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 INFRACȚIUNILOR 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 cybercrime investigation, cyber security.

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

Prima prezentare publică a reţelei ARPA a avut loc în 1972 şi din acel moment a apărut conceptul creării unei reţele globale.

După o dezvoltare exponenţială a sistemului, avem un număr de zeci de milioane de calculatoare conectate la reţeaua Internet, prin acesta creând un imens potenţial pentru utilizatori în domeniile vieţii sociale, intelectuale şi culturală.

Odată cu dezvoltarea şi modernizarea tehnologiilor informaţionale în lume a luat naştere şi amploare infracţionalitatea cibernetică, care ne obligă pe noi, în calitate de garant al *securităţii şi siguranţei statului şi a cetăţenilor să reacţionăm prompt în contracararea acestora.*

Scopul studiului. Autorii îşi propun să facă o examinare a doctrinei privind metodologia desfăşurării testării cu aplicarea poligrafului la cercetarea infracţiunilor informatice, precum şi o analiză a elementelor care compun specificul personalităţii infractorului cibernetic.

Metode şi materiale aplicate. În scopul realizării acestei cercetări, autorii valorifică metode de cercetare specifice teoriei şi doctrinei juridice, printre care metoda logică, metoda analizei comparative, analiza sistemică, descrierea, deducţia, metoda istorică. Materialele utilizate în vederea realizării studiului sunt publicaţiile savanţilor din domeniu, precum şi legislaţia relevantă. De asemenea, baza ştiinţifică a cercetării o constituie diverse studii cuprinse în culegeri de materiale ale conferinţelor, articole ştiinţifice, comentarii aplicative etc.

Rezultate obţinute şi discuţii. Este cunoscut faptul că atacurile pe domeniul informaticii sânt tot mai des întâlnite, fiind în continuă îmbunătăţire şi modul lor de realizare. În perspectiva următorilor ani se aşteptă o creştere a numărului de dispozitive conectate la reţeaua Internet şi suntem siguri că aceasta va contribui la o creştere a numărului de infracţiuni cibernetice. Unele studii aflate în acces liber, fac referire la date conform cărora în 2024 vor fi conectate la reţeaua globală Internet în jur de 22,3 miliarde de dispozitive.

Unul din obiectivele propuse de instituţiile de aplicare a legii ar fi de a construi un spaţiu cibernetic securizat ţi sigur, fapt care ar spori încrederea utilizatorilor în serviciile digitale, dar la fel de important este şi elaborarea unor metode şi tehnici eficiente în lupta cu infracţionalitatea din zona „cyber".

În decembrie 2020, Comisia Europeană şi Serviciul European de Acţiune Externă (SEAE) au prezentat o nouă strategie de securitate cibernetică a UE. Scopul acestei strategii este de a consolida reziliența Europei *la ameninţările cibernetice şi de a asigura faptul că toţi cetăţenii şi toate întreprinderile pot beneficia pe deplin de servicii şi instrumente digitale fiabile şi de încredere. Noua strategie conţine propuneri concrete de punere în aplicare a unor instrumente de reglementare, de investiţii şi de politică.*

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

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

– Proliferarea armelor de distrugere în masă;

– Terorismul şi criminalitatea organizată;

– Securitatea energetică;

– Schimbările climatice;

– Securitatea cibernetică.

Economiile moderne se bazează foarte mult pe infrastructura critică, inclusiv transportul, comunicaţiile şi aprovizionarea cu energie, dar şi 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: 260^1-260^6, care prevedeau noi tipuri de infracțiuni, cum ar fi interceptarea ilegală a unei transmisii de date, perturbarea funcționării sistemului informatic, falsul informatic, frauda 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, corelaţiile diferitelor persoane implicate în evenimentul respectiv, precum şi personalitatea subiectului care a săvârşit infracţiunea [5].

În opinia noastră, circumstanţele care urmează a fi stabilite în cadrul cercetării infracţiunilor informatice sunt condiţionate de acţiuni 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);
– coparticipanţii la comiterea faptei;
– mobilul faptei.

Pentru o mai bună înţelegere a subiectului, **suntem de părere că** o atenţie sporită trebuie acordată profilului psihologic al infractorului „cibernetic". Infractorii informatici sunt persoane cu flexibilitate înaltă de trecere operativă de la dimensiunea reală la cea virtuală, de la o relaţie mediată de un spaţiu emotiv-fizic la o relaţie mediată de un spaţiu emotiv-artificial, având o percepţie alterată diminuată asupra ilegalităţii comportamentului său, daunei provocate, riscurilor de a fi denunţat, descoperit şi sancţionat, cu sau fără cunoştinţe tehnice în domeniul tehnologiilor informaţionale. Ei sunt categorisiţi în funcţie de rolul şi sarcinile pe care le au în procesul de comitere a infracţiunii, cu un profil predominant non-violent, având un limbaj comun cu terminologie specifică şi cu motivaţie infracţională diversificată (materială, sexuală, ideologică, politică, obsedată de statut sau de investigaţie). În majoritatea covârşitoare a cazurilor ei sunt de gen masculin, cu vârste cuprinse între 16 şi 55 de ani, care acţionează în grup, neavând antecedente penale.

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

Mulţi dintre infractorii cibernetici au o gândire creativă, fiind foarte talentaţi şi pricepuţi. Un exemplu în acest sens este cazul în care ofiţerii de urmărire penală, deplasându-se la faţa locului pentru a ridica tehnica de calcul – instrument al comiterii infracţiunii informatice, au fost martorii faptului că aparatajul 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 şi iscusinţei infractorului, organele de urmărire penală au rămas fără o probă importantă.

O anumită dificultate prezintă chiar şi stabilirea comiterii infracţiunii. Acest lucru se datorează faptului că acţiunile infractorului sunt mai puţin evidente, dacă e să le comparăm cu o infracţiune „clasică". La comiterea infracţiunilor informatice, rareori există daune materiale vizibile şi palpabile. De exemplu, copierea ilegală a informaţiilor de pe un computer rămâne cel mai adesea nedescoperită, introducerea cu intenţie a unui virus într-un computer de cele mai multe ori arată ca o greşeală a unui administrator de sistem, care nu a putut „securiza" sistemul respectiv.

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

Cu siguranţă, un ofiţer de urmărire penală – profesionist în domeniul cibernetici – va administra cu succes dosare privind infracţiunile informatice. Acesta ar trebui să posede cunoştinţe profunde în domeniului computerului, să fie un programator excelent sau cel puţin să înţeleagă complexitatea utilizării şi capacităţile tehnologiei informatice.

Atestăm totuşi un număr foarte mic de ofiţeri cu un grad avansat de cunoaştere a tehnologiilor informaţionale în cadrul Ministerului Afacerilor Interne.

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

În 2014, Directorul FBI, James B. Comey, a declarat că este imposibil de pregătit ofiţeri pentru combaterea *cybercrime.* Este necesar de angajat specialişti deja formaţi, cu o cunoaştere temeinică a fenomenului cibernetic. El spunea: un hacker se formează din copilărie, ocupaţia acestuia fiind iniţial un hobby, după care la maturitate devine un stil de viaţă, o componentă a personalităţii [6].

Pledăm pentru dezvoltarea programelor de îmbunătăţire a competenţelor ofiţerilor de urmărire penală în investigarea acestei categorii de infracţiuni.

Mijloacelor obişnuite de apreciere a sincerităţii sau nesincerităţii celor ce se regăsesc în cadrul procesului penal în diverse calităţi, mai ales a suspectului sau a inculpatului, li s-a adăugat, în ultimele decenii, un mijloc obiectiv de investigare a principalelor modificări psihofiziologice ce însoţesc emoţia în situaţia 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 emoţionale [7].

Testarea cu utilizarea poligrafului este o totalitate de acţiuni netraumatizante, inofensive pentru viaţa şi sănătatea omului, orientate spre verificarea de către poligrafolog a veridicităţii informaţiilor comunicate de persoana testată [8].

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

În opinia noastră, *poligrafologul* este persoana care efectuează examinări psiho-fiziologice cu ajutorul tehnicii poligraf, interpretând reacţiile 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, depoziţii, precum şi pentru determinarea adevărului în orice situaţie în care se impune verificarea sincerităţii 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 săvârşirea infracţiunii informatice are particularităţile sale. Anume poligrafologul va trebui să dea dovadă de competenţă şi abilităţi profesionale, la etapa pregătirii bateriei de teste pentru această grupă specifică de infracţiuni.

Un rol semnificativ îl joacă gradul de calificare profesională a poligrafologului, cunoaşterea normelor şi regulilor din domeniul securităţii cibernetice, cuprinse în actele normative.

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

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

– tabloul infracţional;

– detaliile care caracterizează obiectul nemijlocit al infracţiunii;

– împrejurările care în totalitatea lor reprezintă latura obiectivă a infracţiunii;

– circumstanţele de loc şi de timp ale săvârşirii actului infracţional;

– personalitatea persoanei ce urmează a fi testată;

– elementele care caracterizează activitatea făptuitorului, modul de operare a acestuia;

– cercul de suspecţi;

– mijloacele şi procedeele aplicate la săvârşirea infracţiunii;

– instrumentarul, uneltele, utilajul folosit la săvârşirea infracţiunii;

– unităţile de transport implicate la săvârşirea infracţiunii;

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

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

Fără o cunoaştere a forţei motivaţionale care a determinat făptuitorul să conceapă şi să pună în executare rezoluţia cu privire la comiterea infracţiunii informatice, este dificil de a nu se poate stabili gradul de pericol social pe care îl prezintă infractorul, fapt care poate duce la calificări greşite şi încadrări juridice incorecte a faptei.

Gândite cu atenţie, acţiunile ce urmează la etapa pre-test sunt în măsură să subordoneze psihicul persoanei ce urmează să fie testată şi să devină un stimulent suplimentar pentru a da declaraţii adevărate sau de a recunoaşte benevol participarea la comiterea faptei antisociale. Observăm că poligraful poate juca rolul unui instrumentar de influenţă psihologică asupra persoanelor implicate la comiterea infracţiunilor.

La etapa pre-test este extrem de important să stabilim gradul de percepţie a vinovăţiei persoanei testate în contextul infracţiunilor informatice. Există situaţii când infractorul nu este conştient de urmările periculoase ale acţiunilor sale. Organismul celui ce urmează a fi testat va reacţiona instinctiv la situaţii periculoase şi, prin urmare, reacţiile psihofiziologice la întrebările relevante, însoţite de stresul emoţional, vor fi mai pronunţate şi informative.

La etapa acumulării probelor vinovăţiei, o atenţie deosebită trebuie acordată metodei CIT (Concealed Information Test) – testul ce prezumă vinovăţia.

Particularităţile metodologice ale testului CIT constau în utilizarea unor informaţii specifice, circumstanţe referitoare la o infracţiune, pentru a identifica dacă o persoană posedă cunoştinţe despre ele. Întrebările se referă la detaliile cunoscute doar de autorul faptei. În acest context, doar persoana vinovată va reacţiona 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 şi 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: *Consideraţi că baza de date a băncii CEC Bank a fost spartă de către cetăţeanul Y?*

Knowledge: *Sunteţi sigur că cunoaşteţi cine a spart baza de date a băncii CEC Bank?*

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

Generalizând cele menţionate supra, susţinem că fenomenul criminalităţii informatice este unul aflat în permanentă dezvoltare şi perfecţionare, se diversifică ca urmare a dezvoltării continui a tehnicii şi tehnologiilor, permiţând infractorilor o anumită performanţă în acest sens şi creând noi oportunităţi de săvârşire a infracţiunilor informatice.

Referinţe 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 проведений следственных действий при расследовании «киберпреступлений»*. Материалы Международного молодежного научного форума «Ломоносов-2017», ISBN 978-5-317-05504-2.
5. Gheorghiță M. „Tratat de metodică criminalistică". Chișinău: 2015.
6. https://www.crime-research.org/articles/4002/ (vizitat la 05.07.2022).
7. RUIU Marin, „Criminalistică". Bucureşti: Editura Universul Juridic, 2013, p. 170
8. Legea Republicii Moldova Nr. 269 cu privirea 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. „Competenţe şi abilităţi profesionale a specialistului poligrafolog". Conferinţa ştiinţifică naţională interuniversitară a studenţilor-doctoranzi cu genericul „Prevenirea şi combaterea criminalităţii – probleme, soluţii şi perspective", ediţia a IV-a, 27 ianuarie 2022, Academia „*Ştefan cel Mare*" a MAI. Chişinău.

DESPRE AUTORI

Iurie ODAGIU,
doctor în drept, conferenţiar universitar,
prim-prorector pentru studii
şi managementul calităţii al Academiei
„Ştefan cel Mare" a MAI,
e-mail: criminalistic@gmail.com

Andrei LUNGU,
doctorand,
Şcoala doctorală „Ştiinţe penale şi drept public"
a Academiei „Ştefan cel Mare" a MAI,
e-mail: andrei.lungu@mai.gov.md