Metode futuriste de detectare a criminalităţii

Futuristic Methods to Detect Crime

Lect. univ. dr. ***Laura Maria STĂNILĂ****
Universitatea de Vest din Timişoara
Facultatea de Drept

Abstract

In the context of new ways of committing crimes arising, with technological and transnational elements, it is imperative for law enforcement agents to adapt and use appropriate means of investigation. Reluctance to innovative tools and approaches and delaying the use of artificial intelligence algorithms could dramatically affect criminal investigation and allow criminals to escape criminal liability and evade the state repressive system.

Thus, researchers were concerned to identify futuristic methods and tools for detecting crime, anchored in the new technological dimension of this phenomenon. To the present date, several artificial intelligence methods and tools are being tested and used in the criminal investigation phase: chatbots, Big Data analysis performed by VoIP companies, specific software used to manage evidence or block the spread of crime.

Keywords: *artificial intelligence; chatbot; Sweetie; criminal investigation; software; virtual victim.*

Rezumat

În contextul în care apar noi modalităţi de comitere a infracţiunilor, având componente tehnologice şi transnaţionale, este obligatoriu ca agenţii de aplicare a legii să se adapteze şi să utilizeze mijloace adecvate de investigare. Reticenţa pentru instrumente şi abordări inovatoare şi amânarea utilizării algoritmilor de inteligenţă artificială ar putea afecta dramatic investigaţia penală şi ar permite infractorilor să scape de răspunderea penală şi să eludeze sistemul represiv statal.

Astfel, cercetătorii au fost preocupaţi să identifice metode şi instrumente futuriste de detectare a criminalităţii, ancorate în noua dimensiune tehnologică a acestui fenomen. Până în prezent, mai multe metode şi instrumente AI sunt testate şi utilizate în faza de investigaţie penală: chatbots, analiza Big Data realizată de către companiile VoIP, software-uri specifice folosite pentru gestionarea probelor sau blocarea răspândirii formelor de criminalitate.

Cuvinte-cheie*: inteligenţă artificială; chatbot; Sweetie; investigaţie penală; software; victimă virtuală.*

1. Noi metode şi instrumente de inteligenţă artificială utilizate în faza de investigaţie penală

Inteligenţa artificială (AI) a cucerit în ultimii zece ani, pas cu pas, fiecare domeniu al vieţii sociale. Justiţia penală, un bastion străvechi şi tradiţionalist nu a reuşit să reziste noilor tehnologii, astfel că, urmare a rezultatelor remarcabile în materie de obiectivitate şi rapiditate a interpretării datelor, algoritmii AI au ajuns să fie indispensabili în interpretarea statistică a datelor privind fenomenul infracţional şi trăsăturilor sale într-o perioadă dată. În plus, extinderea criminalităţii în domeniul online, transformarea AI într-un mijloc extrem de eficient de comitere a infracţiunii a dus la o reacţie adaptare a investigaţiei penale. O infracţiune care se comite în mediul online nu ar putea fi investigată prin mijloace tradiţionale, ci necesită, în mod evident, utilizarea unor mijloace specifice prin care să se aducă probe în acuzarea celor care comit astfel de fapte reprobabile.

* laura.stanila@e-uvt.ro.

Printre noile metode şi instrumente AI utilizate în investigarea criminalistică se numără *chatbot*-urile, analiza Big Data realizată de către companiile VoIP şi software-urile specifice folosite pentru gestionarea probelor sau blocarea răspândirii formelor de criminalitate.

1.1. Chatbots

Un *chatbot* este o aplicaţie software folosită pentru a realiza o conversaţie online (text sau discurs) în locul unui contact direct cu un agent uman[1]. *Chatbot*-ul este conceput pentru a simula comportamentul uman într-o conversaţie şi necesită de obicei ajustare şi testare continuă. *Chatbot*-urile sunt utilizate de obicei în diverse scopuri: servicii pentru clienţi, formularea cererilor, colectarea informaţiilor, iar în ultima perioadă, aria lor de utilizare s-a extins la investigarea infracţiunilor şi la identificarea potenţialilor infractori.

Chatbot-urile au evoluat de la dispozitive total dependente de conduita unui agent uman la software-uri independente. *Chatbot*-urile dependente de actorii umani sunt simple „marionete" manipulate de oameni, astfel „conduita" lor este, de fapt, conduita operatorului uman. *Chatbot*-urile automate acţionează independent şi învaţă din propria experienţă şi ar putea crea noi strategii de prevenire a criminalităţii. De departe, experimentul *Sweetie chatbot* realizat de *Terre des Hommes* Olanda este un exemplu remarcabil al modului în care o idee extrem de simplă poate fi aplicată în lupta împotriva formelor specifice de criminalitate, cum ar fi pornografia infantilă virtuală[2].

Cercetătorii au declarat că *chatbot*-urile ar putea fi folosite ca agenţi sub acoperire. Însă, în timp ce versiunea iniţială a *chatbot*-urilor este perfect compatibilă cu instituţia agentului sub acoperire, versiunile avansate independente automate sunt, din păcate, necompatibile cu vreo instituţie procedural-penală, deoarece sunt consideraţi agenţi non-umani. „(…) Calitatea de a fi o fiinţă umană este un element necesar al investigatorilor sub acoperire în acest moment. Cu toate acestea, în abordarea propusă, agenţii umani ar fi implicaţi doar în evaluarea conversaţiilor stocate realizate între *chatbot*-uri şi potenţiali infractori, şi nu în timpul efectuării propriu-zise a operaţiunilor sub acoperire, adică în momentul în care ar avea loc aceste conversaţii. Cadrul legal pentru investigarea online a abuzurilor sexuale asupra copiilor ar trebui modificat pentru a efectua astfel de operaţiuni sub acoperire fără agenţi umani"[3]. Utilizarea agenţilor sub acoperire este strict prevăzută de lege, cadrul legal fiind extrem de restrictiv privind caracteristicile, condiţiile şi situaţiile în care se poate utiliza o astfel de metodă de investigare cu caracter excepţional. Versiunea avansată a lui *Sweetie* este de fapt un model hibrid de *chatbot*, care nu este complet independent de actorul uman. În viitor, există proiecte pentru dezvoltarea unui *chatbot* complet automatizat care ar putea elimina factorul uman, ridicând doar întrebări serioase cu privire la legalitatea utilizării unei astfel de metode în procesul penal.

1.2. Analiza Big Data de către companiile VoIP

Voice-over-IP (VoIP) este o metodă eficientă de comunicare. VoIP implică trimiterea de transmisii vocale sub formă de pachete de date utilizând Protocolul Internet (IP), prin care vocea utilizatorului este transformată într-un semnal digital, comprimată şi defalcată într-o serie de astfel de pachete. Pachetele sunt apoi transportate prin reţele IP private sau publice şi reasamblate şi decodate de entitatea care le primeşte[4].

Companiile VoIP derulează două tipuri de analiză Big Data: analiza metadatelor şi analiza conţinutului datelor.

---

[1] V. Crăciun, *Ce este un chatbot?,* Today Software Magazine, nr. 72, 2018, https://www.todaysoftmag.ro/article/2645/ce-este-un-chatbot.

[2] A se vedea video cu privire la *Sweetie*: https://youtu.be/aGmKmVvCzkw?t=10.

[3] K. V. Açar, *Webcam Child Prostitution: An Exploration of Current and Futuristic Methods of Detection*, International Journal of Cyber Criminology, Ianuarie – Iunie 2017, vol. 11(1): 98–109, p. 103, DOI: 10.5281/zenodo.495775.

[4] U. Varshney, A. Snow, M. McGivern, C. Howard, *Voice over IP*, Communications of the ACM, 45(1): 89-96, 2002, p. 89, https://dl.acm.org/doi/10.1145/502269.502271.

a) Analiza metadatelor. Metadatele sunt de fapt date care furnizează informaţii despre alte date, rezumând informaţii de bază despre acestea, uşurând găsirea şi operarea anumitor categorii de date. Cu alte cuvinte, Metadatele sunt reprezentări prescurtate ale datelor la care se referă[5].

Metadatele prezintă unele atribute ale comunicaţiilor, cum ar fi data, creatorul şi adresele IP, fără a compromite în mod sever confidenţialitatea comunicaţiilor. Prin urmare, colectarea de metadate este mai uşoară atât din punct de vedere tehnic, cât şi din punct de vedere legal, deoarece ocupă mai puţin spaţiu pe disc şi implică informaţii personale mai puţin intruzive decât datele despre conţinut. Această metodă este utilizată pentru a detecta pornografia infantilă online, precum şi alte categorii de infracţiuni care ar putea fi comise prin Internet, printr-o analiză tipologică a metadatelor comunicaţiilor VoIP (locaţie, sursă, IP) care ar putea conduce anchetatorii la potenţiale victime sau infractori[6].

De exemplu, un copil care provine dintr-o ţară care în mod „tradiţional" furnizează victime minore, ia legătura cu pedofili din diferite ţări într-o perioadă limitată de timp (o săptămână). În acest caz, compania VoIP citeşte „semnalele" sau indicatorii de infracţionalitate - un locuitor al unui oraş foarte sărac discută cu mai mulţi străini din ţări relativ mai bogate - apoi dezvăluie adresele IP şi alte informaţii utile precum adrese de e-mail autorităţii de aplicare a legii pentru investigaţii suplimentare[7].

b) Analiza conţinutului datelor. Analiza de conţinut a datelor expune informaţii specifice despre conversaţiile VoIP realizate între părţi: texte, fişiere audio, video şi este extrem de intruzivă. Pentru realizarea acestui tip de analiză este nevoie de obţinerea unor autorizaţii legale şi de operatori instruiţi[8]. O analiză a *Skype* – aplicaţie folosită de milioane de oameni din întreaga lume pentru a comunica la distanţă - arată anumite caracteristici ale acestuia - cum ar fi traducerea în timp real. Pentru a detecta pornografia infantilă online, de exemplu, o analiză a conţinutului ar putea folosi cuvinte de cod precum cuvinte cu sens sexual pentru a dezvălui comportamente suspecte. Atunci când rezultatele unei astfel de analize sunt coroborate cu alte date precum tipul transferului de bani (ex. PayPal, bitcoin) şi locaţia IP, rezultatul final ar putea fi extrem de util pentru anchetatori.

1.3. Software conceput în mod expres pentru a fi utilizat în faza de investigare a procesului penal

Există multe exemple de software concepute în mod expres pentru a fi utilizate în faza de investigare a procesului penal. *Analist Notebook* by IBM[9] şi *HOLMES 2 (Home Office Large Major Enquiry System)*[10] sunt amândouă proiectate în 2006 şi utilizate în Marea Britanie, în timp ce Olanda a folosit experimental *BRAINS* în investigarea infracţiunilor cu un anumit succes în 2004. *FLINTS (Forensic-Led Intelligence System)*[11] este un alt exemplu care a fost folosit pentru prima dată de poliţia britanică în 1999 pentru gestionarea probelor medico-legale.

Compania Microsoft a creat un software care recunoaşte identitatea persoanelor din fotografii, chiar acestea dacă au fost modificate sau alterate, care este utilizat în investigarea pornografiei infantile, pentru a ajuta anchetatorii să se concentreze pe noile imagini care apar pe internet. Un alt software, *Adobe Systems Photoshop*, este utilizat pentru a identifica victimele pornografiei infantile cu instrumente care accentuează imaginile pentru a dezvălui indicii.

Alte iniţiative care folosesc inteligenţa artificială sunt realizate împreună cu *Google*, care blochează termenii de căutare ce sunt asociaţi pornografiei infantile şi cu *Thorn*, o fundaţie susţinută de actori de

---

[5] J. Hare, *What is metadata and why is it as important as data itself?* Opendatasoft, 25 August 2016, https://www.opendatasoft.com/blog/2016/08/25/what-is-metadata-and-why-is-it-important-data.

[6] K.V. Açar, *op. cit.,* p. 103.

[7] K.V. Açar, *op. cit.*, p. 104.

[8] K.V. Açar, *op. cit.*, p. 105.

[9] https://www.ibm.com/security/intelligence-analysis/i2/law-enforcement.

[10] HOLMES 2 (*Home Office Large Major Enquiry System*) este un sistem de tehnologia informației utilizat de Poliția din Marea Britanie pentru a facilita investigațiile în descoperirea omorurilor și a fraudei. A fost dezvoltat de Unisys fiind susținut de Inițiativa Financiară Privată. Denumirea aleasă face referire la personajul scriitorului Arthur Conan Doyle, Sherlock Holmes. Mai multe informații pot fi găsite la adresa http://www.holmes2.com/holmes2/index.php.

[11] E. Nissan, *Computer Applications for Handling Legal Evidence, Police Investigation and Case Argumentation*, Vol. 1, Springer, 2012, p. 767-836. În ceeea ce priveşte FLINTS (*Forensic-Led Intelligence System*) şi beneficiile sale, a se vedea, de asemenea, A.R.W. Jackson, J.M. Jackson, *Forensic Science,* ediția a doua, Pearson, 2008, p. 7.

la Hollywood, care a creat o bază de date pentru urmărirea imaginilor cunoscute cu conţinut sexual şi extragerea lor offline[12].

După cum au subliniat oamenii de ştiinţă, chiar dacă aceste programe software sunt extrem de utile în faza de investigare, rezultatele cercetării penale sunt „în totalitate dependente de raţionamentul uman, iar structurile rezultate din acest raţionament nu pot fi înregistrate şi analizate de software”[13].

2. Un instrument controversat de investigaţie: Sweetie

2.1. Despre Sweetie şi versiunile sale

Aşa cum s-a explicat anterior, *Sweetie* este un *chatbot*, un program AI, conceput pentru a combate pedofilia online (acte cu conţinut sexual explicit care implică copii, realizate cu ajutorul webcam-ului) şi pentru a ajuta la identificarea suspecţilor, infractorilor şi victimelor. Acest *chatbot* a fost creat de organizaţia *Terre des Hommes*[14] din Olanda în 2013. De la prima utilizare în 2013, *Sweetie* a condus la condamnarea mai multor cetăţeni englezi, danezi, olandezi şi belgieni pentru pedofilie online[15].

În prima sa versiune – *Sweetie 1.0* – *chatbot*-ul întruchipa o persoană de sex feminin de 10 ani din Filipine şi a fost folosit pentru a identifica şi demasca pedofilii amatori de turism sexual. Întrucât în prima sa versiune *Sweetie* nu era automat, *chatbot*-ul a fost operat de un agent uman. Conversaţiile cu pedofilii au fost purtate de agenţi de poliţie, Sweetie fiind doar avatarul acestora. În ciuda succesului iniţial, utilizarea lui *Sweetie* a fost limitată de faptul că a fost operat de un actor uman, ceea ce a dus la realizarea unui număr limitat de conversaţii online purtate simultan. Însă numărul suspecţilor – amatori de wecam sex – a fost de peste 2000 pe oră 2000! În aceste condiţii, resursele umane ale poliţiei nu puteau face faţă, astfel că a fost creat *Sweetie 2.0*, o versiune mai avansată a *chatbot*-ului. „Principala diferenţă dintre *Sweetie 1.0* şi *Sweetie 2.0* este acesta din urmă nu mai este operat de un agent uman, fiind un sistem AI semi-autonom, care se poate angaja într-o conversaţie semnificativă cu un suspect”[16]. *Sweetie 2.0* este de fapt un model hibrid de *chatbot*, care nu este complet independent de actorul uman. În viitor, există proiecte pentru dezvoltarea unui *chatbot* complet automatizat care ar putea elimina factorul uman, cu toate acestea, ar pune probleme serioase cu privire la legalitatea utilizării unei astfel de metode în procesul penal.

Principalul avantaj în utilizarea *Sweetie* este că anchetatorii pot interacţiona direct cu pedofilii fără a pune pe nimeni în pericol, cu alte cuvinte, nu există victime potenţiale, ci doar potenţiali suspecţi. Este ca şi cum am descoperi o infracţiune înainte de a fi fost comisă. În ciuda entuziasmului generat de această inovaţie investigativă, este evident că există mari probleme de calificare juridică a „faptelor” descoperite de *Sweetie*: nu există infracţiune consumată sau tentată, nu există victime umane şi, prin urmare, legea penală nu ar putea fi aplicată nimănui! Pentru a pedepsi „prădătorii sexuali” ca urmare a utilizării *Sweetie* în conformitate cu cerinţele şi standardele procesual-penale, sunt necesare intervenţii legislative importante. Spre exemplu ar trebui ca, minimal, interacţiunea cu *Sweetie* să fie calificată de lege ca şi comportament infracţional tentat. „Dacă nu se va realiza acest lucru, atunci va fi mult mai greu, dacă nu chiar imposibil de dovedit că suspectul a comis sau a încercat să comită o faptă infracţională. La rândul său, acest lucru va face mai dificilă justificarea folosirii lui *Sweetie* ca metodă de investigare”[17].

Folosirea lui Sweetie ca metodă de investigare a determinat crearea a două tabere: tabăra susţinătorilor alcătuită din membrii societăţii civile şi tabăra celor care resping această inovaţie alcătuită de jurişti teoreticieni şi practicieni. Întrucât *Sweetie* a fost proiectat şi dezvoltat de o organizaţie

---

[12] K. Schweizer, *Avatar Sweetie exposes sex predators*, The Age, 26 Aprilie 2014, https://www.theage.com.au/-world/avatar-sweetie-exposes-sex-predators-20140425-379kf.html.

[13] F. Bex, S. Van den Braak, H. Van Oostendorp, H. Prakken, B. Verheij, G. Vreeswijk, *Sense-making software for crime investigation: how to combine stories and arguments?*, Law, Probability and Risk, vol. 6, Issue 1-4, Martie 2007, p. 146, https://doi.org/10.1093/lpr/mgm007.

[14] Site oficial: www.terredeshommes.nl.

[15] Terre des Hommes, *First conviction for child abuse in Belgium thanks to Sweetie*, 9.04.2015, https://www.terredeshommes.nl/en/news/first-conviction-child-abuse-belgium-thanks-sweetie.

[16] B. W.Schermer, I. Georgieva, S. Van der Hof, B-J. Koops, *Legal Aspects of Sweetie 2.0.*, Leiden/Tilburg: TILT, 2016, p. 10.

[17] B. W. Schermer, *et al., op. cit.,* p. 12.

non-profit, Agenţia Europeană de Poliţie *Europol* a exprimat rezerve cu privire la utilizarea acestuia, în ciuda obiectivului său nobil: „Considerăm că investigaţiile penale care utilizează măsuri de supraveghere intruzive ar trebui să fie responsabilitatea exclusivă a agenţiilor de aplicare a legii", a declarat purtătorul de cuvânt Soren Pedersen agenţiei de ştiri Reuters[18].

2.2. Probleme referitoare la utilizarea lui Sweetie în procesul penal

Pe măsură ce renumele lui *Sweetie* a tot crescut, acesta a devenit subiect al unei analize juridice detaliate, care a dus la concluzia că acest instrument de investigare nu îndeplineşte cerinţele legii pentru a fi recunoscut şi utilizat[19]. Raportul a fost publicat în 2016 şi a avut un efect dramatic, demoralizându-i pe susţinătorii entuziaşti ai lui *Sweetie*.

Principalele probleme identificate de cercetători în utilizarea lui Sweetie au fost:

a) Lipsa elementului uman

Varianta upgradată a lui *Sweetie 2.0* nu mai este operată de un agent uman, ci de un algoritm autonom de inteligenţă artificială care se poate angaja într-o conversaţie cu un suspect. Dacă agreăm ideea că *Sweetie* este un agent sub acoperire, lipsa operatorului uman este elementul care elimină posibilitatea utilizării *Sweetie* ca atare. Întrucât toate legislaţiile procesual penale interne reglementează agenţii sub acoperire ca fiind fiinţe umane, atunci nu mai putem aduce niciun argument în această direcţie.

b) Probleme etice privind natura non-umană a lui Sweetie. Conceptul de „victimă virtuală"

Deoarece *Sweetie* este un avatar, un personaj virtual, programat să arate şi să vorbească ca un copil, fiind evident că niciun copil real nu va fi vreodată implicat în procesul de identificare a pedofililor, şi pentru că funcţionarea lui *Sweetie* nu presupune un comportament sexual explicit din partea „victimei", s-a pus problema dacă, în acest caz există o victimă reală[20].

Conceptul de victimă este înţeles, de asemenea, doar prin raportare la o fiinţă umană, de vreme ce doar fiinţele umane sunt subiect al protecţiei penale, exercită drepturi şi sunt titulare ale valorilor sociale ocrotite de legea penală[21]. Această concluzie ridică o altă întrebare: ar putea fi considerat *Sweetie* o victimă virtuală şi, dacă da, ce este, de fapt, o victimă virtuală?

O victimă virtuală este de fapt un subiect pasiv virtual al infracţiunii. Victima virtuală poate fi un subiect pasiv al unei infracţiuni comise în mediul virtual de către un subiect activ virtual (avatar) sau poate fi o victimă simulată, care are rolul de „momeală" pentru un infractor uman care comite infracţiuni în spaţiul virtual.

Sweetie 1.0 ar putea fi calificat drept victimă umană, deoarece, în acest caz, un agent uman (prădătorul sexual) comite fapta împotriva unui avatar controlat de un alt agent uman, folosind un avatar. În acest caz, Sweetie este doar un instrument AI, în timp ce agentul uman care îl operează este un agent sub acoperire. Situaţia ar putea fi justificată legal prin interpretarea extensivă a reglementărilor procedural-penale existente privind activitatea şi scopul investigatorilor sub acoperire.

Sweetie 2.0, fiind însă o entitate AI care funcţionează independent în mare parte, care a fost doar proiectată şi programată de un agent uman, ar putea fi considerată o victimă virtuală – un utilizator

---

[18] A., Crawford, *Computer-generated 'Sweetie' catches online predators*, BBC News, 5 Noiembrie 2013, https://www.bbc.com/news/uk-24818769.

[19] B. W. Schermer *et al., op. cit.,* pp. 82-86.

[20] B. W. Schermer *et al., op. cit.,* p. 29.

[21] Această concluzie nu trebuie absolutizată, de vreme ce există exemple de „victime non-umane" a căror lezare atrage consecinţe penale: Legea 205/2004 privind protecţia animalelor, republicată în Monitorul Oficial al României, Partea I, nr. 320 din 30 aprilie 2014, modificată prin Legea nr. 171/2017 publicată în Monitorul Oficial al României, Partea I, nr. 576 din 19 iulie 2017, interzice sub sancţiune penală prin prevederile art. 23: uciderea animalelor, cu intenţie, fără drept; practicarea tirului pe animale domestice sau pe animale sălbatice captive; organizarea de lupte între animale sau cu animale; folosirea de animale vii pentru dresajul animalelor sau pentru a le controla agresivitatea; rănirea sau schingiuirea animalelor; intervenţiile chirurgicale destinate modificării aspectului unui animal sau altor scopuri necurative, cum ar fi codomia, cuparea urechilor, secţionarea corzilor vocale, ablaţia ghearelor, coltilotul ciocului şi dinţilor. Pedeapsa principală în acest caz este închisoarea de la 3 luni la 1 an sau amenda, putându-se aplica şi pedeapsa complementară a interdicţiei de a deţine animale pentru o perioadă de la un an la 5 ani. Prin urmare, în acest caz, animalele nu sunt considerate simple obiecte 1animate", ci adevărate victime. În opinia mea, astfel de prevederi penale deschid, chiar dacă timid, calea acceptării conceptului de „victimă non-umană".

uman comite fapta împotriva unui agent complet virtual folosind un avatar. În acest caz *Sweetie însăşi* este un agent sub acoperire care acţionează ca o victimă virtuală pentru a expune conduita infracţională a făptuitorului uman.

Dintr-o perspectivă etică, cea mai importantă caracteristică şi, în acelaşi timp, marele avantaj a lui *Sweetie* este faptul că nu pune efectiv în pericol copiii (victimele minore)[22], însă această caracteristică este în acelaşi timp şi defectul său principal: în majoritatea sistemelor de drept penal, este nevoie de victimă „reală" – a se înţelege „umană" – pentru a putea acuza un suspect de comiterea unei fapte penale. Legea penală şi procesual-penală în vigoare nu recunoaşte victimele virtuale… (încă?!?)

c) Probleme privind caracterul infracţional al faptelor săvârşite de făptuitor

Deoarece funcţionarea lui *Sweetie* nu presupune adoptarea unor comportamente sexuale explicite sau cel puţin acte de nuditate, animaţiile *Sweetie* nu pot fi calificate ca acte de pornografie infantilă. În consecinţă, actorul uman care interacţionează cu Sweetie nu poate comite infracţiunea de accesare (şi eventual stocare) de pornografie infantilă. Din perspectiva aplicării legii, acest lucru reprezintă o problemă majoră, având în vedere că în majoritatea statelor, accesul la pornografie infantilă (virtuală) reprezintă un element de tipicitate al faptei[23].

Impunerea răspunderii penale pentru o tentativă la o infracţiune sexuală în cazul interacţiunii cu *Sweetie* este condiţionată de incriminarea acelor acte de către legiuitorul naţional.

d) lipsa prevederilor procesual-penale în legislaţiile naţionale privind utilizarea instrumentelor AI în faza de investigaţie

Sweetie este un instrument AI creat pentru a facilita acţiunile de investigare ale organelor judiciare, şi ar opera pe platformele publice online într-o manieră independentă (*Sweetie 2.0.*). „Chatbot-ul / avatarul va fi folosit ca un agent provocator pentru presupusul infractor, dar va fi, de asemenea, capabil să interacţioneze cu suspectul, să înregistreze şi să stocheze interacţiunile şi conversaţiile cu acesta, precum şi informaţiile disponibile online despre suspect, cum ar fi, de exemplu, adresa IP a acestuia"[24]. Există puţine dispoziţii legale care ar putea permite utilizarea *Sweetie* ca metodă de investigare în ancheta penală, atât timp cât utilizarea acestui instrument se încadrează în limitele stabilite de lege. Deoarece *Sweetie* este proiectat să identifice şi să atragă suspecţii într-o manieră comparabilă cu modul de operare al investigatorilor sub acoperire, regulile care reglementează activitatea acestora din urmă vor trebui extinse şi la utilizarea lui *Sweetie*. În plus, *chatbot*-ul va colecta anumite informaţii despre presupusul infractor şi despre dispozitivele pe care acesta le foloseşte şi va stoca conţinutul comunicărilor dintre acea persoană şi Sweetie în scop de investigare, în vederea adunării de probe în acuzare. În consecinţă, regulile care autorizează aceste competenţe de investigare diferite ar fi aplicabile conjugat în cazul *chatbot*-ului[25].

2.3. Evaluarea Sweetie în conformitate cu dreptul penal olandez. Noul cadru legislativ olandez

În anul 2016, *Sweetie* a făcut obiectul unei analize tehnice şi juridice detaliate de către o echipă de cercetători, finalizate cu întocmirea unui raport, ale cărui concluzii au fost prezentate de Bart Schermer, profesor asociat la Centrul pentru Tehnologie Digitală şi Drept al Universităţii Leiden: „Conform dreptului penal olandez, utilizarea copiilor (virtuali) pentru a provoca comiterea infracţiunii nu este încă permisă în mod explicit şi nu este clar dacă efectuarea de acte sexuale prin intermediul webcam-ului cu o persoană virtuală este pedepsibilă"[26], acest lucru „datorându-se tipului de sistem juridic din Olanda. Justiţia penală olandeză este orientată către acţiuni: trebuie să se fi comis toate elementele de tipicitate

[22] B. W. Schermer *et al., op. cit.,* p. 29.

[23] B. W. Schermer *et al., op. cit.,* p. 31.

[24] B. W. Schermer *et al., op. cit.,* p. 48.

[25] *Ibidem.*

[26] Terre des Hommes, *Dutch criminal law too limited to use Sweetie*, 20.20.2016, https://www.terredes hommes.nl/en/news/dutch-criminal-law-too-limited-use-sweetie.

obiectivă ale infracţiunii sexuale iar victima trebuie să fie o persoană care nu a împlinit vârsta de optsprezece ani, în caz contrar, infracţiunea nu există. Sweetie nu este o persoană reală[27]".

Acest raport nu a constitui altceva decât o oportunitate pentru adoptarea unei noi legislaţii în Olanda. La 21 septembrie 2018, *Legea privind criminalitatea informatică III (Wet Computercriminaliteit III)* a fost publicată în Monitorul Guvernului Olandez şi a intrat în vigoare la 1 martie 2019. Acest act normativ a reuşit să îmbunătăţească legislaţia procedurală şi substanţială penală olandeză prin modificarea Codului penal olandez (DCC) şi Codul de procedură penală olandez (DCCP). Legea a constituit un răspuns la evoluţiile rapide ale tehnologiei, internetului şi criminalităţii informatice, continuând direcţia şi principiile stabilite în 1993 prin *Legea privind criminalitatea informatică I* şi consolidate în 2006 prin *Legea privind criminalitatea informatică II.*

Legea privind criminalitatea informatică III permite instanţelor şi poliţiei să acceseze calculatoarele în mod disimulat şi la distanţă pentru a investiga infracţiuni grave, cum ar fi pornografia infantilă, traficul de droguri şi utilizarea premeditată a armelor de foc. Această putere se extinde asupra computerelor personale, telefoanelor mobile şi serverelor. În plus, Legea oferă agenţilor de investigaţii puterea de a aplica diverse tactici de investigare, cum ar fi ca anumite date să fie făcute inaccesibile, să copieze fişiere şi să acceseze diferite canale de comunicare. Acest lucru va face mai dificilă utilizarea Internetului pentru infractori, pentru a evita descoperirea faptelor de către autorităţi.

Alte dispoziţii permit ofiţerilor de investigaţie să utilizeze „adolescenţi momeală" pentru a facilita identificarea şi urmărirea penală a „groomerilor"[28] care intră online în contact cu minori în scopuri sexuale[29].

Una dintre cele mai controversate prevederi se referă la aşa-numita „competenţă de *hacking*" (prevăzută de art. 126nba, 126uba 126zpa DCCP). Agenţii de aplicare a legii au o nouă atribuţie: au puterea de a accesa sistemele informatice de la distanţă prin sustragerea de date în condiţii specifice. Astfel, agenţii de investigaţii desemnaţi pot accesa de la distanţă şi sustrage date dintr-un un sistem computerizat (computer, smartphone sau un server) folosit de un suspect, vor putea pirata sistemul prin spargerea sau eludarea securităţii sistemului sau prin utilizarea unor *software*-uri sau alte instrumente tehnice.

Întrucât orice punere în aplicare a competenţei de *hacking* constituie o încălcare severă a vieţii private a persoanei în cauză, legiuitorul olandez a permis acest lucru în condiţii restrictive: interes de investigaţie urgentă, un mandat al unui judecător de anchetă, infracţiunea suspectată trebuie să constituie o încălcare gravă a legii, pentru care legea prevede o pedeapsă cu închisoare de opt ani sau mai mare etc.).

Orice date susceptibile de înregistrare pot fi copiate în scopul constituirii unei probe într-o anchetă penală, legiuitorul olandez stabilind o garanţie suplimentară în acest sens: cerinţa „logării" (autentificarea înregistrării datelor) în timpul anchetei (secţiunea 126ee DCCP). Cu toate acestea, datele autentificate nu vor fi adăugate (automat) la dosarul cauzei, partea interesată trebuind să solicite acest lucru în mod expres.

Printre alte modificări se află şi incriminarea extinsă a faptei de „grooming"[30] (articolele 248a şi 248e DCC). Până la intrarea în vigoare a noii legi, autorităţile de aplicare a legii au fost nevoite să folosească victime aparente, în esenţă ofiţeri de poliţie sub acoperire care să impersoneze minori sub 16 ani (deoarece jurisprudenţa olandeză a stabilit că un suspect de grooming nu ar putea fi pedepsit decât dacă

---

[27] *Ibidem*.

[28] *Grooming*-ul este o metodă utilizată de prădătorii sexuali pentru a pregăti un copil pentru abuz sexual. Adulţii care utilizează această tactică se numesc *„groomeri". Grooming*-ul este planificat foarte atent şi poate dura săptămâni, luni sau chiar ani. Metoda presupune convingerea minorului că sexul cu infractorul este normal sau că nu are de ales. Infractorii fac acest lucru prin construirea unei relaţii şi conexiuni emoţionale cu copilul. Această relaţie poate lua diferite forme: relaţie de iubire, relaţie de tip mentorat, sau relaţie de tip parental. Ceea ce face această tehnică deosebit de periculoasă, este aparenţa existenţei unei relaţii pozitive, care face victimele să aibă încredere, sporindu-le astfel vulnerabilitatea. A se vedea ThinkUKnow, *What is sexual grooming*, https://www.thinkuknow.co.uk/parents/articles/what-is-sexual-grooming/.

[29] https://www.government.nl/latest/news/2019/02/28/new-law-to-help-fight-computer-crime.

[30] Fapta de a coopta minori pe Internet în scopul realizării unui abuz sexual.

victima este persoană care nu a împlinit vârsta de 16 ani, în conformitate cu articolul 248e DCC). În conformitate cu *Legea privind criminalitatea informatică III*, articolele 248a şi 248e DCC au fost modificate pentru a se asigura că infracţiunea se poate comite, de asemenea şi în modalitatea cooptării, în scopuri sexuale, a oricărei persoane care „impersonează un minor care nu a împlinit încă vârsta de 16 sau 18 ani”[31].

Unele dintre modificările aduse prin *Legea privind criminalitatea informatică III* ar putea face posibilă utilizarea *Sweetie* în faza de urmărire penală, permiţând agenţilor de ordine olandezi să obţină un rezultat eficient în lupta lor împotriva pedofiliei online, însă mai sunt multe modificări legislative de făcut în vederea realizării acestui scop.

3. Recomandări ale Consiliul UE

Consiliul Uniunii Europene a adoptat recomandări[32] prin care să-i determine pe legiuitorii naţionali să adopte un mod de gândire *„outside the box”*[33] reiterând importanţa reacţiilor în timp util pentru investigarea şi urmărirea penală a infractorilor şi salvarea copiilor victime ale abuzurilor sexuale şi exploatării sexuale. Autorităţile competente naţionale au fost invitate să dea cea mai extinsă utilizare posibilă a instrumentelor legale şi mecanismelor existente disponibile la nivel naţional şi al UE, şi în special la Europol şi Eurojust. Consiliul a subliniat necesitatea de a avea instrumente adecvate şi specifice pentru a lupta împotriva abuzurilor online comise asupra copiilor, incluzând posibilitatea autorităţilor competente de a exploata datele colectate în timpul investigaţiilor. În acest scop, Consiliul a reamintit concluziile Consiliului JHA din 6 şi 7 iunie 2019, subliniind că păstrarea datelor este esenţială pentru investigarea şi urmărirea eficientă a infracţiunilor grave. În plus, reformele legislative ar trebui să menţină posibilitatea legală a schemelor de păstrare a datelor, în conformitate cu principiile stabilite în Carta Drepturilor Fundamentale a UE.

În acest sens, Consiliul a încurajat statele membre să dezvolte şi să aplice metode de investigaţie inovatoare, precum şi să ia în considerare alocarea de resurse specializate pentru aplicarea legii pentru combaterea abuzului şi exploatării sexuale a copiilor. Schimbul de bune practici între statele membre adaugă valoare acestor iniţiative.

Consiliul UE consideră că platformele online constituie un contributor esenţial la prevenirea şi eradicarea abuzurilor şi exploatării sexuale a copiilor, inclusiv la eliminarea rapidă a materialelor cu conţinut sexual din mediul online. În pofida eforturilor curente, Consiliul constată că trebuie să depună eforturi suplimentare pentru a veni în întâmpinarea provocările tehnice, juridice şi umane care împiedică activitatea eficientă a autorităţilor competente.

Având în vedere creşterea exponenţială a materialelor pornografice cu minori în mediul online, Consiliul UE îndeamnă factorii implicaţi, inclusiv furnizorii de servicii on-line să îşi dea concursul şi să asigure accesul legal la probe digitale în vederea aplicării legii de către autorităţile competente. Consiliul invită furnizorii de servicii online să elimine sau să restricţioneze accesul la conţinutul identificat drept material pornografic cu minori cât mai curând posibil, după ce au luat cunoştinţă de acest conţinut, şi solicită Comisiei să propună măsuri pentru a rezolva această provocare în creştere.

Nu în ultimul rând Consiliul UE a subliniat că o abordare globală şi coordonată pentru combaterea acestui tip de criminalitate este extrem de importantă, cooperarea cu state terţe şi cu alte părţi interesate.

4. Concluzii privind utilizarea instrumentelor futuriste în investigaţia penală

---

[31] Nosh van der Voort, David Schreuders, *Pioneering Dutch Computer Crime Act III entered into force*, 1 martie 2019, https://www.simmons-simmons.com/en/publications/ck0bi70lg7kew0b94qi4inld1/280219-pioneering-dutch-computer-crime-act-iii-entered-into-force.

[32] Consiliul Uniunii Europene, *Conclusions on combating the sexual abuse of children* – Council conclusions 12862/19, 8 Octombrie 2019, paras. 10-15, https://data.consilium.europa.eu/doc/document/ST-12862-2019-INIT/en/pdf.

[33] Expresie utilizată pentru gândirea creativă.

Utilitatea instrumentelor AI în investigaţia penală este mai mult decât evidentă. Utilizarea aplicaţiilor şi software-urilor speciale permite anticiparea cu un grad mare de acurateţe a locului şi momentului comiterii infracţiunii, cu un nivel de rapiditate imposibil de atins de către agenţii umani.

Alte mijloace mai inventive, de tipul *chatbot*-urilor, permit, aşa cum am văzut, prinderea unui infractor chiar înainte ca acesta să comită infracţiunea. Însă tocmai această „eficienţă" este de fapt şi punctul slab, din punct de vedere juridic, al utilizării unor astfel de instrumente. În sistemul de drept contemporan, infracţiunea nu poate fi concepută decât prin raportare la un infractor uman şi la o victimă umană, cu observarea principiului legalităţii: o faptă nu poate fi sancţionată de legea penală decât dacă este prevăzută, ca formă consumată sau ca tentativă, de această lege. Or, aşa cum am arătat, în cazul *Sweetie*, nu există nici victimă umană şi nici infracţiune (nici măcar în forma tentativei), condiţii esenţiale pentru o intervenţie penală represivă.

Singura soluţie pentru utilizarea unui *chatbot* pentru prinderea infractorilor o reprezintă o intervenţie legislativă în sensul introducerii în rândul prevederilor procesual penale a unor noi metode de supraveghere sau cercetare penală pe de o parte, iar pe de altă parte, introducerea unor menţiuni speciale în legislaţia penală referitoare la faptul că, în situaţia comiterii faptei împotriva unei victime virtuale, aceasta va fi asimilată tentativei şi sancţionată ca atare. Doar astfel standardele unui proces echitabil pot fi întrunite. Punerea în aplicare a recomandărilor Consiliului UE privind dezvoltarea şi aplicarea de metode de investigaţie inovatoare nu poate să ducă la încălcări ale principiului legalităţii şi nici ale standardului unui asigurării unui proces echitabil, oricât de eficient ar fi rezultatul acestor demersuri în lupta de combatere a criminalităţii. Un lucru este cert: legislaţia penală şi cea procesuală penală trebuie să ţină pasul cu digitalizarea infracţionalităţii şi trebuie să se adapteze la noile forme de criminalitate, altfel instrumentele legale de reacţie vor fi lipsite total de eficienţă.