ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA” DIN IAŞI
TOMUL LXV/SUPLIMENT, ŞTIINŢE JURIDICE, 2019

Criminalistica predictivă – un reper important în evoluţia criminalisticii

Predictive Forensics: a Milestone for the Development of Forensic Sciences

Ancuţa Elena Franţ[1]

Rezumat:
Lucrarea de faţă analizează un aspect mai puţin studiat în literatura de specialitate, şi anume potenţialul Criminalisticii de a contribui la prevenirea săvârşirii infracţiunilor. Concret, sunt explorate modalităţile prin care informaţiile din sfera Criminalisticii pot fi folosite pentru a preveni săvârşirea de fapte antisociale, atât în mod fizic, cât şi în mediul virtual. Modalităţile analizate de prezenta lucrare au în vedere rezultatele preventive care pot fi obţinute prin integrarea datelor furnizate de Criminalistică în programe informatice. În ceea ce priveşte prevenirea în mod fizic a săvârşirii de infracţiuni, asemenea softuri pot indica locurile în care există un risc crescut de a se comite fapte antisociale. În ceea ce priveşte săvârşirea infracţiunilor în spaţiul virtual, astfel de softuri pot să prevină accesul programelor rău-intenţionate în diverse site-uri şi, în consecinţă, pot preveni săvârşirea unor fraude financiare sau a altor tipuri de fapte antisociale. Rezultatele bune obţinute până acum în prevenirea infracţiunilor prin colaborarea dintre Criminalistică şi Informatică încurajează dezvoltarea în continuare a acestei colaborări.

Cuvinte-cheie: Criminalistică; Criminalistică predictivă; Informatică; CAPTCHA.

Abstract:
The present paper analyses a less studied aspect in the specialised literature, namely the potential of Forensic Science to add a contribution to crime prevention. The study explores the ways in which information provided by Forensic Science can be used, in order to prevent the occurence of crimes, both in the physical and virtual environment. Specifically, the study takes into account the results that can be achieved by integrating the data provided by Forensics into computer programs. As regards the crimes committed in a physical form, such software may indicate the locations where there is an increased risk for committing antisocial acts. As regards the crimes committed in the virtual environment, such software can prevent malicious programs from accessing various sites and, as a result, prevent financial fraud or other crimes. So far, the cooperation between Forensic Science and Computer Science has lead to good results, which stimulates further development of this cooperation.

[1] Lector univ. dr., Universitatea „Alexandru Ioan Cuza” din Iaşi, Facultatea de Drept, email: ancuta.frant@uaic.ro.

Keywords: Forensic Science; Predictive Forensics; Computer Science; CAPTCHA.

1. Introducere. Rolul preventiv al Criminalisticii predictive

Aşa cum arată majoritatea lucrărilor de specialitate, una dintre părţile componente ale Criminalisticii este cea preventivă[2]. Deşi este recunoscută, această latură preventivă este mai puţin analizată decât alte componente ale Criminalisticii. În ceea ce ne priveşte, aşa cum am afirmat şi cu alte ocazii[3], apreciem că prevenirea săvârşirii de fapte antisociale trebuie să fie o preocupare constantă a tuturor ramurilor de drept. În consecinţă, credem că se impune o cercetare permanentă a efectului preventiv pe care Criminalistica îl poate avea.

Prezenta lucrare analizează valenţele preventive ale unui domeniu relativ nou al Criminalisticii, numit *Criminalistică predictivă*. În esenţă, acest domeniu utilizează informaţiile descoperite în urma investigării unor fapte antisociale, pentru a şti care este contextul care permite săvârşirea unor astfel de fapte. Ştiind care sunt factorii care favorizează comiterea faptelor antisociale, pot fi luate măsuri pentru a contracara asemenea factori, înainte ca aceştia să ducă la săvârşirea concretă a unor infracţiuni.

În lucrarea de faţă vom analiza două ipostaze ale Criminalisticii predictive: una care are în vedere faptele antisociale săvârşite în mod fizic şi alta care are în vedere faptele antisociale săvârşite în mediul virtual.

2. Criminalistica predictivă aplicată cu privire la faptele antisociale săvârşite în mod fizic

La modul ideal, dacă ar putea fi supravegheate toate persoanele despre care se poate presupune că prezintă riscul de a săvârşi infracţiuni, s-ar reduce considerabil numărul infracţiunilor săvârşite. Totuşi, o asemenea activitate este foarte greu de realizat. În primul rând, nu există suficiente resurse (umane şi tehnice) pentru a asigura supravegherea tuturor persoanelor care prezintă un asemenea risc. În al doilea rând, din punct de vedere statistic, pentru o parte dintre aceste persoane, supravegherea s-ar dovedi a fi inutilă, deoarece unele persoane, în cele din urmă, nu se vor implica în acţiuni antisociale, chiar dacă erau considerate de risc. În al treilea rând, ar rămâne multe persoane nesupravegheate,

---

[2] A se vedea A. Ciopraga, I. Iacobuță, *Criminalistică*, Editura Junimea, Iași, 2001, p. 9; F. Ionescu, *Criminalistica*, Editura Universitară, București, 2008, pp. 25-26; E. Stancu, *Tratat de Criminalistică*, ediția a VI-a, revăzută, Editura Universul Juridic, București, 2015, p. 29.

[3] A se vedea A.E. Franț, *Interacțiunea dintre Bioetică și Dreptul penal. Conștientizare și justificare* (*The Interaction between Bioethics and Criminal Law: Becoming Aware of the Issue*), în volumul Conferinței Internaționale Uniformization of the Law – Legal Effects and Social, Political, Administrative Implications, Iași, 23-25 octombrie 2014 / Universitatea Titu Maiorescu, Editura Hamangiu, București, 2014, pp. 654-661; A.E. Franț, *Delimitări conceptuale privind rolul educației în prevenirea săvârșirii infracțiunilor* (*Conceptual delimitations regarding the role of education in preventing crime*), în Acta Universitatis George Bacovia. Juridica, Vol. 6, nr. 1/2017, pp. 147-168.

deoarece este foarte greu de stabilit toate categoriile care pot fi considerate de risc (de exemplu, sunt persoane care săvârşesc fapte antisociale fără a se încadra în tiparele clasice ale potenţialilor infractori). În al patrulea rând, ar putea fi create disensiuni legate de potenţiala discriminare a unor categorii sociale sau etnice (care ar putea fi considerate ca având o predispoziţie spre săvârşirea de infracţiuni). În acest context, se pune problema dacă poate fi găsită o modalitate de a preveni săvârşirea de fapte antisociale pornind de la alte elemente decât *persoana* celui care ar putea deveni infractor.

O modalitate de a preveni pe baze obiective săvârşirea infracţiunilor a fost dezvoltată pornindu-se de la observarea faptului că există anumite *locuri* în care se săvârşesc mai des infracţiuni, deci locuri în care există un risc mai mare de a se săvârşi fapte antisociale. Un asemenea criteriu are potenţial preventiv ridicat, deoarece permite concentrarea forţelor de ordine în locurile evidenţiate ca fiind de risc. Un demers de acest gen este mult mai uşor de realizat decât supra-vegherea individuală a potenţialilor infractori.

Elementele prezentate mai sus au fost integrate în programe computerizate, numite generic *Geospatial predictive modeling*[4]. Acest tip de programe evidenţiază locurile în care există un risc de săvârşire a infracţiunilor, pornind de la analiza zonelor în care s-au săvârşit anterior fapte antisociale într-un anumit spaţiu (de exemplu, într-un cartier, într-un oraş sau în altă zonă administrativ-teritorială). Pe baza istoricului infracţiunilor dintr-o anumită zonă, aceste programe au arătat că, de regulă, infracţiunile nu se săvârşesc pur şi simplu la întâmplare, ci depind de anumiţi factori (infrastructură, mediu socio-cultural, mediu topografic etc.)[5].

Stabilirea în mod computerizat a zonelor de risc se poate face prin două metode: deductivă şi inductivă.

Metoda deductivă presupune o generalizare mai mare[6], ceea ce duce doar la evidenţierea zonelor cu risc ridicat (aceasta fiind o limitare a acestei metode).

Metoda inductivă[7] presupune stabilirea empirică a relaţiei dintre faptele săvârşite şi factorii de mediu. În acest mod, soft-urile pot evidenţia corelaţiile cunoscute, dar şi cele necunoscute dintre diferiţi factori de mediu şi faptele

---

4 În limba română, „Modele predictive geospaţiale”.

5 Y. Xue, D. E. Brown, *Spatial Analysis with Preference Specification of Latent Decision Makes for Criminal Event Prediction*, în Decision Support Systems, Vol. 41, nr. 3, 2006, pp. 560-573, [Online] la https://doi.org/10.1016/j.dss.2004.06.007, accesat la data de 10.01.2020; D. Brown, J. Dalton, H. Hoyle, *Spatial Forecast Methods for Terrorist Events in Urban Environments*, în H. Chen, R. Moore, D.D. Zeng, J. Leavitt (editori), Intelligence and Security Informatics, ISI 2004, Vol. 3073, Springer, Berlin, Heidelberg, pp. 426-435, [Online] la https://doi.org/10.1007/978-3-540-25952-7_33, accesat la data de 11.01.2020.

6 A se vedea S. Greco, L. Pontieri, E. Masciari, *Combining Inductive and Deductive Tools for Data Analysis*, Ai Communications, Vol. 14 (2), 2001, pp. 69-82; L.K. Soiferman, *Compare and Contrast Inductive and Deductive Research Approaches*, ERIC Number: ED542066, 2010, [Online] la https://eric.ed.gov/?id=ED542066, accesat la data de 11.01.2020.

7 A se vedea S. Greco *et al.*, *op. cit.*; L.K. Soiferman, *op. cit.*

antisociale. Astfel, se obţin valori cantitative, care sunt ulterior procesate de programe statistice, evidenţiindu-se atât zonele cu risc crescut, cât şi zonele cu risc scăzut de săvârşire a infracţiunilor. Altfel spus, un anumit spaţiu poate fi împărţit în zone cu diferite grade de risc. În acest mod, metoda inductivă duce la o aproximare mai precisă a riscului, deci la o distribuire eficientă a factorilor de prevenire a săvârşirii infracţiunilor (cum ar fi forţele de ordine publică).

O aplicare concretă a unui asemenea program computerizat de prevenire a infracţiunilor s-a realizat în anul 2005 în oraşul Memphis din Statele Unite ale Americii. Programul, numit Blue CRUSH (CRUSH fiind acronimul de la Criminal Reduction Utilising Statistical History[8]) a fost dezvoltat de Departamentul de Poliţie din Memphis, Universitatea din Memphis (Departamentul de Criminologie şi Cercetare) şi IBM. Programul Blue CRUSH nu s-a limitat doar la utilizarea informaţiilor referitoare la locul de săvârşire a infracţiunilor, ci a avut în vedere şi alte elemente, precum profilul infractorilor sau vremea. Datele oficiale arată că, în urma utilizării acestui program de către poliţia din Memphis, numărul infracţiunilor a scăzut cu 31%, iar numărul infracţiunilor săvârşite cu violenţă a scăzut cu 15%. În plus, s-a constatat că aplicarea programului Blue CRUSH a dus la îmbunătăţirea stării morale generale a membrilor forţelor de ordine, datorită sentimentului că activitatea lor reduce numărul infracţiunilor[9].

O variantă modificată a programului Blue CRUSH, numită CRASH (acronimul de la Crash Reduction Analysing Statistical History[10]), a fost dezvoltată şi utilizată în Tennessee, pentru prevenirea accidentelor rutiere[11].

Am prezentat mai sus faptul că programul Blue CRUSH ia în considerare nu doar factori care ţin de locul săvârşirii infracţiunii, ci şi factori care ţin de persoana despre care se presupune că prezintă un anumit risc de a săvârşi o infracţiune. Aşa cum am arătat însă în prima parte a acestei secţiuni, se doreşte, pe cât posibil, o reducere a implicării factorului uman în generarea modelelor geospaţiale statistice de risc în săvârşirea infracţiunilor. Totuşi, se pare că introducerea elementelor referitoare la potenţialul anumitor persoane de a săvârşi infracţiuni, alături de elementele referitoare strict la factorii de mediu, oferă un plus de precizie în generarea modelelor de risc referitoare la săvârşirea de fapte antisociale.

---

8 În limba română, Reducerea criminalității prin analiza istoricului statistic.

9 L.P. Walter, B. McInnis, C.C. Price, S.C. Smith, J.S. Hollywood, *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*, RAND Corporation, 2013, pp. 67-69; J. Ericson, *A Cop When You Need One*, Information Management, iulie 2010, [Online] la https://www.information-management.com/news/a-cop-when-you-need-one, accesat la data de 11.01.2020.

10 În limba română, Reducerea accidentelor prin analiza istoricului statistic.

11 D. Crawford, *CRASH Predicts „Unpredictable" in Traffic Incidents,* ITS International, septembrie-octombrie 2015, [Online] la https://www.itsinternational.com/categories/gis-mapping/features/crash-predicts-unpredictable-in-traffic-incidents/, accesat la data de 11.01.2020.

De altfel, au fost elaborate programe predictive computerizate menite să estimeze potenţialul infracţional al persoanelor condamnate (asemenea programe fiind lipsite, aşadar, de caracterul obiectiv al programelor care au la bază evidenţierea zonelor de risc). Ministerul de Justiţie din Statele Unite ale Americii foloseşte un astfel de program pentru a prefigura care dintre persoanele condamnate prezintă riscul de a săvârşi din nou infracţiuni, pe baza unor criterii precum: existenţa unei locuinţe; nivelul de educaţie; starea financiară; cercul de prieteni; stilul de viaţă; consumul de alcool sau droguri; starea emoţională; atitudinea faţă de forţele de ordine etc. Tot în Statele Unite ale Americii, în Florida, Departamentul de Justiţie utilizează un program similar pentru a evidenţia care dintre tinerii care au săvârşit fapte antisociale prezintă riscul de a săvârşi din nou asemenea fapte; pe baza rezultatelor furnizate de acest program, tinerii care prezintă riscul de a săvârşi din nou astfel de fapte sunt supuşi unui program special de supraveghere şi educare[12].

Aşa cum am prefigurat deja, programele computerizate care evidenţiază riscul săvârşirii de infracţiuni prin analiza elementelor referitoare la persoane (deci nu cele care se referă strict la factorii de mediu) au atras o serie de critici. Principalul motiv de critică are în vedere respectarea drepturilor fundamentale ale omului, despre care se crede că sunt periclitate, din moment ce unei persoane i se poate ataşa stigmatul de „presupus vinovat”[13].

În ceea ce ne priveşte, apreciem că, atât timp cât se doreşte o prevenire reală a săvârşirii infracţiunilor, uneori nu se pot ignora elementele care se referă la riscul ca *o anumită persoană* să comită fapte antisocială.

3. Criminalistica predictivă aplicată cu privire la faptele antisociale săvârşite în spaţiul virtual

Una dintre zonele de interes ale Criminalisticii predictive este reprezentată de spaţiul virtual. Specificul activităţii infracţionale desfăşurate prin utilizarea tehnologiei digitale şi a internetului determină un caracter aparte al activităţilor de prevenire a faptelor antisociale în spaţiul virtual. Deoarece multe dintre infracţiunile săvârşite în mediul on-line au la bază utilizarea de programe informatice rău-intenţionate, o modalitate eficientă de prevenire a activităţii infracţionale din spaţiul virtual este identificarea tipului de utilizator care doreşte să acceseze un program sau un serviciu. Altfel spus, pentru a preveni săvârşirea infracţiunilor în spaţiul on-line, este util să se stabilească dacă utilizatorul este o fiinţă umană sau un program informatic. Dacă se stabileşte cu grad mare de probabilitate că

[12] T. Thompson, *Crime Software May Help Police Predict Violent Offences*, The Guardian, iulie 2010, [Online] la https://www.theguardian.com/uk/2010/jul/25/police-software-crime-prediction, accesat la data de 11.01.2020.

[13] A se vedea L.M. Barrow, R.A. Rufo, S. Arambula, *Police and Profiling in the United States: Applying Theory to Criminal Investigation*, CRC Press, Taylor and Francis Group, 2014, p. 165.

utilizatorul este o persoană, atunci se apreciază că riscul de a se săvârşi o faptă antisocială în mediul virtual este foarte mic.

O metodă care şi-a demonstrat eficienţa în identificarea programelor prin care se doreşte prejudicierea unor persoane este utilizarea sistemului CAPTCHA. Numele este un acronim de la Completely Automated Public Turing test to tell Computers and Humans Apart[14]. Concret, sistemul CAPTCHA este o formă de test Turing administrată automat de un server (testul Turing obişnuit fiind administrat de un om)[15].

Sistemul CAPTCHA a cunoscut mai multe forme de-a lungul timpului. Modificările au fost o necesitate, deoarece s-a reuşit crearea de programe informatice care au „păcălit" acest sistem şi, în consecinţă, s-au creat forme de CAPTCHA din ce în ce mai rezistente la atacurile cibernetice[16].

În forma „clasică", sistemul CAPTCHA se prezintă sub forma unei imagini ce conţine litere cu formă distorsionată, pe care utilizatorul trebuie să le recunoască şi să le introducă din nou, pentru a demonstra că este o persoană şi nu un program informatic. Practic, sistemul CAPTCHA bazat pe recunoaşterea unui text verifică existenţa simultană a trei abilităţi ale utilizatorului: *recunoaşterea literelor*, *separarea literelor* şi *înţelegerea semantică*[17].

Recunoaşterea literelor se bazează pe capacitatea oamenilor de a recunoaşte un caracter scriptural, chiar dacă acesta diferă foarte mult de forma standard. Concret, o persoană poate recunoaşte un număr infinit de variaţii pe care le poate avea o literă, dar un robot poate avea mari dificultăţi în acest demers[18].

---

[14] În limba română, Test Turing public complet automat pentru a diferenția computerele de oameni.

[15] CAPTCHA se mai numeşte și Test Turing inversat. Testul Turing este un sistem care permite unui *om* să facă diferențierea dintre oameni și programe informatice, în timp ce CAPTCHA este un sistem care permite unui *computer* să diferențieze oamenii de programe informatice. A se vedea L. von Ahn, M. Blum, N.J. Hopper, J. Langford, *CAPTCHA: Using Hard AI Problems for Security*, în E. Biham (Editor), EUROCRYPT 2003: International Conference on the Theory and Applications of Cryptographic Techniques, pp. 294-311, [Online] la https://link.springer.com/content/pdf/10.1007/3-540-39200-9_18.pdf, accesat la data de 12.01.2020.

[16] A se vedea A. Hindle, M.W. Godfrey, R.C. Holt, *Reverse Engineering CAPTCHA`s*, Computer Science, în The 15th Working Conference on Reverse Engineering, 2008, pp. 59-68.

[17] A se vedea E. Bursztein, M. Martin, J.C. Mitchell, *Text-based CAPTCHA Strengths and Weaknesses*, ACM Computer and Communication Security, 2011, [Online] la https://elie.net/static/files/text-based-captcha-strengths-and-weaknesses/text-based-captcha-strengths-and-weaknesses-paper.pdf, accesat la data de 12.01.2020; K. Chellapilla, K. Larson, P. Simard, M. Czerwinski, *Designing Human Friendly: Human Interraction Proofs (HIPs)*, Microsoft Research, 2015, [Online] la https://web.archive.org/web/20150410195118/http://research.microsoft.com/pubs/101726/HIPSCHI2005.pdf, accesat la data de 12.01.2020.

[18] E. Bursztein *et al.*, *op. cit.*; K. Chellapilla *et al.*, *op. cit.*

Separarea literelor înseamnă abilitatea de a identifica literele, chiar şi atunci când sunt lipite unele de altele. Pentru o persoană, separarea literelor şi recunoaşterea literelor reprezintă părţi ale aceluiaşi proces şi sunt uşor de realizat; pentru un robot însă, aceste două acţiuni sunt diferite şi prezintă dificultate ridicată[19].

Înţelegerea semantică presupune perceperea sensului cuvântului ca întreg[20].

Ideea de bază a sistemului CAPTCHA constă în faptul că, de regulă, performanţele programelor informatice sunt departe de a fi similare celor umane în ceea ce priveşte existenţa cele trei abilităţi. Totuşi, unele versiuni ale sistemului CAPTCHA bazat pe recunoaşterea textului au fost „învinse" de programe avansate de recunoaştere optică a caracterelor[21]. O altă problemă cu care s-a confruntat sistemul CAPTCHA „clasic", de recunoaştere a unui text, a fost faptul că metoda nu putea fi utilizată de persoanele cu deficienţe de vedere, de intensitate mai mică sau mai mare[22]. Astfel, a fost nevoie de schimbarea sistemului.

O metodă îmbunătăţită de CAPTCHA este cea care solicită utilizatorilor recunoaşterea anumitor obiective dintr-o serie de imagini. Astfel, se contracarează activitatea programelor de recunoaştere optică a caracterelor, care pot acţiona în cazul sistemului CAPTCHA bazat pe recunoaştere de text. De asemenea, această metodă vine în întâmpinarea nevoilor speciale ale persoanelor care au dificultăţi în a identifica literele, dar care pot recunoaşte imagini (de exemplu, persoanele care prezintă dislexie)[23].

O altă metodă care permite utilizarea şi de către persoanele cu disabilităţi (inclusiv cele care şi-au pierdut total simţul vederii) este recunoaşterea vocală (*speech recognition*)[24].

O formă de CAPTCHA care prezintă rezistenţă crescută la atacuri cibernetice este reCAPTCHA. Una dintre modalităţile reCAPTHCA se numeşte No CAPTCHA reCAPTHCA şi presupune doar bifarea de către utilizator a unei căsuţe, certificând faptul că nu este robot. Deşi pare simplă, această formă de CAPTCHA este foarte avansată. Bifarea căsuţei este doar ultima etapă dintr-un şir, etapele anterioare fiind reprezentate, în special, de colectarea de informaţii

---

19 *Ibidem.*

20 *Ibidem.* În domeniul informaticii se realizează cercetări în vederea creării de programe care pot identifica din punct de vedere semantic cuvintele. De exemplu, a se vedea R.-G. Rotari, I. Hulub, Ş. Oprea, M. Plămadă-Onofrei, A.B. Lorenţ, R. Preisler, A. Iftene, D. Trandabăţ, *Wild Devs` at SemEval 2017-Task 2: Using Neural Networks to Discover Word Similarity*, Proceedings of the 11th International Workshop on Semantic Evaluation (SemEval 2017), pp. 267-270, [Online] la https://www.aclweb.org/anthology/S17-2042.pdf, accesat la data de 12.01.2020.

21 S. Azad, K. Jain, *CAPTCHA: Attacks and Weaknesses against OCR Technology*, Global Journal of Computer Science and Technology, Vol. 13 (3), 2013, pp. 14-18 .

22 V.P. Singh, P. Pal, *Survey of Different Types of CAPTCHA*, International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 5 (2), 2014, pp. 2242-2245.

23 *Ibidem.*

24 *Ibidem.*

despre respectivul utilizator (prin analiza așa-numitelor „cookie"-uri), pe o anumită perioadă de timp (de exemplu, de câteva săptămâni). Chiar bifarea căsuței reprezintă o sursă importantă de informații, deoarece permite analiza mai multor elemente, printre care și mișcarea mouse-ului, care are un anumit tipar când utilizatorul este o persoană (tipar care este diferit în ipoteza în care un program informatic dorește să acceseze sistemul)[25].

O formă și mai avansată de CAPTCHA (numită *Invisible* CAPTCHA[26]) nu presupune nicio acțiune din partea utilizatorului. Acesta nici nu știe că a fost supus unui „test" CAPTCHA. Informațiile necesare pentru a prefigura potențialele pericole cibernetice sunt colectate doar prin monitorizarea activității anterioare a utilizatorului[27]. Acest sistem reușește să elimine una dintre problemele formelor „clasice" de CAPTCHA (care presupun o activitate, uneori destul de laborioasă, din partea utilizatorilor), și anume abandonarea accesării site-urilor. Unele studii arată că o parte dintre persoanele care doresc accesarea unor site-uri și care sunt puse în situația de a completa forme complexe de CAPTCHA (recunoaștere de text, recunoaștere de imagini etc.) abandonează accesarea site-ului. Această reacție de abandon se datorează de cele mai multe ori faptului că rezolvarea „problemelor" CAPTCHA poate dura destul de mult, mai ales în situația în care prima încercare eșuează și trebuie solicitat un nou test. Abandonul din partea utilizatorilor a generat nemulțumiri și în rândul companiilor sau persoanelor care administrează diverse site-uri, deoarece s-a înregistrat o scădere a veniturilor[28]. Sistemul „invizibil" de CAPTCHA reușește, așadar, să mulțumească și utilizatorii, și proprietarii site-urilor.

4. Concluzii cu privire la posibilitățile reale de prevenire a infracțiunilor

Informațiile prezentate mai sus arată faptul că prevenirea săvârșirii infracțiunilor este posibilă, iar domeniul Informaticii aduce o contribuție importantă în cadrul demersului de prevenire a fenomenului infracțional. Prevenirea se poate face atât cu referire la faptele antisociale săvârșite în format fizic, cât și cu privire la cele săvârșite în mediul virtual. Metodele cibernetice utilizate pentru a preveni

---

25 A se vedea V. Shet, *Are You a Robot? Introducing „No CAPTCHA reCAPTCHA"*, [Online] la https://security.googleblog.com/2014/12/are-you-robot-introducing-no-captcha.html, accesat la data de 12.01.2020.

26 În limba română, CAPTCHA Invizibil.

27 A se vedea N. Tanthavech, A. Nimkoompai, *CAPTCHA: Impact of Website Security on User Experience*, Proceedings of the 2019 4th International Conference on Intelligent Information, pp. 37-41, [Online] la https://doi.org/10.1145/3321454.3321459, accesat la data de 13.01.2020.

28 A se vedea C. Crumlish, E. Malone, *Designing Social Interfaces: Principles, Patterns, and Practices for Improving the User Experience*, Second Edition, O`Reilly Media, Sebastopol (California, USA), 2015, p. 66; H.M. Gómez Hidalgo, G. Alvarez, *CAPTCHAs: An Artificial Intelligence Application to Web Security*, în M.V. Zelkovits (editor), Advances in Computers, Vol. 83, Academic Press, Elsevier, Londra, p. 147.

infracţiunile în cele două medii de săvârşire sunt diferite, deoarece trebuie să se adapteze specificului fiecărui mediu în parte. În mediul fizic, prevenirea săvârşirii infracţiunilor se poate face prin utilizarea programelor informatice care, analizând mai mulţi parametri, arată *zonele* în care există un risc mai mare de a se săvârşi infracţiuni. Astfel de programe au fost aplicate şi şi-au demonstrat utilitatea. Există, de asemenea, posibilitatea dezvoltării de softuri care să indice care sunt *persoanele* care prezintă risc crescut de a săvârşi fapte antisociale; asemenea softuri au fost criticate, pe motiv că ar crea discriminări şi că ar aduce atingere prezumţiei de nevinovăţie, dar, în esenţă, ele doar aduc în mediul informaticii o activitate care, oricum, este făcută de organele de poliţie. În ceea ce priveşte săvârşirea infracţiunilor în mediul virtual, prevenirea infracţiunilor presupune, în primul rând, evidenţierea riscului ca un utilizator să nu fie o persoană, ci un program informatic. Metodele prin care se poate identifica un astfel de program sunt într-o permanentă evoluţie, pentru a contracara adaptarea rapidă a programelor informatice rău-intenţionate, care de multe ori reuşesc să treacă de sistemele de securitate. Rezultatele bune obţinute până în prezent ca urmare a cooperării dintre Criminalistica predictivă şi Informatică justifică menţinerea şi dezvoltarea, pe viitor, a acestei colaborări.