CZU: 343.98 DOI: https://doi.org/10.67457/lv26.2.02



Iurie ODAGIU[1]
criminalistic@gmail.com

ASPECTE CRIMINALISTICE PRIVIND POTENȚIALUL INFORMATIV ȘI INVESTIGATIV AL URMELOR DIGITALE GENERATE DE VEHICULE

Abstract: *Cercetarea urmelor digitale generate de vehicule reprezintă un domeniu aflat la intersecția criminalisticii, tehnologiilor informaționale și construcției de mașini. Dezvoltarea vehiculelor moderne, dotate cu sisteme de navigație, comunicații fără fir, unități electronice de control și numeroși senzori, a determinat apariția unor noi categorii de urme digitale susceptibile de valorificare în procesul penal. Aceste sisteme generează și conservă informații privind itinerarele parcurse, localizarea vehiculului, parametrii tehnici de funcționare, istoricul comunicațiilor și alte date rezultate din utilizarea sistemelor electronice integrate.*

Din perspectivă criminalistică, interesul cercetării nu îl reprezintă existența acestor date în sine, ci capacitatea lor de a reflecta activități și împrejurări relevante pentru cauza investigată. În consecință, cercetarea urmelor digitale presupune identificarea, extragerea, păstrarea, examinarea și interpretarea informațiilor obținute din sistemele electronice ale vehiculului, cu respectarea cerințelor privind integritatea datelor și documentarea tuturor operațiunilor efectuate.

Utilizarea unor programe și echipamente specializate permite extragerea informațiilor din diferitele componente electronice ale vehiculului și contribuie la reconstituirea accidentelor rutiere, investigarea furturilor de autovehicule sau altor infracțiuni în care vehiculul a fost folosit ca mijloc ori obiect al activității infracționale.

Dezvoltarea continuă a sistemelor electronice și a comunicațiilor dintre vehicul și alte sisteme informatice conduce la extinderea permanentă a categoriilor de urme digitale disponibile pentru cercetare. Totodată, aceasta impune elaborarea unor metode unitare de identificare, păstrare și interpretare a acestor informații, astfel încât ele să poată fi valorificate în condiții de rigoare științifică și procesuală.

Cuvinte-cheie: *urme digitale, criminalistică, investigație penală, vehicule conectate, sisteme electronice ale vehiculelor, examinarea urmelor, reconstituirea evenimentului, sisteme telematice.*

[1] **Conferențiar universitar, doctor în drept, director, Institutul de Cercetări Științifice și Drept Comparat, Academia „Ștefan cel Mare” a MAI al Republicii Moldova (ROR: https://ror.org/036kvxa54), e-mail: academia@ mai.gov.md; e-mail: criminalistic@gmail.com, ORCID ID: https://orcid.org/0000-0002-2474-5299**

CRIMINALISTIC ASPECTS OF THE INFORMATIONAL AND INVESTIGATIVE POTENTIAL OF DIGITAL TRACES GENERATED BY VEHICLES

Abstract: *The examination of digital traces generated by vehicles represents a field situated at the intersection of criminalistics, information technologies, and automotive engineering. The development of modern vehicles equipped with navigation systems, wireless communications, electronic control units, and numerous sensors has led to the emergence of new categories of digital traces that may be exploited in criminal proceedings. These systems generate and preserve information concerning travel routes, vehicle location, technical operating parameters, communication history, and other data resulting from the use of integrated electronic systems.*

From a criminalistic perspective, the primary focus of the investigation is not the mere existence of such data, but rather their capacity to reflect activities and circumstances relevant to the case under examination. Consequently, the examination of digital traces involves the identification, extraction, preservation, analysis, and interpretation of information obtained from the vehicle's electronic systems, while ensuring data integrity and documenting all investigative procedures performed.

The use of specialized software and equipment enables the extraction of information from various electronic components of the vehicle and contributes to the reconstruction of road traffic accidents, the investigation of vehicle thefts, and other criminal offenses in which the vehicle has been used either as an instrument or as an object of criminal activity.

The continuous development of electronic systems and communications between vehicles and external information systems leads to the constant expansion of the categories of digital traces available for forensic examination. At the same time, it necessitates the development of standardized methods for the identification, preservation, and interpretation of such information, so that it may be utilized in accordance with scientific rigor and procedural requirements.

Keywords: *digital traces, criminalistics, criminal investigation, connected vehicles, vehicle electronic systems, trace examination, event reconstruction, telematics systems.*

1. INTRODUCERE

Dezvoltarea tehnologiilor informatice și integrarea acestora în industria constructoare de autovehicule au modificat fundamental natura informațiilor care pot fi valorificate în procesul penal. Dacă, în mod tradițional, cercetarea criminalistică a vehiculelor era orientată cu precădere asupra urmelor materiale: urme de impact, de frânare, de vopsea, de pneuri sau de deformare, în prezent vehiculele moderne generează și păstrează simultan un volum considerabil de informații digitale privind funcționarea lor și activitatea utilizatorilor. Aceste informații constituie o categorie distinctă de urme care pot completa și completează tabloul probator și extind posibilitățile de percepere și reconstituire a evenimentului investigat.

Transformarea autovehiculului dintr-un sistem preponderent mecanic într-un ansamblu complex de componente electronice și informatice a determinat apariția unor noi surse de informații cu relevanță criminalistică. Sistemele de navigație, unitățile electronice de control, sistemele multimedia, comunicațiile fără fir și serviciile integrate de comunicații și monitorizare generează în mod continuu date referitoare la deplasarea vehiculului, parametrii săi tehnici și interacțiunea cu utilizatorul sau cu alte sisteme informatice.[1]

[1] Le-Khac, N.-A.; Jacobs, D.; Nijhoff, J.; Bertens, K.; Choo, K.-K.R. Smart Vehicle Forensics: Challenges and Case Study. Accepted Manuscript. Future Generation Computer Systems, 2018. P.2. Disponibil: https://welib.st/md5/241741f55747308dd768643031ab2638; Ebbers, S.; Ising, F.; Saatjohann, C.; Schinzel, S. Grand Theft App: Digital Forensics of Vehicle Assistant Apps. Proceedings of the 16th International Conference on Availability, Reliability and Security (ARES), 2021. P.1-2. Disponibil: https://arxiv.org/pdf/2106.04974

Cu toate acestea, literatura de specialitate abordează fenomenul în mod predominant din perspectivă tehnică, accentul fiind pus pe modalități de extragere și analiză a datelor informatice. Dar sunt mai puține ca număr acele studii care tratează aceste informații prin prisma importanței criminalistice a urmelor digitale și a valorii lor probatorii. Or, pentru criminalistică, interesul nu îl reprezintă existența unor date informatice ca atare, ci capacitatea acestora de a reflecta activități umane, procese tehnice și interacțiuni relevante pentru stabilirea împrejurărilor cauzelor investigate.

În opinia noastră, vehiculul modern trebuie analizat nu numai ca obiect material al cercetării sau ca mijloc utilizat la săvârșirea unei infracțiuni, ci și ca suport de generare și conservare a unor urme digitale. În consecință, obiectul cercetării criminalistice nu îl constituie sistemele electronice în sine, ci informațiile rezultate din funcționarea și utilizarea acestora, în măsura în care ele permit identificarea, explicarea și reconstituirea unor activități cu relevanță pentru procesul penal. Această delimitare contribuie la integrarea urmelor digitale generate de vehicule în sistemul general al urmelor criminalistice, fără a le reduce la simpla categorie a datelor informatice.

Actualitatea temei este determinată de dezvoltarea continuă a tehnologiilor digitale integrate în vehicule și de extinderea posibilităților de conectare a acestora la dispozitive externe și infrastructuri informatice distribuite. Vehiculele moderne includ numeroase sisteme electronice capabile să genereze și să conserve informații referitoare la deplasare, localizare, parametrii tehnici de funcționare, comunicațiile realizate și interacțiunea utilizatorului cu diferitele componente ale vehiculului. În funcție de circumstanțele concrete ale cauzei, aceste informații pot prezenta interes pentru activitatea de urmărire penală, contribuind la verificarea unor versiuni criminalistice, stabilirea succesiunii anumitor activități și reconstituirea împrejurărilor producerii evenimentului cercetat. Coroborate cu celelalte probe administrate în cauză, acestea pot contribui la stabilirea faptelor relevante pentru soluționarea cauzei penale și la formarea convingerii organului de urmărire penală și instanței de judecată cu privire la circumstanțele investigate.

Scopul prezentului studiu este de a fundamenta conceptul criminalistic al urmelor digitale generate de vehicule, identifica principalele categorii ale acestora și evidenția particularitățile cercetării și valorificării lor în procesul penal. Nu vom efectua o descriere inginerească a sistemelor electronice ale vehiculului, ci vom realiza fundamentarea unei abordări criminalistice unitare privind identificarea, ridicarea, examinarea, interpretarea și valorificarea urmelor digitale generate de acestea.

2. METODE ȘI MATERIALE APLICATE

Prezentul studiu are la bază o abordare interdisciplinară, situată la interferența dintre criminalistică, drept procesual penal și domeniul tehnologiilor informaționale aplicate vehiculelor moderne. La realizarea cercetării au fost utilizate metode generale și speciale de cercetare științifică, selectate în funcție de obiectivele și specificul temei abordate. Metoda analizei a fost utilizată pentru examinarea literaturii de specialitate, standardelor și documentelor tehnice relevante privind urmele digitale, sistemele electronice ale vehiculelor și valorificarea informațiilor digitale în investigațiile penale. Metoda sintezei a permis sistematizarea rezultatelor și formularea concluziilor privind locul și rolul urmelor digitale generate de vehicule în cercetarea criminalistică.

Prin metoda comparativă au fost analizate abordările doctrinare și tehnico-criminalistice existente în literatura națională și internațională, fiind evidențiate atât elementele comune ale cercetării probelor digitale, cât și particularitățile generate de specificul vehiculelor conectate. Metoda sistemică a fost utilizată pentru examinarea urmelor di-

gitale ca elemente ale unui ansamblu de reflectări produse de evenimentul investigat, în corelație cu vestigiile materiale, declarațiile persoanelor, înregistrările video și alte mijloace de probă. Rezultatele cercetării sunt fundamentate pe analiza doctrinei, standardelor internaționale și documentelor tehnice relevante, în vederea formulării unor concluzii cu aplicabilitate teoretică și practică pentru activitatea de urmărire penală.

3. DISCUȚII ȘI REZULTATE OBȚINUTE

Conceptul și obiectul cercetării urmelor digitale generate de vehicule. În literatura de specialitate, cercetarea urmelor digitale este analizată preponderent în contextul investigării sistemelor informatice, dispozitivelor mobile și rețelelor de comunicații. În ceea ce privește vehiculele moderne, o parte semnificativă a lucrărilor publicate este orientată spre identificarea surselor de date, metodelor de accesare, conservare și examinare a acestora.[2] În schimb, problematica locului acestor informații în sistemul general al urmelor criminalistice și a valorii lor pentru verificarea versiunilor investigate este analizată într-o măsură mai redusă. Din perspectivă criminalistică, interesul principal nu îl constituie tehnologia în sine, ci capacitatea informațiilor digitale de a contribui la confirmarea sau infirmarea unor versiuni privind modul de producere a evenimentului cercetat.

Considerăm că cercetarea urmelor digitale generate de vehicule trebuie analizată prin raportare la finalitatea generală a criminalisticii: identificarea, examinarea și interpretarea reflectărilor produse de activitatea umană, în vederea reconstituirii evenimentului investigat. În acest sens, cercetarea digitală presupune utilizarea unor metode științifice validate pentru identificarea, colectarea, validarea, analiza, interpretarea, documentarea și prezentarea unor informații digitale, în scopul facilitării reconstituirii evenimentelor relevante pentru investigație.[3]

În opinia noastră, cercetarea urmelor digitale generate de vehicule reprezintă activitatea criminalistică de depistare, extragere, păstrare, examinare, interpretare și valorificare a informațiilor produse, stocate sau transmise de sistemele electronice ale vehiculului, în scopul stabilirii faptelor și împrejurărilor relevante pentru procesul penal. Definiția propusă evidențiază faptul că finalitatea acestei activități nu constă în simpla accesare a datelor, ci în transformarea acestora, prin interpretare criminalistică, în informații utile pentru stabilirea adevărului în cauzele penale investigate.

Din această perspectivă, obiectul cercetării nu îl reprezintă vehiculul în sine și nici componentele sale electronice privite izolat. Acestea constituie suportul pe care se formează și se păstrează anumite informații. Obiectul real al cercetării îl constituie urmele digitale rezultate din funcționarea și utilizarea sistemelor vehiculului, în măsura în care acestea reflectă activități, interacțiuni sau procese care pot contribui la reconstituirea evenimentului investigat, verificarea versiunilor formulate și stabilirea împrejurărilor relevante pentru cauza penală.

Această delimitare permite diferențierea dintre noțiunea de date informatice și cea de urme digitale. Datele informatice reprezintă categoria generală de informații existente într-un sistem electronic, indiferent de utilitatea lor pentru cauză. Urmele digitale constituie numai acea parte a acestor informații care reflectă o activitate, o interacțiune sau un proces și care, prin examinare și interpretare, poate dobândi relevanță criminalistică. Prin urmare, nu orice informație stocată într-un vehicul poate fi calificată drept urmă digitală

[2] Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3rd Edition, Academic Press, Burlington, MA, 2011, pp. 205–206; André Årnes (ed.), Digital Forensics, John Wiley & Sons, Chichester, 2018, pp. 6–7.

[3] André Årnes (ed.), Digital Forensics, John Wiley & Sons, Chichester, 2018, pp. 4–5.

în sens criminalistic.

Pentru delimitarea corectă a obiectului cercetării se impune clarificarea a două aspecte metodologice esențiale. Primul constă în tendința de a reduce cercetarea urmelor digitale la o simplă operațiune tehnică de extragere a datelor, ca și cum obținerea informației ar echivala cu demonstrarea unei împrejurări de fapt. Al doilea privește tendința de a atribui unei informații digitale o valoare probatorie autonomă. În realitate, existența unei informații demonstrează doar că aceasta a fost generată, prelucrată sau conservată de sistem, în timp ce relevanța sa criminalistică rezultă numai din interpretarea și coroborarea cu ansamblul materialului probator administrat în cauză. Literatura privind reconstrucția criminalistică evidențiază faptul că interpretarea probelor trebuie realizată în contextul întregului sistem de date disponibile, iar concluziile formulate să fie raportate atât la explicațiile alternative plauzibile, cât și la limitele inerente ale procesului de interpretare.[4] Cercetarea urmelor digitale generate de vehicule nu trebuie privită ca o simplă activitate tehnică de examinare a sistemelor electronice, ci ca o activitate criminalistică specializată. Obiectul său îl constituie identificarea și interpretarea informațiilor capabile să reflecte mecanismul producerii unui eveniment și să contribuie la stabilirea adevărului în procesul penal.

Urme provenite din sistemele de navigație. Sistemele de navigație integrate în vehiculele moderne constituie una dintre cele mai importante surse de urme digitale, deoarece funcționarea acestora presupune generarea și stocarea continuă a unor date referitoare la deplasarea vehiculului. În funcție de configurația sistemului, de producător și de modul de utilizare, aceste date pot include destinațiile introduse de utilizator, locațiile recent vizitate, traseele parcurse, punctele de oprire, coordonatele geografice asociate anumitor evenimente și istoricul unor deplasări anterioare. Din perspectivă criminalistică, aceste informații prezintă o valoare probatorie semnificativă, deoarece permit stabilirea sau verificarea prezenței unui vehicul într-o anumită locație, reconstruirea secvenței spațio-temporale a unor activități și confruntarea declarațiilor persoanelor implicate cu datele obiective generate de sistem.[5]

Interesul criminalistic al acestor urme nu rezidă exclusiv în identificarea unui punct de plecare sau a unei destinații, ci în posibilitatea de a reconstitui logica deplasării vehiculului. Analiza succesiunii traseelor și a opririlor intermediare poate conduce la identificarea unor locuri relevante pentru cauză, precum puncte de întâlnire, zone de staționare, locuri de transfer al unor bunuri ori locuri în care vehiculul a fost abandonat sau ascuns. În acest sens, „informațiile de navigație pot contribui la verificarea versiunilor formulate în cadrul investigației și la stabilirea cronologiei unor activități relevante pentru cauza penală”[6].

Totuși, interpretarea acestor informații trebuie realizată cu prudență. Existența unei locații memorate în sistem nu demonstrează, prin ea însăși, prezența unei anumite persoane în acel loc și nici săvârșirea unei infracțiuni. Ea atestă doar faptul că sistemul a înregistrat o anumită informație, a cărei semnificație probatorie trebuie stabilită prin raportare la contextul cauzei și prin coroborare cu celelalte elemente probatorii. În lipsa

[4] Chisum W. Jerry, Turvey E. Brent (eds.), Crime Reconstruction, 2nd Edition, Academic Press, Burlington, 2011, pp. 7–8, 205–206.

[5] N.-A. Le-Khac, D. Jacobs, J. Nijhoff, K. Bertens, K.-K.R. Choo, Smart Vehicle Forensics: Challenges and Case Study, Future Generation Computer Systems, vol. 109, 2020, pp. 500–510, manuscris acceptat consultat de autor, pp. 1–2. Disponibil: https://welib.st/md5/241741f55747308dd768643031ab2638. Ebbers S., Ising F., Saatjohann C., Schinzel S., Grand Theft App: Digital Forensics of Vehicle Assistant Apps, ARES 2021, pp. 1–2.

[6] Casey E., Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3rd ed., Academic Press, Burlington, 2011, pp. 205–206; Årnes A. (ed.), Digital Forensics, Wiley, Chichester, 2018, pp. 6–7.

unei asemenea analize, există riscul atribuirii unei semnificații pe care informația, analizată izolat, nu o poate susține.[7]

În practică, eficiența valorificării acestor urme crește considerabil atunci când informațiile extrase din sistemele de navigație sunt comparate cu date provenite din: sistemele de comunicații ale vehiculului, dispozitivele mobile conectate, înregistrările video, declarațiile persoanelor implicate sau alte urme materiale. Considerăm că numai o asemenea abordare integrată permite transformarea informațiilor de localizare din simple date tehnice în urme digitale cu reală valoare criminalistică. Spre exemplu, existența în sistemul de navigație a unei destinații corespunzătoare unei anumite adrese nu demonstrează, prin ea însăși, că vehiculul s-a deplasat efectiv în acel loc și nici că utilizatorul a fost prezent acolo (adresa a fost introdusă, dar deplasarea nu a avut loc; adresa a fost introdusă de alt utilizator al vehiculului; adresa a fost selectată automat din istoricul anterior; adresa a fost căutată doar pentru orientare; adresa a fost importată dintr-un telefon sincronizat; destinația a fost introdusă în cadrul unei deplasări fără relevanță pentru cauză). Însă, dacă aceeași locație este confirmată prin datele de poziționare înregistrate de vehicul, prin conexiunea unui telefon mobil asociat utilizatorului, prin imagini surprinse de sistemele de supraveghere video din zonă și prin alte urme materiale identificate la fața locului, gradul de credibilitate al concluziei crește semnificativ. Într-o asemenea situație, valoarea probatorie nu rezultă dintr-o singură sursă de date, ci din coroborarea mai multor informații independente care reflectă concordant aceeași împrejurare de fapt.

Urme generate de sistemele multimedia și de comunicații ale vehiculului. Sistemele multimedia și de comunicații integrate în vehiculele moderne reprezintă una dintre cele mai dinamice surse de urme digitale, deoarece facilitează schimbul continuu de informații între vehicul, utilizator, dispozitivele mobile și serviciile informatice externe. Integrarea platformelor Apple CarPlay, Android Auto, Bluetooth și Wi-Fi a transformat sistemele infotainment din simple mijloace de confort și divertisment în platforme complexe de procesare, sincronizare și transmitere a datelor. Cercetările recente evidențiază că aceste sisteme pot genera și conserva o gamă variată de artefacte digitale referitoare la dispozitivele conectate, comunicațiile realizate, aplicațiile utilizate, datele de localizare, istoricul navigării, contactele, mesajele și alte activități desfășurate prin intermediul vehiculului. În consecință, sistemele infotainment au devenit o sursă importantă de informații pentru investigațiile criminalistice, interesul cercetătorilor fiind orientat atât către datele stocate local în vehicul, cât și spre informațiile rezultate din comunicațiile realizate cu dispozitive mobile și servicii externe.[8]

Spre deosebire de unitățile electronice de control, care reflectă în principal funcționarea tehnică a vehiculului, sistemele multimedia surprind interacțiunea dintre utilizator și ecosistemul digital al acestuia. În funcție de configurația tehnică și de aplicațiile utilizate, ele pot conserva informații privind dispozitivele conectate, istoricul sincronizărilor, agenda de contacte, istoricul apelurilor telefonice, mesajele, fișierele multimedia, comenzile vocale, aplicațiile utilizate și destinațiile introduse în sistemele de navigație. Literatura dedicată examinării sistemelor In-Vehicle Infotainment (IVI) arată că o parte dintre informațiile sincronizate între dispozitivul mobil și vehicul poate rămâne

[7] Chisum W. Jerry, Turvey E. Brent (eds.), Crime Reconstruction, 2nd ed., Academic Press, Burlington, 2011, pp. 7–8, 205–206. Brian Carrier, File System Forensic Analysis, Addison-Wesley Professional, Boston, 2005, pp. 5–18.

[8] Yeonghun Shin, Sungbum Kim, Wooyeon Jo, Taeshik Shon, Digital Forensic Case Studies for In-Vehicle Infotainment Systems Using Android Auto and Apple CarPlay, Sensors, Vol. 22, No. 19, 2022, pp. 1–4. Disponibil: https://www.researchgate.net/publication/382671362_Digital_Forensic_Analysis_for_Vehicle_Infotainment_Systems_based_on_Packet_Fingerprinting

disponibilă în memoria sistemului chiar și după deconectarea dispozitivului, putând fi recuperată prin metode specifice de examinare criminalistică.[9]

În opinia noastră, particularitatea acestei categorii de urme constă în faptul că ele nu reflectă exclusiv funcționarea unui echipament electronic, ci relațiile create între utilizator, vehicul și infrastructura digitală externă. Din acest motiv, cercetarea criminalistică nu trebuie limitată la examinarea memoriei sistemului multimedia, ci va urmări întregul circuit informațional generat de utilizarea acestuia.

Valoarea criminalistică a acestor informații rezultă din capacitatea lor de a contribui la reconstituirea activităților desfășurate prin intermediul vehiculului. De exemplu, identificarea momentului conectării unui dispozitiv mobil, succesiunea sincronizărilor sau utilizarea unei anumite aplicații pot constitui indici utili pentru verificarea cronologiei faptelor și confruntarea declarațiilor persoanelor implicate cu datele obiective conservate de sistem. Spre exemplu, într-o cauză privind furtul unui autovehicul, examinarea sistemului multimedia poate evidenția că, în intervalul de timp anterior dispariției mijlocului de transport, a fost conectat un telefon mobil care nu aparținea proprietarului. Coroborarea acestei informații cu imaginile surprinse de camerele de supraveghere, precum și cu datele furnizate de operatorii de comunicații electronice sau cu informațiile provenite din aplicația mobilă a producătorului poate contribui la identificarea persoanei care a utilizat vehiculul ori la verificarea relațiilor dintre participanții la faptă. Totuși, simpla existență a unei conexiuni nu demonstrează că titularul acelui dispozitiv a condus vehiculul sau că a participat la săvârșirea infracțiunii.

Importanța practică a acestor urme este evidentă și la investigarea accidentelor rutiere. Astfel, dacă o persoană afirmă că nu a utilizat vehiculul într-un anumit interval de timp, iar sistemul multimedia indică sincronizarea telefonului său și activarea platformei Android Auto sau Apple CarPlay în aceeași perioadă, această informație poate constitui un indiciu obiectiv pentru verificarea declarației. Cu toate acestea, sincronizarea automată a dispozitivului nu dovedește, prin ea însăși, că titularul telefonului conducea efectiv vehiculul, motiv pentru care concluziile trebuie formulate numai după coroborarea cu celelalte mijloace de probă.

Un alt exemplu îl constituie investigarea traficului de droguri sau a traficului de persoane, unde analiza istoricului destinațiilor, dispozitivelor conectate și comunicațiilor realizate prin intermediul sistemului multimedia poate evidenția deplasări repetate către aceleași locații, conectarea succesivă a unor telefoane aparținând unor persoane diferite ori utilizarea acelorași aplicații de comunicații în intervale de timp relevante pentru cauză. Coroborate cu datele de localizare, înregistrările video și celelalte probe administrate, aceste informații pot contribui la reconstituirea modului de organizare și desfășurare a activității infracționale.

Totuși, interpretarea acestor informații trebuie realizată cu prudență. Existența unei conexiuni Bluetooth, Wi-Fi, Android Auto sau Apple CarPlay nu demonstrează, prin ea însăși, că o anumită persoană a utilizat vehiculul și nici că a participat la activitatea investigată. O astfel de conexiune atestă doar faptul că între sistemele respective a existat o interacțiune tehnică la un moment dat. Semnificația criminalistică a unei asemenea informații poate fi stabilită numai prin raportare la contextul concret al cauzei și prin coroborare cu celelalte date relevante pentru investigație.

Urme generate de unitățile electronice de control și rețelele interne ale vehiculului. Analiza literaturii de specialitate evidențiază că majoritatea cercetărilor dedicate

[9] Yeonghun Shin, Seungyoun Kim, Wonjun Jo, Taeshik Shon, Digital Forensic Case Studies for In-Vehicle Infotainment Systems Using Android Auto and Apple CarPlay, Sensors, Vol. 22, No. 19, 2022, pp. 2–4.

unităților electronice de control sunt orientate spre arhitectura tehnică a vehiculelor și metodele de extragere a datelor. În schimb, implicațiile criminalistice ale informațiilor generate de aceste sisteme sunt tratate într-o măsură mai redusă. Din perspectivă criminalistică, interesul nu îl reprezintă unitatea electronică de control ca echipament tehnic, ci urmele digitale pe care funcționarea acesteia le generează și conservă, întrucât acestea pot reflecta activități și evenimente relevante pentru reconstituirea împrejurărilor cauzei.[10]

Unitățile electronice de control (Electronic Control Units – ECU) constituie elementele fundamentale ale arhitecturii informatice a vehiculelor moderne, fiind responsabile de administrarea funcționării motorului, transmisiei, sistemelor de frânare, direcției asistate, controlului stabilității, iluminării, climatizării și numeroaselor sisteme de asistență a conducătorului auto. Din această perspectivă, vehiculul contemporan poate fi privit ca un sistem informațional distribuit, alcătuit din zeci de module electronice specializate care comunică permanent între ele și schimbă în timp real informații privind starea și funcționarea autovehiculului (Wolf, Automotive Software Architectures[11]; Bosch, Automotive Handbook[12]; Nilsson, Automotive Embedded Systems).

Comunicarea dintre aceste module se realizează prin intermediul unor rețele interne, dintre care cele mai răspândite sunt Controller Area Network (CAN), Local Interconnect Network (LIN), FlexRay și Media Oriented Systems Transport (MOST). Din punct de vedere ingineresc, aceste magistrale permit transmiterea comenzilor și sincronizarea funcționării diferitelor sisteme. Din punct de vedere criminalistic însă, importanța acestor rețele rezidă în faptul că prin intermediul lor sunt transmise informații referitoare la funcționarea vehiculului, interacțiunea dintre diferitele unități electronice de control și reacțiile sistemelor la comenzile utilizatorului sau la procesele automate. Din această perspectivă, rețelele interne de comunicații constituie infrastructura prin care sunt generate, transmise și actualizate numeroase date (mesaje, date, comunicații, semnale, rețele electronice) susceptibile de valorificare criminalistică.[13]

În practică, urmele digitale generate de funcționarea vehiculului nu se concentrează într-o singură componentă, ci sunt distribuite în mai multe unități electronice. Astfel, informațiile privind funcționarea motorului sunt gestionate de Engine Control Module (ECM), cele referitoare la transmisie de Transmission Control Module (TCM), iar datele privind funcționarea sistemelor de frânare și stabilitate sunt administrate de modulele ABS și ESP/ESC. Declanșarea sistemelor de protecție este înregistrată de Airbag Control Module (ACM) sau de Supplemental Restraint System (SRS), iar numeroase vehicule moderne sunt echipate și cu Event Data Recorder (EDR), dispozitiv destinat memorării parametrilor tehnici asociați producerii unui impact, denumit frecvent „cutia neagră" a autovehiculului[14].

[10] E. Casey, Digital Evidence and Computer Crime, 3rd ed., Academic Press, 2011, pp. 205–206; A. Årnes (ed.), Digital Forensics, Wiley, 2018, pp. 6–7; W. J. Chisum, B. E. Turvey (eds.), Crime Reconstruction, 2nd ed., Academic Press, 2011, pp. 7–8, 205–206.

[11] Automotive Software Architectures – lucrare consacrată arhitecturii software a vehiculelor moderne, care analizează organizarea sistemelor electronice de control, interacțiunea dintre componentele software și hardware, precum și principiile de dezvoltare a sistemelor distribuite utilizate în autovehicule. Manfred Broy, Ingolf H. Krüger, Alexander Pretschner, Christian Salzmann (eds.), Engineering Automotive Software, Springer, Berlin, 2007.

[12] Automotive Handbook – manual tehnic de referință elaborat de Bosch, care prezintă principiile de funcționare ale sistemelor mecanice, electrice și electronice utilizate în vehiculele moderne, inclusiv arhitectura rețelelor de comunicații și a unităților electronice de control. Robert Bosch GmbH, Bosch Automotive Handbook, 10th Edition, Wiley, Chichester, 2018.

[13] M. Navet, F. Simonot-Lion (eds.), Automotive Embedded Systems Handbook, CRC Press, 2009, pp. 3–21; Robert Bosch GmbH, Bosch Automotive Handbook, 10th ed., Wiley, 2018, pp. 1088–1105; ISO/SAE 21434:2021, Road Vehicles — Cybersecurity Engineering.

[14] Robert Bosch GmbH, Bosch Automotive Handbook, 10th Edition, Wiley, Chichester, 2018, pp. 1048–1105; National Highway Traffic Safety Administration (NHTSA), Event Data Recorder (EDR) Research, Washington, D.C.

Rezultă astfel că aceeași activitate poate genera simultan urme digitale în mai multe componente ale vehiculului. De exemplu, acționarea bruscă a sistemului de frânare poate determina înregistrarea unor informații în: modulul ABS, unitatea de control a motorului, sistemul de stabilitate, EDR în anumite configurații. În opinia noastră, aceasta reprezintă una dintre particularitățile esențiale ale urmelor digitale generate de vehicule: ele sunt urme distribuite, deoarece aceeași acțiune produce reflectări informaționale multiple, conservate în componente diferite ale aceluiași sistem tehnic.

Această particularitate prezintă o importanță practică deosebită pentru investigația criminalistică. Spre exemplu, într-o cauză privind un accident rutier soldat cu victime, conducătorul auto poate declara că a frânat imediat după observarea obstacolului. Examinarea datelor conservate în sistemele electronice ale vehiculului poate evidenția momentul acționării sistemului de frânare, viteza vehiculului înainte de impact, intervenția sistemului ABS, activarea controlului electronic al stabilității și, după caz, parametrii înregistrați de EDR anterior și în timpul coliziunii. Coroborate cu urmele materiale identificate la fața locului, declarațiile persoanelor implicate și concluziile expertizei tehnice, aceste informații pot contribui la reconstituirea dinamicii producerii accidentului și verificarea versiunilor formulate în cauză.[15]

Un alt exemplu îl constituie investigarea fraudelor în domeniul asigurărilor. Dacă persoanele implicate susțin existența unei coliziuni produse la o viteză ridicată, iar analiza unităților electronice evidențiază lipsa activării sistemelor de siguranță sau parametri incompatibili cu mecanismul descris, aceste neconcordanțe pot constitui indicii importante privind caracterul fictiv al evenimentului și vor orienta cercetările către existența unei tentative de obținere frauduloasă a despăgubirilor.

În procesul de interpretare a datelor generate de unitățile electronice de control trebuie evitată atribuirea unei valori probatorii absolute parametrilor tehnici înregistrați de acestea. O valoare privind viteza, turația motorului sau poziția pedalei de accelerație reflectă starea unui sistem într-un anumit moment, însă nu explică, prin ea însăși, mecanismul complet al evenimentului investigat și nici semnificația juridică a acestuia. Semnificația criminalistică a unor asemenea informații poate fi stabilită numai prin interpretarea lor contextuală și coroborarea cu urmele materiale, declarațiile persoanelor, înregistrările video, datele provenite din sistemele multimedia și de navigație, precum și cu celelalte probe administrate în cauză. O asemenea abordare este compatibilă cu principiile generale ale cercetării criminalistice și recomandările formulate în standardele privind identificarea, colectarea, examinarea și interpretarea probelor digitale.[16]

Unitățile electronice de control și rețelele interne ale vehiculului nu trebuie privite exclusiv ca elemente ale arhitecturii tehnice a autovehiculului. Pentru criminalistică, ele reprezintă surse de urme digitale capabile să reflecte procesele și interacțiunile produse în timpul funcționării vehiculului. Tocmai caracterul obiectiv, automat și distribuit al acestor informații conferă o valoare deosebită cercetării lor, fără a justifica însă transformarea acestora într-o probă autonomă sau infailibilă. Valoarea lor probatorie rezultă

[15] Robert Bosch GmbH, Bosch Automotive Handbook, 10th Edition, Wiley, Chichester, 2018, pp. 1048–1105; National Highway Traffic Safety Administration (NHTSA), Event Data Recorder (EDR) Research, Washington, D.C.; W. Jerry Chisum, Brent E. Turvey (eds.), Crime Reconstruction, 2nd Edition, Academic Press, Burlington, 2011, pp. 7–8, 205–206.

[16] Paul L. Kirk, Crime Investigation: Physical Evidence and the Police Laboratory, 2nd Edition, Interscience Publishers, New York, 1963, pp. 1–15; ISO/IEC 27037:2012, Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence; ISO/IEC 27042:2015, Guidelines for the Analysis and Interpretation of Digital Evidence; ENFSI Digital Evidence Working Group, Guideline for Best Practice in the Forensic Examination of Digital Technology, 2018.

numai din analiza critică și din integrarea în ansamblul materialului probator.

Urme generate de comunicațiile externe, sistemele telematice și infrastructura inteligentă. Dacă în trecut cele mai multe informații erau conservate preponderent în sistemele interne ale vehiculului, în prezent o parte importantă a acestora este transmisă, prelucrată și stocată în infrastructuri externe administrate de producătorii de automobile, furnizorii de servicii telematice, operatorii de comunicații sau administratorii infrastructurilor inteligente de transport. În consecință, cercetarea criminalistică a urmelor digitale generate de vehicule nu mai poate fi limitată exclusiv la examinarea sistemelor interne ale acestora, ci trebuie să ia în considerare întregul ecosistem informațional creat de funcționarea vehiculului și de interacțiunea sa cu sistemele externe.[17]

Literatura de specialitate utilizează conceptele Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I) și Vehicle-to-Everything (V2X) pentru a descrie schimbul automat de informații dintre vehicule și mediul extern. Aceste tehnologii au fost dezvoltate pentru sporirea siguranței circulației și optimizarea managementului traficului, însă generează în același timp noi categorii de urme digitale cu relevanță criminalistică. Particularitatea lor constă în faptul că aceeași activitate poate fi reflectată simultan în memoria vehiculului, echipamentele infrastructurii rutiere, serverele operatorilor de servicii și aplicațiile utilizate de proprietar sau conducătorul auto[18].

Sistemele telematice transformă vehiculul într-un element permanent conectat la infrastructuri informatice externe. Platforme precum Mercedes me, BMW ConnectedDrive, Volvo Cars App, OnStar sau Tesla Connectivity permit monitorizarea și administrarea unor funcții ale autovehiculului prin intermediul aplicațiilor mobile și al serviciilor cloud. În funcție de configurația sistemului și de serviciile activate, acestea pot genera și conserva informații privind localizarea vehiculului, starea acestuia, anumite operațiuni efectuate de utilizator, evenimente tehnice, activități de diagnosticare și alte date asociate exploatării vehiculului. Din perspectivă criminalistică, particularitatea acestor informații constă în faptul că ele pot fi conservate în afara vehiculului, pe serverele furnizorilor de servicii sau în aplicațiile utilizate de proprietar ori conducătorul auto.[19]

Din punct de vedere practic, aceste informații nu se regăsesc într-un singur suport digital. O parte poate fi stocată în memoria vehiculului, alta în telefonul mobil al utilizatorului, iar o altă parte pe serverele producătorului sau ale furnizorului serviciului telematic. În anumite situații, date suplimentare pot exista în infrastructura operatorilor de comunicații electronice sau în sistemele inteligente de management al traficului. Prin urmare, aceeași activitate poate genera urme digitale distribuite, aflate în locații diferite și administrate de entități distincte.

Spre exemplu, într-o cauză privind furtul unui autovehicul, aplicația mobilă a producătorului poate indica ultima localizare cunoscută a vehiculului și momentul deblocării

---

[17] Christina Katsini, George E. Raptis, Christos Alexakos, Dimitrios Serpanos, FoRePlan: Supporting Digital Forensics Readiness Planning for Internet of Vehicles, PCI 2021, pp. 369–370; József Répás, Examining the Application of Drone Forensics Methodology on Highly Automated Civil and Military Vehicles, Hadmérnök, Vol. 19, No. 2, 2024, pp. 17–19; ISO/IEC 27037:2012, Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence.

[18] Rawtani, Deepak, „Vehicle Forensics", în Modern Forensic Tools and Devices: Trends in Criminal Investigation, CRC Press, pp. 68–69.
Katsini, Christina; Raptis, George E.; Alexakos, Christos; Serpanos, Dimitrios, „FoRePlan: Supporting Digital Forensics Readiness Planning for Internet of Vehicles", Proceedings of PCI 2021, ACM, 2021, pp. 368–369.

[19] S. Ebbers, F. Ising, C. Saatjohann, S. Schinzel, Grand Theft App: Digital Forensics of Vehicle Assistant Apps, Proceedings of the 16th International Conference on Availability, Reliability and Security (ARES 2021), 2021, pp. 2–4; Christina Katsini, George E. Raptis, Christos Alexakos, Dimitrios Serpanos, FoRePlan: Supporting Digital Forensics Readiness Planning for Internet of Vehicles, PCI 2021, pp. 369–370.

acestuia, în timp ce serverele serviciului telematic pot conserva informații privind deplasările ulterioare sau comenzile executate de la distanță. Coroborate cu datele extrase din sistemul de navigație și imaginile surprinse de camerele de supraveghere, aceste informații pot contribui la reconstituirea traseului parcurs și identificarea persoanelor implicate.

Un alt exemplu poate fi întâlnit la investigarea traficului de droguri sau a traficului de persoane, unde vehiculul este utilizat ca mijloc de transport și coordonare logistică. Analiza datelor telematice poate evidenția deplasări repetitive către aceleași locații, opriri de scurtă durată, activarea unor funcții la distanță sau sincronizarea cu anumite dispozitive mobile. Coroborate cu datele operatorilor de comunicații, cu înregistrările video și cu celelalte mijloace de probă, aceste informații pot contribui la reconstituirea modului de organizare și desfășurare a activității infracționale.

În opinia noastră, principala particularitate a urmelor generate de comunicațiile externe constă în dispersia lor informațională. Spre deosebire de urmele clasice, acestea nu sunt localizate într-un singur suport și nici nu aparțin unui singur deținător. Investigatorul trebuie să identifice toate sursele potențiale de date și să stabilească relațiile dintre acestea. Din acest motiv, obiectul cercetării nu îl constituie un anumit suport digital, ci ansamblul reflecțiilor informaționale generate de aceeași activitate și distribuite în ecosistemul tehnologic al vehiculului.

Această caracteristică impune aplicarea unei metodologii integrate de cercetare. Informațiile extrase din vehicul trebuie comparate cu cele provenite de la aplicațiile mobile, serviciile cloud, operatorii de comunicații, infrastructura inteligentă de transport și alte sisteme externe. Concordanța dintre aceste surse poate consolida concluziile investigației, iar eventualele neconcordanțe trebuie analizate critic, deoarece pot fi determinate de diferențele dintre momentele de actualizare a datelor, limitele tehnice ale sistemelor sau intervențiile ulterioare asupra informațiilor. Considerăm că numai o asemenea abordare integrată permite valorificarea eficientă a urmelor digitale generate de vehiculele conectate și evitarea concluziilor bazate pe analiza izolată a unei singure surse de informații.

Urme generate de interacțiunea utilizatorului cu vehiculul. Activitatea desfășurată de utilizator prin intermediul sistemelor electronice ale vehiculului generează urme digitale care reflectă interacțiunea dintre persoană și infrastructura informatică a autovehiculului. Introducerea unei destinații, conectarea unui telefon mobil, sincronizarea unui cont, efectuarea unei convorbiri, accesarea unei aplicații, redarea unui fișier multimedia sau modificarea unor setări pot furniza informații utile investigației. Cercetările recente dedicate aspectelor criminalistice ale sistemelor infotainment demonstrează că aceste platforme pot conserva istoricul destinațiilor, informații privind utilizarea Android Auto și Apple CarPlay, date referitoare la dispozitivele mobile asociate, istoricul aplicațiilor utilizate, configurațiile de conectare și diferite înregistrări privind interacțiunea utilizatorului cu serviciile digitale integrate în vehicul.[20]

Din punct de vedere criminalistic, această categorie de urme impune o distincție esențială: urma digitală poate demonstra existența unei activități informatice, dar nu identifică automat persoana care a realizat-o. Stabilirea autorului unei operațiuni presupune coroborarea informațiilor digitale cu alte date: urme materiale, declarații, imagini video, localizări independente, profiluri de utilizator, dispozitive conectate sau date

[20] Haein Kang, Hojun Seong, Ilkyu Kim, Wookjae Jeong, Seong-Je Cho, Minkyu Park, Sangchul Han, „Android-Based Audio Video Navigation System Forensics: A Case Study", Applied Sciences, Vol. 13, No. 10, 2023, pp. 3–8.

provenite din infrastructuri externe. În acest sens, Casey E. subliniază că datele informatice trebuie interpretate în contextul tuturor circumstanțelor cauzei și al celorlalte probe administrate, deoarece aceeași activitate digitală poate admite explicații factuale diferite.[21] Examinările efectuate asupra sistemelor infotainment moderne au demonstrat că informațiile privind dispozitivele asociate, istoricul apelurilor, contactele sincronizate și momentele conectării pot contribui la stabilirea unei legături între utilizator și vehicul, însă numai prin coroborarea acestora cu alte categorii de probe[22].

Această precizare este deosebit de importantă în cazul vehiculelor utilizate succesiv de mai multe persoane, vehiculelor de serviciu și celor închiriate sau la care sunt conectate simultan ori succesiv mai multe dispozitive. În asemenea cazuri, aceeași platformă informatică poate conserva urme aparținând mai multor utilizatori, iar delimitarea lor necesită analiză contextuală și evaluare critică. Practica criminalistică relevă faptul că sistemele infotainment pot stoca informații privind dispozitivele conectate, istoricul conexiunilor Bluetooth, contactele sincronizate, jurnalele apelurilor, mesajele, destinațiile de navigație și istoricul interacțiunilor cu aplicațiile mobile, toate acestea putând aparține unor utilizatori diferiți care au utilizat vehiculul în perioade distincte[23].

Particularitatea acestor urme constă în faptul că ele reflectă, în principal, comportamentul utilizatorului și nu exclusiv funcționarea tehnică a vehiculului. Dacă informațiile generate automat de senzorii și modulele electronice ale vehiculului descriu starea și funcționarea unor sisteme tehnice, datele rezultate din interacțiunea utilizatorului pot evidenția intenții, preferințe, relații și modele comportamentale. Introducerea repetată a anumitor destinații, conectarea constantă a aceluiași dispozitiv mobil sau utilizarea recurentă a unor servicii și aplicații pot constitui indicatori relevanți pentru reconstituirea activităților desfășurate anterior și stabilirea unor conexiuni între utilizator și vehicul. Din perspectiva teoriei urmelor digitale, aceste informații reprezintă materializarea unor interacțiuni dintre utilizator și mediul informatic, susceptibile de identificare, conservare și interpretare criminalistică.[24]

În practică, examinarea criminalistică a acestor urme presupune identificarea și extragerea informațiilor stocate atât în sistemele infotainment și modulele telematice ale vehiculului, cât și în dispozitivele mobile asociate ori în serviciile externe cu care acestea comunică. Cercetările recente privind criminalistica vehiculelor conectate evidențiază faptul că aceeași activitate a utilizatorului poate genera simultan urme digitale în: memoria sistemului infotainment, dispozitivul mobil asociat și infrastructura cloud a furnizorului de servicii, ceea ce impune o abordare integrată a procesului de identificare, conservare, examinare și interpretare a urmelor digitale[25]. Spre exemplu, un autoturism utilizat de membrii aceleiași familii este implicat într-un accident rutier soldat cu părăsirea locului accidentului. Proprietarul susține că la volan se afla o altă persoană. Examinarea sistemului infotainment evidențiază că, cu câteva minute înainte de producerea accidentului, vehiculul era conectat la telefonul proprietarului, fiind accesată lista sa de contacte și efectuat un apel prin interfața vehiculului. De asemenea, sistemul păstrea-

[21] Casey, E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 3rd ed. Academic Press, 2011.
[22] Shin, Yeonghun & Yu, Geon & Shon, Taeshik. Digital Forensic Analysis for Vehicle Infotainment Systems based on Packet Fingerprinting. 2024. 10.21203/rs.3.rs-4664910/v1.
[23] Yoon, Y. et al. Forensic Investigation of an Android Jellybean-Based Car AVN System Installed in Kia K5. DFRWS APAC Proceedings, 2024. p. 118–123.
[24] Carrier, B. File System Forensic Analysis. Addison-Wesley, 2005. p. 11–14. Garfinkel, S. L. Digital Forensics Research: The Next 10 Years. Digital Investigation, 2010, Vol. 7(S), p. S65–S68.
[25] Cho, S. et al. Forensic Investigation of Vehicle-Related Data in Android Devices. Computer Networks, 2025. p. 8–12; ISO/IEC 27037:2012, p. 5–8; NIST SP 800-86, 2006, p. 3–5.

ză profilul de utilizator activ și istoricul comenzilor vocale asociate aceluiași dispozitiv. Aceste informații nu identifică în mod direct conducătorul auto, însă constituie indicii relevante privind persoana care utiliza vehiculul în intervalul de timp analizat și pot fi coroborate cu imaginile video, datele de localizare și alte mijloace de probă. Totodată, s-a constatat că persoana a fost singură în autoturism, fără pasageri.

Urme generate de sistemele de siguranță și de înregistratoarele de evenimente. Sistemele de siguranță activă și pasivă ale vehiculului generează o categorie distinctă de urme digitale, caracterizate prin faptul că sunt produse automat de infrastructura electronică a mijlocului de transport în procesul monitorizării condițiilor de deplasare și al reacției la evenimente critice. Din această categorie fac parte sistemele de antiblocare a frânelor (Anti-lock Braking System – ABS), sistemele electronice de control al stabilității (Electronic Stability Control – ESC/ESP), sistemele de frânare automată de urgență (Automatic Emergency Braking – AEB), sistemele de avertizare privind coliziunea frontală (Forward Collision Warning – FCW), sistemele de menținere a benzii de circulație (Lane Keeping Assist – LKA), controlul adaptiv al vitezei (Adaptive Cruise Control – ACC) și alte funcții avansate de asistență a conducătorului auto incluse în categoria ADAS (Advanced Driver Assistance Systems). Funcționarea acestora presupune colectarea și procesarea continuă a informațiilor provenite de la senzori, camere video, radare și alte dispozitive electronice integrate în arhitectura vehiculului.[26]

În procesul funcționării, aceste sisteme generează și conservă informații referitoare la viteza vehiculului, accelerație, frânare, poziția volanului, stabilitatea direcțională, intervențiile sistemelor electronice de control, detectarea obstacolelor și reacțiile automate ale vehiculului la anumite situații de trafic. Din perspectivă criminalistică, aceste date prezintă o importanță deosebită, deoarece permit reconstituirea unor secvențe de evenimente care au precedat, însoțit sau urmat producerii unui accident rutier. Literatura de specialitate subliniază că sistemele ADAS au transformat vehiculul modern într-o sursă complexă de informații digitale, capabilă să reflecte nu doar starea tehnică a autovehiculului, ci și interacțiunea acestuia cu mediul rutier și cu ceilalți participanți la trafic.[27]

O importanță aparte o prezintă Event Data Recorder (EDR), dispozitiv sau funcție integrată în sistemele electronice ale vehiculului, destinată înregistrării automate a unor parametri tehnici relevanți în cazul producerii unui eveniment semnificativ. Potrivit reglementărilor federale americane privind înregistratoarele de evenimente, EDR reprezintă un sistem capabil să înregistreze date dinamice referitoare la funcționarea vehiculului într-un interval temporal imediat anterior, concomitent și ulterior producerii unei coliziuni sau unui eveniment declanșator stabilit de producător[28]. În funcție de configurația vehiculului, aceste date pot include viteza de deplasare, poziția pedalei de accelerație, utilizarea sistemului de frânare, turația motorului, intervențiile sistemelor ABS și ESC, utilizarea centurilor de siguranță, poziția persoanelor din vehicul și activarea airbagurilor.[29]

Valoarea criminalistică a datelor EDR derivă din caracterul lor automat și din faptul că acestea sunt generate independent de voința utilizatorului. Spre deosebire de declarațiile persoanelor implicate într-un accident sau de alte surse de informații susceptibile unor erori de percepție ori memorie, datele înregistrate de sistemele electronice

[26] Daily, Jeremy; Shigemura, Hiroyuki; Peterson, Nathan. Forensic Examination of Electronic Vehicle Systems. 3rd Edition. Academic Press, 2021, 394 p.
[27] Le-Khac, Jacobs, Nijhoff, Bertens & Choo, 2020, p. 503–506.
[28] National Highway Traffic Safety Administration (NHTSA), Event Data Recorders, 49 CFR Part 563, Code of Federal Regulations, Title 49 – Transportation, Washington, D.C. Disponibil: https://www.ecfr.gov/current/title-49/subtitle-B/chapter-V/part-563
[29] Daily, Shigemura & Peterson, 2021, p. 81–88.

reflectă reacția tehnică a vehiculului la condițiile concrete de deplasare. Din acest motiv, ele sunt utilizate frecvent pentru reconstrucția accidentelor rutiere și verificarea unor ipoteze privind mecanismul producerii evenimentului.

De exemplu, într-o cauză penală privind un accident rutier soldat cu vătămarea gravă a unei persoane, conducătorul auto poate declara că a observat pericolul din timp, a frânat energic și a încercat să evite impactul. Analiza datelor extrase din EDR poate demonstra însă că, în ultimele cinci secunde anterioare coliziunii, vehiculul circula cu o viteză superioară celei declarate, pedala de accelerație era încă acționată, iar sistemul de frânare nu a fost activat decât cu o fracțiune de secundă înainte de impact.[30] Coroborate cu urmele de la locul accidentului și cu expertiza auto-tehnică, asemenea informații pot contribui la stabilirea modului real de producere a evenimentului și verificarea veridicității declarațiilor persoanelor implicate.

Cu toate acestea, datele generate de sistemele de siguranță și înregistratoarele de evenimente nu trebuie considerate infailibile. Parametrii înregistrați reflectă doar informațiile selectate de producător pentru monitorizare și sunt condiționați de particularitățile tehnice ale sistemului analizat. În consecință, interpretarea lor necesită cunoașterea: arhitecturii electronice a vehiculului; algoritmilor de funcționare a sistemelor implicate; semnificației tehnice a fiecărui parametru înregistrat. Daily, Shigemura și Peterson subliniază că interpretarea datelor EDR trebuie realizată cu precauție, deoarece aceeași valoare tehnică poate avea semnificații diferite în funcție de modelul vehiculului, versiunea software și condițiile concrete în care a fost generată[31].

Din perspectiva teoriei urmelor electronice, informațiile generate de sistemele de siguranță și de înregistratoarele de evenimente reprezintă configurații informaționale create automat în urma interacțiunii dintre vehicul și mediul său operațional. Aceste urme permit reconstituirea unor secvențe de activitate tehnică și oferă informații relevante privind comportamentul vehiculului în momente critice. Cu toate acestea, semnificația lor probatorie poate fi stabilită numai prin coroborarea cu alte categorii de probe, inclusiv urmele materiale identificate la locul accidentului, avariile vehiculelor, datele provenite din alte module electronice, înregistrările video și concluziile expertizelor tehnice. Analiza detaliată a acestor informații permite valorificarea corectă a urmelor generate de sistemele de siguranță și înregistratoarele de evenimente în procesul de investigare criminalistică.[32]

Particularități practice ale cercetării și valorificării urmelor digitale generate de vehicule. Analiza categoriilor de urme digitale generate de vehiculele moderne evidențiază existența unor particularități practice care influențează atât procesul de identificare și examinare a acestora, cât și modul de valorificare a rezultatelor în cadrul investigației criminalistice. Aceste particularități derivă din caracteristicile tehnice ale vehiculului contemporan, care funcționează ca un ecosistem informațional complex, alcătuit din unități electronice de control, sisteme de comunicații, senzori, platforme telematice, aplicații mobile și servicii externe interconectate.

Prima particularitate este dispersia informațională a urmelor digitale. Spre deosebire de urmele clasice, care sunt localizate într-un anumit suport fizic, informațiile generate de vehicule pot fi distribuite simultan în mai multe sisteme și medii de stocare. O singură acțiune desfășurată de utilizator poate produce înregistrări în: sistemul de navigație, modulele electronice de control, sistemul infotainment, telefonul mobil conectat, aplicația

[30] Daily, Shigemura & Peterson, 2021, p. 88–92.
[31] Daily, Shigemura & Peterson, 2021, p. 91–96.
[32] Casey, 2011, p. 530–534; ISO/IEC 27037:2012, p. 5–8. Disponibil: https://www.iso.org/standard/44381.html

producătorului și infrastructura cloud asociată vehiculului. Din acest motiv, examinarea unei singure surse oferă, de regulă, doar o imagine parțială asupra circumstanței cercetate. Studii recente dedicate cercetării urmelor electronice ale vehiculelor conectate arată că informații relevante pentru investigație sunt frecvent distribuite între sistemele interne ale vehiculului, dispozitivele utilizatorului și serviciile externe, ceea ce impune o abordare integrată a procesului de examinare.[33]

A doua particularitate este caracterul dinamic al datelor. Urmele digitale generate de vehicul nu reprezintă configurații informaționale statice, ci sunt susceptibile de modificare continuă ca urmare a utilizării ulterioare a vehiculului, sincronizării cu dispozitive externe, actualizărilor software, funcționării serviciilor cloud sau mecanismelor automate de suprascriere a memoriei. În consecință, intervalul de timp dintre producerea evenimentului investigat și efectuarea cercetărilor poate influența semnificativ cantitatea și calitatea informațiilor disponibile. Din această perspectivă, identificarea rapidă a surselor relevante și conservarea (fixarea) datelor în condiții adecvate constituie cerințe esențiale ale investigării criminalistice. Standardul ISO/IEC 2703[34] evidențiază că valoarea probatorie a datelor digitale depinde direct de modul în care acestea sunt identificate, colectate și conservate încă din fazele inițiale ale investigației.

A treia particularitate privește integritatea și trasabilitatea examinării. Procesul de identificare, colectare, extragere și analiză a datelor trebuie realizat astfel încât să excludă riscul modificării informațiilor originale și să permită verificarea ulterioară a rezultatelor obținute. În cazul vehiculelor moderne, această cerință prezintă o importanță sporită, deoarece simpla conectare la anumite sisteme, pornirea vehiculului sau accesarea unor interfețe software poate genera noi înregistrări ori modifica informațiile existente. Din acest motiv, documentarea etapelor de lucru, păstrarea „lanțului de custodie", utilizarea unor metode reproductibile și înregistrarea instrumentelor tehnice folosite reprezintă condiții necesare pentru asigurarea credibilității concluziilor formulate de specialist sau expert.[35]

O a patra particularitate se referă la interpretarea datelor obținute. Informațiile digitale nu posedă o semnificație probatorie automată și nu trebuie confundate cu faptele pe care „par să le descrie". O locație memorată într-un sistem de navigație nu demonstrează prin ea însăși prezența unei anumite persoane într-un loc; o conexiune Bluetooth nu identifică automat utilizatorul vehiculului; iar un parametru tehnic înregistrat de un sistem electronic nu explică în mod autonom mecanismul producerii unui accident. Fiecare informație trebuie analizată în contextul concret al cauzei, prin raportare la condițiile tehnice în care a fost generată și la celelalte probe administrate. După cum remarcă Casey, valoarea unei probe digitale rezultă nu din existența izolată a datelor, ci din capacitatea acestora de a fi interpretate în contextul investigației.[36]

Aceste particularități conduc la necesitatea adoptării unei abordări integrate a valorificării urmelor digitale generate de vehicule. În acest context poate fi formulat un principiu practic al investigației criminalistice, denumit convergență informațională –procesul de confirmare reciprocă a unei împrejurări relevante prin intermediul unor surse independente de informații. O concluzie investigativă dobândește un grad superior de credibilitate atunci când aceeași împrejurare este reflectată concordant de mai multe categorii de date: informații extrase din vehicul, date provenite din dispozitive mobile, în-

[33] Le-Khac, Jacobs, Nijhoff, Bertens & Choo, 2020, p. 503–506; Daily, Shigemura & Peterson, 2021, p. 73–80.
[34] ISO/IEC 27037:2012, p. 5–8.
[35] Casey, 2011, p. 23–25; NIST SP 800-86, 2006, p. 3–5. Disponibil: https://csrc.nist.gov/pubs/sp/800/86/final?utm
[36] Casey, 2011, p. 23–25.

registrări telematice, imagini video, urme materiale și declarații ale persoanelor implicate.

De exemplu, stabilirea prezenței unui vehicul într-o anumită locație poate rezulta din coroborarea istoricului de navigație, datelor GPS, informațiilor telematice, localizării dispozitivului mobil conectat, imaginilor surprinse de camerele de supraveghere și urmelor materiale identificate la fața locului. În asemenea situații, credibilitatea concluziei nu este determinată de existența unei singure înregistrări, ci de convergența unor surse independente care descriu aceeași realitate. În mod similar, eventualele neconcordanțe dintre surse nu trebuie ignorate, ci analizate critic, deoarece pot indica existența unor erori tehnice, utilizarea vehiculului de către persoane diferite, sincronizări automate, modificări ale datelor sau versiuni criminalistice insuficient fundamentate științific.

Prin urmare, cercetarea urmelor digitale generate de vehicule nu trebuie redusă la identificarea și extragerea informațiilor stocate în sistemele electronice. Valoarea criminalistică a acestor urme derivă din capacitatea investigatorului de a integra date provenite din surse multiple, verifica autenticitatea și semnificația lor, precum și de a le interpreta în raport cu ansamblul circumstanțelor cauzei. În acest sens, convergența informațională (în dreptul procesual penal acest termen se asociază cu coroborarea probelor) reprezintă nu doar o metodă practică de lucru, ci și un criteriu de apreciere a forței probatorii a urmelor digitale generate de vehiculele moderne.

Valoarea probatorie, limitele interpretării și verificarea versiunilor. Urmele digitale generate de vehicule pot avea o valoare probatorie semnificativă în procesul de verificare a versiunilor formulate în cadrul urmăririi penale. Informațiile extrase din sistemele de navigație, modulele electronice de control, sistemele infotainment, dispozitivele telematice, înregistratoarele de evenimente și aplicațiile asociate vehiculului pot contribui la stabilirea unor împrejurări relevante privind utilizarea vehiculului, traseul parcurs, momentul și durata deplasării, locațiile vizitate, dispozitivele conectate, funcțiile activate sau reacțiile sistemelor electronice în anumite situații de trafic.[37] În numeroase cazuri, aceste informații permit confirmarea sau infirmarea unor declarații ale persoanelor implicate și oferă investigatorului repere obiective pentru verificarea ipotezelor formulate în cauză.

Valoarea principală a acestor urme constă în capacitatea lor de a reflecta activități și evenimente desfășurate anterior examinării. Sistemele electronice ale vehiculului conservă frecvent informații referitoare la operațiuni efectuate în mod automat sau ca urmare a interacțiunii utilizatorului, ceea ce permite reconstituirea unor secvențe temporale și identificarea unor relații între persoane, vehicule, dispozitive și locații. În acest sens, urmele digitale pot contribui la verificarea unor afirmații privind prezența vehiculului într-un anumit loc, utilizarea sa într-un anumit interval de timp sau asocierea acestuia cu anumite dispozitive și conturi digitale.[38]

Cu toate acestea, interpretarea informațiilor obținute impune o abordare prudentă și critică. Sistemele electronice reflectă interacțiuni tehnice și procese informatice, nu intenții, motive sau conduite în sens juridic. O locație memorată într-un sistem de navigație demonstrează existența unei operațiuni informatice de introducere sau procesare a unei destinații, dar nu dovedește automat deplasarea efectivă a vehiculului către acel loc. În mod similar, existența unei conexiuni Bluetooth indică asocierea unui dispozitiv cu sistemul vehiculului, fără a demonstra în mod necesar identitatea persoanei care l-a utilizat. Aceeași urmă digitală poate admite mai multe explicații compatibile din punct de vedere tehnic: utilizare obișnuită, sincronizare automată, testare a sistemului, actualizare software, utilizare a vehiculului de către o altă persoană sau chiar generare automată a

[37] Daily, Shigemura & Peterson, 2021, p. 81–92.
[38] Casey, 2011, p. 530–534.

unor date de către sistemele informatice ale vehiculului. Din acest motiv, alegerea unei explicații nu poate fi fundamentată pe simple presupuneri, ci trebuie să rezulte din analiza critică a întregului material probator.[39]

O limită importantă a interpretării rezultă și din caracterul selectiv al datelor conservate. Sistemele electronice ale vehiculelor nu înregistrează întreaga activitate desfășurată, ci doar anumite categorii de informații stabilite prin arhitectura tehnică și configurația software a fiecărui model. În plus, unele date pot fi șterse, suprascrise, modificate prin actualizări sau distribuite între mai multe sisteme și servicii externe. Prin urmare, absența unei anumite informații nu poate fi interpretată automat ca dovadă a inexistenței unui fapt sau a unei activități. În criminalistică, lipsa unei urme trebuie evaluată cu aceeași prudență ca și existența acesteia, fiind necesară analiza condițiilor tehnice care au putut influența generarea, conservarea sau pierderea informației.[40]

În procesul verificării versiunilor, urmele digitale generate de vehicule prezintă o utilitate deosebită, deoarece permit confruntarea afirmațiilor persoanelor implicate cu date obiectivate tehnic. Astfel, declarația unei persoane privind traseul urmat poate fi verificată prin analiza datelor de navigație și informațiilor telematice; susținerea că vehiculul nu a fost utilizat într-un anumit interval poate fi verificată prin examinarea jurnalelor de activitate ale sistemelor electronice; afirmațiile referitoare la împrejurările producerii unui accident pot fi confruntate cu informațiile înregistrate de sistemele ADAS și EDR. În asemenea situații, urmele digitale nu oferă întotdeauna răspunsuri definitive, însă permit confirmarea, infirmarea sau reformularea versiunilor criminalistice și contribuie la delimitarea explicațiilor plauzibile de cele incompatibile cu datele obiective disponibile.[41]

Totodată, urmele digitale nu substituie celelalte activități procesuale de colectare a probelor și nu trebuie transformate într-o categorie privilegiată de probe. Valoarea lor rezultă din integrarea în ansamblul probator și din coroborarea cu urmele materiale, documentele, înregistrările video, declarațiile persoanelor, rezultatele expertizelor și celelalte informații relevante pentru cauză. Numai această abordare permite reconstituirea cât mai fidelă a mecanismului producerii unui eveniment și formularea unor concluzii fundamentate științific.

În acest context, principiul convergenței informaționale, formulat anterior, dobândește o importanță practică deosebită. O concluzie a investigatorului devine cu atât mai credibilă cu cât este susținută de un număr mai mare de surse independente și concordante. Dimpotrivă, existența unor date numeroase, dar necoroborate, poate crea doar aparența certitudinii. Astfel, valoarea urmelor digitale generate de vehicule nu rezidă în volumul informațiilor conservate, ci în capacitatea acestora de a reflecta activități relevante și de a se integra într-un sistem coerent de date convergente care susțin același detaliu sau circumstanță. Prin urmare, obiectivul investigatorului nu este acumularea mecanică a unor cantități cât mai mari de date, ci identificarea și interpretarea acelor informații care contribuie efectiv la verificarea versiunilor și stabilirea adevărului în cauză.

Locul urmelor digitale generate de vehicule în sistemul general al urmelor în criminalistică. Dezvoltarea tehnologiilor integrate în vehicule nu modifică principiile fundamentale ale criminalisticii, ci extinde sfera suporturilor pe care activitatea umană se poate reflecta, conserva și ulterior examina. În teoria generală a urmelor, orice activitate produce modificări ale mediului, iar aceste modificări pot dobândi relevanță criminalistică atunci când sunt susceptibile de identificare, fixare, examinare și interpretare. În cazul

[39] Casey, 2011, p. 23–25.
[40] ISO/IEC 27037:2012, p. 5–8; NIST SP 800-86, 2006, p. 3–5.
[41] Daily, Shigemura & Peterson, 2021, p. 88–96.

vehiculelor moderne, o parte importantă a acestor schimbări nu se mai manifestă exclusiv sub forma urmelor materiale, specifice traseologiei judiciare, ci prin informații conservate în sisteme electronice, unități de control, medii de stocare, aplicații mobile, platforme telematice și infrastructuri externe.

Prin urmare, urmele digitale generate de vehicule nu trebuie privite ca un domeniu separat de criminalistică, rupt de teoria generală a urmelor. Ele reprezintă o manifestare particulară a procesului general de reflectare, diferența fiind determinată de natura suportului pe care se conservă informația și de metodele tehnice necesare pentru identificarea, extragerea și examinarea acesteia. Dacă urma materială clasică (urmă formă sau urmă materie) exprimă o modificare produsă asupra unui suport fizic perceptibil nemijlocit, urma digitală exprimă o modificare informațională produsă și conservată în cadrul unui sistem electronic. Această perspectivă permite integrarea urmelor digitale generate de vehicule în sistemul general al urmelor criminalistice. Principiile de bază ale cercetării criminalistice precum legalitatea, obiectivitatea, integritatea, trasabilitatea, interpretarea contextuală, coroborarea și verificabilitatea rămân aplicabile indiferent dacă urma se conservă pe un suport material tradițional sau într-o infrastructură electronică. Particularitatea urmelor digitale nu justifică abandonarea acestor principii, ci impune adaptarea metodelor de lucru la specificul suporturilor informatice și al sistemelor conectate.

O asemenea abordare permite evitarea unei duble confuzii. Pe de o parte, cercetarea urmelor digitale generate de vehicule nu trebuie redusă la informatică aplicată sau la simpla extragere tehnică a datelor. Pe de altă parte, aceste urme nu trebuie separate artificial de criminalistica tradițională, deoarece ele exprimă același fenomen fundamental al reflectării activității umane în mediul înconjurător. Diferența constă în faptul că mediul în care se produce reflectarea include astăzi sisteme electronice, rețele de comunicații, aplicații mobile și servicii digitale externe. Din această perspectivă, cercetarea urmelor digitale generate de vehicule trebuie înțeleasă ca o dezvoltare firească a criminalisticii, determinată de noile modalități prin care activitatea umană, funcționarea tehnică a vehiculului și interacțiunea cu infrastructurile externe se obiectivează în forme informaționale. Vehiculul modern devine astfel nu doar un obiect material al cercetării criminalistice, ci și o sursă complexă de date, în care se reflectă itinerare, conexiuni, acțiuni ale utilizatorului, reacții ale sistemelor de siguranță și comunicări cu medii digitale externe.

În consecință, locul urmelor digitale generate de vehicule în sistemul general al urmelor criminalistice este acela al unei categorii particulare de urme informaționale, formate și conservate în medii electronice, dar supuse acelorași exigențe metodologice generale ale criminalisticii. Valoarea lor nu rezultă doar din caracterul tehnologic al suportului, ci din posibilitatea de a fi integrate într-un proces riguros de identificare, conservare, examinare, interpretare și coroborare cu celelalte categorii de probe.

4. CONCLUZII

Cercetarea realizată evidențiază că evoluția tehnologiilor integrate în vehicule a determinat apariția unor surse noi de urme digitale, relevante pentru investigarea infracțiunilor și altor evenimente cu semnificație juridică. Sistemele de navigație, platformele multimedia, unitățile electronice de control, rețelele interne de comunicații, sistemele telematice, aplicațiile mobile și sistemele de siguranță pot furniza informații utile pentru stabilirea împrejurărilor cauzei și reconstituirea mecanismului producerii evenimentului investigat.

Valoarea criminalistică și procesuală a acestor urme nu rezultă din simpla existență a informațiilor în sistemele electronice ale vehiculului, ci din identificarea, conservarea,

examinarea, interpretarea și coroborarea informațiilor obținute din acestea cu datele rezultate din celelalte categorii de urme și din celelalte mijloace de probă administrate în cauză. Urmele digitale generate de vehicule trebuie apreciate ca reflectări informaționale ale activităților desfășurate prin intermediul acestora, nu ca dovezi autonome, absolute sau indubitabile ale unor împrejurări de fapt.

O concluzie importantă a studiului constă în caracterul distribuit al acestor urme. Aceeași activitate poate fi reflectată simultan în: vehicul, dispozitive conectate, aplicații mobile, platforme telematice și infrastructuri informatice externe. Această particularitate impune o abordare integrată a cercetării și aplicarea principiului convergenței informaționale. Potrivit acestui principiu, concluziile criminalistice sunt mai solide atunci când mai multe surse independente reflectă concordant aceeași împrejurare.

În același timp, interpretarea urmelor digitale generate de vehicule trebuie realizată cu prudență. O locație memorată, o conexiune între vehicul și un telefon mobil, o comandă transmisă printr-o aplicație sau un parametru tehnic înregistrat de un sistem de siguranță nu identifică automat autorul unei fapte și nu explică, prin sine, semnificația juridică a evenimentului. Fiecare informație trebuie analizată critic, în raport cu contextul cauzei, limitele tehnice ale sistemului examinat și posibilele explicații alternative.

Urmele digitale generate de vehicule trebuie integrate în sistemul general al cercetării criminalistice a urmelor. Particularitatea lor nu constă într-un mecanism fundamental diferit de formare, ci în suportul informațional pe care se conservă și metodele tehnice necesare examinării. Din această perspectivă, dezvoltarea vehiculelor conectate și autonome nu impune abandonarea principiilor criminalisticii, ci adaptarea acestora la noile forme de reflectare a activității umane în mediul tehnologic.

În perspectivă, se impune elaborarea unor proceduri unitare privind identificarea, conservarea, examinarea și interpretarea urmelor digitale generate de vehicule, precum și dezvoltarea unei metodologii criminalistice care să integreze datele provenite din vehicul, dispozitive conectate, infrastructuri externe și surse materiale tradiționale. Numai o asemenea abordare poate asigura valorificarea eficientă, riguroasă și verificabilă a acestor urme în activitatea organelor de urmărire penală și a experților criminaliști.

BIBLIOGRAFIE
BIBLIOGRAPHY

ÅRNES, André (ed.). Digital Forensics. Chichester: John Wiley & Sons, 2018.

BOSCH GmbH. Bosch Automotive Handbook. 10th Edition. Chichester: Wiley, 2018.

BROY, Manfred; KRÜGER, Ingolf H.; PRETSCHNER, Alexander; SALZMANN, Christian (eds.). Engineering Automotive Software. Berlin: Springer, 2007.

CARRIER, Brian. File System Forensic Analysis. Boston: Addison-Wesley Professional, 2005.

CASEY, Eoghan. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 3rd Edition. Burlington, MA: Academic Press, 2011.

CHISUM, W. Jerry; TURVEY, Brent E. (eds.). Crime Reconstruction. 2nd Edition. Burlington, MA: Academic Press, 2011.

CHO, S. et al. Forensic Investigation of Vehicle-Related Data in Android Phones Connected to In-Vehicle Infotainment Systems. Computer Networks, Vol. 254, 2025, Article 111370.

DAILY, Jeremy; SHIGEMURA, Hiroyuki; PETERSON, Nathan. Forensic Examination of Electronic Vehicle Systems. 3rd Edition. London: Academic Press, 2021.

EBBERS, Sebastian; ISING, Fabian; SAATJOHANN, Christian; SCHINZEL, Sebastian. Grand Theft App: Digital Forensics of Vehicle Assistant Apps. In: Proceedings of the 16th International Conference on Availability, Reliability and Security (ARES 2021). New York: ACM, 2021.

ENFSI Digital Evidence Working Group. Guideline for Best Practice in the Forensic Examination of Digital Technology. Wiesbaden: ENFSI, 2018.

GARFINKEL, Simson L. Digital Forensics Research: The Next 10 Years. Digital Investigation, 2010, Vol. 7 (Supplement), pp. S64–S73.

ISO/IEC 27037:2012. Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence. Geneva: International Organization for Standardization, 2012.

ISO/IEC 27042:2015. Guidelines for the Analysis and Interpretation of Digital Evidence. Geneva: International Organization for Standardization, 2015.

ISO/SAE 21434:2021. Road Vehicles – Cybersecurity Engineering. Geneva: International Organization for Standardization / SAE International, 2021.

KANG, Haein; SEONG, Hojun; KIM, Ilkyu; JEONG, Wookjae; CHO, Seong-Je; PARK, Minkyu; HAN, Sangchul. Android-Based Audio Video Navigation System Forensics: A Case Study. Applied Sciences, 2023, Vol. 13, No. 10, Article 6176.

KATSINI, Christina; RAPTIS, George E.; ALEXAKOS, Christos; SERPANOS, Dimitrios. ForePlan: Supporting Digital Forensics Readiness Planning for Internet of Vehicles. In: Proceedings of the 25th Pan-Hellenic Conference on Informatics (PCI 2021). New York: ACM, 2021.

KENT, Karen; CHEVALIER, Suzanne; GRANCE, Tim; DANG, Hung. Guide to Integrating Forensic Techniques into Incident Response. NIST Special Publication 800-86. Gaithersburg, MD: National Institute of Standards and Technology, 2006.

KIRK, Paul L. Crime Investigation: Physical Evidence and the Police Laboratory. 2nd Edition. New York: Interscience Publishers, 1963.

LE-KHAC, Nhien-An; JACOBS, Daniel; NIJHOFF, Jelle; BERTENS, Koen; CHOO, Kim-Kwang Raymond. Smart Vehicle Forensics: Challenges and Case Study. Future Generation Computer Systems, 2020, Vol. 109, pp. 500–510.

NAVET, Michel; SIMONOT-LION, Françoise (eds.). Automotive Embedded Systems Handbook. Boca Raton: CRC Press, 2009.

NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION (NHTSA). Event Data Recorders. 49 CFR Part 563, Title 49 – Transportation. Washington, D.C.: U.S. Department of Transportation.

RAWTANI, Deepak; HUSSAIN, Chaudhery Mustansar (eds.). Modern Forensic Tools and Devices: Trends in Criminal Investigation. Hoboken, NJ: John Wiley & Sons / Scrivener Publishing, 2023.

RÉPÁS, József. Examining the Application of Drone Forensics Methodology on Highly Automated Civil and Military Vehicles. Hadmérnök, 2024, Vol. 19, No. 2, pp. 17–29.

SHIN, Yeonghun; KIM, Sungbum; JO, Wooyeon; SHON, Taeshik. Digital Forensic Case Studies for In-Vehicle Infotainment Systems Using Android Auto and Apple CarPlay. Sensors, 2022, Vol. 22, No. 19, Article 7196.

SHIN, Yeonghun; YU, Geon; SHON, Taeshik. Digital Forensic Analysis for Vehicle Infotainment Systems Based on Packet Fingerprinting. 2024. DOI: 10.21203/rs.3.rs-4664910/v1.

YOON, Y. et al. Forensic Investigation of an Android Jellybean-Based Car AVN System Installed in Kia K5. DFRWS APAC Proceedings, 2024.