

K získaniu dôkazov z automatizovaných vozidiel a pokročilých asistenčných systémov vozidiel

Vojtuš, F., Kordík, M.*

VOJTUŠ, F., KORDÍK, M.: K získaniu dôkazov z automatizovaných vozidiel a pokročilých asistenčných systémov vozidiel.** Právny obzor, 109, 2026, č. 2, s. 157 – 190. <https://doi.org/10.31577/pravnyobzor.2026.2.04>

To obtain evidence from automated vehicles and advanced vehicle assistance systems.

The paper deals with the issue of automated vehicles and their relationship to criminal law, particularly in the area of evidence in criminal proceedings. The introduction analyzes the legal and technical definition of automated vehicles within the European Union and the Slovak Republic, based on the SAE J3016 standard, relevant EU legal acts, and Slovak legislation. The following section focuses on defining the relationship between automated vehicles and criminal law. This is followed by an analysis of the possibility of securing evidence from an Event Data Recorder (EDR), which, according to EU legislation, is an advanced driving assistance system, namely for the purposes of criminal proceedings. EDR data can play a key role in reconstructing traffic accidents and proving criminal offenses, particularly in determining liability and the facts of the case. The paper analyzes the legal possibilities of obtaining and securing data from the EDR system through procedural institutions of the Criminal Procedure Code, also with regard to the principles of legality, proportionality, and subsidiarity. In the following section, the paper focuses on the expected problems of obtaining electronic evidence from fully automated vehicles of levels 4 and 5 according to the SAE standard, which use artificial intelligence. It identifies new legal and technological challenges associated with this. Finally, the current legal restrictions on the use of possible future automated vehicle systems in obtaining evidence for profiling or biometric identification of persons are presented. The article also indicates the growing importance of data generated by vehicle assistance systems and automated vehicles, especially their potential as a source of electronic evidence in criminal proceedings. At the same time, it presents the issue of procedural securing of such evidence in criminal proceedings, both in terms of the existing legal framework and potential future challenges.

Key words: *autonomous vehicles, artificial intelligence, criminal procedure, e-evidence, EDR, criminal liability*

Úvod

Umelá inteligencia, či už vo forme softvéru alebo jej začlenenia v rámci rôznych systémov (strojov, výrobkov), sa stáva čoraz viac a viac bežnou súčasťou našich životov. S touto realitou je spojený aj možný dosah a vplyv umelej inteligencie samotnej alebo

* JUDr. Ing. František Vojtuš, PhD., vyšetrovateľ PZ, externý spolupracovník Katedry trestného práva, kriminológie a kriminalistiky Právnickej fakulty UK v Bratislave. e-mail: vojtus1@uniba.sk. ORCID: <https://orcid.org/0000-0002-1912-4666>. Autorský podiel 70 percent.

Doc. JUDr. Marek Kordík, PhD., Katedra trestného práva, kriminológie a kriminalistiky Právnickej fakulty UK v Bratislave. e-mail: marek.kordik@flaw.uniba.sk. ORCID: <https://orcid.org/0000-0002-4290-8354>. Autorský podiel 30 percent.

** Táto práca bola podporená Agentúrou na podporu výskumu a vývoja na základe zmluvy č. APVV-23-0519 Právne a technické výzvy inteligentnej mobility na zvýšenie bezpečnosti cestnej premávky.

systémov ju obsahujúcich na rôzne spoločenské vzťahy, a to vrátane právnych vzťahov, ktoré sú predmetom záujmu práva ako takeého.¹¹ V súčasnosti jedným z najbežnejšie známych príkladov aplikácie a využívania umelej inteligencie sú práve automatizované (autonómne) vozidlá.

Za posledné desaťročia automobilový priemysel prešiel rapidnou digitálnou transformáciou. Došlo k nárastu inovácií so zameraním na vývoj prepojených automatizovaných vozidiel (Connected and Autonomous Vehicles – CAV), aby sa v budúcnosti mohli vyrábať vozidlá, ktoré budú fungovať bez zásahu človeka a s rozšírenými jazdnými schopnosťami.¹² Moderné vozidlá môžu obsahovať viac ako 150 elektronických riadiacich jednotiek (Electronic Control Unit – ECU) a viac ako 100 miliónov riadkov počítačového kódu. Moderné vozidlá majú komplexnú vnútornú architektúru a sú alebo môžu byť bezdrôtovo pripojené k internetu, iným vozidlám a infraštruktúre.¹³

Automatizované vozidlá, ktoré budú komunikovať s inými vozidlami či inteligentnými dopravnými systémami, môžu prijímať, produkovať, spracovávať a prenášať obrovské množstvo údajov. Takéto vozidlá možno označiť za prepojené automatizované (autonómne¹⁴) vozidlá (CAV). V prvom rade tieto údaje zahŕňujú údaje vo vozidle (in-vehicle data), ktoré sa získavajú prostredníctvom rôznych technológií, ktoré následne komunikujú s inými vnútornými komponentmi vozidiel rôznymi sieťami. Medzi tieto siete patrí napr. Flexray, sieť Ethernet, Controller Area Network (CAN) a iné. Ako príklady údajov vo vozidle možno uviesť technické údaje o vozidle (informácie o rýchlosti, zrýchlení, teplote vzduchu, hladine paliva, a pod.), údaje o stave premávky, údaje o počasí, údaje o správaní počas jazdy a dokonca aj údaje o zdravotnom stave vodiča. Prepojené automatizované vozidlá môžu taktiež prijímať údaje, ktoré sú odosielané z iných vozidiel, cestnej infraštruktúry, ako sú semaforey, značky, alebo od iných účastníkov premávky (cyklisti, chodci). V tomto ohľade je automatizované vozidlo prepojenou entitou, ktorá prijíma údaje z externého zdroja a môže zdieľať údaje, ktoré sú zaznamenané so

¹¹ K právnemu výskumu v oblasti umelej inteligencie pozri napr. ROSCA, C., COVRIG, et al. *Return of the AI: An Analysis of Legal Research on Artificial Intelligence Using Topic Modeling*. In ALETRAS, N., ANDROUSOPOULOS, I., BARRETT, L., MEYERS A. & PREOIUC-PIETRO, D. (eds.), *Proceedings of the Natural Legal Language Processing Workshop 2020*, CEUR-WS.org, s. 3 – 10. Dostupné na: <http://ceur-ws.org/Vol-2645/paper1.pdf> (citácia z 01.10.2025).

¹² BROWN, A., JOHNSON, D. S., TUPTUK, N. A scoping study: crime and connected and autonomous vehicles. In *Crime Scienc*. Vol. 14, article 2, 2025, s. 1. Dostupné na: <https://doi.org/10.1186/s40163-025-00245-x>.

¹³ STRANDBERG, K., NOWDEHI N., OLOVSSON T. A Systematic Literature Review on Automotive Digital Forensics: Challenges, Technical Solutions and Data Collection. In *IEEE Transactions on Intelligent Vehicles*, Vol. 8, No. 2, 2023, s. 1350. Dostupné na: <http://dx.doi.org/10.1109/TIV.2022.3188340>.

¹⁴ V odbornej literatúre sa možno stretnúť ako s pojmom automatizované, tak aj s pojmom autonómne vozidlo, pričom ide o pojmy v zásade označujúce z hľadiska schopnosti vozidla samostatne vykonávať dynamické jazdné úlohy. S ohľadom na pojmy používané v legislatíve Európskej únie (nariadenie Európskeho parlamentu a Rady (EÚ) 2019/2144) a právnom poriadku Slovenskej republiky (zákon č. 429/2022 Z. z.), ktoré definujú pojem automatizované vozidlo, budeme na účely tohto článku používať pojem automatizované vozidlo. K tomu pozri napr. ANDRAŠKO, J., KORDÍK, M. Úlohy a oprávnenia orgánov Policajného zboru v ére automatizovaných vozidiel. In *STUDIA IURIDICA Cassoviensia*, Vol. 12, No.1, 2024, s. 7. Dostupné na: <https://doi.org/10.33542/SIC2024-1-01>.

vzdialenou tretou stranou, na rôzne účely. Do prepojených automatizovaných vozidiel môžu byť importované údaje ako zoznam telefónnych kontaktov, cieľové destinácie pre navigáciu a údaje vytvorené vodičom a cestujúcimi (napr. navštívené webové stránky, preferencie online nakupovania atď.). Externým zdrojom údajov môžu byť aj údaje, ktoré produkujú rôzne orgány verejnej moci zodpovedné za cestnú premávku a cestnú infraštruktúru. Informácie o cestnej premávke a údaje o infraštruktúre zahŕňajú napr. dynamické rýchlostné limity, pravidlá cestnej premávky, polohu stojacich vozidiel, názvy ciest, stav a dostupnosť vozoviek, dĺžku ciest, typ vozoviek, upozornenia na práce na ceste, počet a polohu semaforov a značiek atď.⁵

Uvedené skutočnosti znamenajú na jednej strane vysoké riziko kybernetických útokov a iných možných trestnoprávných konaní, na strane druhej zároveň predstavujú možný zdroj veľkého množstva dát a informácií, ktoré môžu prispieť k dokumentovaniu a objasňovaniu trestnej činnosti. Zároveň existencia množstva rôznych dát a informácií rezultuje aj k potrebe riešenia otázok podmienok ich získania a použiteľnosti v rámci trestného konania a dokazovania, najmä s ohľadom na potrebu rešpektovania a ochrany základných práv a slobôd.

Na uvedený vývoj musí reagovať a aj reaguje právo, a to ako na medzinárodnej úrovni, tak aj na úrovni Európskej únie (ďalej aj „EÚ“), ale aj v rámci Slovenskej republiky (ďalej aj „SR“), a to najmä definovaním samotných automatizovaných vozidiel a ich prípadných úrovní, ako aj definovaním podmienok a obmedzení niektorých (asistenčných) systémov používaných vo vozidlách, resp. ohľadom využívania umelej inteligencie samotnej, a to najmä s ohľadom na zaznamenávané dáta a informácie. Otázkou je do akej miery je súčasná slovenská úprava trestného konania, a ňou využívané trestnoprocenčné inštitúty, pripravená čeliť výzvam spojeným so získavaním údajov a informácií, teda elektronických dôkazov zo systémom automatizovaných vozidiel.

Cieľom nášho príspevku je na základe doktrínálnej a komparatívnej analýzy právnej úpravy automatizovaných vozidiel a asistenčných systémov vozidiel *de lege lata* na úrovni SR a EÚ preskúmať súčasne možnosti a obmedzenia procesného zaistenia informácií a dôkazov z takýchto vozidiel a ich systémov na účely trestného konania, ako aj prípadného využitia automatizovaných vozidiel a asistenčných systémov ako prostriedku na získavanie dôkazov a informácií pre trestné konanie. Pri tom budeme vychádzať jednak z technického riešenia týchto systémov, ako aj z prijatých právnych požiadaviek a obmedzení konštrukčných riešení takýchto systémov. Naším zámerom je určiť, či súčasná slovenská právna úprava inštitútov zaistenia vecí, resp. dôkazov na účely trestného konania v rámci Trestného poriadku je dostatočná a umožňuje zaistenie informácií a dôkazov z automatizova-

⁵ Bližšie k architektúre a funkciám a systémom prepojených automatizovaných vozidiel pozri AN-DRAŠKO, J., DRAŽOVÁ, P., GYURÁSZ, Z., et al. *Biela kniha. Regulácia autonómnych vozidiel v Európskej únii a Slovenskej republike*. Bratislava : Univerzita Komenského v Bratislave, Právnická fakulta, 2022, s. 17 a nasl. Dostupné na: https://comeniusvyskum.flaw.uniba.sk/wp-content/uploads/2023/01/Biela-kniha_FINAL.pdf alebo STRANDBERG K., NOWDEHI N., OLOVSSON T. A Systematic Literature Review on Automotive Digital Forensics: Challenges, Technical Solutions and Data Collection. s. 1350 – 1352 alebo BROWN, A., JOHNSON, D. S., TUPTUK, N. A scoping study: crime and connected and autonomous vehicles. s. 4 – 5.

ných vozidiel a asistenčných systémov, a ak áno, za akých podmienok a akým postupom. Súčasne poukážeme, najmä v prípade automatizovaných vozidiel úrovne 5, na možné problémy vyplývajúce najmä zo súčasného stavu technického riešenia.

V rámci odbornej literatúry sa záujem autorov z hľadiska skúmania vzťahu automatizovaných vozidiel a asistenčných systémov a trestného práva zameriava najmä na skúmanie otázok trestnoprávných následkov spojených s používaním alebo zneužívaním asistenčných vozidiel a ich systémov⁶, otázky trestnej zodpovednosti spojené s používaním a prevádzkovaním automatizovaných vozidiel najmä z hľadiska v nich obsiahnutej umelej inteligencie⁷ a na otázky spojené s (kriminalistickými) postupmi pri zaisťovaní dát z takýchto vozidiel z hľadiska ich následnej použiteľnosti a spoľahlivosti.⁸ Len okrajovo sú riešené otázky týkajúce sa samotného trestnoprocesného postupu pri získavaní dôkazov z automatizovaných vozidiel a asistenčných systémov a pri ňom použitých zaisťovacích inštitútov trestného práva.⁹ Kľúčovým cieľom nášho príspevku, ako už bolo uvedené, je preskúmanie možnosti využitia konkrétnych trestnoprocesných inštitútov a procesných postupov pri zaisťovaní dôkazov a informácií z automatizovaných vozidiel a ich asistenčných systémov, a to s ohľadom na právnu úpravu *de lege lata*, technické a legislatívne obmedzenia týchto systémov a možné aplikačné problémy súvisiace s najmä s očakávaným využívaním automatizovaných vozidiel úrovne 5.

Náš príspevok je členený v prvej časti na rozbor právnej úpravy automatizovaných vozidiel a asistenčných systémov vozidiel, následne na vymedzenie vzťahov automatizovaných vozidiel vo vzťahu k trestnému právu, osobitne ako dôkazu alebo ich zdroja pre trestné konanie. V druhej časti sa príspevok zaoberá jednak možnosťami využitia a najmä spôsobom získania údajov zo zariadenia na záznam údajov o udalostiach vozidla (EDR), ako aj problémami a možnosťami ich riešenia vo vzťahu k získaniu elektronických dôkazov z automatizovaných vozidiel *pro futuro*.

1. Čo je automatizované vozidlo, jeho úrovne a ich právne vymedzenie v EÚ a SR

Z technického hľadiska je v odbornej literatúre najčastejšie zaužívané delenie automatizovaných vozidiel podľa štandardu SAE J3016_202104 Taxonómia a definície poj-

⁶ Pozri napríklad BROWN, A., JOHNSON, D. S., TUPTUK, N. A scoping study: crime and connected and autonomous vehicles. In *Crime Scienc*e, s. 1 – 41.

⁷ Pozri napríklad GURNEY, K., J. Driving Into The Unknown: Examining The Crossroads of Criminal Law and Autonomous Vehicles. In *Wake Forest Journal of Law and Policy*, 2015, Vol. 5, Iss. 2, s. 393 – 442.

⁸ Pozri napríklad STRANDBERG K., NOWDEHI N., OLOVSSON T. A Systematic Literature Review on Automotive Digital Forensics: Challenges, Technical Solutions and Data Collection. s. 1350 – 1367, alebo HOQUE, A., M., HASAN, R. AVGuard: A Forensic Investigation Framework for Autonomous Vehicles, In *ICC 2021 – IEEE International Conference on Communications*, Montreal, QC, Canada, 2021, s. 1 – 6, doi: 10.1109/ICC42927.2021.9500652.

⁹ Pozri napríklad GLESS, S., LEDERER, F., WEIGEND, T. AI-Based Evidence In Criminal Trials? In *Tulsa Law Review*, Vol. 59, No. 1, 2024, s. 1 – 37 alebo QUEZADA-TAVÁREZ, K., VOGIATZOGLOU, P., ROYER, S. Legal challenges in bringing AI evidence to the criminal courtroom. In *New Journal of European Criminal Law*, Vol. 12, Iss. 4, 2021, s. 531 – 551, <https://doi.org/10.1177/20322844211057019>.

mov súvisiacich so systémami automatizovaného riadenia pre cestné motorové vozidlá (ďalej len „SAE štandard“)¹⁰. Na základe schopnosti systémov vozidla vykonávať trvalo samostatne časť alebo celú škálu dynamických jazdných úloh bez zásahu vodiča vozidla, tento štandard určuje 6 úrovni automatizovaných vozidiel (úrovne 0 až 5), ktoré sa stupňujú. Na úrovni 0 (bez automatizácie) sú dynamické jazdné úlohy vykonávané výlučne ľudským vodičom a na úrovni 5 (úplná automatizácia) sú takéto úlohy vykonávané výlučne automatizovaným systémom riadenia bez zásahu vodiča. Keďže ide skôr o technické vymedzenie automatizácie vozidiel, ktoré nemá právnu záväznosť, nebudeme sa popisu týchto úrovni bližšie venovať. Pojmu automatizované vozidlo z hľadiska platnej legislatívy zodpovedajú vozidlá definované týmto štandardom od úrovne 3 a vyššie.¹¹

Európska únia na zavádzanie automatizovaných vozidiel a asistenčných systémov vozidiel reagovala najmä nariadením Európskeho parlamentu a Rady (EÚ) 2019/2144 o požiadavkách na typové schvaľovanie motorových vozidiel a ich prípojných vozidiel a systémov, komponentov a samostatných technických jednotiek určených pre tieto vozidlá, pokiaľ ide o ich všeobecnú bezpečnosť a ochranu cestujúcich vo vozidle a zraniteľných účastníkov cestnej premávky¹² (ďalej len „nariadenie EÚ 2019/2144“), ktoré definovalo pojmy automatizované vozidlo a plne automatizované vozidlo, ako aj povinnosti vybavenia vozidiel pokročilými systémami vozidla a minimálnymi požiadavkami na pokročilé systémy vozidla.¹³ Na základe čl. 12 nariadenia EÚ 2019/2144 komisia EÚ prijala viacero delegovaných nariadení (aktov), z ktorých na účely nášho príspevku má najväčší význam delegované nariadenie komisie (EÚ) 2022/545 z 26. januára 2022, ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) 2019/2144 stanovením podrobných pravidiel týkajúcich sa osobitných skúšobných postupov a technických požiadaviek na typové schvaľovanie motorových vozidiel vzhľadom na ich zariadenie na záznam údajov o udalostiach a na typové schvaľovanie týchto systémov ako samostatných technických jednotiek, a ktorým sa mení príloha II k uvedenému nariadeniu (ďalej „delegované nariadenie 2022/545“). Predmetné delegované nariadenie 2022/545 vo svojich ustanoveniach upravuje technické požiadavky na systém zariadenia na záznam údajov o udalostiach vozidla (*event data recorder* – EDR, niekedy označovaný aj ako tzv. čierna skrinka). Samotné delegované nariadenie 2022/545 pritom odkazuje sčasti na technické požiadavky stanovené pre EDR pred-

¹⁰ Štandard SAE J3016_202104: Taxonómia a definície pojmov súvisiacich so systémami automatizovaného riadenia pre cestné motorové vozidlá. Dostupné na: https://www.sae.org/standards/content/j3016_202104/ (cit. 26.08.2025).

¹¹ Bližšie k vymedzeniu úrovne automatizácie vozidiel podľa SAE štandardu pozri napr. ANDRAŠKO, J., DRAŽOVÁ, P., GYURÁSZ, Z., et al. *Biela kniha. Regulácia autonómnych vozidiel v Európskej únii a Slovenskej republike*. s. 8 – 12.

¹² Na úrovni Európskej únie je problematika schvaľovania motorových vozidiel, ako aj systémov pre takéto vozidlá upravená nariadením Európskeho parlamentu a Rady (EÚ) 2018/858 z 30. mája 2018 o schvaľovaní motorových vozidiel a ich prípojných vozidiel, ako aj systémov, komponentov a samostatných technických jednotiek určených pre takéto vozidlá a o dohľade nad trhom s nimi, ktorým sa menia nariadenia (ES) č. 715/2007 a (ES) č. 595/2009 a zrušuje smernica 2007/46/ES.

¹³ Zoznam pokročilých systémov vozidla je uvedený v čl. 6 ods. 1 nariadenia EÚ 2019/2144. Ide o systém inteligentného prispôsobenia rýchlosti, umožnenie montáže alkoholového imobilizéra, systém varovania vodiča pred ospalosťou a stratou pozornosti, pokročilý systém varovania vodiča pred rozptýlením, signál núdzového brzdenia, detekcia spätného chodu a zariadenie na záznam údajov o udalostiach.

pisom OSN č. 160 – Jednotné ustanovenia na účely typového schvaľovania vozidiel vzhľadom na zariadenie na záznam údajov [2021/1215], séria zmien 01 (uverejnený v Úradnom vestníku EÚ L 265, 26.07.2024, s. 3).

Na úrovni práva Európskej únie je potrebné v prípade automatizovaných (a to osobitne v prípade plnoautomatizovaných vozidiel, teda vozidiel úrovne 4 a vyššie podľa SAE štandardu) zohľadňovať aj ustanovenia nariadenia Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (ďalej ako „Akt o umelej inteligencii“), pretože základom takýchto vozidiel je práve využívanie umelej inteligencie. Z hľadiska trestného práva pôjde najmä o otázky používania zakázaných praktík využívajúcich umelú inteligenciu (ďalej aj „AI“) podľa čl. 5 aktu o umelej inteligencii (napr. systémov biometrickej kategorizácie osôb), ako aj možnosti využívania vysokorizikových systémov podľa článku 6 ods. 2 aktu o umelej inteligencii, najmä s ohľadom na bod 2. prílohy III aktu o umelej inteligencii, ktorý medzi vysokorizikové systémy AI radí aj systémy AI, ktoré sa majú používať ako bezpečnostné komponenty pri riadení a prevádzke cestnej premávky.

Z hľadiska slovenskej legislatívy reagoval slovenský zákonodarca na zavádzanie automatizovaných vozidiel a právne akty EÚ prijatím zákona č. 429/2022 Z. z., ktorým sa menia a dopĺňajú niektoré zákony v súvislosti s rozvojom automatizovaných vozidiel (ďalej len „zákon o automatizovaných vozidlách“).¹⁴ Týmto zákonom boli v § 2 ods. 2 zákona č. 106/2018 Z. z. o prevádzke vozidiel v cestnej premávke pod písmenami ac) až ae) zadané v slovenskom právnom poriadku legálne definície pojmov automatizované vozidlo, plne automatizované vozidlo a automatizovaný systém riadenia. Automatizované vozidlo bolo definované ako *automatizované vozidlo podľa osobitného predpisu*¹⁵ alebo iné motorové vozidlo navrhnuté a skonštruované tak, aby sa dokázalo určitý čas samostatne pohybovať bez nepretržitého dohľadu vodiča, pri ktorom sa však zásah vodiča predpokladá alebo vyžaduje. Plne automatizovaným vozidlom sa podľa slovenského právneho poriadku rozumie *plne automatizované vozidlo podľa osobitného predpisu*¹⁶ alebo iné motorové vozidlo navrhnuté a skonštruované tak, aby sa dokázalo pohybovať samostatne, a automatizovaným systémom riadenia sa rozumie *systém riadenia vozidla, ktorý na zabezpečenie dynamickej kontroly nad vozidlom trvalo využíva hardvér a softvér*. Zákon o automatizovaných vozidlách zároveň novelizoval aj ustanovenia zá-

¹⁴ Z hľadiska iných národných úprav napríklad nemecký zákonodarca reagoval na pokrok vo vývoji automatizovaných vozidiel úpravou zákona o cestnej premávke Straßenverkehrsgesetz (StVG) a prijatím nariadenia – Autonome Fahrzeuge Genehmigung und Betriebs Verordnung z 24. júna 2022 (BGBl. I S. 986), skrátené AFGVBV, ktoré upravuje podmienky schvaľovania prevádzky takýchto vozidiel vrátane rozsahu uchovávaných údajov. Veľká Británia reagovala prijatím osobitného zákona – Automated Vehicles Act 2024, ktorým komplexne upravila reguláciu uvádzania vozidiel úrovne 4 a 5 SAE štandardu do prevádzky, povinnosti vodičov automatizovaných vozidiel úrovne 4 a licencovaných operátorov plne automatizovaných vozidiel úrovne 5, ako aj zodpovednosť týchto subjektov v súvislosti s prevádzkou takýchto vozidiel.

¹⁵ Týmto osobitným predpisom je nariadenie EÚ 2019/2144.

¹⁶ Týmto osobitným predpisom je nariadenie EÚ 2019/2144.

kona č. 8/2009 Z. z. o cestnej premávke a určil v § 3 ods. 4 predmetného zákona povinnosť spočívajúcu v tom, že *každé pohybujúce sa vozidlo a každá pohybujúca sa jazdná súprava musí mať vodiča*. Podľa slovenského právneho poriadku, teda v prípade, ak by došlo k typovému schváleniu plne automatizovaných vozidiel do premávky (teda automatizovaných vozidiel úrovne 5), museli by mať tieto vozidlá stále vodiča. Vzhľadom na zmenu definície vodiča uvedenú v § 2 ods. 2 písm. v) zákona č. 8/2009 Z. z. o cestnej premávke vykonanú zákonom o automatizovaných vozidlách¹⁷, je však možné považovať za vodiča aj osobu, ktorá vykonáva len dohľad nad plne automatizovaným vozidlom, a to aj prípadne na diaľku. Zákon nevyžaduje priamu prítomnosť vodiča v takomto vozidle. Uvedená skutočnosť vyplýva aj z nového ustanovenia § 5 ods. 6 zákona č. 8/2009 Z. z. o cestnej premávke, podľa ktorého *osoba, ktorá vykonáva dohľad nad vozidlom, ktoré na jazdu využíva automatizovaný systém riadenia, je povinná včas a bezpečne prevziať vedenie vozidla na výzvu automatizovaného systému riadenia alebo, ak to vyžadujú okolnosti, aj bez tejto výzvy, a to prípadne aj na diaľku; na tento účel je povinná sledovať situáciu v cestnej premávke*. Zákon o automatizovaných vozidlách zároveň zaviedol v zákone č. 8/2009 Z. z. o cestnej premávke aj ustanovenia týkajúce sa schvaľovania skúšobnej prevádzky automatizovaného vozidla alebo plne automatizovaného vozidla využívajúceho automatizovaný systém riadenia v cestnej premávke. Slovenská legislatíva z hľadiska definovania automatizovaných vozidiel nadväzuje na európsku legislatívu.

2. Automatizované vozidlá a ich systémy z pohľadu trestného práva

Automatizované vozidlá, ich systémy, ako aj samotná umelá inteligencia obsiahnutá v nich, resp. v ich systémoch, môžu byť predmetom trestnoprávnych vzťahov z hľadiska riešenia viacerých možných situácií. Možné oblasti interakcie automatizovaných vozidiel a ich systémov a trestného práva môžeme v súčasnosti zhrnúť do troch základných oblastí, ktoré sú, alebo v budúcnosti môžu byť predmetom právnej regulácie týkajúcej sa automatizovaných vozidiel, ich systémov vrátane umelej inteligencie v nich obsiahnutej:

- a) automatizované vozidlá a ich systémy ako objekt ochrany trestného práva,
- b) automatizované vozidlá a ich systémy ako nástroj alebo predmet na páchanie trestnej činnosti,
- c) automatizované vozidlá a ich systémy ako zdroj dát o trestnej činnosti, resp. ako dôkaz.

Oblasti uvedené pod písmenami a) a b) predstavujú oblasti, v ktorých primárne trestnoprávna úprava je, alebo v budúcnosti bude doménou právnych predpisov trestného práva hmotného a ich vývoja, a to vrátane hmotnoprávnej časti teórie trestného práva. Oblasť uvedená pod písmenom c) je naopak bude doménou úpravy právnych predpisov trestného práva procesného a jeho teórie.

Z hľadiska riešenia otázok týkajúcich sa oblastí pod písm. a) a b) je z pohľadu trestného práva možné na tieto oblasti aplikovať buď úplne, alebo len s menšími úpravami

¹⁷ Vodičom sa podľa § 2 ods. 2 písm. v) rozumie vodičom *osoba, ktorá vedie vozidlo, alebo osoba, ktorá vykonáva dohľad nad vozidlom, ktoré na jazdu využíva automatizovaný systém riadenia*.

súčasnú trestnoprávnu úpravu nachádzajúcu sa v hmotnoprávných predpisoch, teda v TZ, resp. TZPO. Súčasne je možné na tieto situácie aplikovať aj poznatky trestnoprávnej teórie.¹⁸

Automatizované vozidlá a ich systémy z hľadiska ich vzťahov k trestnému právu opísaných vyššie pod písmenom c) predstavujú pre trestné konanie zdroj informácií o trestnom čine, resp. trestnej činnosti ako takej. Inak povedané, informácie nimi získané alebo v nich obsiahnuté môžu slúžiť ako potenciálny dôkaz v trestnom konaní. Z trestnoprocesného hľadiska je ďalšou možnou interakciou automatizovaných vozidiel s trestným konaním (zatiaľ iba v rovine teoretických úvah) možnosť postihovania automatizovaných vozidiel, resp. umelej inteligencie, ktorá je základom ich fungovania, a to ako páchatel'ov trestnej činnosti, teda subjektov trestného konania v pozícii podozrivého, resp. obvineného. Nad posledne uvedeným prepojením je možné v teoretickej rovine *pro futuro* uvažovať v rámci úrovne 5 automatizovaných vozidiel, keď takéto vozidlo riadené umelou inteligenciou bude úplne samostatne vykonávať a rozhodovať o dynamických jazdných úlohách. Riešenie tejto otázky je spojené s otázkou riešenia trestnoprávnej zodpovednosti umelej inteligencie ako takej, čo je aktuálne predmetom mnohých diskusií a odborných príspevkov.¹⁹ V našom príspevku sa však budeme hlavne a prioritne zamerať na možnosti využitia automatizovaných vozidiel a ich systémov pri dokazovaní v trestnom konaní. Preto otázku trestnej zodpovednosti automatizovaných vozidiel úrovne 5, resp. umelej inteligencie budeme riešiť len doplnkovo a informatívne v rámci problematiky získavania dôkazov z automatizovaných vozidiel úrovne 5.

3. Automatizované vozidlá a ich systémy ako dôkaz v trestnom konaní

Vo všeobecnosti automatizované vozidlo (plne automatizované vozidlo) a jeho systémy môžu v rámci dokazovania v trestnom konaní vystupovať najmä ako

- a) vecný (fyzický) dôkazný prostriedok alebo
- b) elektronický dôkazný prostriedok.

V prípade vecného dôkazného prostriedku samotné vozidlo je nositeľom dôkazných informácií vyplývajúcich zo skutočnosti, že samotné vozidlo sa stalo predmetom útoku, prípadne bolo použité pri páchaní trestného činu. Zdrojom informácií však v takomto prípade nie sú samotné elektronické systémy vozidla, ktoré zbierajú údaje. Vozidlo je zdrojom informácií, ktoré vyplývajú z toho, že sa na ňom nachádzajú fyzické alebo iné materiálne stopy po trestnom čine, resp. vzniknuté v súvislosti s jeho páchaním (napr. chemické, biologické). Typicky pôjde o prípady poškodenia vozidla alebo jeho systémov, či už v dôsledku konania inej fyzickej osoby (vandalizmus) alebo v dôsledku nehodového deja alebo iných okolností, ktoré zanechajú na vozidle materiálne stopy, resp. informácie.

¹⁸ ANDRAŠKO, J., DRAŽOVÁ, P., GYURÁSZ, Z., et al. *Biela kniha. Regulácia autonómnych vozidiel v Európskej únii a Slovenskej republike*. s. 24.

¹⁹ K problematike a prehľadu prístupov pozri napr. VOJTUŠ, F., KORDÍK, M., DRAŽOVÁ, P. Umelá inteligencia, jej využívanie a trestnoprávna zodpovednosť – výzvy, problémy a možné riešenia. In *Právnik*, roč. CLXII, č. 6, 2023, s. 549 – 570.

Práca autorov A. Brown, S. D. Johnson a N. Tuptuk²⁰ na základe rozboru analýzy dát z voľne dostupných zdrojov a informácií z médií uvádza prehľad trestných činov (incidentov), ktoré už boli reálne spáchané na automatizovaných vozidlách alebo prostredníctvom nich, resp. ich systémov (vrátane asistenčných systémov). Ide jednak o trestné činy, ktoré sú bežné aj vo vzťahu ku klasickým vozidlám, ako sú krádeže samotných vozidiel alebo ich súčiastok a súčastí, prípadne predmetov v takýchto vozidlách, poškodenie takýchto vozidiel (vandalizmus), poisťné podvody, použitie vozidla ako zbrane (fyzický útok za pomoci vozidla). Na druhej strane ide o trestné činy, ktoré s ohľadom na úroveň systémov automatizovaných vozidiel nie je možné spáchať bežne používanými vozidlami, resp. vozidlami bez asistenčných systémov. Ide o trestné činy spojené s kyberkriminalitou, ako sú krádeže dát zo systémov vozidla (napr. na účely páchania inej trestnej činnosti alebo prípadne vydierania obete alebo doxing-u), hacknutie vozidla a prevzatie kontroly nad vozidlom, alebo spojené s kyberšikanou (elektronické sledovanie, prípadne spojené aj s domácim násilím napríklad cez sledovanie osoby systémami vozidla, resp. obmedzovanie používania vozidla obeťou blokovaním alebo limitovaním používania systémov).

Ďalej uvedení autori na základe analýzy odbornej literatúry a štúdií identifikovali (a rozobrali) možné skupiny trestných činov, ktoré prichádzajú do úvahy v budúcnosti v súvislosti so zavádzaním automatizovaných vozidiel, resp. asistenčných systémov do premávky. Ide o trestné činy spojené s útokmi na komunikačné siete vozidiel, útokmi na vnútornú komunikáciu a systémy vozidiel, útokmi na senzory vozidiel, útokmi na informačno-zábavné systémy (infotainment) vozidiel, útokmi na systémy vstupu, autorizácie a autentifikácie vozidiel, útokmi na systémy analýzy údajov vozidiel, malvér namierený proti vozidlám a útokmi na podpornú infraštruktúru vozidiel.²¹

Ak je automatizované vozidlo alebo jeho systémy elektronickým dôkazným prostriedkom, tak zdrojom trestnoprávne relevantných informácií sú informácie zaznamenané systémami vozidla v súvislosti s trestným činom, ktorého vozidlo:

- bolo buď priamym účastníkom (napr. nehoda alebo samotné poškodenie vozidla, jeho zneužitie ako nástroja na spáchanie trestného činu), alebo
- nebolo priamym účastníkom a informácie o trestnom čine boli získané v rámci prevádzky vozidla (napr. prostredníctvom senzorov bola zaznamenaná iná dopravná nehoda, násilný trestný čin, trestná činnosť vodiča spočívajúca napríklad v telefonickom vyhrážaní sa inej osobe pri telefonovaní počas jazdy vozidla a iné). Automatizované vozidlo (jeho systémy) „vystupuje v pozícii akéhosi svedka trestného činu“. V súvislosti s druhou alternatívou (trestnoprávne relevantné informácie získané pri prevádzke) vystupuje následne do popredia otázka týkajúca sa oprávnenosti získavania takýchto údajov a ich následného uchovávaní a zabezpečenia s ohľadom na možný zásah do základných práv a slobôd, najmä práva na súkromie a ochranu osobných údajov pri používaní vozidiel.

²⁰ BROWN, A., JOHNSON, D. S., TUPTUK, N. A scoping study: crime and connected and autonomous vehicles. In *Crime Scienc.* s. 10 – 16.

²¹ Tamže, s. 17 – 24.

Z pohľadu trestnoprocésneho aspektu, ktorý vníma autonómne vozidlo výlučne ako nosiča dát a informácií významných pre trestné stíhanie, nemá v súčasnosti procesný význam rozlišovať, o akú úroveň automatizácie vozidla ide pri poskytovaní dát, resp. pri procese ich získavania na účely trestného stíhania. Súčasná právna úprava Trestného poriadku, ako i úprava de lege ferenda, pristupuje k autonómnemu vozidlu ako k dátovému nosiču a zdroju digitálnych údajov, ktorých zaisťovanie, vydanie, skúmanie a ukladanie sa riadi jednak príslušnými ustanoveniami Trestného poriadku, ale taktiež príslušnými medzinárodnými ISO štandardmi aplikovanými pre oblasť kybernetickej bezpečnosti a elektronických dôkazov.²²

S ohľadom na rozsah článku sa však budeme ďalej bližšie zaoberať možnosťami procesného získania a zadokumentovania dôkazov (informácií) jednak z existujúcich (pokročilých) asistenčných systémov vozidiel, ako aj (*pro futuro*) z plne automatizovaných vozidiel. Konkrétne sa budeme podrobnejšie zaoberať jednak možnosťami procesného získania a využitia ako dôkazu vyplývajúceho z informácií z už v bežnej prevádzke zavedeného a používaného asistenčného systému – zariadenia na záznam údajov o udalostiach vozidla (ďalej aj ako „EDR“ – *event data recorder*),²³ ako aj možnosťami procesného získania dôkazov v prípade plne automatizovaných vozidiel, ak by došlo v budúcnosti k ich plnému zavedeniu do cestnej prevádzky.

4. Systém EDR z hľadiska dokazovania v trestnom konaní

Asistenčné systémy vozidiel (Driving Assistance Systems – DAS) zohrali a zohrávajú kľúčovú rolu vo vývoji automatizovaných vozidiel, a to poskytovaním kritickej podpory na ovládanie a bezpečnosť vozidla. Prvá generácia asistenčných systémov vozidiel sa objavila v 80. rokoch 20. storočia a využívala senzory, ktoré hodnotili vnútorný stav vozidla, so zameraním predovšetkým na bezpečnosť a stabilitu – išlo napríklad o systémy kontroly trakcie (TCS), protiblokovací systém bŕzd (ABS), elektronický systém kontroly stability (ESC). Druhá generácia asistenčných systémov vozidiel sa objavila na začiatku 90. rokov 20. storočia, a bola vybavená senzormi na detekciu vonkajšieho prostredia jazdy (napr. RADAR, LiDAR a kamery). Najnovšia generácia asistenčných systémov vozidla, označovaných aj ako pokročilé asistenčné systémy (Advanced Driving Assistance Systems – ADAS), bola vyvinutá na prevenciu kolízií.²⁴

Systém EDR je legislatívou EÚ považovaný za jeden z pokročilých (asistenčných) systémov vozidla.²⁵ Tento systém vo vozidlách má predchodcu v obdobnom zariadení – zapisovači letových údajov, tzv. čiernej skrinke, ktorá sa začala používať v leteckom

²² ANDRAŠKO, J., DRAŽOVÁ, P., GYURÁSZ, Z., et al. *Biela kniha. Regulácia autonómnych vozidiel v Európskej únii a Slovenskej republike*. s. 21.

²³ Uvedené zariadenie musí byť v súčasnosti povinne namontované vo všetkých vozidlách, ktoré sú registrované v rámci Európskej únie po júli 2024.

²⁴ K tomu pozri ALHABIB, R., YADAV, P. Data authorisation and validation in autonomous vehicles: a critical review. In *Discover Applied Science*, Vol. 7, No. 735, 2025, s. 3 – 5. Dostupné na: <https://doi.org/10.1007/s42452-025-07333-2>.

²⁵ Pozri čl. 6 ods. 1 nariadenie EÚ 2019/2144.

priemysle koncom päťdesiatych rokov minulého storočia.²⁶ V súčasnosti sú údaje v čiernych skrinkách lietadiel bežne využívaným zdrojom informácií pri vyšetrovaní leteckých nehôd a ich prínos pri objasňovaní ťažkostí je nespochybniteľný.

V rámci práva EÚ definuje pojem EDR čl. 3 bod 13. nariadenia EÚ 2019/2144, podľa ktorého sa za zariadenie na záznam údajov o udalostiach (EDR) považuje *systém, ktorého jediným účelom je zaznamenávanie a uchovávanie kritických parametrov a informácií súvisiacich so zrážkou, a to krátko pred zrážkou, počas nej a ihneď po nej*. Uvedené nariadenie EÚ 2019/2144 ďalej v čl. 6 bod 4. určuje, že zariadenia na záznam údajov o udalostiach musia spĺňať najmä tieto požiadavky:

- a) *údaje, ktoré sú schopné zaznamenávať a uchovávať v období krátko pred zrážkou, počas nej a bezprostredne po nej, musia zahŕňať prinajmenšom rýchlosť vozidla, brzdenie, polohu a sklon vozidla na ceste, stav a rýchlosť aktivácie všetkých jeho bezpečnostných systémov, palubného systému eCall využívajúceho službu tiesňovej linky 112, aktiváciu brzd a relevantné vstupné parametre z palubných systémov aktívnej bezpečnosti a predchádzania nehodám, pričom tieto údaje musia mať vysokú úroveň presnosti a musí byť zabezpečené ich zachovanie po nehode;*
- b) *zariadenia nesmie byť možné deaktivovať;*
- c) *spôsob, akým dokážu zaznamenávať a uchovávať údaje, musí byť taký, aby:*
 - i) fungovali v uzavretom systéme;
 - ii) údaje, ktoré získavajú, boli anonymizované a chránené proti manipulácii a zneužívaniu; a
 - iii) na základe údajov, ktoré získavajú, bolo možné určiť presný typ, variant a verziu vozidla, a najmä aktívne systémy bezpečnosti a predchádzania nehodám namontované vo vozidle; a
- d) *údaje, ktoré sú schopné zaznamenávať, možno sprístupniť vnútroštátnym orgánom na základe práva Únie alebo vnútroštátneho práva len na účely výskumu a analýzy nehôd vrátane účelov typového schvaľovania systémov a komponentov a v súlade s nariadením (EÚ) 2016/679, a to cez štandardizované rozhranie.*

Podľa čl. 6 bod 5. nariadenia EÚ 2019/2144 však zariadenie na záznam údajov o udalostiach *nesmie byť schopné zaznamenať a uchovávať posledné štyri číslice poradového čísla vozidla v rámci identifikačného čísla vozidla ani žiadne iné informácie, ktoré by umožnili identifikáciu samotného vozidla, jeho majiteľa alebo držiteľa.*

Podľa čl. 3 bod 1. delegovaného nariadenia 2022/545 *údaje o zrážke, ktoré zariadenie na záznam údajov o udalostiach zaznamenáva a uchováva, musia byť chránené pred manipuláciou tým, že spĺňajú príslušné technické požiadavky a prechodné ustanovenia pôvodnej série alebo akýchkoľvek neskorších sérií zmien predpisu OSN č. 155 – Jednotné ustanovenia na účely typového schvaľovania vozidiel vzhľadom na kybernetickú bezpečnosť a systém riadenia kybernetickej bezpečnosti. Podľa bodu 2. musia byť ďalej aktualizácie*

²⁶ Pozri NOWACKI, G., NIEDZICKA, A., KRYSIUK, C. The Use Of Event Data Recorder (EDR) – Black Box. In *Advances in Science and Technology Research Journal*, Vol. 8, No. 21, March 2014, s. 64, doi: 10.12913/22998624.1091881. K systému EDR pozri aj KOSTĚNCOVÁ, V., NOUZOVSKÝ, L. *Technologie EDR a její principy*. Praha : České vysoké učení technické v Praze, 2020, 109 s.

softvéru vykonávané na zariadení na záznam údajov o udalostiach chránené, aby sa primerane zabránilo poškodeniu a aby sa primerane zabránilo neplatným aktualizáciám.

Nariadenie EÚ 2019/2144 teda určuje minimálny rozsah údajov, ktoré systém EDR zaznamenáva zároveň s podmienkou, že tieto údaje sa týkajú len obdobia krátko pred zrážkou, počas nej a bezprostredne po nej. To znamená, že systém EDR zaznamenáva údaje v cyklickom režime, pričom údaje sa uzamknú v prípade nehody alebo prekročenia prednastavených hodnôt. Zaznamenávajú sa údaje z niekoľkých sekúnd pred zaznamenanou udalosťou (zvyčajne do 5 sekúnd) a krátkeho obdobia po udalosti (približne 300 milisekúnd). Záznam pracuje na princípe uzamknutej slučky, kde sa neustále prepisujú najnovšie dáta, až kým nedôjde k nehode, ktorá dáta uzamkne a uloží ich natrvalo. Takto získané uzamknuté údaje je potom možné využiť v trestnom konaní ako zdroj informácií o nehodovom deji a o tom, čo mu predchádzalo.

Spôsobenie dopravnej nehody v praxi je pomerne často spojené s trestnoprávne relevantnými následkami. Inak povedané, priebeh dopravnej nehody a v jej dôsledku spôsobené následky často napĺňajú skutkové podstaty viacerých trestných činov, najmä trestných činov proti životu a zdraviu ako nedbanlivostné formy trestného činu ublíženia na zdraví podľa § 157 TZ alebo § 158 TZ, prípadne úmyselné formy trestného činu ublíženia na zdraví podľa § 155 TZ alebo § 156 TZ. Nie je vylúčené ani spáchanie trestného činu vraždy podľa § 145 TZ alebo úkladnej vraždy podľa § 144 TZ. Ďalej prichádza do úvahy trestný čin neposkytnutia pomoci podľa § 178 TZ. Rovnako tak prichádzajú do úvahy aj trestné činy všeobecne nebezpečné ako všeobecné ohrozenie v úmyselnej forme podľa § 284 TZ alebo nedbanlivostnej forme podľa § 285 TZ. Ďalej trestný čin poškodzovania a ohrozenia prevádzky všeobecne prospešného zariadenia v úmyselnej forme podľa § 286 alebo nedbanlivostnej forme podľa § 288 TZ, trestný čin ohrozenia pod vplyvom návykovej látky podľa § 289. Nie je vylúčené ani spáchanie trestného činu marenia výkonu úradného rozhodnutia podľa § 348 ods. 1 písm. d) TZ v súvislosti s dopravnou nehodou. Na druhej strane, uvedené údaje môžu pomôcť aj pri vyšetrovaní najmä trestného činu poisťovacieho podvodu podľa § 223 TZ, keď uvedené údaje z EDR môžu umožniť zistenie, či došlo alebo nedošlo k fingovaniu dopravnej nehody, resp. k uvádzaniu nepravdivých údajov o jej priebehu.

Získanie údajov zo systému EDR teda môže výrazne napomôcť dokazovaniu v rámci trestného konania, z hľadiska zistenia reálneho skutkového stavu a páchatel'a trestného činu. Pri objasňovaní dopravných nehôd a vyvodzovaní zavinenia majú z údajov EDR kľúčový význam najmä rýchlosť vozidla, brzdenie, poloha a sklon vozidla na ceste pred udalosťou a tesne po nej. Práve tieto údaje sú často predmetom dokazovania v rámci trestného konania, pretože ich poznanie má význam z hľadiska určenia, kto zavinil dopravnú nehodu, či sa jej vzniku dalo predísť a za akých okolností a pod. Tieto údaje zároveň majú význam aj v prípade objasňovania trestného činu poisťovacieho podvodu podľa § 223 TZ, pretože umožňujú zistiť, či k dopravnej nehode vôbec došlo, resp. či k nej došlo tak, ako ju oznamovateľ opisuje. Preto získanie takýchto údajov o priebehu skutkového deja a toho, čo mu predchádzalo, zo systému EDR procesne správnym a zákonným spôsobom, má teda kľúčový význam pre trestné konanie.

Pri riešení otázky, akým spôsobom procesne zaistiť na účely trestného konania informácie (dôkazy) zaznamenané systémom EDR, musíme – podľa nášho názoru – zobrať do úvahy aj samotnú konštrukciu, resp. umiestnenie systému EDR vo vozidle, ako aj prístup k jeho obsahu.

Vychádzajúc z čl. 4 bod 1 delegovaného nariadenia 2022/545, *údaje o zrážke zaznamenané zariadeniami na záznam údajov o udalostiach sa sprístupňujú na načítanie cez sériový dátový port na normalizovanom spojovacom dátovom konektore. Ak sériový dátový port po zrážke nie je funkčný, údaje sa musia dať načítať priamym pripojením k zariadeniu na záznam údajov o udalostiach.*

Podľa čl. 4 bod 4 delegovaného nariadenia 2022/545, *údaje zaznamenané zariadením na záznam údajov o udalostiach nesmú byť k dispozícii na načítanie cez rozhrania, ktoré sú prístupné bez toho, aby bolo potrebné vozidlo odomknúť alebo použiť nástroje, ani cez rozhrania vozidla pre bezdrôtové pripojenia. Zároveň podľa bodu 5. písm. b) údaje zariadenia na záznam údajov o udalostiach sprístupnené podľa odseku 1 nesmú obsahovať žiadne informácie, ktoré by umožnili spojiť tieto údaje s fyzickou osobou, ani nesmú byť sprístupnené spolu s takýmito informáciami.*

Z uvedených obmedzení k prístupu do systému EDR vo vozidle vyplýva, že získanie dát zo systému EDR nie je možné bez priameho napojenia na dátový port, ku ktorému nie je možný prístup bez odomknutia (teda sprístupnenia vozidla). To je z nášho pohľadu kľúčové na využitie konkrétnych trestnoprocesných inštitútov pre získanie dát, a teda informácií (dôkazov) pre trestné konanie zadovážených systémom EDR.

V praxi teda môžu nastať v zásade dve situácie. V jednom prípade majú orgány činné v trestnom konaní alebo súd k dispozícii vozidlo zaistené ako celok, resp. jeho časť (v prípade poškodenia vozidla), ktorá obsahuje prístup k systému EDR. V druhom prípade orgány činné v trestnom konaní alebo súd samotným vozidlom, resp. s jeho časťou obsahujúcou systém EDR aj s prístupom k nemu nedisponujú a toto vozidlo, resp. jeho časť má v dispozícii iný subjekt (napr. majiteľ vozidla, poisťovňa, a pod.). Abstrahujeme teraz od situácie, že síce vozidlo alebo jeho časť so systémom EDR fyzicky existuje, ale orgány činné v trestnom konaní alebo súd nemajú vedomosť, kde sa nachádza, resp. je nedostupné (napr. z dôvodu krádeže, potopenia vozidla v priehrade a pod.).

V prvom prípade orgány činné v trestnom konaní alebo súd (ďalej len „OČTK a súd“) získajú vozidlo so systémom EDR, resp. jeho časť vrátane systému EDR, do svojej dispozície vykonaním zaisťovacieho úkonu, ktorého predmetom je vozidlo ako celok, prípadne časť vozidla so systémom EDR, nie však samostatný a samotný systém EDR. V praxi pôjde najčastejšie o zaistenie vozidla ako vecného dôkazu na účely dokazovania v rámci vykonania obhliadky miesta činu – dopravnej nehody. Ďalšími do úvahy prichádzajúcimi alternatívami sú zaistenie vozidla ako veci dôležitej pre trestné konanie v rámci domovej prehliadky podľa § 100 TP alebo prehliadky iných priestorov alebo pozemkov podľa § 101 TP. Ďalšími do úvahy prichádzajúcimi zaisťovacími inštitútmi, ktorými možno zaistiť vozidlo ako celok (prípadne jeho časť so systém EDR), sú inštitúty vydania veci podľa § 89a TP, odňatia veci podľa § 90 TP alebo prevzatia zaisťovanej veci podľa § 92 TP, ak sú vozidlo alebo jeho časť potrebné zaistiť na účely doka-

zovania. Ak je potrebné vozidlo (jeho časť) zaistiť ako nástroj alebo výnos z trestnej činnosti, prichádza do úvahy aj jeho zaistenie prostredníctvom inštitútu zaistenia hnuiteľnej veci podľa § 96f TP.²⁷

Výhradným alebo prioritným cieľom v prípade použitia uvedených zaisťovacích inštitútov vo vzťahu k vozidlu ako celku alebo jeho časti, ktorá zahŕňa aj systém EDR, však nemôže byť získanie údajov zo systému EDR. V prípade aplikácie týchto procesných inštitútov vo vzťahu k celému vozidlu alebo jeho časti (ktorá zahŕňa aj systém EDR) za takýmto účelom by došlo k porušeniu princípov proporcionality a subsidiarity, ktoré vychádzajú zo zásady primeranosti a zdržanlivosti uvedenej v § 2 ods. 2 TP. Ich porušenie by mohlo viesť až k nepoužiteľnosti dôkazov získaných na základe informácií zo systému EDR.

Na druhej strane, ak dôvodom zaistenia vozidla ako celku alebo jeho časti (vrátane systému EDR) bola jeho potreba ako veci dôležitej pre trestné konanie, ktoré nezahŕňala len výhradne jeho potrebu za účelom získania údajov zo systému EDR, ale napríklad aj potrebu zistenia ďalších dôkazov napríklad v podobe zistenia miery a charakteru poškodenia vozidla, zaistenia stôp po trestnom čine nachádzajúcich sa na vozidle alebo v ňom, je využitie vyššie uvedených zaisťovacích inštitútov plne oprávnené a voľba použitia konkrétneho inštitútu bude závisieť od konkrétnych okolností daného prípadu pri rešpektovaní zásad legality, legitimacy, proporcionality a subsidiarity použitia zaisťovacích inštitútov. Prístup OČTK a súdu k systému EDR a informáciám v ňom bude daný z dôvodu zaistenia vozidla ako celku alebo jeho časti, ktorá zahŕňa aj systém EDR. V takomto prípade nebude potrebné podľa nášho názoru potrebné v zásade vykonávať osobitný zaisťovací úkon vo vzťahu k informáciám obsiahnutým v systéme EDR. Ak bola teda vec dôležitá pre trestné konanie zaistená jedným zo zaisťovacích procesných inštitútov, nie je ju potrebné na účely vykonania dôkazu v konkrétnom konaní opätovne zaisťovať iným zaisťovacím inštitútom, ktorý predpokladá získanie určitého druhu dôkazu obsiahnutého v už zaistenej veci.²⁸

²⁷ K jednotlivým zaisťovacím inštitútom a podmienkam ich použitia, ako aj otázkam zmien dôvodu zaistenia pozri napr. STRÉMY, T., ŠAMKO, P., KURILOVSKÁ, L. a kol. *Trestný poriadok. Praktický komentár*. Praha : Wolters Kluwer ČR, a. s., 2024, s. 259 – 340 alebo ČENTĚŠ, J., KURILOVSKÁ, L., ŠIMOVČEK, I., BURDA, E. a kol. *Trestný poriadok I*. § 1 – 195. Bratislava : C. H. Beck, 2021, s. 464 – 556.

²⁸ Pozri k tomu primerane aj R 47/2017. Uvedené možno dovodiť aj využitím *argumentum a simili* zo znenia § 89 ods. 2 prvá veta TP, ktorý prioritizuje ako dôvod zaistenia veci potrebu veci na účely dokazovania. Keďže TP osobitne upravuje procesné inštitúty zaistenia veci na účely dokazovania a osobitne procesné inštitúty na účely zaistenia veci ako nástrojov trestnej činnosti a výnosov z trestnej činnosti, možno z toho logicky dovodiť, že inštitúty zaistenia veci na účely dokazovania (vydanie veci, odňatie veci, prevzatie veci a uchovanie, vydanie a odňatie počítačových údajov) majú byť pri súčasnej existencii viacerých dôvodov zaistenia využité prednostne a výhradne. Nie je teda potrebné vec zaisťovať súčasne dvoma rôznymi zaisťovacími inštitútmi (na účely dokazovania a súčasne ako nástroj alebo výnos z trestnej činnosti), ak jedným z dôvodov zaistenia je zaistenie na účely dokazovania. Uvedené vyplýva aj z § 89 ods. 2 posledná veta TP, keď sa nevyžaduje zmena účelu zaistenia, ak vec bola zaistená na účely dokazovania a ide o vec, vo vzťahu ku ktorej sú splnené podmienky na uplatnenie sankcie postihujúcej veci, ktoré sú nástrojom alebo výnosom trestnej činnosti. Ak v takomto prípade nie je potrebné meniť dôvod zaistenia, tak podľa nášho názoru, ak sa takto nemeň dôvod zaistenia, nie je potrebné aplikovať na zaistenie veci (zaistenej na účely dokazovania) opakované zaistenie (prezaistenie) niektorým z inštitútov zaistenia veci ako nástroja alebo výnosu z trestnej činnosti.

V praxi bude potom bude v prípade zaistenia celého vozidla alebo jeho časti so systémom EDR na účely dokazovania najčastejším postupom, akým sa OČTK a súd dostanú k údajom (informáciám) zo systému EDR, pribratie znalca postupom podľa § 142 a nasl. TP a zadanie znaleckého skúmania znalcovi z odboru cestná doprava, ktorému OČTK a súd sprístupnia, resp. poskytnú vozidlo (jeho časť) na účely jeho znaleckého preskúmania, v rámci ktorého znalec za účelom objasnenia zadaných otázok (úloh) vykoná extrakciu dát zo systému EDR, ktoré následne využije pri znaleckom skúmaní. Extrakciu dát znalec vykoná napr. za pomoci čítačky údajov EDR (Crash data retrieval tool – CDR) zn. BOSCH cez sériový dátový port na normalizovanom spojovacom dátovom konektore. Takto získané dáta o vozidle tesne pred dopravnou nehodou, resp. v dobe, keď sa stala a bezprostredne po nej následne v rámci znaleckého skúmania skomparuje s ostatnými zisteniami o dopravnej nehode (skutkovom deji) získanými z ostatných dôkazov zabezpečených OČTK a súdom (napr. obhliadkou miesta činu, kamerovými záznamami) a vypracuje znalecký posudok ako osobitný dôkazný prostriedok, v ktorom obsiahnuté závery znalca slúžia ako dôkaz v trestnom konaní.

Nie je vylúčené, že bude potrebné využiť údaje s EDR samostatne mimo znaleckého skúmania znalcom z odboru cestná doprava. V takom prípade by ich zaistenie prichádzalo do úvahy prostredníctvom znalca z odvetvia kriminalistická informatika, prípadne niektorého z odvetví odboru elektrotechnika, napr. riadiaca technika, výpočtová technika (hardvér), počítačové programy (softvér), bezpečnosť a ochrana informačných systémov za účelom ich extrakcie a následného sprístupnenia OČTK formou znaleckého posudku, ak sú takéto dáta potrebné na účely dokazovania z iného dôvodu ako potreby objasnenia priebehu nehodového deja.

V druhom prípade, teda ak OČTK a súd nemajú samotné vozidlo alebo jeho časť so systémom EDR k dispozícii,²⁹ sa procesný postup bude odvíjať od toho, či takéto vozidlo alebo jeho časť so systémom EDR je potrebné zabezpečiť do trestného konania ako celok z dôvodu potreby zaistenia aj iných stôp, informácií a dôkazov ako len samotných údajov zo systému EDR. V prípade potreby zaistenia vozidla alebo jeho časti ako celku bude potrebné postupovať ako v prvom prípade, teda vozidlo (jeho časť) zaistiť niektorým z už spomenutých zaisťovacích inštitútov (úkonov), a to takým, aby boli rešpektované princípy proporcionality a subsidiarity týchto úkonov.

Ak je však potrebné na účely trestného konania získať údaje výhradne zo systému EDR, a zároveň OČTK a súd nepotrebujú vozidlo alebo jeho časť zaistiť aj na účely získania iných stôp a informácií (resp. ho nemajú fyzicky z iného zákonného dôvodu vo svojej dispozícii), bude potrebné vo vzťahu k získaniu údajov zo systému EDR postupovať podľa § 91 TP, teda za využitia inštitútu uchovania, vydania a odňatia počítačových údajov. V takomto prípade vydá prokurátor v predsúdnom konaní alebo predseda senátu v súdnom konaní príkaz podľa § 91 ods. 1 písm. b) a písm. e) TP, ktorý osobe, ktorá je držiteľom vozidla alebo jeho časti so systémom EDR, uloží povinnosť umožniť vyhotovenie a ponechanie si kópie takých údajov, a ich vydanie na účely dokazovania. Samotnú

²⁹ Napríklad bolo vozidlo medzičasom vrátené majiteľovi, resp. nebolo zaistené pri obhliadke miesta činu – miesta dopravnej nehody a pod.

extrakciu dát vykonaná v praxi zvyčajne pribratý znalec za pomoci čítačky údajov EDR (CDR) cez sériový dátový port na normalizovanom spojovacom dátovom konektore, ako už bolo spomínané. V prípade, ak by osoba tomuto príkazu podľa § 91 ods. 1 písm. b) a písm. e) TP nevyhovela, môžu byť takéto údaje podľa § 91 ods. 6 TP odňaté.

Vzhľadom na to, že vozidlo je považované aplikačnou praxou za iný priestor a v zmysle čl. 4 bod 4 delegovaného nariadenia 2022/545 získanie dát zo systému EDR nie je možné bez priameho napojenia na dátový port, ku ktorému nie je možný prístup bez odomknutia (teda sprístupnenia vozidla), tak v prípade „nespolupráce“ držiteľa vozidla pri realizácii príkazu na uchovanie, vydanie a odňatie počítačových údajov podľa § 91 ods. 1 písm. b) a písm. e) TP, je potrebné vykonať takýto úkon postupom podľa § 107 TP, teda s primeraným použitím ustanovení o prehliadke iných priestorov alebo pozemkov podľa § 101 a nasl. TP a následne odňatí dát zo systému EDR.

Samotné spracovanie informácií a údajov zaistených zo systému EDR bude úlohou znalca z príslušného odboru a odvetvia, ktorého OČTK a súd priberú a stanoví mu konkrétne úlohy, resp. otázky.

Samozrejme, v rámci trestného konania je potrebné vopred skúmať dodržanie najmä zásad proporcionality a subsidiarity vo vzťahu k dosiahnutiu cieľa, teda objasnenie trestného činu, teda či údaje o trestnom čine získané vykonaním získavania údajov z EDR cez už uvedené inštitúty nie je možné vykonať menej invazívnym spôsobom, resp. iným procesným úkonom, napr. cez znalecké skúmanie bez využitia údajov zo systému EDR a pod.

V súvislosti s potrebou získania dát zo systému EDR je pre úplnosť potrebné spomenúť, že mnohí prevádzkovatelia vozidiel (najmä subjekty podnikajúce v osobnej alebo nákladnej cestnej doprave) si nechávajú montovať, už pomerne dlhší čas, do vozidiel rôzne systémy, ktoré poskytujú obdobné údaje ako systém EDR. Ide o systémy *lokalizácie vozidiel cez GPS*³⁰ (prípadne aj *auto-kamery*) s *funkciou EDR*, ktoré môžu vykonávať:

- sledovanie GPS a polohy, keď poskytujú informácie o aktuálnej polohe vozidla a jeho histórii pohybu v reálnom čase,
- analýzu jazdného štýlu, keď merajú rýchlosť, monitorujú akceleráciu a brzdenie,
- detekciu incidentov, kedy vďaka vstavaným senzorom, ako je akcelerometer a g-senzor, dokážu zaznamenať prudké udalosti, ako sú nehody alebo nárazy,
- nahrávanie obrazu (prípadne obrazu a zvuku), keď nahrávajú videozáznam z jazdy, často s možnosťou živého vysielania alebo dodatočného stiahnutia záznamu,
- zasielanie upozornení, kedy odosielať upozornenia na akékoľvek zaznamenané udalosti, napríklad prostredníctvom e-mailu.

Údaje z takýchto systémov s funkciami systému EDR môžu do určitej miery nahradiť potrebu získania údajov, ktoré inak má uchovávať systém EDR, a to najmä v prípade vozidiel, ktoré neboli, resp. nie sú povinne vybavené systémom EDR (napr. z dôvodu ich uvedenia na trh pred tým, ako bola táto povinnosť v rámci EÚ ustanovená). Získanie údajov z týchto systémov môže spočívať jednak v postupe, keď tieto údaje poskytnú

³⁰ Pozri napr. stránku <https://infocar.sk/gps-monitoring-vozidiel/> (citované 16.09.205).

samotní ich držitelé v rámci účinnosti orgánem činným v trestném konání, například jako přílohu trestných oznámení nebo postupem podle § 3 Trestního řádku. Když údaje získané z těchto systémů nebudou většinou uloženy přímo v systémech vozidla, ale mimo něho (u poskytovatele služby nebo přímo majitele vozidla) na ich vyžádání v případě nespokojenosti těchto subjektů bude zřejmě potřebné vydání příkazu na uchování, vydání a odtahování počítačových údajů podle § 91 TP, který případně může být spojený s vydáním příkazu na prohlídku jiných prostorů nebo pozemků podle § 101 TP nebo domovní prohlídku podle § 100 TP, a to za účelem zabezpečení možnosti realizace příkazu na uchování, vydání a odtahování počítačových údajů podle § 91 TP.³¹

5. Automatizované vozidlo úrovně 4 a 5 a získání elektronických důkazů z nich

V této části se budeme zabývat možnostmi procesního postupu získání informací a důkazů z automatizovaných vozidel, které odpovídají úrovni 4 a 5 podle SAE standardu. Automatizované vozidlo předmetné úrovně se momentálně v rámci SR a ani EÚ v řadnej, resp. běžnej cestnej prevádzke nenachádzajú. Prebieha však ich testovanie v reálnych podmienkach.³² Vzhľadom na to budú naše úvahy a navrhované postupy návrhmi *pro futuro*, ktorých reálna možnosť aplikácie bude závisieť od budúcej právnej regulácie prevádzky takýchto vozidiel a ich technologického rozvoja. Poukážeme pritom najmä na možné problémy, ktoré vyplývajú zo súčasného stavu poznania, a ktoré bude potrebné do budúcnosti riešiť pri získavaní elektronických dôkazů z automatizovaných vozidiel úrovně 4 a 5 podľa SAE standardu.

Vo všeobecnosti sa automatizované vozidlo skladajú zo systémů, ktoré vykonávajú niektorú z troch až piatich základných funkcií, ktorými sú: vnímanie situácie (percepčia), lokalizácia, plánovanie, dohľad a navigácia, a správa (manažment) systému:

- a) **Vnímanie** sa týka zberu údajů a získavania relevantných informácií z okolia, ako je detekcia dopravných značiek, ako aj detekcia a klasifikácia objektů. Tieto detekčné úlohy vykonávajú rôzne senzory, ako sú kamery a rádiové detekčné a meracie zariadenia (RADAR).
- b) **Lokalizácia** sa týka schopnosti AV systému určiť polohu vozidla a jeho orientáciu vo vzťahu k okoliu.
- c) **Plánovanie** pozostáva z troch fáz:

³¹ Inštalácia týchto zariadení v týchto vozidlách musí byť v súlade s požiadavkami a zásadami na ochranu osobných údajů. K týmto otázkam pozri napr. Usmernenie 1/2020 k spracúvaniu osobných údajů v súvislosti s prepojenými vozidlami a aplikáciami týkajúcimi sa mobility vydané Európskym výborom pre ochranu údajů 9. marca 2021 dostupné on-line na <https://dataprotection.gov.sk/files/metod-edpb/usmernenia_k_spracovaniu_osobnych_udajov_v_suvvislosti_s_prepojenymi_vozidlami_a_aplikaciami_tykajucimi_sa_mobility.pdf> (citácia z 10.10.2025).

³² Napríklad v podobe skúšobnej prevádzky automatizovaných autobusů v Barcelone (Španielsko) v marci 2025 alebo Zürichu (Švajčiarsko) od januára 2025 – pozri <<https://futuretransport-news.com/renault-group-trials-autonomous-vehicles-in-europe/#~:text=Barcelona%2C%20Spain:%20Urban%20Public%20Transport%20Trials%20From,through%20accessible%2C%20efficient%2C%20and%20low%20Demission%20transport%20solutions.>> (citácia z 08.10.2025).

- použitie algoritmov plánovačom trasy na určenie najefektívnejšej geometrickej trasy.
- plánovač správania určí optimálne správanie na základe trasy naplánovanej plánovačom trasy.
- odhad najlepšej možnej trasy s ohľadom na dynamiku vozidla a obmedzenia prostredia.

d) Dohľad (kontrola) sa týka vykonávania naplánovaných akcií a riadenia pohybov vozidla, ako je zmena jazdného pruhu.

e) Manažment (riadenie) systému zahŕňa všetky funkcie súvisiace so záznamníkmi udalostí, interakciami človek – stroj zahŕňajúcimi rozhrania vo vozidle a externými rozhraniami človek – stroj.

Alternatívny prístup delí systémy automatizovaných vozidiel na dve hlavné zložky: systém vnímania a systém rozhodovania.³³

Automatizované vozidlá v prípade ich uvedenia do bežnej prevádzky budú generovať obrovské množstvo údajov, ktoré môžu slúžiť ako kľúčové dôkazy v trestných konaniach, najmä v prípadoch dopravných nehôd alebo trestných činov spáchaných na takýchto vozidlách alebo s ich pomocou. Tieto údaje (dáta) zahŕňajú, resp. by v budúcnosti mali zahŕňať najmä:

- **údaje zo senzorov a diagnostické záznamy** ako informácie z kamier, LiDAR-u, radaru, GPS a akcelerometrov, ktoré umožňujú rekonštruovať rýchlosť, polohu, trajektóriu a vnímanie okolia vozidla tesne pred nehodou a počas nej;
- **údaje o stave systému**, ako sú protokoly označujúce úroveň zapojenej autonómie (napr. autopilot, úplné autonómne riadenie), varovania dané ľudskému vodičovi vo vozidle (alebo vodičovi/užívateľovi vykonávajúcemu dohľad na diaľku) a informácie o tom, či vozidlo žiadalo človeka, aby prevzal kontrolu;
- **údaje o úkonoch užívateľa**, ako sú záznamy o interakcii človeka vo vzťahu k vozidlu, napríklad pohyb volantu, použitie brzdového/akceleračného pedálu alebo iné manuálne zásahy;
- **údaje o stave riadiaceho softvéru (systému) vozidla**, ktoré zahŕňujú údaje o aktualizácii softvéru, chybových hláseniach, prípadných neoprávnených vstupoch (zášachoch) a pod., ktoré dokumentujú najmä presnosť a spoľahlivosť údajov, ako aj ich vierohodnosť.

V súvislosti s následným získavaním takýchto údajov, a tým aj elektronických dôkazov, z automatizovaných vozidiel na účely trestného konania vzniká viacero praktických problémov, ktoré vyplývajú najmä z množstva a charakteru dát (údajov) a informácií prijímaných, spracovávaných a uchovávaných automatizovanými vozidlami. Ide najmä o nasledujúce problémy vyplývajúce z veľkého rozsahu dát (údajov) spracovávaných automatizovanými vozidlami:

- **fragmentácia dát** na rôzne typy a formáty vyplývajúca z množstva systémov s ktorými automatizované vozidlo pracuje. S tým je spojená aj existencia rôznych typov

³³ ALHABIB, R., YADAV, P. Data authorisation and validation in autonomous vehicles: a critical review. In *Discover Applied Scienc.* s. 6 – 8.

portov, cez ktoré je možné k týmto dátam u jednotlivých systémov pristupovať a takto ich na účely dokazovania zisťovať. Zároveň majú jednotlivé systémy rôznu úroveň zabezpečenia prístupu k ich dátam;

- **časové obmedzenia dostupnosti** niektorých dát využívaných automatizovanými vozidlami pri ich rozhodovaní (napr. údaje z vonkajších senzorov, na základe ktorých sa systém automatizovaného vozidla rozhoduje, ktoré sú dostupné v reálnom čase, teda v čase rozhodovania, avšak následne ich už systém neuloží);
- **externé ukladanie dát a údajov**, teda uchovávanie niektorých typov dát mimo samotné automatizované vozidlo. Ide o dáta týkajúce sa najmä aktualizácii softvéru vozidla zo strany výrobcu, zdrojových kódov a pod., ktoré nie sú uchovávané priamo vo vozidle, ale mimo neho, napr. na rôznych cloudových úložiskách, prípadne serveroch výrobcu vozidla. Z toho vyplýva, že dáta a informácie z automatizovaných vozidiel môžu byť vo vlastníctve alebo držbe viacerých subjektov súčasne;
- **veľké objemy dát** spracovávané systémami automatizovaných vozidiel a z toho vyplývajúce nároky v prípade potreby ich uchovávaní;
- **otázka skúmania a overenia presnosti, spoľahlivosti a aktuálnosti** dát prijímaných a spracovávaných automatizovanými vozidlami v rámci ich rozhodovania;
- **súlady informácií získavaných vonkajšími a vnútornými senzormi automatizovaných vozidiel s právnymi predpismi** na úseku ochrany osobných údajov ako aj ochrany základných práv a slobôd³⁴ (pôjde napríklad o informácie získané kamerovými systémami automatizovaného vozidla snímajúcimi okolie, záznamy komunikácie medzi vozidlom a osobami vnútri vozidla, informácie získané vozidlo prostredníctvom internetu od poskytovateľov elektronických služieb a pod.).

Ďalšou problematickou oblasťou spojenou s využívaním umelej inteligencie v automatizovaných vozidlách úrovne 4 a najmä 5 SAE štandardu je otázka vyvodzovania trestnoprávnej zodpovednosti v prípade konaní s účasťou plne automatizovaných vozidiel, teda vozidiel úrovne 5, ktoré sú riadené umelou inteligenciou, alebo konaní umelej inteligencie pri automatizovaných vozidlách úrovne 4 podľa SAE štandardu počas toho, ako táto samostatne vykonáva dynamické jazdné úlohy (riadi vozidlo). V súčasnosti existujúce modely trestnej zodpovednosti sa môžu ukázať v budúcnosti ako neadekvátne alebo nedostatočné vo vzťahu k predpokladanej budúcej roli umelej inteligencie v trestnoprávne relevantných konaniach spojených s užívaním automatizovaných vozidiel. Limity modelov (konceptov) trestnoprávnej zodpovednosti v tomto smere môžu viesť k narušeniu princípu právnej istoty, keď umelá inteligencia alebo systém, ktorý ju obsa-

³⁴ V príspevku sa podrobnejšie nezaobráame otázkami, ako dáta zbierané, resp. využívané, spracovávané a uchovávané automatizovanými vozidlami úrovne 4 a 5 zasahujú do oblasti ochrany osobných údajov a základných práv a slobôd, pretože uvedená problematika by výrazne prekračovala akceptovateľný rozsah príspevku a vyžaduje si vzhľadom na množstvo možných interakcií skôr samostatný príspevok, prípadne štúdiu. K tejto problematike pozri napr. usmernenie 1/2020 k spracúvaniu osobných údajov v súvislosti s prepojenými vozidlami a aplikáciami týkajúcimi sa mobility vydané Európskym výborom pre ochranu údajov 9. marca 2021, dostupné na: https://dataprotection.gov.sk/files/metodedpb/usmernenia_k_spracuvaniu_osobnych_udajov_v_suvvislosti_s_prepojenymi_vozidlam_i_aplikaciami_tykajucimi_sa_mobility.pdf (citácia z 10.10.2025).

huje, uskutoční konanie, ktoré bude naplňať znaky trestného činu z pohľadu objektu a objektívnej stránky, avšak bez dostatočného prepojenia tohto konania na podmienky zodpovednosti za konkrétny čin, tak aby boli naplnené všetky znaky skutkovej podstaty trestného činu.³⁵

Z hľadiska riešenia prístupu k trestnoprávnej zodpovednosti za konania spojené s umelou inteligenciou je zrejme najcitovanejšou Hallevyho práca.³⁶ V nej sú prezentované tri základné modely (koncepty) prístupov k riešeniu trestnej zodpovednosti umelej inteligencie, resp. systémov, ktoré ju využívajú. Ide o:

- 1) model spáchania prostredníctvom iného (*perpetration by another*), inak koncept tzv. nepriameho páchatel'stva;
- 2) model prirodzene predvídateľných následkov (*natural probable consequence*), inak model zavinenia založený na nedbanlivosti;
- 3) model priamej zodpovednosti (*direct liability*).

Zatiaľ čo prvé dva prístupy predstavujú aplikáciu a prispôsobenie už aplikovaných a existujúcich prístupov k riešeniu a vyvodzovaniu trestnej zodpovednosti v kontinentálnych právnych poriadkoch, tretí prístup uvažujúci s priamou zodpovednosťou umelej inteligencie naráža na limity existujúcich prístupov k otázke trestnej zodpovednosti. Pri bližšom skúmaní jednotlivých modelov je však možné rovnako naraziť na isté úskalia.³⁷

Doterajšie prijaté právne úpravy pristupujú k riešeniu problematiky trestnej zodpovednosti pri prevádzke automatizovaných (autonómnych) vozidiel rôzne a nejednotne.³⁸ Britský Autonomous Vehicles Act 2024 trestnú zodpovednosť pri využívaní automatizovaných vozidiel rieši tak, že vodiči automatizovaných vozidiel majú imunitu voči trestnej zodpovednosti vyplývajúcej zo spôsobu jazdy vozidla, keď je aktivovaný automatizovaný riadiaci systém vozidla. Autonomous Vehicles Act 2024 na druhej strane vytvára licencované a regulované subjekty, ktoré, naopak, majú zodpovednosť za spôsob jazdy automatizovaného vozidla, teda sú zodpovedné za následky spojené s jazdou automatizovaného vozidla pri zapnutom automatizovanom riadiacom systéme.³⁹ Nemecká právna úprava, naopak, priamo trestnú zodpovednosť vodiča automatizovaného vozidla, resp. osoby dohliadajúcej na automatizované vozidlo priamo nerieši. Vychádzajúc z § 7 ods. 1

³⁵ Pozri KING, C. T., AGGARWAL, N., TADDEO, M., FLORIDI, L. Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions. In *Science and Engineering Ethics*. Vol. 26, Iss. 1, 2020, s. 95, dostupné na: <https://doi.org/10.1007/s11948-018-00081-0>.

³⁶ HALLEVY, G. The Criminal Liability of Artificial Intelligence Entities – from Science Fiction to Legal Social Control. In *Akron Intellectual Property Journal*. Vol. 4, Iss. 2, Article 1, 2010, s. 171 – 201, dostupné na: <https://ideaexchange.uakron.edu/akronintellectualproperty/vol4/iss2/1> (citácia z 10.10.2025).

³⁷ Bližšie k otázkam trestnoprávnej zodpovednosti umelej inteligencie pozri VOJTUŠ, F., KORDÍK, M., DRAŽOVÁ, P. *Umelá inteligencia, jej využívanie a trestnoprávna zodpovednosť – výzvy, problémy a možné riešenia*. s. 549 – 570.

³⁸ K problematike trestnej zodpovednosti pri prevádzke automatizovaných vozidiel v rámci EÚ pozri napr. GLESS, S., LIGETI, K. (2023). Regulating driving automation in the European Union – criminal liability on the road ahead? In *New Journal of European Criminal Law*, Vol. 15, Iss. 1, 2024, s. 33 – 57, dostupné na: <https://doi.org/10.1177/20322844231213336>.

³⁹ Pozri Automated Vehicles Act 2024 Explanatory Notes, 2024, vydané The Stationery Office, s. 6 a 10, dostupné na: https://www.legislation.gov.uk/ukpga/2024/10/pdfs/ukpgaen_20240010_en.pdf (citácia z 10.10.2025).

a ods. 2 nemeckého zákona o cestnej premávke – Straßenverkehrsgesetz (StVG) – je možné konštatovať, že vodič (držiteľ vozidla) je zodpovedný za akékoľvek škody alebo zranenia spôsobené osobám alebo na majetku v dôsledku prevádzky vozidla, iba že by sa preukázalo, že k nim došlo v dôsledku *vis maior*.

Zo slovenskej úpravy (opísanej v predošlom texte) je zrejmé, že každé vozidlo vybavené automatizovaným systémom riadenia, teda aj plne automatizované vozidlo, musí mať vodiča, resp. osobu, ktorá nad ním vykonáva dohľad, a to prípadne na diaľku. Táto osoba je povinná prevziať riadenie, ak si to okolnosti v cestnej premávke vyžadujú bez ohľadu, či bola na to vozidlom vyzvaná alebo nie. Tým je podľa nás v slovenskej právnej úprave vo všeobecnosti daná zodpovednosť vodiča (vrátane trestnoprávnej) za následky spôsobené prevádzkou automatizovaného vozidla.⁴⁰ Tejto zodpovednosti by sa mohol prípadne zbaviť, ak by sa preukázalo, že k následku došlo v dôsledku chyby automatizovaného riadiaceho systému, ktorú nemohol predvídať a ani jej zabrániť.

Z hľadiska trestného konania je možné z nášho pohľadu *umelú inteligenciu autonómneho vozidla vnímať, za predpokladu jej aspoň čiastočnej právnej subjektivity de lege ferenda, ako subjekt trestného konania s analytickými schopnosťami, ktorý vie poskytnúť orgánom činným v trestnom konaní alebo súdu či už samostatne, alebo prostredníctvom znalca výstupy, predikcie alebo údaje, ktoré sú dôležité pre trestné stíhanie na podklade doručených súhlasov, alebo príkazov..., pričom by malo ísť o takú úroveň samostatného konania, ktoré je analogické so všeobecnou doktrínálnou definíciou svedka ako subjektu, ktorý dokáže vypovedať o skutočnostiach dôležitých pre trestné stíhanie, ktoré vnímal svojimi zmyslami, ktoré by boli v prípade umelej inteligencie nahradené jej senzormi, kamerami atď. V týchto prípadoch by malo ísť o situácie, keď autonómne vozidlo získa informácie dôležité pre trestné stíhanie, elektronické dôkazy, v rámci štandardnej (obvyklej) prevádzky samotného vozidla, resp. jeho senzorov, ktoré sa predpísaným spôsobom ukladajú a ex post vznikne potreba ich využitia na účely trestného stíhania.*⁴¹

V tomto smere zaujímavo vyznieva napríklad práca autorov GLESS, S., LEDERER, F., WEIGEND, T.,⁴² ktorí rozoberajú cez komparáciu pravidiel a princípov dokazovania v americkom právnom systéme a v nemeckom právnom systéme možnosť využitia dôkazu získaného činnosťou umelej inteligencie (automatizovaného vozidla). Úvodom pri tom predstavujú fikciu spočívajúcu vo vylúčení plne automatizovaného vozidla v rámci trestného konania vo vzťahu k priebehu nehody a jej okolnostiam. Následne rozoberajú otázky použiteľnosti a vierohodnosti takéhoto dôkazu aj s ohľadom na presnosť a spoľahlivosť dát, z ktorých pri svojich odpovediach vychádza umelá inteligencia.

Možnosťou a riešením vo vzťahu k získavaniu procesne dostupných údajov z automatizovaných vozidiel úrovne 4 a 5 podľa SAE štandardu na účely dokazovania v trestnom konaní, ktoré niektoré z už uvedených problémov dokáže eliminovať, je (podľa

⁴⁰ Pozri § 5 ods. 6 v spojení s § 2 ods. 2 písm. v) zákona č. 8ú2009 Z. z. o cestnej premávke.

⁴¹ ANDRAŠKO, J., DRAŽOVÁ, P., GYURÁSZ, Z. et al. *Biela kniha. Regulácia autonómnych vozidiel v Európskej únii a Slovenskej republike*. s. 21 – 22.

⁴² GLESS, S., LEDERER, F., WEIGEND, T. AI-Based Evidence In Criminal Trials? In *Tulsa Law Review*, Vol. 59, No. 1, 2024, s. 1 – 37.

nášho názoru) povinné umiestnenie a využívanie systému EDR vo vozidlách, ktorý však bude (oproti súčasnosti) vyžadovať zber a uchovávanie väčšieho množstva údajov o činnosti (resp. získaných činnosťou) automatizovaného vozidla. Na túto skutočnosť by mala reagovať *pro futuro* aj legislatíva.

Všetky osobné vozidlá v zmysle legislatívy EÚ (konkrétne nariadenia EÚ 2019/2144), automatizované vozidlá nevynímajúc, musia v súčasnosti už obsahovať aj systém EDR. Problémom je, že na skúmanie (najmä dopravných nehôd), ktorých účastníkom budú automatizované vozidlá úrovne 4 a 5, podľa SAE štandardu nebudú zjavne postačovať len údaje výslovne uvedené v čl. 6 bod 4. nariadenia EÚ 2019/2144. Nariadenie však v tomto prípade ustanovuje len minimálny rozsah údajov zaznamenávaných v systéme EDR. Z hľadiska právnej istoty a úpravy *de lege ferenda* bude zrejme potrebné legislatívne (buď na úrovni EÚ), alebo na národnej úrovni stanoviť presný rozsah dát zaznamenávaných systémom EDR (prípadne jeho iným variantom) v automatizovaných vozidlách, pričom časový rozsah a spôsob zaznamenávania údajov by vyplýval z charakteru dát. Dáta z vonkajších a vnútorných senzorov vozidiel (kamerové záznamy, LiDAR, RADAR, údaje z infotainment a pod.), ktoré svojim charakterom môžu predstavovať zásah do ochrany osobných údajov a základných práv a slobôd a uchovávali by sa len nevyhnutnú dobu a len za určité konkrétne (zákonom, nariadením) vymedzené obdobie, ktoré predchádzalo a nasledovalo po nehodovom deji alebo inej udalosti, ktorá by sa týkala napríklad poškodenia automatizovaného vozidla (napr. v dôsledku vandalizmu a pod.). Informácie týkajúce sa spoľahlivosti, presnosti, autenticity, aktuálnosti kľúčového riadiaceho softvéru vozidla (teda systému umelej inteligencie), ako aj ním využívaných systémov (asistenčné systémy), teda najmä údaje o vykonaných aktualizáciách, prístupové logy do systému, úpravy (autorizované, neautorizované) systému a pod., by sa ukladali od uvedenia vozidla do prevádzky, aby bolo možné posúdiť najmä otázky spoľahlivosti a presnosti dát, na základe ktorých sa systém riadiaci automatizované vozidlá rozhodoval.

Budúce využitie dát z automatizovaných vozidiel úrovne 4 a 5 si bude, okrem iného, vyžadovať aj podrobné stanovenie, či udalosť vznikla v dôsledku ľudského zásahu, poruchy hardvéru alebo skrytej poruchy softvéru. Táto analýza vyžaduje, aby sa štandardy vo vzťahu k systému EDR vyvinuli nad rámec jednoduchého zaznamenávania základnej dynamiky a rýchlosti vozidla, čo je charakteristické pre súčasné systémy EDR. Ako vhodné riešenie na získavanie elektronických dôkazov zo systémov automatizovaných vozidiel sa preto javí zavedenie alebo doplnenie systému EDR aj o systém ukladania údajov pre automatizované riadenie (Data Storage System for Automated Driving – DSSAD).

Pre úroveň automatizovaných vozidiel 3 a vyššiu podľa SAE štandardu, kde systém dokáže vykonávať všetky úlohy spojené s riadením počas určitého času, nie je systém EDR (bez systému DSSAD), ktorý by indikoval, kto mal počas nehody kontrolu nad vozidlom, dostatočným nástrojom na následné určenie povinnosti a zodpovednosti. Zatiaľ čo systém EDR v podstate predstavuje systém na ukladanie dát na základe udalostí, systém DSSAD predstavuje systém nepretržitého ukladania špecifických súborov úda-

jov o automatizovanom riadení vozidla. Systém DSSAD teda poskytuje informácie o tom, kto v danom čase ovládal riadenie vozidla, na základe údajov zahŕňajúcich polohu a časové údaje o prepnutí automatického riadiaceho systému z jedného režimu do druhého, údajov o tom, či je systém aktivovaný, manuálne alebo automaticky deaktivovaný. Preto zaznamenáva aj čas a polohu a kedy je vodič vyzvaný na prevzatie riadenia, polohu a časové údaje o prekonaní brzdového ovládania vodičom, polohu a časové údaje o požiadavke na zmenu režimu zo strany automatického riadiaceho systému. Takto je možné odvodiť povahu dôvodov požiadavky na zmenu režimu alebo deaktiváciu systému.⁴³

Procesný postup zaistenia údajov a informácií z automatizovaného vozidla, resp. plne automatizovaného vozidla by následne prebiehal spôsobom popísaným v prípade zaistovania údajov zo systému EDR, a to pri využití tam uvedených procesných inštitútov v závislosti od toho, či vozidlo, resp. jeho časť s prístupom do systému EDR/DSSAD majú OČTK a súd vo fyzickej dispozícii alebo nie.

Vo vzťahu k dátam, ktoré sa nachádzajú mimo vozidla a má ich vo vlastníctve alebo držbe konkrétny subjekt, by sa postupovalo podľa § 91 TP, teda za využitia inštitútu uchovania, vydania a odňatia počítačových údajov. Na základe príkazu podľa § 91 ods. 1 písm. b) a písm. e) TP sa subjektu, ktorý má v moci uvedené dáta, uloží povinnosť umožniť vyhotovenie a ponechanie si kópie takých údajov a ich vydanie na účely dokazovania. Samotnú extrakciu dát vykonaná v praxi zvyčajne pribratý znalec. V prípade, ak by osoba tomuto príkazu podľa § 91 ods. 1 písm. b) a písm. e) TP nevyhovela, môžu byť takéto údaje podľa § 91 ods. 6 TP odňaté. Ak by sa takýto subjekt nachádzal v inom členskom štáte EÚ, museli by OČTK alebo súd postupovať prostredníctvom zákona č. 236/2017 Z. z. o európskom vyšetrovacom príkaze v trestných veciach.

V naposledy spomenutom prípade treba poukázať aj na to, že EÚ prijala v roku 2023 nariadenie Európskeho parlamentu a Rady (EÚ) 2023/1543 z 12. júla 2023 o európskych príkazoch na predloženie elektronických dôkazov a európskych príkazoch na uchovanie elektronických dôkazov v trestnom konaní a na výkon trestu odňatia slobody v nadväznosti na trestné konanie (ďalej „nariadenie o e-evidence“), ktoré sa však plne začne aplikovať až v roku 2026. Toto nariadenie o e-evidence rieši práve otázky získavania elektronických dôkazov⁴⁴ od poskytovateľov sieťových služieb v prípadoch, ak požadované elektronické dôkazy sa nachádzajú v inom štáte EÚ, ako je štát, ktorý ich vyžaduje (štát vydávajúci príkaz). Príslušný justičný orgán členského štátu bude môcť v rámci trestného konania v súlade s týmto nariadením nariadiť poskytovateľovi služieb, ktorý ponúka služby v EÚ, aby poskytol alebo uchoval elektronické dôkazy na základe európskeho príkazu na predloženie dôkazov alebo európskeho príkazu na uchovanie dôkazov.

Problémy týkajúce sa hodnotenia správnosti, presnosti, spoľahlivosti a aktuálnosti dát získaných z automatizovaných vozidiel, ako aj hodnotenia vplyvu možných chýb

⁴³ ALHABIB, R., YADAV, P. Data authorisation and validation in autonomous vehicles: a critical review. s. 18 – 19.

⁴⁴ Podľa čl. 3 bod 8. nariadenia o e-evidence sa elektronickými dôkazmi rozumejú údaje o účastníkovi, prevádzkové údaje alebo obsahové údaje uchovávané poskytovateľom služieb alebo v mene poskytovateľa služieb v elektronickej podobe v čase prijatia osvedčenia o európskom príkaze na predloženie dôkazov (OEP-PD) alebo osvedčenia o európskom príkaze na uchovanie dôkazov (OEPUD) týmto poskytovateľom služieb.

softvéru, prípadne hardvéru by bolo možné eliminovať prostredníctvom vytvorenia nového odvetvia v rámci odboru cestná doprava, ktoré by sa zaoberalo technickou analýzou automatizovaných vozidiel a priebehu nehôd s ich účasťou vrátane skúmania prípadných chýb automatizovaného riadiaceho systému takýchto vozidiel, či už na úrovni hardvérového, ale najmä softvérového riešenia (umelá inteligencia). Riešilo by teda aj prípadnú otázku nevhodného naprogramovania umelej inteligencie. Riešenie tejto otázky vyplýva aj z existencie problému tzv. efektu čiernej skrinky (black-box effect) pri rozhodovaní umelej inteligencie, keď ani sami tvorcovia často nevedia uviesť, prečo sa umelá inteligencia rozhodla pre dané riešenie a na základe akých postupov.⁴⁵ Overenie validity dát prostredníctvom znaleckého skúmania by v takomto prípade eliminovalo možné námietky obvinených a obhajoby v tomto smere.

6. K možnosti využitia automatizovaných vozidiel so systémom umelej inteligencie určeným na profilovanie, biometrickú kategorizáciu alebo biometrickú identifikáciu

Ako už bolo skôr uvedené, druhou významnou polohou využitia automatizovaných vozidiel v trestnom práve je jeho samotné využitie orgánmi činnými v trestnom konaní ako záznamového nosiča informácií, zbieraných v okolí automatizovaného vozidla, resp. v jeho dosahu ako novej formy informačno-technického prostriedku.⁴⁶ Táto optika posúva požiadavky na automatizované vozidlá, ich systémy a komponenty v zmysle čl. 1 písm. a) nariadenia EÚ 2019/2144 z režimu všeobecných požiadaviek vozidla na bezpečnosť cestnej premávky do režimu počítačového systému s umelou inteligenciou v zmysle Aktu o umelej inteligencii. V takom prípade bude potrebné takéto vozidlo posudzovať jednak podľa požiadaviek podľa nariadenia EÚ 2019/2144, ale taktiež z pohľadu požiadaviek na systémy umelej inteligencie podľa Aktu o umelej inteligencii.

Súčasnne uvádzame, že ak by sa na ďalej analyzované systémy vzťahovali metriky a zásady Aktu o umelej inteligencii, bez uvedených výnimiek, išlo by o vysoko rizikové systémy.⁴⁷ V praxi by to automaticky neznamenalo zákaz nasadenia takéhoto systému, avšak bol by kladený zvýšený dôraz na zamýšľaný účel a kontext používania systému AI a systém riadenia rizík, ktorý má zaviesť poskytovateľ,⁴⁸ ktorý by mal pozostávať z nepretržitého procesu plánovaného a prebiehajúceho počas celého životného cyklu vysokorizikového systému AI.⁴⁹ Na účely posúdenia súladu je potrebné pri vysokorizikových

⁴⁵ K otázkam black-box efektu pri používaní umelej inteligencie v trestnom práve pozri napr. QUEZADA-TAVÁREZ, K., VOGIATZOGLOU, P., ROYER, S. Legal challenges in bringing AI evidence to the criminal courtroom. In *New Journal of European Criminal Law*, Vol. 12, Iss. 4, 2021, s. 531 – 551, dostupné na: <https://doi.org/10.1177/20322844211057019>; prípadne pozri KING, C., T., AGGARWAL, N., TADDEO, M., FLORIDI, L. Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions. In *Science and Engineering Ethics*. Vol. 26, Iss. 1, 2020, s. 95, dostupné na: <https://doi.org/10.1007/s11948-018-00081-0>.

⁴⁶ Porovnaj §10 ods. 20 TP.

⁴⁷ Recitál 54 Aktu o umelej inteligencii a príloha III. Aktu o umelej inteligencii.

⁴⁸ Recitál 64 Aktu o umelej inteligencii.

⁴⁹ Recitál 65 a 66 Aktu o umelej inteligencii.

modeloch uchovávať použité súbory na tréning, technickú dokumentáciu a uchovávanie záznamov, udržiavať transparentnosť systému, ľudský dohľad a spoľahlivosť, presnosť a kybernetickú bezpečnosť.⁵⁰

Na účely tohto článku budú predmetom právnej analýzy a podmienok využitia dve možnosti, keď automatizované vozidlo bude vybavené systémom s umelou inteligenciou s cieľom (možnosťou) vykonávať:

- profilovania osoby, že sa stane páchatel'om trestného činu;⁵¹
- biometrickú kategorizáciu osôb⁵² alebo biometrickú identifikáciu osôb v reálnom čase.⁵³

Ostatné formy využitia v zásade možno zaradiť pod pojmy technického sledovania podľa ustanovení § 113 TP, alebo vyhotovenia obrazových, zvukových, alebo obrazovo zvukových záznamov podľa § 114 TP, či *packet sniffing* podľa § 116 TP, alebo § 91 TP, ak netvorí predmet telekomunikačného tajomstva⁵⁴ a v zásade ich bude možné zaradiť pod existujúce právne nástroje, ktorých zákonné použitie je ustálené dlhodobou aplikačnou praxou.⁵⁵

Použitie systému umelej inteligencie *na účely profilovania fyzickej osoby, z hľadiska toho, či spácha trestný čin*, je všeobecne zakázané, čo nevyplýva iba z Aktu o umelej inteligencii, ale taktiež z čl. 11 ods. 3 smernice EÚ 2016/680.⁵⁶ Zákaz sa vzťahuje na predvídanie rizika, že osoba spácha trestný čin na základe informácií o jej štátnej príslušnosti, miesta narodenia, miesta bydliska, počtu detí, výšky dlhu alebo typu vozidla. I keď pojem profilovanie a predpovedanie rizika, že osoba sa stane páchatel'om trestného činu nie je nikde definované⁵⁷ – vo všeobecnosti ide o rôzne pokročilé technológie a analyticky

⁵⁰ Recitál 65 a 66 Aktu o umelej inteligencii.

⁵¹ Čl. 5 ods.1, písm. d) Aktu o umelej inteligencii.

⁵² Čl. 5 ods.1, písm. g) Aktu o umelej inteligencii.

⁵³ Čl. 5 ods.1, písm. h) Aktu o umelej inteligencii upravuje iba tzv. Life Face Recognition (ďalej len LFR), identifikáciu v reálnom čase a nie identifikáciu osôb po spáchaní skutku tzv. post event/after facial recognition (AFR), čo predstavuje bežný postup orgánov presadzovania práva porovnávania tvári napr. z bezpečnostných kamier po spáchaní skutku počas tzv. pátrania po horúcej stope. Porovnaj EUROPOL: *AI AND POLICING. The benefits and challenges of artificial intelligence for law enforcement*. An Observatory Report from the Europol Innovation Lab. Luxembourg: Publications Office of the European Union, 2024, s. 24, dostupné na: <https://www.europol.europa.eu/publication-events/main-reports/aiandpolicing#:~:text=With%20the%20AI%20and%20policing%20report%2C%20produced%20through,more%20efficient%2C%20responsive%20and%20effective%20law%20enforcement%20model> (citácia z 21.10.2025).

⁵⁴ § 117 ods.1 zákona č. 452/2021 Z. z. o elektronických komunikáciách v znení neskorších predpisov.

⁵⁵ Pozri STRÉMY, T., ŠAMKO, P., KURILOVSKÁ, L. *Trestný poriadok. Praktický komentár*. s. 268 – 273, 358 – 388.

⁵⁶ Smernica Európskeho parlamentu a Rady (EÚ) 2016/680 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV (ďalej aj ako „smernica EÚ 2016/680“).

⁵⁷ Čl. 3 bodu 4 smernice EÚ 2016/680 o presadzovaní práva v oblasti ochrany údajov s poukazom na čl. 5 ods. 1 písm. d) Aktu o umelej inteligencii, profilovanie (všeobecne) vymedzuje použitím čl. 4 bodu 4 nariadenia 697/2016 – všeobecného nariadenia o ochrane osobných údajov ako „akúkoľvek formu automatizovaného spracúvania osobných údajov, ktoré pozostáva z použitia osobných údajov na vyhodnotenie určitých osobných aspektov týkajúcich sa fyzickej osoby, predovšetkým analýzy alebo predvídania aspektov dotknutej fyzickej osoby súvisiacich s výkonnosťou v práci, majetkovými pomermi, zdravím, osobnými preferenciami, záujmami, spoľahlivosťou, správaním, polohou alebo pohybom“.

ké metódy aplikované na veľký počet často historických ukazovateľov (vrátane sociálno-ekonomických údajov, záznamov OČTK a zložiek presadzujúcich právo atď.), ktoré sa v kombinácii s kriminologickými teóriami a štatistickými metódami používajú na strategické plánovanie síl a prostriedkov orgánov presadzovania práva a prevenciu kriminality.⁵⁸ Z uvedenej zakázanej praktiky je všeobecne vyňatá riziková analýza páchania trestnej činnosti na základe polohy, geopriestorových informácií o spáchaní trestného činu (tzv. hot spot analýza) za podmienky, že rozhodnutie sa musí uskutočniť vždy individuálnym ľudským posúdením.⁵⁹

Biometrická kategorizácia fyzických osôb je všeobecne zakázaná, ak je cieľom odvodiť alebo vyvodiť obmedzený počet citlivých charakteristík: rasu, politické názory, členstvo v odboroch, náboženské alebo filozofické presvedčenie, sexuálny život alebo sexuálnu orientáciu.⁶⁰ Možno však uviesť, že Akt o umelej inteligencii považuje za výnimky z uvedených zakázaných praktík biometrickej kategorizácie, tie ktoré sú právom dovolené využívať najmä zložkami presadzujúcimi právo pri plnení ich úloh, ako je tvorba rizikových analýz a predikcie páchania trestnej činnosti. resp. viktimizácie osôb najmä v spojení s terorizmom a obchodovaním s ľuďmi vo vzťahu k mladým ľuďom a deťom⁶¹, škálovanie osôb podľa všeobecných charakteristík pre účely rôznych identikitov, databáz častí tvare, očí, vlasov, pier a pod.⁶² Selekcii a mapovanie dát biometrických údajov by mali vykonávať systémy biometrickej kategorizácie práve pre to, aby bolo zaručené, že v sume zbieraných údajov budú zastúpené všetky demografické skupiny a zber sa nebude zameriavať na jednu konkrétnu skupinu. Opäť aj v tomto prípade platí všeobecná požiadavka finálneho ľudského posúdenia.⁶³ Avšak akákoľvek kategorizácia fyzických osôb na základe ich biometrických údajov zložkami vynucujúcimi právo s cieľom použiť ich rasu, politické názory, členstvo v odboroch, náboženské alebo filozofické presvedčenie, sexuálny život alebo sexuálnu orientáciu, a to aj v oblasti presadzovania práva je zakázané nielen v zmysle čl. 5 ods. 1 písm. d) Aktu o umelej inteligencii, ale taktiež je v rozpore čl. 11 ods. 3 smernice EÚ 2016/680.

Používanie systému umelej inteligencie s diaľkovou *biometrickou identifikáciou v reálnom čase (LFR)* vo verejne prístupných priestoroch je vo všeobecnosti zakázané, pretože predstavuje významný zásah do súkromia osôb.⁶⁴ Akt o umelej inteligencii sa však neaplikuje na systémy biometrickej identifikácie nasadené v oblasti národnej bez-

⁵⁸ EUROPOL: *AI and policing. The benefits and challenges of artificial intelligence for law enforcement*. s. 15.

⁵⁹ Rozsudok Súdneho dvora z 21. júna 2022, Ligue des droits humains, C-817/19, ECLI:EU:C:2022:491.

⁶⁰ Usmernenia Komisie o zakázaných praktikách využívajúcich umelú inteligenciu stanovených v nariadení (EÚ) 2024/1689, Oznámenie Európskej komisie C(2025) 5052 final z 29. 07. 2025, s. 100, ods. 283, dostupné na: [Guidelines_on_prohibited_artificial_intelligence_practices_established_by_Regulation_EU_20241689_AI_Act_Slovak_3mP9dTPmycBiuhqnN6dcPoPx8_118644.PDF](#) (citácia z 21.10.2025).

⁶¹ EUROPOL: *AI and policing. The benefits and challenges of artificial intelligence for law enforcement*. s. 52.

⁶² Recitál 30 Aktu o umelej inteligencii.

⁶³ Rozsudok Súdneho dvora z 21. júna 2022, Ligue des droits humains, C-817/19, ECLI:EU:C:2022:491.

⁶⁴ Recitál 33 Aktu o umelej inteligencii.

pečnosti, a to bez ohľadu na typ subjektu,⁶⁵ a pri predchádzaní trestnej činnosti. Ide o porovnávanie rozpoznávacích znakov osôb bez výrazného časového oneskorenia proti referenčnej databáze⁶⁶ na verejne prístupných miestach.⁶⁷

Pod pojem národná bezpečnosť možno zahrnúť záujem na ochrane základných funkcií štátu a základných záujmov spoločnosti, taktiež zahŕňa prevenciu a represiu aktivít, ktoré smerujú proti základným politickým, ústavným alebo spoločenským štruktúram krajiny, a najmä môžu priamo ohroziť spoločnosť, obyvateľstvo alebo samotný štát, ako sú napríklad teroristické aktivity.⁶⁸ Národná bezpečnosť nezahŕňa napríklad činnosti súvisiace s bezpečnosťou cestnej premávky⁶⁹ alebo organizáciou či výkonom spravodlivosti.⁷⁰

Vo vzťahu k biometrickej identifikácii v reálnom čase v zmysle uvedeného platí, že táto je možná, ak ide o:⁷¹

- cielené pátranie po konkrétnych obetiach únosov, obchodovania s ľuďmi alebo sexuálneho vykorisťovania ľudí, ako aj pátranie po nezvestných osobách;
- predchádzanie konkrétnemu, závažnému a bezprostrednému ohrozeniu života alebo fyzickej bezpečnosti fyzických osôb alebo skutočnej a existujúcej alebo skutočnej a predvídateľnej hrozbe teroristického útoku;
- lokalizáciu alebo identifikáciu osoby podozrivej zo spáchania trestného činu na účel vykonávania vyšetrovania alebo stíhania trestného činu alebo výkonu trestnej sankcie za trestné činy uvedené v prílohe II, za ktoré možno v konkrétnom členskom štáte uložiť trest odňatia slobody alebo ochranné opatrenie obmedzujúce slobodu s hornou hranicou trestnej sadzby najmenej štyri roky.⁷² Tento postup je aplikateľ-

⁶⁵ Rozsudok Súdneho dvora zo 6. októbra 2020, *La Quadrature du Net a i.*, C-511/18, C-512/18 a C-520/18, EU:C:2020:791, bod 13.

⁶⁶ Usmernenia Komisie o zakázaných praktikách využívajúcich umelú inteligenciu stanovených v nariadení (EÚ) 2024/1689, Oznámenie Európskej komisie C(2025) 5052 final z 29. 07. 2025, s. 106 – 107.

⁶⁷ Prístupnosť pre vopred nie stanovený počet osôb, nezávisle od kapacitných alebo bezpečnostných obmedzení, ako sú kúpa vstupenky alebo cestovného lístka, predchádzajúca registrácia alebo určitá veková hranica. Možnosť prístupu do priestoru, že priestor je verejne prístupný, ak existujú znaky alebo oznámenia, ktoré naznačujú opak (napríklad označenie obmedzujúce prístup) K tomu pozri: Usmernenia Komisie o zakázaných praktikách využívajúcich umelú inteligenciu stanovených v nariadení (EÚ) 2024/1689 z 29. 07. 2025, s. 108.

⁶⁸ Rozsudok Súdneho dvora zo 6. októbra 2020, *La Quadrature du Net a i.*, C-511/18, C-512/18 a C-520/18, EU:C:2020:791, bod 13.

⁶⁹ Rozsudok Súdneho dvora z 22. júna 2021, *Latvijas Republikas Saeima*, C-439/19, EU:C:2021:504, bod 68.

⁷⁰ Rozsudok Súdneho dvora z 5. júna 2023, *Komisija v. Poľsko*, C-204/21, EU:C:2023:442, bod 319.

⁷¹ Čl. 5 ods.1, písm. h) body I až III Aktu o umelej inteligencii.

⁷² Terorizmus, obchodovanie s ľuďmi, sexuálne vykorisťovanie detí a detská pornografia, nedovolené obchodovanie s omamnými alebo psychotropnými látkami, nedovolené obchodovanie so zbraňami, strelivom alebo s výbušnínami, vražda, ťažká ujma na zdraví, nedovolené obchodovanie s ľudskými orgánmi alebo tkanivami, nedovolené obchodovanie s jadrovými alebo rádioaktívnymi materiálmi, únos, obmedzovanie osobnej slobody alebo branie rukojemníka, trestné činy podliehajúce právomoci Medzinárodného trestného súdu, nezákonné ovládnutie lietadla alebo plavidla, znásilnenie, trestné činy proti životnému prostrediu, organizovaná alebo ozbrojená lúpež, sabotáž, účasť v zločineckej organizácii zapojenej do jedného alebo viacerých uvedených trestných činov.

ný aj v konaní o európskom zatýkacom rozkaze ako i medzinárodnom zatýkacom rozkaze.⁷³

Tieto výnimky netvoria právny základ takýchto systémov. Právnym základom je vnútroštátny predpis upravujúci podmienky využívania tohto biometrického systému. Ak takýto predpis neexistuje, je používanie systému na diaľkovú identifikáciu od 01. 02. 2025 zakázané.⁷⁴

Cielené pátranie zahŕňa lokalizáciu a identifikáciu obetí troch kategórií trestných činov:

- *únosov;*
- *obchodovania s ľuďmi a*
- *sexuálneho vykorisťovania*⁷⁵ a
- *pátrania po nezvestných osobách.*

Pri nezvestných osobách je možné zdôrazniť, že tento postup nie je postupom v rámci trestného konania, ale osobitného správneho konania, ktoré sa preto nepovažujú za postupy pri vyšetrovaní trestnej činnosti. V podmienkach SR je takýto postup upravený v § 2 ods. 1 písm. l) v spojení s § 69b a § 81b zákona č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov, pričom na toto použitie sa nevzťahuje biometrická identifikácia podľa Aktu o umelej inteligencii, ale nasadenie biometrickej identifikácie podľa Všeobecného nariadenia o ochrane osobných údajov.⁷⁶

Konkrétne, závažné a bezprostredné ohrozenie života alebo fyzickej bezpečnosti fyzických osôb bezprostredné ohrozenie života alebo fyzickej bezpečnosti fyzických osôb ako druhý dôvod môže zahŕňať aj bezprostredné ohrozenie kritickej infraštruktúry, ak by narušenie alebo zničenie takejto kritickej infraštruktúry viedlo k bezprostrednému ohrozeniu života alebo fyzickej bezpečnosti osoby, a to aj v dôsledku vážnej ujmy na poskytovaní základných dodávok pre obyvateľstvo alebo výkone základných funkcií štátu.⁷⁷ Bezprostredné ohrozenie života alebo fyzickej bezpečnosti je ohrozenie, ktoré môže nastať v ktoromkoľvek okamihu a vyžaduje si „prijatie okamžitých opatrení“. ⁷⁸ Konkrétne ohrozenie znamená, že ohrozenie je jasne vymedzené, individualizované a špecifické, teda že by nemalo byť hypotetické.⁷⁹

Pojem *skutočná a existujúca alebo skutočná a predvídateľná hrozba teroristického útoku*, ako sa používa v článku 5 ods. 1 písm. h) bode ii) je autonómnym pojmom práva

⁷³ Usmernenia Komisie o zakázaných praktikách využívajúcich umelú inteligenciu stanovených v nariadení (EÚ) 2024/1689, Oznámenie Európskej komisie C(2025) 5052 final z 29. 07. 2025, s. 117, ods. 354.

⁷⁴ Čl. 5 ods. 5 Aktu o umelej inteligencii.

⁷⁵ V podmienkach SR ide o trestný čin obchodovania s ľuďmi podľa § 179 TZ, trestný čin vydierania podľa § 189 TZ, trestný čin sexuálneho násillia podľa § 200, trestný čin sexuálneho zneužívania podľa § 201 TZ alebo trestný čin kupliarstva podľa § 367 TZ.

⁷⁶ Čl. 9 Všeobecného nariadenia o ochrane osobných údajov.

⁷⁷ Usmernenia Komisie o zakázaných praktikách využívajúcich umelú inteligenciu stanovených v nariadení (EÚ) 2024/1689, Oznámenie Európskej komisie C(2025) 5052 final z 29. 07. 2025, s. 114.

⁷⁸ Odôvodnenie 37 nariadenia (EÚ) 2023/1543.

⁷⁹ Usmernenia Komisie o zakázaných praktikách využívajúcich umelú inteligenciu stanovených v nariadení (EÚ) 2024/1689, Oznámenie Európskej komisie C(2025) 5052 final z 29. 07. 2025, s. 115.

Únie, a preto by sa mal v zásade posudzovať nezávisle od vnútroštátneho vymedzenia.⁸⁰ Musí ísť o skutočnú a reálnu hrozbu.⁸¹

Lokalizáciu alebo identifikáciu osoby podozrivej zo spáchania vybraných trestných činov je možné vykonávať na účel vedenia vyšetrovania alebo stíhania trestného činu alebo výkonu trestnej sankcie za vybrané trestné činy aby sa zistila alebo potvrdila totožnosť špecificky zacieleného jednotlivca.⁸² Z uvedeného vyplýva, že nemusí ísť iba o známu osobu, ale i jednotlivca, ktorého totožnosť je potrebné zistiť, ak je vyšpecifikovaný inak napr. kamerovým záznamom z bezpečnostnej kamery z miesta činu a pod.. Podmienky používania systémov diaľkovej biometrickej identifikácie v reálnom čase na účely presadzovania práva vo verejne prístupných priestoroch, musia byť:⁸³

- určité,
- taxatívne a
- primerané,

ak existuje „*nevyhnutná potreba*“ dosiahnuť „*významný verejný záujem*“, ktorý „*prevažuje nad rizikami*“, ktoré to predstavuje pre základné práva. Akékoľvek iné používanie systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva, ktoré nie je uvedené v článku 5 ods. 1 písm. h) bodoch i) až iii) Aktu o umelej inteligencii, je zakázané.

Vo vzťahu k prvému a tretiemu bodu výnimiek je zrejmé, že ide o identifikáciu známej osoby, resp. určiteľnej osoby, ktorej totožnosť sa má zistiť⁸⁴ a ktorej údaje sa porovnávajú voči údajom napr. z bezpečnostných kamier s použitím diaľkovej biometrickej identifikácie, s jasným cieľom stotožniť túto osobu, a to i pre potreby vyšetrovania. Súčasne ide o reaktívny prístup na skutočnosť predpokladanú v danom ustanovení.

Výnimka formulovaná v bode 2 je vágnejšia, avšak v zmysle výkladu Súdneho dvora musí ísť o konkrétne skutočnosti a nie všeobecnú prevenciu pred určitou hrozbou z dôvodu „*zhoršenia bezpečnostnej situácie*“⁸⁵. Avšak aj tu platí, že týmto spôsobom je možné zisťovať totožnosť vrátane lokalizácie.⁸⁶

Aplikácie umelej inteligencie v oblasti presadzovania práva sú taktiež vysoko rizikové vzhľadom na ich významný potenciál ovplyvniť individuálne práva a slobody.⁸⁷ Me-

⁸⁰ Tamže, s. 115.

⁸¹ Rozsudok Súdneho dvora z 20. septembra 2022, SpaceNet, C-793/19 (spojené veci C-793/19, C794/19), ECLI:EU:C:2022:702, bod 93;

⁸² Usmernenia Komisie o zakázaných praktikách využívajúcich umelú inteligenciu stanovených v nariadení (EÚ) 2024/1689, Oznámenie Európskej komisie C(2025) 5052 final z 29. 07. 2025, s. 120.

⁸³ Usmernenia Komisie o zakázaných praktikách využívajúcich umelú inteligenciu stanovených v nariadení (EÚ) 2024/1689, Oznámenie Európskej komisie C(2025) 5052 final z 29.07.2025, s. 117. ods. 354.

⁸⁴ Čl. 2 ods. 3 Aktu o umelej inteligencii.

⁸⁵ Rozsudok Súdneho dvora EÚ z 21. decembra 2016 vo veci *Tele2 Sverige AB a Secretary of State for the Home Department v. Post-och telestyrelsen a i.* C-203/15 a C-698/15, para. 117 – 119; Rozsudok Súdneho dvora EÚ 6. októbra 2020 vo veci *La Quadrature a i.* C-511/18, C-512/18, 520/18, para: 150.

⁸⁶ Usmernenia Komisie o zakázaných praktikách využívajúcich umelú inteligenciu stanovených v nariadení (EÚ) 2024/1689 Oznámenie Európskej komisie C(2025) 5052 final z 29. 07. 2025, s. 120. Čl. 2 ods. 3 Aktu o umelej inteligencii.

⁸⁷ EUROPOL: *AI and policing. The benefits and challenges of artificial intelligence for law enforcement.* s. 42.

dzi aplikácie považované za vysoko rizikové patria biometrické systémy používané na jedinečnú identifikáciu jednotlivcov, ako sú nástroje na rozpoznávanie emócií. Medzi ďalšie vysoko rizikové aplikácie patria niektoré kategorizačné systémy, ako aj systémy určené na hodnotenie rizika viktimizácie alebo páchania trestných činov prostredníctvom analýzy pravdepodobnosti, že sa jednotlivci stanú obeťami alebo páchatelmi trestných činov vrátane obchodovania s ľuďmi, domáceho násillia alebo počítačovej kriminality, či systémy biometrickej identifikácie.⁸⁸

Uplatnenie uvedeného systému biometrickej identifikácie v reálnom čase navyše okrem obsahuje ďalšie poistky, ktoré by mali brániť jeho zneužitiu vo forme primeranosti nebezpečnej vzniknutej situácie a primeranosti následkov pre dotknutých jednotlivcov.⁸⁹

Súčasne je v zmysle čl. 5 ods. 3 Aktu o umelej inteligencii pre použitie tejto výnimky potrebný súhlas nezávislej justičnej autority alebo nezávislého správneho regulačného orgánu, a to len po nevyhnutnú dobu, tento súhlas resp. príkaz je navyše možné vydať len po vykonaní posúdenia vplyvu na základné ľudské práva a slobody podľa čl. 27, ibaže vec neznesie odklad.⁹⁰ Vo vzťahu k slovenským právnym reáliám, by nasadenie tohto prostriedku malo podliehať príkazu sudcu pre prípravné konanie alebo súhlasu sudcu krajského súdu analogicky podľa zákona č. 166/2003 Z. z. pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním) v znení neskorších predpisov.

Posúdenie vplyvu podľa čl. 27 Aktu o umelej inteligencii, ktoré je povinné v zmysle čl. 5 ods. 2, sa odlišuje od posúdenia vplyvu na jednotlivca pri spracovaní osobných údajov.⁹¹ Posúdenie vplyvu musí obsahovať⁹²:

- opis používania diaľkovej biometrickej identifikácie a procesov nasadzujúceho subjektu v súvislosti s týmto používaním, spolu s jeho zamýšľaným účelom a referenčnou databázou a opisom technológie s právnym základom použitia systému;
- časový úsek, frekvenciu a spôsob používania vrátane súhlasu justičnej autority alebo správneho orgánu;
- kategórie osôb a skupín, ktoré sú systémom dotknuté. Je potrebné rozlišovať medzi zacielenou osobou, ktorá môže byť obeťou trestného činu, páchatelom alebo podozrivou osobou, osobami, ktorých biometrické údaje sú zahrnuté v referenčnej databáze, a kategóriami osôb, ktoré sa nachádzajú v okolitých oblastiach, kde bude systém diaľkovej biometrickej identifikácie nasadený. Dotknuté budú aj práva iných osôb, ktorých biometrické údaje sa používajú na účely porovnania, okoloidúcich a osôb,

⁸⁸ Tamže, s. 43.

⁸⁹ Čl. 5, ods. 2 Aktu o umelej inteligencii.

⁹⁰ Čl. 5 ods. 3 Aktu o umelej inteligencii.

⁹¹ Podľa článku 27 smernice EÚ 2016/6801 o presadzovaní práva, článku 35 Všeobecného nariadenia o ochrane osobných údajov alebo článku 39 nariadenia EÚ 2018/1725, ktorým sa stanovujú pravidlá ochrany údajov pre inštitúcie, orgány, úrady a agentúry EÚ.

⁹² Čl. 27 Aktu o umelej inteligencii a usmernenia Komisie o zakázaných praktikách využívajúcich umelú inteligenciu stanovených v nariadení (EÚ) 2024/1689, oznámenie Európskej komisie C(2025) 5052 final z 29. 07. 2025, s. 124 – 126.

ktoré sa náhodne nachádzajú v oblasti pátrania. Opis geografického rozsahu oblasti pátrania, na ktorú sa vzťahuje systém diaľkovej biometrickej identifikácie v reálnom čase, ovplyvní aj počet osôb, ktoré sú systémom dotknuté;

- opatrenia na zabezpečenie ľudského dohľadu počas prevádzky systému, a spôsob interpretácie výstupov v kontexte rozhodovacieho procesu a objasniť úlohu človeka pri overovaní a interpretácii výstupov;
- opatrenia na zmiernenie rizika a vysvetlenie nápravných opatrení v prípade, že sa riziko naplní vrátane postupov riešenia sťažností.

Všetky tieto aspekty treba brať do úvahy pri hodnotení zákonnosti získania možnosti využitia informácií a dôkazov získaných s pomocou automatizovaných vozidiel a ich asistenčných systémov v prípade používania profilovania osoby za účelom zistenia, či sa stane páchatel'om trestného činu alebo v prípade ich využívania na biometrickú kategorizáciu osôb alebo biometrickú identifikáciu osôb v reálnom čase.

Záver

Pri riešení otázok súvisiacich s vyvodzovaním prípadnej trestnej zodpovednosti subjektov v súvislosti s používaním, resp. manipulovaním s automatizovanými vozidlami, resp. s vozidlami, ktoré využívajú pokročilé asistenčné systémy, môžu byť do veľkej miery kľúčové elektronické dôkazy získané z informácií pochádzajúcich zo systémov týchto vozidiel. Otázkou je voľba vhodných trestnoprocených inštitútov smerujúcich k zaisteniu týchto elektronických dôkazov a informácií. Táto voľba sa do určitej miery odvíja a bude odvíjať nielen od charakteru týchto dôkazov, ale aj samotného prístupu k systémom, ktoré tie informácie obsahujú.

Právna úprava v rámci EÚ, ako aj Slovenskej republiky už reagovala na postupné zavádzanie automatizovaných vozidiel úrovne 3 a vyšších podľa štandardu SAE, a to legislatívnym vymedzením jednak pojmov „automatizované vozidlo“ a „plne automatizované vozidlo“, ako aj špecifikáciou povinností vodiča takéhoto vozidla a technických požiadaviek na pokročilé asistenčné systémy nachádzajúce sa v týchto vozidlách. Našou úlohou bolo preveriť, či súčasne inštitúty trestného práva umožňujú zabezpečovanie a získavanie informácií a dôkazov z automatizovaných vozidiel, resp. v nich zabudovaných asistenčných systémov na účely trestného konania a identifikovať prípadné problémy v tomto smere vrátane možností ich riešenia.

V rámci príspevku sme poukázali na možné problémy spojené s procesom získavania a následného zaist'ovania dôkazov z asistenčných systémov automatizovaných vozidiel, resp. samotných plne automatizovaných vozidiel, ktoré vychádzajú najmä z charakteru a formy zaist'ovaných údajov. Tieto problémy majú však skôr technický ako právny charakter.

Z nášho pohľadu súčasná trestnoprávna úprava zaist'ovacích inštitútov vo vzťahu k možnosti zaist'ovania elektronických dôkazov z v súčasnosti prevádzkovaných automatizovaných vozidiel a ich systémov, najmä vo vzťahu k dokazovaniu dopravných nehôd, sa momentálne javí ako dostatočná a umožňujúca aj zaistenie takýchto údajov aj

v budúcnosti (aj s ohľadom na prijatie nariadenia o e-evidence). Uvedené však bude do značnej miery závisieť od technického pokroku a rozvoja pokročilých asistenčných systémov a od toho sa odvíjajúcich spôsobov, ako sa bude technicky možné dostať k potrebným údajom. V tomto smere je potrebný legislatívny vývoj, a to s cieľom napríklad zavedenia povinnosti umiestnenia do automatizovaných vozidiel a plne automatizovaných vozidiel okrem systému EDR aj systém DSSAD vrátane presne stanoveného rozsahu, formátu a charakteru zaznamenávaných údajov, aby mohli byť následne dostupné OČTK a súdom na účely trestného konania po splnení zákonných predpokladov.

Osobitne boli z našej strany prezentované právne limity (najmä z pohľadu práva EÚ) týkajúce sa používania systémov umelej inteligencie v automatizovaných vozidlách z hľadiska ich možného využívania na profilovanie osoby za účelom zistenia, či sa stane páchatel'om trestného činu. alebo v prípade ich využívania na biometrickú kategorizáciu osôb alebo biometrickú identifikáciu osôb v reálnom čase.

Vo vzťahu k využívaniu automatizovaných vozidiel a ich asistenčných systémov ako dôkazov, resp. ako zdrojov dôkazov v trestnom konaní v budúcnosti je z nášho pohľadu nevyhnutná ďalšia legislatívna adaptácia a interdisciplinárna spolupráca, ktorá zohľadní najnovšie technologické trendy a ich možné konkrétne právne dôsledky, najmä v prípade zavádzania plne automatizovaných vozidiel do prevádzky. Pôjde nielen o riešenie otázok zasahovania systémov obsiahnutých v týchto vozidlách do základných práv a slobôd osôb využívajúcich tieto vozidlá alebo osôb, ktoré s nimi prichádzajú do styku, a to vrátane ochrany osobných údajov, ale aj otázky spojené s používaním umelej inteligencie ako takej (napr. z hľadiska zodpovednosti za spôsobenú škodu alebo trestný čin).

Literatúra

- ALHABIB, R., YADAV, P. Data authorisation and validation in autonomous vehicles: a critical review. In *Discover Applied Science*, Vol. 7, No. 735, 2025, s. 6 – 8, <https://doi.org/10.1007/s42452-025-07333-2>
- ANDRAŠKO, J., KORDÍK, M. Úlohy a oprávnenia orgánov policajného zboru v ére automatizovaných vozidiel. In *STUDIA IURIDICA Cassoviensia*, 2024, Vol. 12, No.1, s. 7 (4 – 28), dostupné na: <https://doi.org/10.33542/SIC2024-1-01>
- ANDRAŠKO, J., DRAŽOVÁ, P., GYURÁSZ, Z., et al. *Biela kniha. Regulácia autonómnych vozidiel v Európskej únii a Slovenskej republike*. Bratislava : Univerzita Komenského v Bratislave, Právnická fakulta, 2022, s. 17 a nasl., dostupné na: https://comeniusvyskum.flaw.uniba.sk/wp-content/uploads/2023/01/Biela-kniha_FINAL.pdf
- BROWN, A., JOHNSON, D., S., TUPTUK, N. A scoping study: crime and connected and autonomous vehicles. In *Crime Science*. Vol. 14, article 2, 2025, s. 1 – 39, dostupné na: <https://doi.org/10.1186/s40163-025-00245-x>
- ČENTÉŠ, J., KURILOVSKÁ, L., ŠIMOVIČEK, I., BURDA, E. a kol. *Trestný poriadok I. § 1 – 195*. Bratislava : C. H. Beck, 2021, 1232 s.
- GLESS, S., LEDERER, F., WEIGEND, T. AI-Based Evidence In Criminal Trials? In *Tulsa Law Review*, Vol. 59, No. 1, 2024, s. 1 – 37
- GLESS, S., LIGETI, K. Regulating driving automation in the European Union – criminal liability on the road ahead? In *New Journal of European Criminal Law*, Vol. 15, Iss. 1, 2024, s. 33 – 57, <https://doi.org/10.1177/20322844231213336>;
- GURNEY, K., J. Driving Into The Unknown: Examining The Crossroads of Criminal Law and Autonomous Vehicles. In *Wake Forest Journal of Law and Policy*, 2015, Vol. 5, Iss. 2, s. 393 – 442

- HALLEVY, G. The Criminal Liability of Artificial Intelligence Entities – from Science Fiction to Legal Social Control. In *Akron Intellectual Property Journal*. Vol. 4, Iss. 2, Article 1, 2010, s. 171 – 201, dostupné na: <https://ideaexchange.uakron.edu/akronintellectualproperty/vol4/iss2/1>
- HOQUE, A., M., HASAN, R. AVGuard: A Forensic Investigation Framework for Autonomous Vehicles. In *ICC 2021 – IEEE International Conference on Communications*, Montreal, QC, Canada, 2021, s. 1 – 6, doi: 10.1109/ICC42927.2021.9500652
- KING, C., T., AGGARWAL, N., TADDEO, M., FLORIDI, L. Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions. In *Science and Engineering Ethics*. Vol. 26, Iss. 1, 2020, s. 89 – 120, <https://doi.org/10.1007/s11948-018-00081-0>
- KOSTĚNCOVÁ, V., NOUZOVSKÝ, L. *Technologie EDR a její principy*. Praha : České vysoké učení technické v Praze, 2020, 109 s.
- QUEZADA-TAVÁREZ, K., VOGIATZOGLU, P., ROYER, S. Legal challenges in bringing AI evidence to the criminal courtroom. In *New Journal of European Criminal Law*, Vol. 12, Iss. 4, 2021, s. 531 – 551, dostupné na: <https://doi.org/10.1177/20322844211057019>
- NOWACKI, G., NIEDZICKA, A., KRYSIUŁ, C. The Use Of Event Data Recorder (EDR) – Black Box. In *Advances in Science and Technology Research Journal*, Vol. 8, No. 21, March 2014, s. 62–72, doi: 10.12913/22998624.1091881
- ROSCA, C., COVRIG, et al. *Return of the AI: An Analysis of Legal Research on Artificial Intelligence Using Topic Modeling*. In Aletras, N., Androutsopoulos, I., Barrett, L., Meyers A. & Preoiuc-Pietro, D. (eds.), *Proceedings of the Natural Legal Language Processing Workshop 2020*, CEUR-WS.org, 2020, s. 3 – 10, dostupné na: <http://ceur-ws.org/Vol-2645/paper1.pdf>
- STRANDBERG K., NOWDEHI N., OLOVSSON T. A Systematic Literature Review on Automotive Digital Forensics: Challenges, Technical Solutions and Data Collection. In *IEEE Transactions on Intelligent Vehicles*, Vol. 8, No. 2, 2023, s. 1350 – 1367, dostupné na: <http://dx.doi.org/10.1109/TIV.2022.3188340>
- STRĚMÝ, T., ŠAMKO, P., KURILOVSKÁ, L. et al. *Trestný poriadok. Praktický komentár*. Praha : Wolters Kluwer ČR, 2024, 1336 s.
- VOJTUŠ, F., KORDÍK, M., DRAŽOVÁ, P. Umělá inteligencia, jej využívanie a trestnoprávna zodpovednosť – výzvy, problémy a možné riešenia. In *Právnik*, 2023, Roč. CLXII, č. 6, s. 549 – 570

Judikatura

R 47/2017

Rozsudok Súdneho Dvora EÚ z 21. decembra 2016, Tele2 Sverige AB a Secretary of State for the Home Department v. Post-och telestyrelsen a i., C-203/15 a C-698/15, ECLI:EU:C:2016:970

Rozsudok Súdneho dvora zo 6. októbra 2020, La Quadrature du Net a i., C-511/18, C-512/18 a C-520/18, ECLI:EU:C:2020:791

Rozsudok Súdneho dvora z 22. júna 2021, Latvijas Republikas Saeima, C-439/19, ECLI:EU:C:2021:504

Rozsudok Súdneho dvora z 21. júna 2022, Ligue des droits humains, C-817/19, ECLI:EU:C:2022:491

Rozsudok Súdneho dvora z 5. júna 2023, Komisja/Polsko, C-204/21, ECLI:EU:C:2023:442

Rozsudok Súdneho dvora z 20. septembra 2022, SpaceNet, C-793/19 (spojené veci C-793/19, C794/19), ECLI:EU:C:2022:702

Ostatné zdroje

Európsky výbor pre ochranu údajov: *Usmernenie 1/2020 k spracúvaniu osobných údajov v súvislosti s prepojenými vozidlami a aplikáciami týkajúcimi sa mobility*. Prijaté 9. marca 2021, dostupné na: https://dataprotection.gov.sk/files/metod_edpb/usmernenia_k_spracuvaniu_osobnych_udajov_v_suvislosti_s_prepojenymi_vozidlami_a_aplikaciami_tykajucimi_sa_mobility.pdf

EUROPOL: *AI and policing. The benefits and challenges of artificial intelligence for law enforcement*. An Observatory Report from the Europol Innovation Lab. Luxembourg: Publications Office of the European Union, 2024, 59 s., dostupné na: <https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing#:~:text=With%20the%20AI%20and%20policing%20report%2C%20produced%20through,more%20efficient%2C%20responsive%20and%20effective%20law%20enforcement%20model>

Štandard SAE J3016_202104: Taxonómia a definície pojmov súvisiacich so systémami automatizovaného riadenia pre cestné motorové vozidlá. Dostupné na: https://www.sae.org/standards/content/j3016_202104/

Usmernenia Komisie o zakázaných praktikách využívajúcich umelú inteligenciu stanovených v nariadení (EÚ) 2024/1689. Oznámenie Európskej komisie C(2025) 5052 final z 29.07.2025, 144 s., dostupné na: [Guidelines_on_prohibited_artificial_intelligence_practices_established_by_Regulation_EU_20241689_AI_Act_Slovak_3mP9dTPmycBiuhqnN6dcPoPx8_118644.PDF](#)

Straßenverkehrsgesetz v znení uverejnenom 5. marca 2003 (BGBl. I S. 310, 919) zmenený a doplnený článkom 70 zákona z 23. októbra 2024 (BGBl. 2024 I, Nr. 323), skrátené StVG

Autonome Fahrzeuge Genehmigungs und Betriebs Verordnung z 24. júna 2022 (BGBl. I S. 986), skrátené AFGBV

Automated Vehicles Act 2024

Automated Vehicles Act 2024 Explanatory Notes, 2024, Vyd. The Stationery Office (GB), 62 s., dostupné na: https://www.legislation.gov.uk/ukpga/2024/10/pdfs/ukpgaen_20240010_en.pdf

<https://infocar.sk/gps-monitoring-vozidiel/>

<https://futuretransport-news.com/renault-group-trials-autonomous-vehicles-in-europe/#:~:text=Barcelona%2C%20Spain:%20Urban%20Public%20Transport%20Trials%20From,through%20accessible%2C%20efficient%2C%20and%20low%2Demission%20transport%20solutions>