

CZU 343.98:004

DOI 10.5281/zenodo.6988448



Iurie ODAGIU,  
*dr., conf. univ.*  
*PhD,*  
*associate professor*



Andrei LUNGU,  
*doctorand*  
*PhD student*

## ASPECTE CRIMINALISTICE ALE APLICĂRII POLIGRAFULUI LA CERCETAREA INFRAȚIUNILOR INFORMATICE

*În acest articol ne propunem să facem o analiză și evaluare a unor aspecte legate de aplicarea poligrafului în activitatea poliției la cercetarea infracțiunilor informatice. Vom acorda o atenție deosebită abilităților și competențelor profesionale ale specialiștilor poligraf, pe care aceștia ar trebui să le posede în contextul aplicării poligrafului la cercetarea actelor din domeniul securității cibernetice.*

*Vom stabili circumstanțele ce urmează a fi elucidate prin aplicarea poligrafului. Vom analiza profilul psiho-criminologic al infractorilor digitali – element de importanță majoră la alcătuirea bateriei de teste pentru testarea poligraf.*

*Ne vom concentra asupra modului și metodologiei de desfășurare a examinării poligraf și vom face recomandări pentru cercetările ulterioare în domeniul aplicării poligrafului.*

*Cuvinte cheie: poligraf, detectarea minciunii, etape ale testării poligraf, aplicarea poligrafului la cercetarea infracțiunilor informatice, securitate cibernetică.*

## FORENSIC ASPECTS OF THE USE OF THE POLYGRAPH IN THE INVESTIGATION OF CYBERCRIMES

*In this article we intend to make an analysis and evaluation of some aspects related to the application of the polygraph in the activity of the police to the investigation of cybercrimes.*

*We will pay attention to the skills and competences of polygraph specialists that they should possess in the context of applying polygraph to the research of cyber security documents.*

*We will establish the circumstances to be elucidated by applying the polygraph.*

*We will analyze the psycho-criminological profile of digital criminals - an element of major importance in compiling the battery of tests for polygraph testing.*

*We will focus on the manner and methodology of conducting the polygraph examination and make recommendations for further research in the field of polygraph application.*

*Keywords: polygraph, lie detection, polygraph testing stages, polygraph application to cyber-crime investigation, cyber security.*

**Introducere.** În ultimele decenii tehnica de calcul a cunoscut o dezvoltare fulminantă și prin urmare a crescut considerabil numărul aparatelor electronice destinate prelucrării datelor și executării diferitor tipuri de operațiuni electronice.

Prima prezentare publică a rețelei ARPA a avut loc în 1972 și din acel moment a apărut conceptul creării unei rețele globale.

După o dezvoltare exponențială a sistemului, avem un număr de zeci de milioane de calculatoare conectate la rețeaua Internet, prin acesta creând un imens potențial pentru utilizatori în domeniile vieții sociale, intelectuale și culturală.

Odată cu dezvoltarea și modernizarea tehnologiilor informaționale în lume a luat naștere și amploare infraționalitatea cibernetică, care ne obligă pe noi, în calitate de garant al securității și siguranței statului și a cetățenilor să reacționăm prompt în contracararea acestora.

**Scopul studiului.** Autorii își propun să facă o examinare a doctrinei privind metodologia desfășurării testării cu aplicarea poligrafului la cercetarea infrațiilor informatice, precum și o analiză a elementelor care compun specificul personalității infractorului cibernetic.

**Metode și materiale aplicate.** În scopul realizării acestei cercetări, autorii valorifică metode de cercetare specifice teoriei și doctrinei juridice, printre care metoda logică, metoda analizei comparative, analiza sistemică, descrierea, deducția, metoda istorică. Materialele utilizate în vederea realizării studiului sunt publicațiile savanților din domeniu, precum și legislația relevantă. De asemenea, baza științifică a cercetării o constituie diverse studii cuprinse în culegeri de materiale ale conferințelor, articole științifice, comentarii aplicative etc.

**Rezultate obținute și discuții.** Este cunoscut faptul că atacurile pe domeniul informaticii sânt tot mai des întâlnite, fiind în continuă îmbunătățire și modul lor de realizare. În perspectiva următorilor ani se așteaptă o creștere a

numărului de dispozitive conectate la rețeaua Internet și suntem siguri că aceasta va contribui la o creștere a numărului de infracțiuni cibernetice. Unele studii aflate în acces liber, fac referire la date conform cărora în 2024 vor fi conectate la rețeaua globală Internet în jur de 22,3 miliarde de dispozitive.

Unul din obiectivele propuse de instituțiile de aplicare a legii ar fi de a construi un spațiu cibernetic securizat și sigur, fapt care ar spori încrederea utilizatorilor în serviciile digitale, dar la fel de important este și elaborarea unor metode și tehnici eficiente în lupta cu infraționalitatea din zona „cyber”.

În decembrie 2020, Comisia Europeană și Serviciul European de Acțiune Externă (SEAE) au prezentat o nouă strategie de securitate cibernetică a UE. Scopul acestei strategii este de a consolida reziliența Europei la amenințările cibernetice și de a asigura faptul că toți cetățenii și toate întreprinderile pot beneficia pe deplin de servicii și instrumente digitale fiabile și de încredere. Noua strategie conține propuneri concrete de punere în aplicare a unor instrumente de reglementare, de investiții și de politică.

La 22 martie 2021, Consiliul a adoptat concluzii privind Strategia de securitate cibernetică, care subliniază că securitatea cibernetică este esențială pentru construirea unei Europe reziliente, verzi și digitale [1].

Potrivit raportului privind punerea în aplicare a strategiei europene de securitate [2], au fost identificate o serie de amenințări și provocări la adresa intereselor Europei în materie de securitate, și anume:

- Proliferarea armelor de distrugere în masă;
- Terorismul și criminalitatea organizată;
- Securitatea energetică;
- Schimbările climatice;
- Securitatea cibernetică.

Economiile moderne se bazează foarte mult pe infrastructura critică, inclusiv transportul, comunicațiile și aprovizionarea cu energie, dar și pe internet. Strategia UE pentru

o societate informațională sigură, adoptată în 2006, abordează criminalitatea bazată pe internet. Cu toate acestea, atacurile împotriva sistemelor IT private sau guvernamentale din statele membre ale UE i-au conferit acestei Strategii o nouă dimensiune, aceea de posibilă armă economică, politică și militară. Sunt necesare mai multe eforturi în acest domeniu, pentru a explora abordări cuprinzătoare la nivelul UE, pentru a crește gradul de sensibilizare și a spori colaborarea internațională.

Reglementarea infracțiunilor informatice în legislația națională a venit ca o adaptare firească a legislației la realități ce nu puteau fi ignorate. Astfel, în Codul penal al Republicii Moldova, adoptat prin Legea nr. 985 din 18.04.2002, în vigoare din 12.06.2003, în premieră a fost introdus capitolul „Infracțiuni informatice și Infracțiuni în domeniul telecomunicațiilor”, care cuprindea inițial trei articole: art. 259 – Accesul ilegal la informația computerizată; art. 260 – Producerea, importul, comercializarea sau punerea ilegală la dispoziție a mijloacelor tehnice sau produselor program; art. 261 – Încălcarea regulilor de securitate a sistemului informatic.

După ratificarea Convenției Consiliului Europei privind criminalitatea informatică, adoptată la Budapesta la 23.11.2001, prin Legea nr. 6 din 02.02.2009, Codul penal al Republicii Moldova, fiind armonizat în conformitate cu prevederile Convenției prin Legea nr. 278 din 18.12.2008, ambele publicate în MO la 20.02.2009, a fost suplinit cu articole noi: 260<sup>1</sup>-260<sup>6</sup>, care prevedeau noi tipuri de infracțiuni, cum ar fi interceptarea ilegală a unei transmisii de date, perturbarea funcționării sistemului informatic, falsul informatic, fraudă informatică [3].

Criminalitatea în mediul virtual, a cunoscut o evoluție dramatică și *în opinia noastră*, a luat prin surprindere organele de aplicare a legii, care s-au dovedit a fi nepregătite pentru o combatere în forță a acestui nou fenomen, sub denumirea de „criminalitate cibernetică”.

**Considerăm că** investigarea infracțiunilor informatice și identificarea infractorului

este o problemă extrem de dificilă, presupunând abilități și competențe specifice.

Statistica pe statele CSI ne demonstrează că infracțiunile informatice se află în stare de latență, fiind dezvăluite doar 10% din acestea și cu o rată de descoperire de 1% [4].

Un număr impunător de atacuri informatice împotriva persoanelor fizice sau juridice rămân deseori nedeclarate, nedetectate sau nedescoperite, astfel făptuitorii fiind încurajați să continue activitatea infracțională, inclusiv datorită nesancționării la timp a ilegalităților săvârșite.

Pentru mulți ofițeri de urmărire penală, cercetarea infracțiunilor informatice este o sarcină foarte dificilă, datorită particularității acestui tip de infracțiuni. Iar majoritatea ofițerilor din cadrul MAI posedă cunoștințe în domeniul informaticii la nivel de „utilizator obișnuit”.

Infracțiunile informatice reprezintă un tip de activitate infracțională specifică, care poate fi realizată în mai multe etape succesive, grupările implicate fiind organizate foarte riguros și desfășurându-și activitatea prin intermediul rețelelor mondiale.

Un grad sporit de pericol este constituit prin caracterul transfrontalier al acestor infracțiuni. Asemenea lucruri impun o conlucrare cu alte organe de aplicare a legii naționale și/sau internaționale. Caracteristica și modelul criminalistic al infracțiunilor informatice constituie o categorie distinctă, iar prin cercetarea științifică a acestora se asigură un suport esențial organelor de drept în prevenirea și combaterea categoriei respective de infracțiuni.

Cercetarea criminalistică, după cum se știe, este un proces destul de complicat, care are ca scop restabilirea evenimentului infracțional produs în trecut, după probele descoperite de către ofițerul de urmărire penală. Cel mai important element, determinant, al structurii organizatorice și psihologice a activității ofițerului de urmărire penală constă în acumularea și studierea celor mai diverse elemente de fapt, circumstanțe, date în baza cărora el va restabili

complet evenimentul produs în trecut, corelațiile diferitelor persoane implicate în evenimentul respectiv, precum și personalitatea subiectului care a săvârșit infracțiunea [5].

În opinia noastră, circumstanțele care urmează a fi stabilite în cadrul cercetării infracțiunilor informatice sunt condiționate de acțiuni specifice, ce se referă la:

- natura faptei;
- locul comiterii faptei;
- timpul comiterii faptei;
- modul de operare (modalitatea comiterii faptei);
- persoana care a comis fapta (autorul faptei);
- coparticipanții la comiterea faptei;
- mobilul faptei.

Pentru o mai bună înțelegere a subiectului, **suntem de părere că** o atenție sporită trebuie acordată profilului psihologic al infractorului „cibernetici”. Infractorii informatici sunt persoane cu flexibilitate înaltă de trecere operativă de la dimensiunea reală la cea virtuală, de la o relație mediată de un spațiu emotiv-fizic la o relație mediată de un spațiu emotiv-artificial, având o percepție alterată diminuată asupra ilegalității comportamentului său, daunei provocate, riscurilor de a fi denunțat, descoperit și sancționat, cu sau fără cunoștințe tehnice în domeniul tehnologiilor informaționale. Ei sunt categorisiți în funcție de rolul și sarcinile pe care le au în procesul de comitere a infracțiunii, cu un profil predominant non-violent, având un limbaj comun cu terminologie specifică și cu motivație infracțională diversificată (materială, sexuală, ideologică, politică, obsedată de statut sau de investigație). În majoritatea covârșitoare a cazurilor ei sunt de gen masculin, cu vârste cuprinse între 16 și 55 de ani, care acționează în grup, neavând antecedente penale.

În funcție de vârstă, 33% din ei comit infracțiunea neavând 20 de ani, 13% au peste 40 de ani, iar 54% dintre infractorii cibernetici au vârste cuprinse între 20 și 40 de ani.

Mulți dintre infractorii cibernetici au

o gândire creativă, fiind foarte talentați și pricepuți. Un exemplu în acest sens este cazul în care ofițerii de urmărire penală, deplasându-se la fața locului pentru a ridica tehnica de calcul – instrument al comiterii infracțiunii informatice, au fost martorii faptului că aparatura a luat foc. S-a dovedit că, cu mult înainte de sosirea oamenilor legii, atacatorul a instalat în prag un senzor, care creează un câmp magnetic puternic ce distruge sistemul informatic în cazul oricărei încercări de a scoate echipamentul din cameră. Prin urmare, datorită priceperii și iscusinței infractorului, organele de urmărire penală au rămas fără o probă importantă.

O anumită dificultate prezintă chiar și stabilirea comiterii infracțiunii. Acest lucru se datorează faptului că acțiunile infractorului sunt mai puțin evidente, dacă e să le comparăm cu o infracțiune „clasică”. La comiterea infracțiunilor informatice, rareori există daune materiale vizibile și palpabile. De exemplu, copierea ilegală a informațiilor de pe un computer rămâne cel mai adesea nedescoperită, introducerea cu intenție a unui virus într-un computer de cele mai multe ori arată ca o greșeală a unui administrator de sistem, care nu a putut „securiza” sistemul respectiv.

Practica judiciară ne arată că deseori nu se efectuează cercetarea la fața locului, din motiv că acesta nu poate fi identificat. Este remarcat caracterul transfrontalier al comiterii infracțiunii informatice, și anume: compania atacată se află într-un stat, serverele se pot afla în altul, iar infractorul într-o țară terță.

Cu siguranță, un ofițer de urmărire penală – profesionist în domeniul ciberneticii – va administra cu succes dosare privind infracțiunile informatice. Acesta ar trebui să posede cunoștințe profunde în domeniului computerului, să fie un programator excelent sau cel puțin să înțeleagă complexitatea utilizării și capacitățile tehnologiei informatice.

Atestăm totuși un număr foarte mic de ofițeri cu un grad avansat de cunoaștere a tehnologiilor informaționale în cadrul Ministerului Afacerilor Interne.

Situația este similară la nivel mondial. Începând cu 2015, Congresul SUA a decis să înroleze în rândurile organelor de aplicare a legii câte 2000 de angajați pe an.

În 2014, Directorul FBI, James B. Comey, a declarat că este imposibil de pregătit ofițeri pentru combaterea *cybercrime*. Este necesar de angajat specialiști deja formați, cu o cunoaștere temeinică a fenomenului cibernetic. El spunea: un hacker se formează din copilărie, ocupația acestuia fiind inițial un hobby, după care la maturitate devine un stil de viață, o componentă a personalității [6].

**Pledăm** pentru dezvoltarea programelor de îmbunătățire a competențelor ofițerilor de urmărire penală în investigarea acestei categorii de infracțiuni.

Mijloacelor obișnuite de apreciere a sincerității sau nesincerității celor ce se regăsesc în cadrul procesului penal în diverse calități, mai ales a suspectului sau a inculpatului, li s-a adăugat, în ultimele decenii, un mijloc obiectiv de investigare a principalelor modificări psihofiziologice ce însoțesc emoția în situația falsificării adevărului. Este vorba despre înregistrarea pe cale obiectivă, cu ajutorul unor aparate speciale de tip poligraf, a modificărilor fiziologice ale organismului provocate de diverse stări emoționale [7].

**Testarea cu utilizarea poligrafului** este o totalitate de acțiuni netraumatizante, inofensive pentru viața și sănătatea omului, orientate spre verificarea de către poligrafolog a veridicității informațiilor comunicate de persoana testată [8].

Observăm deci, că o testare cu aplicarea poligrafului are două componente: poligraful și specialistul poligraf (poligrafolog).

În opinia noastră, *poligrafologul* este persoana care efectuează examinări psiho-fiziologice cu ajutorul tehnicii poligraf, interpretând reacțiile fiziologice umane corelate cu răspunsurile furnizate de o persoană la întrebări legate de o cauză punctuală, în scopul stabilirii comportamentului sincer sau simulat, referitor la veridicitatea unor fapte, evenimente, depozi-

ții, precum și pentru determinarea adevărului în orice situație în care se impune verificarea sincerității unei persoane [9].

**Considerăm** că poligrafologul este componenta *forte* a testării cu aplicarea poligrafului, care face valoroasă acest mijloc de investigare. Testarea cu aplicarea poligrafului a unei persoane implicate în săvârșirea infracțiunii informatice are particularitățile sale. Anume poligrafologul va trebui să dea dovadă de competență și abilități profesionale, la etapa pregătirii bateriei de teste pentru această grupă specifică de infracțiuni.

Un rol semnificativ îl joacă gradul de calificare profesională a poligrafologului, cunoașterea normelor și regulilor din domeniul securității cibernetică, cuprinse în actele normative.

Studierea și cunoașterea de către poligrafolog a materialului probator este necesară pentru o bună și eficientă pregătire a setului de întrebări ce urmează să fie utilizat. Specialistul poligrafolog va studia cu atenție detalii cu privire la făptuitor, întrucât acestea vor folosi la alegerea corectă a metodologiei testării ce urmează să fie aplicată, precum și va contura în mare parte întreg mecanismul producerii infracțiunii.

Activitatea de pregătire se va finaliza cu alcătuirea bateriei de teste, în care se va ține cont de:

- tabloul infracțional;
- detaliile care caracterizează obiectul nemijlocit al infracțiunii;
- împrejurările care în totalitatea lor reprezintă latura obiectivă a infracțiunii;
- circumstanțele de loc și de timp ale săvârșirii actului infracțional;
- personalitatea persoanei ce urmează a fi testată;
- elementele care caracterizează activitatea făptuitorului, modul de operare a acestuia;
- cercul de suspecți;
- mijloacele și procedeele aplicate la săvârșirea infracțiunii;

– instrumentarul, uneltele, utilajul folosit la săvârșirea infracțiunii;

– unitățile de transport implicate la săvârșirea infracțiunii;

– antecedentele penale pe comiterea infracțiunilor similare celor ce formează obiectul testării;

– împrejurarea care trebuie să fie cu certitudine stabilită este reprezentată prin mobilul sau scopul infracțiunii;

Fără o cunoaștere a forței motivaționale care a determinat făptuitorul să conceapă și să pună în executare rezoluția cu privire la comiterea infracțiunii informatice, este dificil de a nu se poate stabili gradul de pericol social pe care îl prezintă infractorul, fapt care poate duce la calificări greșite și încadrări juridice incorecte a faptei.

Gândite cu atenție, acțiunile ce urmează la etapa pre-test sunt în măsură să subordoneze psihicul persoanei ce urmează să fie testată și să devină un stimulent suplimentar pentru a da declarații adevărate sau de a recunoaște benevol participarea la comiterea faptei antisociale. Observăm că poligraful poate juca rolul unui instrumentar de influență psihologică asupra persoanelor implicate la comiterea infracțiunilor.

La etapa pre-test este extrem de important să stabilim gradul de percepție a vinovăției persoanei testate în contextul infracțiunilor informatice. Există situații când infractorul nu este conștient de urmările periculoase ale acțiunilor sale. Organismul celui ce urmează a fi testat va reacționa instinctiv la situații periculoase și, prin urmare, reacțiile psihofiziologice la întrebările relevante, însoțite de stresul emoțional, vor fi mai pronunțate și informative.

La etapa acumulării probelor vinovăției,

o atenție deosebită trebuie acordată metodei CIT (Concealed Information Test) – testul ce prezumă vinovăția.

Particularitățile metodologice ale testului CIT constau în utilizarea unor informații specifice, circumstanțe referitoare la o infracțiune, pentru a identifica dacă o persoană posedă cunoștințe despre ele. Întrebările se referă la detaliile cunoscute doar de autorul faptei. În acest context, doar persoana vinovată va reacționa puternic la întrebările relevante din cadrul testării.

Este important ca specialistul poligrafolog în procesul formării bateriei de teste să identifice obiecte/elemente, care sunt semnificative și memorabile pentru infractor, dar necunoscute persoanei nevinovate.

Recomandăm ca testarea cu aplicarea poligrafului să se finalizeze cu testul american după metoda SKY.

SKY provine de la abrevierea cuvintelor: **S**uspicion, **K**nowledge, **Y**ou did.

Spre exemplu,

**Suspicion:** *Considerați că baza de date a băncii CEC Bank a fost spartă de către cetățeanul Y?*

**Knowledge:** *Sunteți sigur că cunoașteți cine a spart baza de date a băncii CEC Bank?*

**You did:** *Dvs. ați spart baza de date a băncii CEC Bank?*

**Generalizând** cele menționate supra, susținem că fenomenul criminalității informatice este unul aflat în permanentă dezvoltare și perfecționare, se diversifică ca urmare a dezvoltării continue a tehnicii și tehnologiilor, permițând infractorilor o anumită performanță în acest sens și creând noi oportunități de săvârșire a infracțiunilor informatice.

**Referințe bibliografice:**

1. <https://www.consilium.europa.eu/ro/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy/> (vizitat la 04.07.2022).
2. <https://www.consilium.europa.eu/media/30815/qc7809568roc.pdf>.
3. Codul penal al Republicii Moldova, nr. 985-XV din 18.04.2002. În: Monitorul Oficial al Republicii Moldova nr.128-129/1012 din 13.09.2002. Republicat în: Monitorul Oficial al Republicii Moldova nr.72-74/195 din 14.04.2009.
4. Кимпаев К.М. Проблемы проведения следственных действий при расследовании «киберпреступлений». Материалы Международного молодежного научного форума «Ломоносов-2017», ISBN 978-5-317-05504-2.
5. Gheorghită M. „Tratat de metodică criminalistică”. Chișinău: 2015.
6. <https://www.crime-research.org/articles/4002/> (vizitat la 05.07.2022).
7. RUIU Marin, „Criminalistică”. București: Editura Universul Juridic, 2013, p. 170
8. Legea Republicii Moldova Nr. 269 cu privire la aplicarea testării la detectorul comportamentului simulat (poligraf), adoptată de Parlamentul Republicii Moldova la 12-12-2008. În: Monitorul Oficial al Republicii Moldova, 2008.
9. ODAGIU Iurie, LUNGU Andrei. „Competențe și abilități profesionale a specialistului poligrafolog”. Conferința științifică națională interuniversitară a studenților-doctoranzi cu genericul „Prevenirea și combaterea criminalității – probleme, soluții și perspective”, ediția a IV-a, 27 ianuarie 2022, Academia „Ștefan cel Mare” a MAI. Chișinău.

**DESPRE AUTORI****Iurie ODAGIU,**

*doctor în drept, conferențiar universitar,  
prim-prorector pentru studii  
și managementul calității al Academiei  
„Ștefan cel Mare” a MAI,  
e-mail: criminalistic@gmail.com*

**Andrei LUNGU,**

*doctorand,  
Școala doctorală „Științe penale și drept public”  
a Academiei „Ștefan cel Mare” a MAI,  
e-mail: andrei.lungu@mai.gov.md*