile pentru a identifica tipare, a descoperi infracțiuni unice și a urmări entitățile implicate. Rapoartele STR ar trebui, de asemenea, să facă referire la rapoartele anterioare legate de aceeași rețea infracțională pentru a construi o narațiune coerentă și a evita raportările duplicate. Este important ca instituțiile raportoare să respecte convențiile de denumire stabilite de FIU-urile naționale, în special pentru infracțiuni de mare profil, cum ar fi traficul de persoane. Respectarea acestor convenții ajută la asigurarea conformității cu așteptările de reglementare, sporește credibilitatea raportării instituției și ajută la identificarea tendințelor criminalității financiare. De exemplu, FinCEN din SUA recomandă etichetarea rapoartelor STR legate de traficul de persoane drept „Consultativ privind traficul de persoane”, în timp ce FINTRAC din Canada

sugerează utilizarea etichetei „Project Protect”. Instituțiile care nu au aceste sisteme de codificare ar putea lua în considerare parteneriate public/private pentru a le implementa.

În sectorul public, se recomandă utilizarea bazelor de date STR ale unităților de informații financiare (FIU) pentru toate investigațiile privind traficul de persoane (TFU), deoarece această infracțiune implică de obicei câștiguri financiare. Autoritățile de aplicare a legii ar trebui să utilizeze, de asemenea, instrumente precum citațiile și mandatele pentru a încuraja băncile și alte entități raportoare să depună STR-uri legate de investigațiile deschise. În ciuda importanței lor, STR-urile au fost criticate pentru numărul tot mai mare de rapoarte de calitate scăzută. De exemplu, un raport OSCE din 2014 a evidențiat că, în Italia, doar 23 din 37.000 de STR-uri au fost considerate utile pentru investigațiile penale. O comisie de reformă juridică din Marea Britanie din 2019 a exprimat preocupări similare, sugerând necesitatea unor îmbunătățiri în raportarea STR-urilor pentru a reduce volumul de transmiteri de calitate slabă. Prin implementarea unora dintre recomandările menționate, cum ar fi referirea la STR-urile istorice, calitatea rapoartelor viitoare poate fi îmbunătățită.

Pasul 8: După finalizarea unei investigații într-o instituție privată, cum ar fi o bancă, trebuie luată o decizie cu privire la continuarea relației cu clientul investigat. Acest proces, cunoscut sub numele de „reducerea riscului”, implică încheierea relației, dacă este necesar. Este important să se facă distincția între victimă și agresor pentru a evita pedepsirea pe nedrept a victimei, în special în cazuri precum traficul de persoane. Dacă un cont aparține unei victime a traficului de persoane, trebuie depuse eforturi pentru a menține relația, cu excepția cazului în care există încălcări multiple sau complicități. Reducerea riscului trebuie abordată cu prudență, deoarece împingerea activităților suspecte pe piețele ilegale poate îngreuna investigațiile forțelor de ordine. În unele jurisdicții, forțele de ordine pot solicita ca conturile bancare să fie menținute deschise pentru a evita perturbarea investigațiilor. Dacă reducerea riscului devine necesară,

trebuie utilizate mesaje standard pentru a evita acuzațiile false, iar înregistrările entităților care au fost anterior reduse la risc pentru referințe viitoare.

Pasul 9: Identificarea cazurilor reale de trafic de persoane (TFU) bazate exclusiv pe tranzacții financiare este dificilă din cauza lipsei de informații contextuale. În plus, faptul că anchetatorii lucrează într-o instituție publică sau într-o organizație privată influențează probabilitatea de a găsi cazuri concludente de TFU. Organizațiile private, cum ar fi furnizorii de servicii financiare, nu sunt obligate să dovedească dincolo de orice îndoială rezonabilă că a avut loc o infracțiune predicat înainte de a depune un raport de tranzacții suspecte(STR) la o unitate de informații financiare (FIU). Pragul de raportare este adesea scăzut, deoarece instituțiile financiare pot vedea doar o parte a imaginii de ansamblu. Mai mult, FIU-urile de obicei nu oferă feedback dacă STR-urile duc la infracțiuni predicat confirmate, ceea ce face mai dificilă pentru sectorul privat validarea activităților legate de TFU.

Întrucât transparența cu privire la rezultatul investigațiilor financiare privind traficul de persoane (THB) nu este întotdeauna posibilă, cazurile dovedite ar trebui utilizate pentru a facilita instruirea și atenuarea riscurilor viitoare. Furnizorii de servicii financiare pot identifica cazurile dovedite de THB prin:

- Monitorizarea zilnică a fluxurilor de știri negative (Adverse Media) pentru identificarea unor conexiuni cu subiecții investigați intern.
- Abonarea la actualizări de la autoritățile de aplicare a legii sau de la unitățile de informații financiare privind combaterea traficului de persoane și corelarea acestora cu cazurile interne.
- Crearea unui canal direct de sesizare a autorităților de aplicare a legii în legătură cu anchetele privind traficul de persoane.

Se recomandă partajarea informațiilor provenite din cazurile dovedite de trafic de persoane cu echipa de anchetă mai largă, nu doar cu unitatea specializată în traficul de persoane. Acest lucru este în conformitate cu îndrumările din Pasul 1 (Centralizarea supravegherii) și poate stimula moralul anchetatorilor, poate crea un sentiment de scop și poate îmbunătăți șansele de alocare a resurselor sau de colaborare între echipe.

Pasul 10: În ultimii ani, importanța și prevalența parteneriatelor public-private (PPP) în combaterea infracțiunilor financiare, în special a traficului de persoane în mediul de afaceri, au crescut semnificativ. Un efort global de eliminare a traficului de persoane a dus la o mai mare colaborare între concurenții din industrie pentru a aborda infracțiunile financiare. Profesioniștii în domeniul combaterii infracțiunilor financiare și-au dat seama că traficanții se deplasează între diferite instituții și bănci, ceea ce a determinat cooperarea pentru a aborda aceste probleme. Printre principalele PPP-uri se numără Grupul de lucru comun pentru informații privind spălarea banilor (JMLIT) din Marea Britanie, Alianța Fintel din Australia și Proiectul Protect din Canada. SUA are, de asemenea, mecanisme precum Legea PATRIOT 314(a) din SUA pentru schimbul de informații.

Printre stimulentele pentru participarea la PPP-uri se numără expunerea la diverse abordări în investigațiile financiare, dezvoltarea mai rapidă a indicatorilor THB, construirea unor relații mai puternice cu colegii și cu autoritățile de aplicare a legii, investigații îmbunătățite, resurse comune și un angajament față de binele social. Cu toate acestea, OSCE recunoaște provocările în stabilirea unei cooperări eficiente între FIU-uri, autoritățile de aplicare a legii și entitățile care depun rapoarte de tranzacții suspecte (STR). O astfel de provocare este fluxul unilateral de informații din partea FIU-urilor, care adesea limitează capacitatea acestora de a partaja informații în afara organizației lor.

Feedback-ul privind rapoartele de tranzacții suspecte de înaltă calitate ar putea îmbunătăți instruirea, metodele de detectare și calitatea STR-urilor.

Lipsa feedback-ului din partea FIU-urilor și absența bazelor de date internaționale privind infractorii care practică traficul de persoane subliniază necesitatea unor parteneriate public-private (PPP). Crearea unui PPP nu necesită întotdeauna legi noi; se pot utiliza cadrele juridice existente. De exemplu, Project Protect din Canada a funcționat cu succes în cadrul juridic al guvernului național, concentrându-se pe tipologii și indicatori generali, respectând în același timp legislația privind confidențialitatea. Este esențial să se înțeleagă limitele legale și să se lucreze în cadrul acestora pentru a încuraja colaborarea. Obiectivele pe termen lung ale PPP-ului pot include susținerea modificărilor legislației pe baza colaborărilor reușite. Inițierea sau participarea la un PPP ar trebui să urmeze stabilirii unui proces de investigație solid, dar colaborarea timpurie este valoroasă. Aceasta poate oferi perspective care modelează procesul de investigație în moduri care ar fi dificil de realizat după ce procesul este deja instituit. Participarea la un PPP va spori caracterul complet al unei abordări de investigare a traficului de persoane.

Pasul 11: Investigațiile privind traficul de persoane, în special în sectorul bancar, pot avea un impact negativ asupra supraviețuitorilor. Acest lucru subliniază importanța Etapei 4 (Evaluarea investigației privind activitatea de trafic de persoane), care asigură că activitățile legate de traficul de persoane sunt clar definite la nivel de echipă sau instituțional. Executarea corectă a Etapei 4 poate ajuta la reducerea muncii inutile ulterioare, asigurându-se că persoanele nevinovate nu sunt excluse în mod eronat. Întrucât traficanții manipulează adesea situațiile financiare ale victimelor lor, se recomandă ca supraviețuitorii care au scăpat de trafic să aibă oportunități de a-și reconstrui profilurile financiare.

Un exemplu de succes de sprijinire a supraviețuitorilor traficului de persoane este un program lansat de HSBC în Regatul Unit în iunie 2019. Acest program ajută

supraviețuitorii trimiși prin Mecanismul Național de Trimitere din Regatul Unit să se confrunte cu provocări precum furnizarea dovezii adresei și a identității. În plus, Planul Inițiativei Lichtenstein pentru Mobilizarea Finanțelor Împotriva Sclaviei și Traficului de Persoane, creat în parteneriat cu Universitatea Națiunilor Unite și diverse guverne, a reunit mai multe instituții financiare pentru a extinde eforturile HSBC în diferite instituții și jurisdicții. Scotiabank, în colaborare cu programul de combatere a traficului de persoane Deborah's Gate al Armatei Salvării, a fost prima bancă care a deschis conturi pentru supraviețuitori în cadrul acestei inițiative de incluziune financiară. Se așteaptă ca și alte instituții financiare participante să urmeze exemplul și să dezvolte programe similare.

Întrucât atenția și eforturile continuă să se concentreze asupra celor care facilitează traficul de persoane, este important să nu pierdem din vedere victimele. Parteneriatele public-private și colaborarea cu grupuri interguvernamentale pot crea o abordare cuprinzătoare a combaterii traficului de persoane, în beneficiul nu numai al instituțiilor implicate, ci și al victimelor, adesea cu costuri minime de execuție.

9.5.4Identificarea activităților financiare suspecte

OSCE a publicat o listă de indicatori financiari tranzacționali și așa-numiți semnale de alarmă aplicabili traficului de persoane și, în special, exploatării prin muncă. Următoarea listă a fost preluată din raportul OSCE, iar trei indicatori aparent specifici pentru prelevarea de organe, precum și șapte pentru exploatarea sexuală, au fost eliminați pentru a o face mai potrivită pentru exploatarea prin muncă, chiar dacă, în cazuri speciale, indicatorii pot varia și se suprapune (OSCE, 2019, p. 61 și următoarele).

- Utilizarea persoanelor interpuse în relație cu contul comercial
- Neplata impozitelor, a indemnizațiilor pentru accidente de muncă și a altor taxe către o autoritate fiscală

- Rata de plată pentru fiecare perioadă de plată este identică (fără modificări pentru ore suplimentare, concediu de odihnă, concediu medical, plăți bonus etc.) în locurile de muncă în care acest lucru nu ar fi așteptat.
- Plăți recurente pentru salarii la sume nerezonabil de mici (cum ar fi mult mai mici decât salariul minim)
- Pondere semnificativă din capitalul companiei în depozite la termen – rotație financiară incomparabilă
- Împrumuturi acordate de un acționar persoanei juridice afiliate și transfer ulterior înapoi, împrumut fictiv
- Structurare prin intermediul entităților comerciale și transfer de bani folosind contract de împrumut
- Exces de ridesharing după miezul nopții
- Lipsa cheltuielilor de trai, cum ar fi mâncarea, benzina, utilitățile și chiria
- Achiziții la restaurant și room service, fără camere
- Utilizarea mai multor persoane pentru efectuarea de operațiuni bancare
- Cheltuieli mari și/sau frecvente în aeroporturi, porturi, alte noduri de transport sau în străinătate, incompatibile cu uzul personal al persoanei sau cu activitatea comercială declarată în străinătate
- Depuneri de numerar efectuate în diferite orașe din țară
- Plăți către agenții de ocupare a forței de muncă sau de recrutare a studenților care nu sunt autorizate/înregistrate sau care au încălcări ale legislației muncii
- Cheltuieli relativ mari pentru articole incompatibile cu scopul afacerii declarate

- Tranzacții care au loc în afara perioadei în care se desfășoară operațiunile comerciale cunoscute
- Transferuri transfrontaliere de fonduri incompatibile cu scopul comercial declarat al titularului de cont și/sau între tipare inexplicabile de tranzacții transfrontaliere, între rute de trafic cunoscute sau zone în care există un risc mai mare de trafic.
- Utilizarea pe scară largă a numerarului, inclusiv pentru achiziționarea activelor întreprinderilor
- Transferuri interne de la companii active în sectoare sensibile la frauda socială, banii sunt retrași în numerar imediat după aceea
- Utilizarea instituțiilor care nu aparțin sistemului financiar (netradiționale)
- Utilizarea serviciilor de curier și retrageri repetate de numerar
- Achiziționarea de ordine bancare plătibile unui cazinou imediat după depuneri
- Profituri mari inexplicabile/nejustificate pentru o companie
- Depozite în numerar adesea puțin sub pragul de raportare
- Depuneri de numerar la mai multe sucursale sau bancomate
- Achiziționarea de mandate poștale pentru plata facturilor în loc de emiterea de cecuri personale
- Conturi de afaceri cu deduceri aparente din salariile angajaților pentru diverse tipuri de costuri, cum ar fi locuința și alimentele
- Cecuri de salarizare încasate, unde majoritatea fondurilor sunt fie depuse înapoi în contul angajatorului, fie păstrate de angajator
- Remitent sau beneficiar cu informații incomplete
- Achiziționarea de ordine bancare plătibile unui cazinou imediat după depuneri

- Transferuri din diferite regiuni către aceleași persoane în țări cunoscute ca prezentând un risc mai marepentru operațiuni de trafic.
- Cecuri de asistență guvernamentală depuse în cont, chiar dacă titularul poate avea o sumă substanțială de bani
- Transferurile/transferurile electronice pot fi, de asemenea, structurate
- Amestecarea numerarului cu surse legitime de venit
- Activitate de rafinare (schimbarea bancnotelor de valoare mică în bancnote de valoare mai mare)
- Achiziții frecvente în multipli de sume mici de Bitcoin sau monede virtuale, direct de către client sau prin intermediul exchange-urilor
- Transferuri de fonduri care implică terțe părți, cu denumiri alternative furnizate între paranteze
- Contul primește plăți salariale de la agenții de personal legitime, adesea la nivel național, dar fondurile rămân apoi neatinse pentru perioade lungi de timp.
- Restaurante fast-food: achiziții frecvente de valoare mică în intervale de timp relativ scurte și inconsistente cu activitatea așteptată
- Contul pare să funcționeze ca un cont de canalizare

Următorul studiu de caz realizat de Francavilla Lyon și De Cock (2024) exemplifică modul în care modelele tranzacțiilor financiare pot servi drept indicatori ai unei potențiale exploatări prin muncă în sectorul ospitalității. Acest exemplu subliniază rolul esențial al analizei financiare în identificarea riscurilor de trafic de persoane și detectarea formelor ascunse de sclavie modernă:

Situația inițială: Un cetățean chinez de sex masculin își deschide un cont privat și declară că lucrează la restaurantul X. Analiza relației de afaceri arată că adresa acestei persoane și adresa Restaurantului X sunt identice. Unele dintre plățile salariale primite sunt retrase din nou în numerar sau transferate către terți (fără nicio legătură familială evidentă). Plățile salariale se efectuează neregulat și în sume variabile. În timpul unei conversații dintre bancă și client, acesta din urmă a declarat băncii că plățile din străinătate erau pensii alimentare pe care le-a plătit fostei sale soții și pentru copiii acestora. Conform KYC, însă, clientul nu are copii. În plus, conform contractului său de muncă, clientul are un post permanent cu un salariu fix și nu lucrează pe oră. Cheltuielile zilnice preconizate (mâncare, chirie, asigurare etc.) lipsesc.

Indicatorii în acest scenariu sunt:

- Naționalitate de risc (client)
- Sector de risc pentru exploatarea prin muncă
- Tranzacții pass-through
- Tranzacții în numerar
- Absența cheltuielilor zilnice preconizate
- Adresă privată identică cu adresa de la serviciu
- Declarații contradictorii din partea clientului

9.5.5Provocări în investigațiile financiare

O provocare semnificativă în investigațiile financiare este natura evolutivă a tehnicilor de anonimizare utilizate de infractori pentru a ascunde urmele financiare. Tehnici precum serviciile de mixing, chain-hopping și utilizarea criptomonedelor axate pe confidențialitate

reprezintă obstacole semnificative pentru anchetatori. De exemplu, serviciile de mixing, cunoscute și sub numele de tumblers, permit utilizatorilor să ascundă originea fondurilor lor prin punerea în comun și redistribuirea acestora. Chain-hopping-ul implică conversia rapidă a criptomonedelor între diferite platforme, ceea ce face mai dificilă urmărirea mișcării fondurilor. În plus, monedele de confidențialitate precum Monero și Zcash oferă funcții îmbunătățite de anonimat, complicând și mai mult eforturile de aplicare a legii.

Pentru a aborda aceste provocări, anchetatorii financiari se bazează din ce în ce mai mult pe colaborarea cu experți în criminalistică digitală. Criminalistica digitală permite anchetatorilor să extragă și să analizeze dovezi electronice, cum ar fi comunicațiile criptate, adresele IP și metadatele tranzacțiilor. Această abordare interdisciplinară este crucială în descoperirea rețelelor financiare ascunse și urmărirea fluxurilor financiare ilicite peste granițe. Având în vedere natura transnațională a infracțiunilor financiare, cooperarea dintre instituțiile financiare, organismele de reglementare și organizațiile internaționale este esențială pentru investigații financiare eficiente. „Modalitățile inovatoare de a muta bani, combinate cu o conștientizare tot mai mare în rândul profesioniștilor în domeniul criminalității financiare a faptului că traficanții trec de la o instituție la alta, de la o bancă la alta, i-au determinat să colaboreze.” (OSCE, 2019, p. 43).

9.5.6Dezvoltări și tendințe tehnologice

Dezvoltările tehnologice recente au influențat semnificativ criminalitatea financiară, conturând noi metode de activitate ilicită, oferind în același timp instrumente îmbunătățite pentru investigațiile financiare. De exemplu, creșterea numărului de criptomonede și a tehnologiei blockchain a facilitat diverse forme de criminalitate financiară, inclusiv spălarea de bani, frauda și chiar traficul de persoane. Utilizarea sporită a activelor digitale permite infractorilor să transfere fonduri peste granițe cu un anonimat sporit, ocolind

instituțiile financiare tradiționale și controalele de reglementare. Deși Bitcoin rămâne cea mai cunoscută criptomonedă, există o trecere tot mai mare către alternative mai axate pe confidențialitate, cum ar fi Monero și Zcash, care complică și mai mult eforturile de aplicare a legii.

O tendință majoră este utilizarea tehnicilor de anonimizare concepute special pentru activele digitale. Infractorii se bazează din ce în ce mai mult pe instrumente precum mixere, tumblere și portofele private pentru a ascunde urmele tranzacțiilor și a evita detectarea. Aceste metode îngreunează urmărirea fluxurilor financiare ilicite de către autorități, în special în cazurile legate de traficul de persoane, unde traficanții folosesc monede digitale pentru a colecta plăți și a spăla veniturile. Natura descentralizată și pseudonimizată a tranzacțiilor bazate pe blockchain a creat un peisaj în care criminalitatea financiară poate prospera, cu excepția cazului în care este contracarată prin tehnici avansate de investigație.

În același timp, infractorii financiari devin mai autosuficienți, renunțând la dependența de sponsori sau intermediari externi. Această tendință este evidentă în creșterea fraudelor cibernetice, a atacurilor ransomware și a escrocheriilor online, care generează fonduri pentru rețelele de crimă organizată, inclusiv cele implicate în traficul de persoane. Utilizarea tot mai mare a piețelor online frauduloase, a campaniilor de strângere de fonduri false și a platformelor de comerț electronic înșelătoare a extins și mai mult oportunitățile pentru infracțiuni financiare.

În ciuda acestor provocări, progresele tehnologice oferă și noi instrumente pentru combaterea criminalității financiare. Analiza blockchain și inteligența artificială joacă un rol crucial în investigațiile financiare, ajutând autoritățile să urmărească tranzacțiile ilicite și să identifice tipare suspecte. Sistemele de monitorizare a tranzacțiilor bazate pe inteligență artificială pot analiza cantități vaste de date în timp real, semnalând anomalii care pot indica activități legate de spălare de bani sau trafic de persoane. În plus,

instrumentele criminalistice blockchain permit anchetatorilor să urmărească mișcările criptomonedelor și să descopere conexiuni ascunse între entități criminale.

9.5.7Recomandări

Un cadru juridic robust pentru urmărirea penală a infracțiunilor financiare este necesar pentru a asigura investigații financiare eficiente. Standardele internaționale, de exemplu recomandările stabilite de Grupul de Acțiune Financiară Internațională (GAFI), oferă o bază pentru măsurile de combatere a spălării banilor și a finanțării terorismului. Aceste reglementări impun autorităților de aplicare a legii să efectueze investigații financiare, să faciliteze cooperarea transfrontalieră și să aplice procedurile de confiscare a activelor. Recomandarea 30 a GAFI, de exemplu, subliniază importanța desemnării unor autorități competente cu competența de a investiga infracțiunile de spălare a banilor și finanțare a terorismului.

Din cauza războiului din Ucraina, persoanele strămutate se confruntă cu un risc crescut de trafic de persoane. Ca răspuns la această vulnerabilitate sporită, organizații precum Organizația pentru Securitate și Cooperare în Europa (OSCE) au dezvoltat resurse specifice pentru a sprijini personalul de intervenție din prima linie. De exemplu, OSCE oferă un Compendiu de cursuri de formare antitrafic pentru personalul de intervenție din prima linie, care include formare specializată privind diverse aspecte ale eforturilor de combatere a traficului de persoane. Printre acestea, cursuri specifice se concentrează pe investigațiile financiare, dotând profesioniștii cu instrumentele necesare pentru a identifica și combate fluxurile financiare ilicite legate de traficul de persoane. Link către prezentarea generală a cursului:https://www.osce.org/cthb/562572.

9.6 Activități sugerate pentru capitol

Masă1Activitate pentru criminalistica digitală și investigații financiare

Numele activității	Activitate pentru criminalistica digitală
Tipul de activitate	Lucru în grup (de exemplu, grupuri de 3-6 persoane)
Durată	15-35 minute
Obiective de învățare	Identificarea urmelor digitale cheie și următorii pași de urmat
Materiale necesare	Exemplu de caz cu suficiente informații generale (de exemplu, versiune tipărită) • Thomas, Day și Jackson (2019) la pp. 31-38 și pp. 38-42 lahttps://airewb.org/wp-content/uploads/PUBLICATIONS/AR_EN_handbook_tools_best_practices.pdf • Crates (2022) la pp. 9-14 lahttps://www.antislaverycommissioner.co.uk/media/h4ggz4c2/iasc-construction-report-april-2022.pdf

	• Blogul Departamentului Muncii al SUA (2022) lahttps://blog.dol.gov/2022/01/11/fighting-human-trafficking-the-legacy-of-the-el-monte-sweatshop • Lam & Skivankova (2009) la p. 5 lahttps://www.antislavery.org/wp-content/uploads/2017/01/trafficking_and_compensation2009.pdf • Rețeaua germană de ONG-uri împotriva traficului de ființe umane KOK (nd) lahttps://www.kok-gegen-menschenhandel.de/menschenhandel/was-ist-menschenhandel/exemplifice(folosiți traducerea automată pentru site și selectați subsecțiunea „Trafic de persoane în scopul exploatării prin muncă”) • Capitolul 8 despre antrenament
Instrucțiuni pentru facilitator	Participanții vor fi împărțiți în grupuri mai mici. Vor primi un studiu de caz pe care îl vor citi (3-4 minute). Apoi, vor începe să discute în grupul lor și vor încerca să identifice ce dovezi digitale s-ar potrivi cel mai bine pentru o investigație criminalistică digitală de succes. În plus, vor discuta ce actori ar fi implicați și în ce moment al procesului de investigație (10-15 minute). • Ce dovezi digitale sunt relevante? Ce dovezi digitale sunt cele mai utile și de ce? • Cum pot experții criminalistici extrage și analiza aceste urme digitale?

	• Cum poate ajuta la identificarea victimelor, a traficanților și a tiparelor? • Ce tipare sau semnale de alarmă sugerează traficul de persoane? • Ce pași ar trebui să facă anchetatorii în continuare? • Cum pot fi folosite aceste dovezi pentru a sprijini victimele? Ulterior, fiecare grup își va prezenta concluziile (5-10 minute).
Debriefing	Facilitatorul moderează prezentarea după terminarea activității în grup.
Sfaturi pentru facilitator	Dacă aveți mai mult timp, puteți folosi diferite scenarii de caz, iar fiecare grup va prezenta pe scurt cazul și apoi rezultatele discuțiilor (în loc ca fiecare grup să lucreze la același caz).
Materiale informative	ede exemplu, studii de caz care ar trebui tipărite și furnizate participanților, eventual completate cu materiale cu extrase imitate din: • Conversații pe WhatsApp între victimă și traficant, cu mesaje de genul „Nu-ți face griji pentru acte, ne vom ocupa noi de tine”, „Vei primi cazare și transport gratuit” sau „Ne întâlnim la autogară. Șterge aceste mesaje”. • Anunțuri de pe platforma de recrutare • Înregistrări ale tranzacțiilor bancare

	• Metadate dintr-o fotografie trimisă victimei cu date de geolocalizare • …
Variații pentru implementare a online	Conducerea online este posibilă, creați sesiuni separate pentru sarcina de grup.
Numele activității	**Activitatea pentru investigații financiare**
Tipul de activitate	Lucru în grup (de exemplu, grupuri de 3-6 persoane)
Durată	15-35 minute
Obiective de învățare	Internalizarea etapelor pentru investigațiile financiare și reflectarea asupra potențialelor provocări care apar în domeniul traficului de persoane
Materiale necesare	de exemplu, studii de caz care ar trebui tipărite și furnizate participanților, eventual completate cu materiale cu extrase imitate din: • Înregistrări ale tranzacțiilor bancare și extrase de cont (pot fi și simple tabele cu coloanele: dată, descriere, Debit (EUR), Credit (EUR) și sold (EUR), arătând când cineva a efectuat tranzacția (+ către ce companie/persoană))

	• Înregistrări salariale • Facturi • …
Instrucțiuni pentru facilitator	Participanții vor fi împărțiți în grupuri mai mici. Vor primi un studiu de caz pe care îl vor citi (3-4 minute). Apoi, vor începe să discute în grupul lor și vor încerca să identifice pașii pentru investigațiile financiare (de exemplu, parcurgând fiecare pas învățat anterior). În plus, vor discuta ce actori ar fi implicați și în ce moment al procesului de investigație (10-15 minute). • Ce tehnici de investigație financiară ar trebui utilizate? • Cum pot colabora autoritățile de aplicare a legii cu unitățile de informații financiare în acest caz? • Ce instrumente juridice ar trebui aplicate? • Ce provocări pot fi identificate? Ulterior, fiecare grup își va prezenta concluziile.
Debriefing	Facilitatorul moderează prezentarea după terminarea activității în grup.
Sfaturi pentru facilitator	Dacă aveți mai mult timp, puteți folosi diferite scenarii de caz, iar fiecare grup va prezenta pe scurt cazul și apoi rezultatele discuțiilor (în loc ca fiecare grup să lucreze la același caz).

Materiale informative	*Un studiu de caz ar trebui tipărit și furnizat participanților* • Thomas, Day și Jackson (2019) la pp. 31-38 și pp. 38-42 lahttps://airewb.org/wp-content/uploads/PUBLICATIONS/AR_EN_handbook_tools_best_practices.pdf • Studiu de caz Top Glove (Malaysia), detalii disponibile lahttps://sevenpillarsinstitute.org/labor-exploitation-case-study-of-top-glove/#:~:text=Acest%20studiu%20de%case%20examine%20acuzațiile%20de%20exploatare%forțată,serves%20as%20the%20home%20of%20this%20multinational%20corporationȘi Malaezia: Camerele ascunse dezvăluie condiții precare de muncă și de viață la fabrica Top Glove, alimentând îngrijorările legate de munca forțată în industria mănușilor; inclusiv comentarii ale companiei - Centrul de Resurse pentru Afaceri și Drepturile Omului
Variații pentru implementare a online	Conducerea online este posibilă, creați sesiuni separate pentru sarcina de grup.

9.7 Referințe

Aronowitz, Alexis și Theuermann, Gerda și Tyurykanova, Elena. (2010). OSCE. Analiza modelului de afaceri al traficului de ființe umane pentru o mai bună prevenire a criminalității.https://www.osce.org/files/f/documents/c/f/69028.pdf

Belser, P. (2005). Munca forțată și traficul de persoane: estimarea profiturilor. Geneva: Biroul Internațional al Muncii.https://ecommons.cornell.edu/bitstream/1813/99623/1/Forced_labor_no__17_Forced_labour_and_human.pdf

Cellebrite. (15 noiembrie 2024). Cum pot forțele de ordine să schimbe situația împotriva traficului de persoane cu ajutorul dovezilor digitale.https://cellebrite.com/en/how-law-enforcement-can-schimba-the-tide-against-human-trafficking-with-digital-evidence/

Dubey, H., Bhatt, S. și Negi, L. (2023). Tehnici și tendințe în criminalistica digitală: o analiză, The International Arab Journal of Information Technology, 20(4), 644-654.

Comisia Europeană. (nd). Investigații financiare.https://home-affairs.ec.europa.eu/policies/internal-security/organised-crime-and-human-trafficking/financial-investigations_ro

Europol. (2020). Provocările combaterii traficului de persoane în era digitală.https://www.europol.europa.eu/cms/sites/default/files/documents/the_challenges_of_countering_human_trafficking_in_the_digital_era.pdf

Europol. (iulie 2024). Combaterea amenințărilor, abordarea provocărilor. Răspunsul Europol la introducerea ilegală de migranți și traficul de ființe umane în 2023 și ulterior. Centrul European pentru Introducerea Illegală de Migranți

(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. și De Cock, M. (2024). Profituri și sărăcie: Economia muncii forțate. OIM.https://www.ilo.org/sites/default/files/2024-10/Profits%20and%20poverty%20-%20The%20economics%20of%20forced%20labour_WEB_20241017.pdf

Fraser, C. (2016). O analiză a rolului emergent al rețelelor de socializare în traficul de persoane: exemple din domeniul muncii și al traficului de organe. International Journal of Development Issues, 15(2), 98-112.

Gorenc, M. (2019). Legea lui Benford ca instrument util pentru determinarea fraudei în situațiile financiare. Management, 14(1). 19-31. 10.26493/1854-4231.14.19-31.

Organizația Internațională a Muncii. (2018). Investigarea cazurilor de trafic de persoane utilizând o abordare centrată pe victimă. Organizația Internațională pentru Migrație.https://publications.iom.int/system/files/pdf/investigating_human_trafficking.pdf

Organizația Internațională a Muncii. (30 iulie 2023). Harta lipsurilor de dovezi privind traficul de persoane.https://rtaproject.org/human-trafficking-egm/#:~:text=The%20Evidence%20Gap%20Maps%20are%20a%20visual%20tool,the%20areas%20where%20doves%20is%20limited%20or%20inexistent.

Kunz, R., Baughman, M., Yarnell, R. și Williamson, C. (2018). Rețelele sociale și procesul de trafic sexual: de la conectare și recrutare, până la vânzări. Ohio: Universitatea din Toledo.https://www.utoledo.edu/hhs/htsji/pdfs/smr.pdf

Lugo-Graulich, K., Meyer, LF, Souza, K., Tapp, SN, Maryfield, B. și Bostwick, L. (2024). Îmbunătățirea identificării victimelor traficului de persoane în scop sexual: Indicatori ai traficului în anunțurile de escorte online. Journal of Human Trafficking, 1-22.

Maras, M.-H. (2014). Criminalistică informatică: Infractorii cibernetici, legi și dovezi (ediția a II-a). Jones și Bartlett.

Mattmann, C., Yan GH, Manjunatha, H., Gowda N, T., Zhou, AJ, Luo, J. și McGibbney, LJ (2016). Analiză criminalistică bazată pe metadate multimedia în datele web privind traficul de persoane. În: Murdock, V., Clarke, CLA, Kamps, J. și J. Karlgren. Căutare și explorare a informațiilor clasificate X. p. 10-13.

OSCE. (7 noiembrie 2019). Pe urmele banilor: Compendiu de resurse și ghid pas cu pas pentru investigațiile financiare legate de traficul de ființe umane. https://www.osce.org/files/f/documents/f/5/438323_0.pdf

Perez, AR și Rivas, P. (2023). Combaterea traficului de persoane în spațiul cibernetic: o metodologie bazată pe procesarea limbajului natural pentru analiza limbajului din reclamele online. arXiv preprint arXiv:2311.13118.

Pizzuro, J. (11 martie 2022). Utilizarea software-ului Magnet Forensics pentru investigațiile privind traficul de persoane. MAGNET FORENSICS.https://www.magnetforensics.com/blog/leveraging-magnet-forensics-software-for-human-trafficking-investigations/

Siavoshi, M. (25 februarie 2025). Dezlegarea misterului legii lui Benford: aplicații în detectarea fraudelor. Statology.https://www.statology.org/unraveling-the-mystery-of-benfords-law-applications-in-fraud-detection/

Thomson Reuters. (2 ianuarie 2025). Tehnologia și traficul de persoane: Ducând lupta cea bună.https://legal.thomsonreuters.com/blog/technology-and-human-trafficking/#:~:text=How%20technology%20can%20fight%20human%20traffickin g%201%20Prevention,in%20mai multe%20ways%20that%20incorporating%20digital%20technology.%20

UNODC. (2019a, mai). Tehnologie care facilitează traficul de persoane.https://www.unodc.org/e4j/en/tip-and-som/module-14/key-issues/technology-facilitating-trafficking-in-persons.html

UNODC. (2019b, martie). Modulul 6: Aspecte practice ale investigațiilor criminalității cibernetice și criminalistică digitală. Gestionarea probelor digitale.https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/handling-of-digital-evidence.html

UNODC. (2020). Raportul global privind traficul de persoane 2020.https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP_2020_15jan_web.pdf

Volodko, A., Cockbain, E. și Kleinberg, B. (2020). „Identificarea semnelor” recrutării online pentru trafic de persoane: explorarea caracteristicilor reclamelor destinate migranților aflați în căutarea unui loc de muncă. Trends in Organized Crime, 23, 7-35.

www.eradicating2project.eu

Co-funded by
the European Union