*https://doi.org/10.5817/RPT2020-2-1*

# ČO VIEŠ O MOJOM VOZIDLE? OCHRANA OSOBNÝCH ÚDAJOV A KYBERNETICKÁ BEZPEČNOSŤ V KONTEXTE AUTONÓMNYCH VOZIDIEL

*JOZEF ANDRAŠKO[1], MATÚŠ MESARČÍK[2]*

**ABSTRAKT**

*Autori sa v článku zameriavajú na vybrané otázky toku údajov v kontexte autonómnych vozidiel. V prvých častiach príspevku sú postupne predstavené základné pojmy danej problematiky a načrtnutá právna úprava. Následne sú charakterizované prieniky s právnou úpravou kybernetickej bezpečnosti a ochrany osobných údajov. Osobitný dôraz je kladený na otázku osobnej pôsobnosti a súvisiacej zodpovednosti v oblasti ochrany osobných údajov medzi jednotlivými aktérmi spracúvania osobných údajov v autonómnom vozidle.*

**KĽÚČOVÉ SLOVÁ**

*autonómne vozidlá, autonómne systémy, automatizované systémy, kybernetická bezpečnosť, ochrana osobných údajov*

**ABSTRACT**

*The authors focus on selected issues of data flow in the context of autonomous vehicles. The first parts of the paper gradually introduce the basic concepts of*

[1] JUDr. Jozef Andraško, PhD., odborný asistent, Ústav práva informačných technológií a práva duševného vlastníctva, Univerzita Komenského v Bratislave, Právnická fakulta, e-mail: jozef.andrasko@flaw.uniba.sk.

[2] JUDr. Matúš Mesarčík, PhD. LL.M, odborný asistent, Ústav práva informačných technológií a práva duševného vlastníctva, Univerzita Komenského v Bratislave, Právnická fakulta, e-mail: matus.mesarcik@flaw.uniba.sk.

*the issue and outline the legislation. Subsequently, the interferences with the legal regulation of cyber security and personal data protection are highlighted. Special emphasis is placed on the issue of personal scope and related liability in the field of personal data protection among the various actors in the processing of personal data in an autonomous vehicle.*

**KEYWORDS**

*autonomous vehicles, autonomous systems, automated systems, cyber security, data protection*

## 1. ÚVOD

Výrobcovia automobilov ako Tesla, Mercedes, Toyota, GM, Nissan, Volkswagen a ďalší už dlhšiu dobu testujú autonómne vozidlá, najmä čiastočne autonómne vozidlá. Plne autonómne vozidlo, kedy sa nevyžaduje, aby ho riadil vodič a kde je možné naplánovať trasu z bodu A do bodu B, sa zdá byť nateraz nedosiahnuteľným konceptom, ktorý by sa mal v spoločnosti uplatniť. Avšak z právneho hľadiska testovanie a najmä následné zavádzanie autonómnych vozidiel spochybňuje viaceré právne inštitúty, najmä v oblasti zodpovednosti, súkromia, ochrany údajov, typového schválenia vozidiel, právnej subjektivity autonómnych systémov, autorských práv a pod.

Tento príspevok sa venuje vybraným právnym otázkam týkajúcich sa autonómnych vozidiel, a to konkrétne otázkam kybernetickej bezpečnosti a ochrany osobných údajov. Otázka kybernetickej bezpečnosti v súvislosti s autonómnymi vozidlami má viacero aspektov. V prvom rade ide o situácie, kedy dochádza ku kybernetickým útokom voči autonómnemu alebo automatizovanému systému, kedy je automobil ovládaný na diaľku útočníkom. Zo sveta sú známe kybernetické útoky, kedy došlo ku kybernetickému bezpečnostnému incidentu, ktorý spôsobil, že útočníci ovládali riadenie, preraďovanie, brzdy, otváranie okien, klimatizáciu automobilu s určitým stupňom automatizácie. Taktiež môže ísť o situácie, kedy útočník nechce získať kontrolu nad vozidlom ale chce získať prístup k lokalizačným

údajom, resp. k iným osobným údajom, ktoré sa spracúvajú v rámci činnosti autonómneho vozidla.

V druhej kapitole tohto príspevku dôjde k objasneniu rozdielu medzi autonómnymi a automatizovanými systémami. Autori sa taktiež budú venovať pojmu autonómne vozidlo v kontexte jednotlivých úrovní automatizácie, ako aj konceptu prepojených vozidiel, kde načrtnú rôzne druhy komunikácie, v rámci ktorej dochádza k spracúvaniu osobných údajov. V ďalšej kapitole sa autori venujú vybraným legislatívnym aktom Európskej únie (ďalej len „EÚ"), ktoré upravujú problematiku autonómnych vozidiel, resp. infraštruktúry s ktorou autonómne a prepojené vozidlá komunikujú, a to z pohľadu kybernetickej bezpečnosti a ochrany osobných údajov. V piatej časti sa autori článku zamýšľajú nad správnym vymedzením postavenie rôznych aktérov spracúvania osobných údajov v autonómnom vozidle. V prvom kroku je načrtnutá osobná pôsobnosť Všeobecného nariadenia na ochranu údajov (GDPR) a súvisiace otázky zodpovednosti. Následne je kriticky vyhodnotené usmernenie Výboru na ochranu údajov (EDPB), ktoré sa týka spracúvania údajov v autonómnych vozidlách. V závere tejto časti sú načrtnuté tri modelové prípady prepojenia autonómnych vozidiel a analýza postavenia jednotlivých potenciálnych aktérov spracúvania osobných údajov.

## 2. AUTONÓMNE SYSTÉMY A AUTOMATIZOVANÉ SYSTÉMY

Autonómne vozidlo (*autonomous vehicle*), automatizované vozidlo (*automated vehicle*),[3] samo jazdiace vozidlo (*self-driving vehicle*) či vozidlo bez vodiča (*driverless vehicle*). Tieto pojmy sa najčastejšie v médiách, ale aj odbornej a vedeckej literatúre spájajú s konceptom vozidla, kedy niektoré alebo všetky jazdné úlohy vykonáva vozidlo, presnejšie povedané, jeho systémy, bez toho, aby ich musel vykonávať vodič.[4] Práve tieto systémy, ktoré sú podstatou vozidiel schopných vykonať všetky alebo niektoré jazdné úlohy bez intervencie vodiča, možno deliť na automatizované a autonómne.

[3] Preklad anglického pojmu *automated* možno v slovenčine preložiť ako automatizovaný alebo automatický.

[4] Pre účely tohto príspevku používame zaužívaný pojem autonómne vozidlo.

Jeden zo spôsobov ako odlíšiť autonómny systém a automatizovaný systémom je zamerať sa na ich schopnosť prispôsobenia sa, učenia sa a rozhodovania, ktoré je integrované do systému. Automatizované systémy zvyčajne fungujú na základe vopred definovaných parametrov a sú veľmi obmedzené v tom, aké úlohy môžu vykonávať. Autonómny systém sa naopak učí prispôsobiť sa meniacemu sa prostrediu a vyvíja sa so zmenou prostredia. Údaje na základe ktorých sa učí sú aj mimo toho, čo sa predpokladalo pri zavedení systému.[5]

Ak sa na to pozrieme z inej perspektívy, automatizovaný systém vykonáva konkrétne úlohy s dobre pochopenými parametrami, ktoré sú známe vopred. Je navrhnutý tak, aby vykonával špecifickú funkciu opakovane a efektívne. Autonómny systém radí a pomáha definovať, aké je správne rozhodnutie alebo úkon pri vyvíjajúcom sa prostredí, ktoré nie je vopred určené.[6]

Konkrétnym príkladom automatizovaného systému sú kontroly súladu (*compliance*) na úrovni infraštruktúry a aplikácií v prostredí spoločnosti. Tieto systémy monitorujú dodržiavanie presne stanoveného súboru noriem súladu a informujú organizáciu, keď systémy nedosiahnu súlad. Tieto systémy môžu tiež vykonať dobre definované úkony na nápravu problému, to však neznamená, že sú autonómne. Výslovne sú nakonfigurované tak, aby podnikli konkrétne úkony, čo organizácii umožňuje dôveru v to, čo sa presne deje s ich prostredím. Tieto systémy často označujú problém, aby užívateľ alebo správca mohol problém vyriešiť. Ide o podpornú technológiu, pri ktorej pomáha človeku vykonávať jeho prácu a nenahrádza ho.[7]

Príkladom autonómneho systému je detekcia narušenia siete, hľadanie anomálií v inak normálnej sieťovej prevádzke. Autonómne systémy sa taktiež využívajú na hľadanie zero-day útokov pred ich vykonaním (*zero- day exploits*).[8] Ďalším príkladom aplikácie autonómneho systému je smart vy-

[5] MATTESON S. *Autonomous versus automated: What each means and why it matters*. [on-line]. Dostupné z: https://www.techrepublic.com/article/autonomous-versus-automated-what-each-means-and-why-it-matters/ [citované 28.9.2020].

[6] Tamže.

[7] Tamže.

[8] Tamže.

sávač Roomba. Jeho funkciou je čistenie podlahy, avšak na základe spätnej väzby z okolia sa rozhoduje, kde bude čistiť. Pri narážaní na objekty sa učí, ako sa im časom vyhnúť a zostaví mapu priestoru, ktorý čistí. Musí sa neustále učiť, pretože nábytok, predmety a domáce zvieratá menia prostredie, v ktorom pôsobí.[9]

Autonómne systémy nemožno stotožňovať len s algoritmom (softvérom).[10] Autonómne systémy nie sú naprogramované len k výkonu určitých činností, ale aj k tomu, aby sa určité činnosti naučili vykonávať sami. Inými slovami, podstata autonómnych systémov nie je len schopnosť autonómne existovať a fungovať, ale aj vytváranie svojho vlastného kódu (softvéru)[11] nezávisle od svojho autora.[12]

Typickým príkladom využitia autonómnych systémov sú autonómne vozidlá, a to najmä úrovne 3 a vyššie. Ako uvádza Polčák, autonómne vozidlá nemožno z pohľadu práva prirovnávať ku klasickým automobilom, a to najmä s ohľadom na skutočnosť, že autonómne vozidlá sa riadia sami.

---

[9] Tamže.

[10] Z právneho pohľadu možno softvér (počítačový program) chápať ako súbor príkazov a inštrukcií vyjadrených v akejkoľvek forme použitých priamo alebo nepriamo v počítači alebo v podobnom technickom zariadení a zároveň musí byť výsledkom tvorivej duševnej činnosti autora. Inými slovami, softvér predstavuje súbor inštrukcií a príkazov, ktoré sú vytvorené priamo alebo sprostredkovane autorom, čiže fyzickou osobou. Naprogramovaný systém má presne stanovené funkcionality a vykonáva to, na čo ho programátor predurčil.

[11] Konkrétnou aplikáciou autonómneho systému bol autonómny robot Tay spoločnosti Microsoft pre sociálnu sieť Twitter. Hlavnou úlohou robota Tay bolo vyhodnocovať obsah komunikácie a následne vytvárať populárne príspevky. Po určitom čase začal Tay vytvárať nenávistné príspevky, najmä kvôli nenávistnému obsahu na sociálnej sieti Twitter. Tay bol naprogramovaný na to, aby sa učil komunikovať, nie na to aby komunikoval. Za týmto účelom sa Tay sám programoval. Softvér, na základe ktorého Tay posielal svoje tweety si vytváral sám, a človek nebol schopný vykonávať úpravy v neustále meniacom sa kóde, ktorý Tay používal na učenie sa. Tay bol po dvoch neúspešných pokusoch o preprogramovanie vypnutý. Bližšie pozri: POLČÁK, R. *Odpovědnost umělé inteligence a informační útvary bez právní osobnosti.* In Bulletin Advokace 11/2018, s. 24. [on-line]. Dostupné z: http://www.bulletin-advokacie.cz/assets/zdroje/casopis/2018/BA_11_2018_web.pdf. [citované 28.9.2020].

[12] POLČÁK, R. *Odpovědnost umělé inteligence a informační útvary bez právní osobnosti*. In Bulletin Advokace 11/2018, s. 24. [on-line]. Dostupné z: http://www.bulletin-advokacie.cz/assets/zdroje/casopis/2018/BA_11_2018_web.pdf. [citované 28.9.2020].

V prípade autonómnych vozidiel by sa nemala používať analógia s automobilom, ale so softvérom, ktorý takýto systém riadi.[13]

V štandarde SAE J3016:Sep 2016: Taxonómia a definície pojmov súvisiacich so systémami automatizovaného riadenia pre cestné motorové vozidlá (ďalej len „SAE štandard"), sa rozlišuje medzi pojmami autonómny (*autonomous*) a automatizovaný (*automation*). Automatizácia predstavuje v zmysle SAE štandardu použitie elektronických alebo mechanických zariadení ako náhrada ľudskej práce. Automatizácia v kontexte jazdy je vhodný termín pre systémy, ktoré vykonávajú časť alebo všetky dynamické jazdné úlohy.[14] [15]

Výraz „autonómny" sa už dlho používa v komunitách výskumu týkajúceho sa robotiky a umelej inteligencie na označenie systémov, ktoré majú schopnosť a oprávnenie nezávisle a sebestačne rozhodovať. Postupom času sa toto použitie náhodne rozšírilo tak, aby zahŕňalo nielen rozhodovanie, ale predstavuje funkčnosť celého systému, čím sa stalo synonymom pre automatizáciu.

V jurisprudencii sa autonómia vzťahuje aj na schopnosť samo riadenia (*self-governance*). V tomto zmysle je „autonómny" tiež nesprávny názov, ktorý sa uplatňuje na automatizovanú technológiu jazdy, pretože ani tie najpokročilejšie systémy automatizovanej jazdy nie sú „samo riadiace". Systémy automatizovanej jazdy skôr fungujú na základe algoritmov a inak sa

---

[13] Tamže, s. 23 – 30.

[14] Dynamické jazdné úlohy (*dynamic driving task,* DDT) sú v zmysle bodu 3.13 SAE štandardu *„Všetky prevádzkové a taktické funkcie v reálnom čase potrebné na prevádzku vozidla v cestnej premávke, s výnimkou strategických funkcií, ako sú plánovanie ciest a výber cieľov a trasových bodov, zahŕňajúc bez obmedzenia:*

*1.1.1 bočné riadenie pohybu vozidla pomocou riadenia (funkčné);*

*2.1.1 pozdĺžne riadenie pohybu vozidla pomocou zrýchlenia a spomalenia (funkčné);*

*3.1.1 monitorovanie jazdného prostredia prostredníctvom detekcie objektov, udalostí, rozpoznávania, klasifikácie a prípravy reakcií (operatívnych a taktických);*

*4.1.1 vykonanie reakcie na objekt a udalosť (operatívna a taktická);*

*5.1.1 plánovanie manévrov (taktické); a zvyšovanie viditeľnosti pomocou osvetlenia, signalizácie a gestikulovania atď. (Taktické)."*

[15] Bod 7.1 SAE štandardu.

riadia príkazmi používateľov. Z tohto dôvodu SAE štandard nepoužíva pojem „autonómny“ na opis automatizácie jazdy.[16]

V závislosti od toho aké systémy sa využívajú pri jednotlivých úrovniach automatizácie, SAE štandard rozlišuje medzi systémom automatizovaného riadenia (*Driving automation system*) a systémom automatického riadenia (*Automated driving system*). Systém automatizácie riadenia (*Driving automation system*) predstavuje *„Hardvér a softvér, ktoré sú kolektívne schopné trvalo vykonávať časť alebo všetky dynamické jazdné úlohy; tento výraz sa všeobecne používa na opis každého systému, ktorý je schopný úrovne 1-5 automatizácie jazdy.“*[17]

Na rozdiel od tohto všeobecného pojmu pre akýkoľvek systém úrovne 1-5, je systém automatického riadenia (*Automated driving system*) špecifickým pojmom pre systém úrovne 3-5. Systém automatického riadenia je definovaný ako *„Hardvér a softvér, ktoré sú kolektívne schopné trvalo vykonávať všetky dynamické jazdné úlohy, bez ohľadu na to, či je obmedzená na konkrétnu doménu prevádzkového návrhu;*[18] *tento výraz sa používa špecificky na opis systému automatizácie riadenia na úrovni 3, 4 alebo 5.“*[19]

SAE štandard taktiež popisuje pojem samo jazdenie (*Self-driving*), ktorý sa týka situácií, keď nie je prítomný žiadny vodič alebo žiadny užívateľ nevykonáva dynamické jazdné úlohy, alebo situácií, keď systém automatizácie jazdy vykonáva akúkoľvek časť dynamických jazdných úloh.[20]

## 3. DEFINÍCIA POJMU AUTONÓMNE VOZIDLO

Autonómne vozidlá sú často chápané ako vozidlá bez vodiča, samo jazdiace a robotické vozidlá. Vo všeobecnosti, sa autonómne vozidlá dajú opísať ako *„počítačom riadené vozidlá, ktoré jazdia samy, spoliehajúc sa na množstvo*

[16] Bod 7.1.1 SAE štandardu.

[17] Bod 3.8 SAE štandardu.

[18] Prevádzková doména v zmysle bodu 3.22 SAE štandardu predstavuje: *„Prevádzkové podmienky, za ktorých je daný systém automatizácie riadenia alebo jeho vlastnosť osobitne navrhnutá tak, aby fungovala, okrem iného vrátane environmentálnych, geografických a denných obmedzení a/alebo požadovanej prítomnosti alebo neprítomnosti určitej premávky alebo charakteristiky vozovky.“*

[19] Bod 3.2 SAE štandardu.

[20] Bod 7.1.3 SAE štandardu.

*zdrojov údajov, aby získali prístup k jazdnému prostrediu a riadili prevádzku vozidla.“*[21]

Pokiaľ ide o vymedzenie pojmu autonómne vozidlo, neexistuje všeobecný konsenzus. Autonómne vozidlo je definované v právnych predpisoch prijatých v niektorých štátoch USA. Každý zo štátov s podrobnou legislatívou o autonómnych vozidlách má inú definíciu. Napríklad Nevada definuje autonómne vozidlá ako *„motorové vozidlo, ktoré je vybavené systémami automatického riadenia, ktoré je navrhnuté tak, aby fungovalo na úrovni automatizácie jazdy na úrovni 3, 4 alebo 5 podľa SAE J3016. Tento pojem zahŕňa plne autonómne vozidlo.*“[22] Plne autonómne vozidlo je definované ako „*vozidlo vybavené systémom automatického riadenia, ktorý je navrhnutý tak, aby fungoval na úrovni automatizácie riadenia na úrovni 4 alebo 5 podľa SAE J3016.“*[23] Nevada bola prvým štátom, ktorý povolil testovanie autonómnych vozidiel na verejných cestách.

Na úrovni členských štátov Európskej únie bola prijatá právna úprava týkajúca sa autonómnych vozidiel v Nemeckej spolkovej republike. Od 21. júla 2017 je účinná novela nemeckého zákona o cestnej premávke (Straßenverkehrsgesetz - StVG), ktorá upravuje problematiku motorových vozidiel s vysoko alebo plne automatizovanými jazdnými funkciami (*highly or fully automated driving functions*) na nemeckých verejných cestách.[24] Vozidlá s vysoko alebo plne automatizovanými jazdnými funkciami v zmysle

---

[21] COLLINGWOOD, L. *Privacy implications and liability issues of autonomous vehicles*. In Information & Communications Technology Law, roč. 26. č. 1, 2017, s. 32-45.

[22] Autonomous Vehicles. State of Nevada Register of Administrative Regulations. § 482A. [online]. Dostupné z: https://www.leg.state.nv.us/NRS/NRS-482A.html#NRS482ASec036. [citované 28.9.2020].

[23] Tamže, § 482A.036.

[24] [On-line]. Dostupné z: https://www.bmvi.de/EN/Topics/Digital-Matters/Automated-Connected-Driving/automated-and-connected-driving.html. [citované 28.9.2020]. Taktiež pozri CZARNECKI, K. *English Translation of the German Road Traffic Act Amendment Regulating the Use of “Motor Vehicles with Highly or Fully Automated Driving Function” from July 17, 2017* [On-line]. Dostupné z: https://www.researchgate.net/profile/Krzysztof_Czarnecki3/publication/320813344_English_Translation_of_the_German_Road_Traffic_Act_Amendment_Regulating_the_Use_of_Motor_Vehicles_with_Highly_or_Fully_Automated_Driving_Function_from_July_17_2017/links/59fbbe680f7e9b9968bb5a0f/English-Translation-of-the-German-Road-Traffic-Act-Amendment-Regulating-the-Use-of-Motor-Vehicles-with-Highly-or-Fully-Automated-Driving-Function-from-July-17-2017.pdf [citované 28.9.2020].

nemeckého zákona o cestnej premávke zodpovedajú úrovni 3 a úrovni 4 autonómnych vozidiel v zmysle taxonómie autonómnych vozidiel zavedených v štandarde SAE J3016:Sep 2016.

Motorové vozidlá s vysoko alebo plne automatizovanými jazdnými funkciami v zmysle nemeckého zákona o cestnej premávke sú vozidlá, ktoré majú technické vybavenie, ktoré:

*1.1.1 „je schopné po aktivácii vykonať jazdnú úlohu - vrátane pozdĺžneho a priečneho riadenia - pre príslušné motorové vozidlo (kontrola vozidla),*

*2.1.1 je schopné dodržať dopravné predpisy vzťahujúce sa na jazdnú úlohu vozidla počas vysoko automatizovanej alebo plne automatizovanej jazdy,*

*3.1.1 vodič môže kedykoľvek manuálne prejsť na ručné ovládanie alebo ho manuálne deaktivovať,*

*4.1.1 je schopné rozpoznať potrebu manuálneho ovládania vozidla vodičom,*

*5.1.1 je schopné vizuálne, akusticky, hmatovo alebo inak zrozumiteľne informovať vodiča vozidla o požiadavke odovzdať vodičovi kontrolu nad vozidlom s dostatočnou časovou rezervou pred odovzdaním kontroly a*

*6.1.1 upozorňuje na použitie, ktoré je v rozpore s popisom systému.“*[25]

Novela nemeckého zákona o cestnej premávke taktiež zaviedla povinné vybavenie vozidla s vysoko alebo plne automatizovanými jazdnými funkciami čiernou skrinkou. V prípade nehody čierna skrinka identifikuje, či vodič alebo systém ovládal vozidlo v danom momente, a preto objasňuje, či zodpovednosť nesie vodič alebo potenciálne výrobca.[26]

[25] § 1a ods. 2 nemeckého zákona o cestnej premávke.

[26] § 63a nemeckého zákona o cestnej premávke.

## 3.1 ÚROVNE AUTOMATIZÁCIE

Na pochopenie autonómnych vozidiel je potrebné v prvom rade pochopiť jednotlivé úrovne automatizácie.[27] Autonómne vozidlá sú klasifikované na základe úrovne automatizácie. Podľa SAE štandardu sú autonómne vozidlá rozdelené do šiestich úrovní, ktoré sa stupňujú. Tieto úrovne sa považujú skôr za opisné ako normatívne a viac technické, než právne. Vo všeobecnosti možno povedať, že úrovne SAE štandardu určujú predovšetkým to, ako je dynamická jazdná úloha rozdelená medzi človeka - vodiča a stroj. Na úrovni 0 (bez automatizácie) je vykonávaná výlučne ľudským vodičom a na úrovni 5 (úplná automatizácia) výlučne systémom automatického riadenia.[28]

1.1.1 Úroveň 0 (bez automatizácie). Ľudský vodič vykonáva všetky úlohy spojené s vedením vozidla.

2.1.1 Úroveň 1 (podpora vodiča). Ľudský vodič riadi vozidlo, ale niektoré jazdné úlohy riadi systém. Príklad: parkovací asistent alebo tempomat.

3.1.1 Úroveň 2 (čiastočná automatizácia). Systém alebo viac systémov dokáže ovládať riadenie a rýchlosť vozidla, zatiaľ čo vodič vozidla musí neustále sledovať dynamické jazdné úlohy a prostredie. Príklady: funkcia automatického parkovania, systém udržiavania jazdného pruhu, systémy núdzového brzdenia.

4.1.1 Úroveň 3 (podmienená automatizácia). Vozidlá úrovne 3 a vyššie sa považujú za vozidlá s autonómnymi jazdnými systémami. Vozidlo monitoruje jazdné prostredie prostredníctvom systémov automatického riadenia. Ľudský vodič nemusí monitorovať dynamické jazdné úlohy, ale musí byť schopný kedykoľvek a bez predchádzajúceho upozornenia prevziať kontrolu nad vozidlom. Vozidlo sa môže samo rozhodovať. Príklady: vozidlo môže pred se-

[27] Pre účely tohto článku používame pojem úrovne automatizácie. V SAE štandarde sa hovorí o úrovniach automatizácie riadenia (*levels of driving automation*) a nie o úrovniach autonómie.

[28] International Transport Forum and Corporate Partnership Board: *Autonomous Driving: Regulatory Issues*. 2015. [on-line]. Dostupné z: https://www.itf-oecd.org/sites/default/files/docs/15cpb_autonomousdriving.pdf. [citované 28.9.2020].

bou rozpoznať pomalšie sa pohybujúce vozidlo a môže sa rozhodnúť, či spomalí alebo ho predbehne. Príklad: diaľničný pilot.

5.1.1 Úroveň 4 (vysoká automatizácia). Za určitých podmienok (špecifické režimy jazdy) môže vozidlo vykonávať všetky jazdné úlohy. Ľudský vodič môže prevziať kontrolu nad vozidlom, najmä ak podmienky menia vopred definované prípady použitia (napr. práce na ceste, odklony od cesty alebo keď si to vodič vozidla želá). Príklad: mestská automatizovaná jazda.

6.1.1 Úroveň 5 je (úplná automatizácia). Ľudský vodič sa nevyžaduje. Systémy automatického riadenia zvládajú všetky aspekty jazdných úlohy bez toho, aby človek musel zasahovať. Vozidlo nevyžaduje žiadne pedále, volant. Systémy automatického riadenia robia nezávislé rozhodnutia. Vozidlo môže zvládnuť situácie, keď nastane nepredvídateľná udalosť alebo sa zmení fyzické prostredie. Príklad: úplná cesta z bodu A do bodu B.[29]

Šesťstupňová škála SAE bola prijatá rôznymi národnými a medzinárodnými orgánmi, ako je napríklad National Highway Traffic Safety Administration v USA (NHTSA), Society of Motor Manufacturers and Traders Australia's National Transport Commission (NTC), the UK's Department for Transport (DfT) a European Road Transport Research Advisory Council (ERTRAC).[30]

## 3.2 PREPOJENÉ VOZIDLÁ

Aby došlo k úplnému využitiu potenciálu autonómnych vozidiel, je potrebné aby tieto vozidlá komunikovali s inými vozidlami, resp. s inými objektmi. V tomto zmysle možno autonómne vozidlá chápať ako prepojené

[29] YEEFEN LIM, H. *Autonomous Vehicles and the Law Technology, Algorithms and Ethics.* Edward Elgar Publishing, 2018, s. 4-5. SKEETE, JP. Level 5 autonomy: *The new face of disruption in road transport.* In Technological Forecasting and Social Change, Elsevier, roč. 134(C), 2018, s. 22-34.

[30] TAEIHAGH, A. and SI MIN LIM, H. *Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks.* Transport Reviews, roč. 39. č.1, 2019, s. 103-128.

vozidlá (*connected vehicles*). Takéto vozidlo integruje prepojenie s autonómiou, čo sú odlišné, ale súvisiace technológie.

Autor Jean-Pauil Skeete objasňuje, že *„plné výhody autonómie možno dosiahnuť iba vtedy, keď vozidlo dokáže rozpoznať aj iné vozidlá (V2V) a jeho fyzické prostredie (vehicle to infrastructure, V2I).“*[31]

Autor Kouroutakis okrem toho tvrdí, že vozidlo komunikuje aj s inými zariadeniami, ako sú smartfóny, tablety, inteligentné hodinky, osobné počítače (*vehicle to device*, *V2D*).[32]

Podľa Inštitútu inžinierstva a technológie možno považovať prepojené vozidlá za vozidlá cestnej premávky, ktoré sú vybavené troma druhmi komunikačných systémov. V prvom prípade ide o internetový prístup a zvyčajne vnútornú sieť, častokrát bezdrôtovú, ktorá umožňuje pripojenie na zariadenia vo vnútri vo vozidle alebo aj mimo vozidla (známe ako *vehicle to Internet*, V2I).[33]

Ďalším druhom komunikačných systémov sú technológie *vehicle to vehicle* (V2V), ktoré umožňujú vozidlám komunikovať navzájom.[34]

Autonómne vozidlá sa taktiež môžu stať súčasťou komunikácie v rámci internetu vecí (*vehicle to IoT*, V2IoT) ako pripojená entita, ktorá prijíma údaje z externého zdroja a zdieľa údaje, ktoré zaznamenáva so vzdialenou treťou stranou pre rôzne účely.[35] Nakoľko ide o výmenu informácií medzi rôznymi zariadeniami a stranami, otázky týkajúce sa kybernetickej bezpečnosti a ochrany osobných údajov sú viac ako na mieste.[36]

---

[31] SKEETE, JP: *Level 5 autonomy: The new face of disruption in road transport.* In Technological Forecasting and Social Change, Elsevier, vol. 134(C), 2018, s. 22-34.

[32] KOUROUTAKIS, A. E.: *Autonomous Vehicles; Regulatory Challenges and the Response From UK and Germany*. 46 Mitchell Hamline Law Review forthcoming. 2019.

[33] The institution of Engineering and Technology: *Automotive Cyber Security. An IET/KTN Thought Leadership Review of risk perspectives for connected vehicles*, s. 7. [on-line]. Dostupné z: https://www.theiet.org/media/2309/iet-automotive-cyber-security-tlr-lr-1.pdf. [citované 28.9.2020].

[34] Tamže.

[35] Tamže.

## 4. PRÁVNA ÚPRAVA[37]

V nasledujúcej časti príspevku budeme analyzovať právne predpisy na úrovni práva EÚ, ktoré upravujú problematiku autonómnych vozidiel, a to najmä z pohľadu kybernetickej bezpečnosti a ochrany osobných údajov. Konkrétne budeme skúmať, či právna úprava už v procese typového schvaľovania vozidiel kladie požiadavky na bezpečnosť automatizovaných, resp. autonómnych systémov, tak aby v rámci komunikácie s inými entitami boli dostatočne zabezpečené a aby nedochádzalo k narušeniu integrity, dôvernosti a dostupnosti informácií. Taktiež sa budeme venovať otázke či legislatíva, ktorá upravuje cestnú infraštruktúru napr. v podobe inteligentného dopravného značenia, upravuje problematiku ochrany osobných údajov a kybernetickej bezpečnosti v rámci komunikácie s vozidlami.

### 4.1 TYPOVÉ SCHVÁLENIE MOTOROVÝCH VOZIDIEL

Pred samotným uvedením vozidiel na trh, tak aby ich bolo možné používať na verejných komunikáciách, musí byť vozidlo typovo schválené v súlade s administratívnymi postupmi a technickými požiadavkami. Právna úprava, ktorá by explicitne upravovala typové schválenie autonómnych vozidiel neexistuje, avšak súčasné právne predpisy EÚ za určitých podmienok dovoľujú zavedenie autonómnych vozidiel na trh.

Problematika schvaľovania motorových vozidiel, ako aj systémov pre takéto vozidlá je upravená na úrovni práva EÚ nariadením Európskeho parla-

[36] Prepojené vozidlá v súčasnosti najčastejšie komunikujú na základe technologických riešení založených na senzoroch alebo založených na prepojení. V prvom prípade ide najmä o stereo kamery, RADAR (*radio detection and ranging*), LIDAR (*light detection and ranging*) a pod. V druhom prípade ide o komunikačné technológie s krátkym dosahom, ktoré pracujú vo vyhradenom frekvenčnom pásme 5,9 GHz alebo technológie s dlhším dosahom ako mobilné siete 3G, 4G či 5G.

[37] Na úrovni EÚ bolo prijatých niekoľko nezáväzných dokumentov, ktoré sa týkajú regulácie umelej inteligencie a výslovne spomínajú v rôznych kontextoch autonómne vozidlá. Príkladom je *White Paper on Artificial Intelligence: a European approach to excellence and trust*. V zmysle tohto dokumentu technológie umelej inteligencie môžu pre používateľov predstavovať nové bezpečnostné riziká, v prípade ak sú zabudované do výrobkov a služieb. Ako príklad sa uvádza autonómne vozidlo, ktoré v dôsledku chyby v technológii rozpoznávania objektov môže nesprávne identifikovať predmet na ceste a spôsobiť nehodu, ktorá má za následok zranenia a materiálne škody.

mentu 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 (ďalej len „nariadenie o typovom schválení vozidiel“). Predmetné nariadenie sa uplatňuje od 1. septembra 2020.

Technológie, ktoré nie sú upravené v nariadení o typovom schválení vozidiel, ako napríklad systém automatického riadenia je možné schváliť prostredníctvom postupu výnimiek, ktoré sú upravené v predmetnom nariadení v čl. 39, ktorý upravuje výnimky pre nové technológie alebo nové koncepcie. V takýchto prípadoch sa schválenie udeľuje na základe vnútroštátneho *ad hoc* posúdenia bezpečnosti, pričom je potrebné povolenie zo strany Komisie. Komisia prijme vykonávacie akty, ktorými rozhodne o udelení povolenia. Vnútroštátny schvaľovací orgán môže do prijatia vykonávacích aktov udeliť predbežné typové schválenie EÚ pre typ vozidla, na ktorý sa vzťahuje požadovaná výnimka. Predbežné povolenie bude platné len na území členského štátu daného schvaľovacieho orgánu, avšak schvaľovacie orgány ostatných členských štátov môžu akceptovať predbežné typové schválenie EÚ na svojom území za predpokladu, že o tom písomne informujú schvaľovací orgán, ktorý predbežné typové schválenie EÚ udelil.[38]

Nariadenie o typovom schválení vozidiel špecificky neupravuje problematiku ochrany osobných údajov či kybernetickej bezpečnosti. V zmysle recitálu 62 predmetného nariadenia sa považuje za dôležité, aby výrobcovia vykonávali všetky opatrenia potrebné na zabezpečenie súladu s pravidlami týkajúcimi sa spracúvania a prenosu osobných údajov, ktoré vznikajú pri používaní vozidla. Pri používaní autonómnych a prepojených vozidiel, kde sú využívané rôzne systémy automatického riadenia či komunikačné systémy dochádza k spracúvaniu a prenosu osobných údajov.

Nakoľko existovali rôzne prístupy pri aplikovaní výnimiek pre nové technológie alebo nové koncepcie, Komisia vydala 12. februára 2019

[38] Čl. 39 nariadenia o typovom schválení vozidla.

Usmernenia týkajúce sa výnimky na schválenie automatizovaných vozidiel EÚ (ďalej len „usmernenia“).[39] Cieľom týchto usmernení je zosúladiť postup členských štátov pri vnútroštátnom *ad hoc* hodnotení automatizovaných vozidiel a zjednodušiť vzájomné uznávanie tohto hodnotenia, ako aj zabezpečiť spravodlivú hospodársku súťaž a transparentnosť. Pokyny sa zameriavajú na automatizované vozidlá, ktoré môžu riadiť samy seba v obmedzenom počte jazdných situácií na úrovni automatizácie 3 a 4 podľa SAE štandardu.[40]

Usmernenie sa oblasti ochrany osobných údajov a kybernetickej bezpečnosti venuje najmä v dvoch častiach. Prvou časťou sú usmernenia o inštalácii nahrávacích zariadení (*event data recorders*). V zmysle usmernení č. 23-27 by automatizované vozidlá mali byť vybavené palubným zariadením, ktoré zaznamenáva prevádzkový stav systému automatického riadenia a stav vodiča s cieľom určiť, kto šoféroval počas nehody. Tieto zhromaždené údaje umožňujú určiť zodpovednosť v prípade nehody a umožňujú posúdiť, či vodič alebo vozidlo správne zareagovali na situáciu. Medzi tieto údaje možno považovať napr. prevádzkový stav systému automatického riadenia, stav vodiča, informácie o okolí, kontrolné informácie o vozidle. Palubné zariadenie musí byť schopné uchovávať údaje zabezpečeným spôsobom, dodržiavať právne predpisy EÚ o ochrane údajov a byť chránené pred manipuláciou, pričom by mal byť umožnený prístup k takým to údajom vnútroštátnym orgánom. Na základe získaných skúseností môžu byť vyvinuté konkrétnejšie požiadavky na zariadenia na záznam údajov (čas záznamu, čas uchovávania, na aké účely sa údaje používajú, štandardizovaný prístup, spôsob zaobchádzania s osobnými údajmi atď.).[41]

Výrobca vozidla je v zmysle usmernení povinný poskytnúť nasledovné informácie:

1 typ uložených údajov,
2 miesto uloženia,
3 trvanie uloženia,

[39] V názve a texte usmernenia sa používa pojem automatizované vozidlo (*automated vehicle*).

[40] Usmernenie, s. 1.

[41] Usmernenie, s. 5.

4 prostriedky na zabezpečenie bezpečnosti a ochrany údajov,

5 prístup k údajom.[42]

V časti o kybernetickej bezpečnosti je v usmerneniach vyjadrená požiadavka, aby vozidlo bolo skonštruované tak, aby chránilo vozidlo pred automatizovaným hacknutím pomocou najmodernejších techník a bolo v súlade s právnymi predpismi EÚ o ochrane údajov. Patrí sem napr. hodnotenie rizika výrobcom, návrhové opatrenia a primerané procesy na zabránenie, zmiernenie a reakciu na kybernetické útoky.

Výrobcovia vozidiel taktiež majú prijať opatrenia, ako napríklad tie, ktoré súvisia s aktualizáciou softvéru atď. nainštalovaného v automatizovaných vozidlách, ktoré sú potrebné na zabezpečenie prevádzkovej kybernetickej bezpečnosti počas celej jej životnosti.[43]

## 4.2 INTELIGENTNÉ DOPRAVNÉ SYSTÉMY

Jedným z praktických príkladov, kedy vozidlo môže komunikovať s IoT, resp. infraštruktúrou sú inteligentné dopravné systémy. Príklady aplikácie inteligentných dopravných systémov v cestnej doprave zahŕňajú riadenie a kontrolné systémy mestskej a diaľničnej premávky, elektronický výber mýta, navigáciu trasy a pod. Problematiku zavádzania inteligentných dopravných systémov upravuje smernica Európskeho parlamentu a Rady 2010/40/EÚ o rámci na zavedenie inteligentných dopravných systémov v oblasti cestnej dopravy a na rozhrania s inými druhmi dopravy (ďalej len „smernica o inteligentných dopravných systémoch“).

Vysoká úroveň bezpečnosti systémov inteligentného značenia má v súvislosti s autonómnymi vozidlami dôležitú úlohu, nakoľko autonómne a prepojené vozidlá pre svoje fungovanie komunikujú s rôznymi inteligentnými dopravnými systémami, kedy dochádza k prijímaniu údajov z externého zdroja, ale aj zdieľaniu údajov, ktoré zaznamenáva so vzdialenou treťou stranou pre rôzne účely.

V mnohých prípadoch bude zavádzanie a využívanie aplikácií a služieb inteligentných dopravných systémov zahŕňať aj spracovanie osobných

[42] Usmernenie, s. 9.

[43] Usmernenie, s. 5.

údajov. Problematika ochrany osobných údajov a bezpečnosti je špecificky upravená v čl. 10, v zmysle ktorého je potrebné, aby sa spracovanie osobných údajov realizovalo jednak v súlade s GDPR, ale aj smernicou o súkromí a elektronických komunikáciách.[44] Taktiež sa od členských štátov požaduje, aby boli osobné údaje chránené pred zneužitím vrátane nezákonného prístupu, zmeny alebo straty.

Pri používaní aplikácií inteligentných dopravných systémov by sa mali uplatňovať zásady obmedzenia účelu a minimalizácie údajov a taktiež by sa mala podporovať anonymizácia ako jedna zo zásad zvyšovania ochrany súkromia jednotlivcov.[45]

Z pohľadu komunikácie medzi vozidlami a cestnou infraštruktúrou zohrávajú dôležitú úlohu kooperatívne inteligentné dopravné systémy. Tieto systémy využívajú technológie, ktoré umožňujú cestným vozidlám komunikovať medzi sebou a s cestnou infraštruktúrou vrátane dopravnej signalizácie. Komisia v marci 2019 prijala Delegované nariadenie komisie ktorým sa dopĺňa smernica o inteligentných dopravných systémoch, pokiaľ ide o zavádzanie a prevádzkové využívanie kooperatívnych inteligentných dopravných systémov (ďalej len „delegované nariadenie“).

V cestnej doprave kooperatívne inteligentné dopravné systémy zvyčajne zahŕňajú komunikáciu medzi vozidlami navzájom (V2V), medzi vozidlom a infraštruktúrou (V2I) alebo medzi infraštruktúrami navzájom (I2I) a komunikáciu medzi vozidlami a chodcami alebo cyklistami (Vehicle-to-Everything, V2X).[46]

Služby ktoré sú poskytované prostredníctvom kooperatívnych inteligentných dopravných systémov sú buď založené na otvorenej sieti umožňujúcej komunikáciu medzi stanicami kooperatívnych inteligentných dopravných systémov (ďalej len „stanice KIDS“) spôsobom „všetci všetkým“ (*many-to-many*) alebo na základe rovnocennosti (*peer-to-peer*). Tento prístup znamená, že všetky stanice KIDS si môžu navzájom bezpečne vymieňať

[44] Smernica Európskeho parlamentu a Rady2002/58/ES z 12. júla 2002, týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách).

[45] Čl. 10 smernice o inteligentných dopravných systémoch.

[46] Delegované nariadenie, s. 1.

správy a nie sú odkázané na výmenu správ len s (jednou) vopred stanovenou stanicou, resp. stanicami.[47]

Stanica KIDS je zostava hardvérových a softvérových komponentov potrebných na zber, uchovávanie, spracovanie, prijímanie a prenos zabezpečených a dôveryhodných správ s cieľom umožniť poskytovanie služby kooperatívnych inteligentných dopravných systémov. V zmysle delegovaného nariadenia sa stanice KIDS namontované vo vozidlách, prenosné alebo namontované popri cestnej infraštruktúre považujú za výrobky, ktoré možno uviesť na trh ako samostatné sústavy alebo ako súčasti väčších zostáv.[48]

V zmysle bodu 25 a 26 preambuly delegovaného nariadenia by sa informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby mali spracúvať za prísneho dodržiavania zásady minimalizácie údajov, len na účely špecifikované v delegovanom nariadení. Taktiež by sa mali ukladať len tak dlho, ako je to potrebné. Bezpečnostné požiadavky na pseudonymizáciu, ktoré sú stanovené v delegovanom nariadení, prispievajú k zníženiu rizika zneužitia údajov. Koncoví používatelia by mali byť jasne a komplexne informovaní o všetkých relevantných informáciách týkajúcich sa spracúvania ich osobných údajov v súlade s GDPR.

Delegované nariadenie sa detailne venuje problematike bezpečnosti v kapitole V, ktorá upravuje bezpečnosť staníc KIDS. Zavádza sa systém EÚ na správu bezpečnostných poverení koordinovaných inteligentných dopravných systémov, ktorý musí spĺňať požiadavky na certifikačnú politiku (príloha III) a bezpečnostnú politiku (príloha IV), v ktorej sa stanovujú požiadavky na riadenie informačnej bezpečnosti v koordinovaných inteligentných dopravných systémoch.[49]

Každý prevádzkovateľ stanice KIDS musí prevádzkovať systém riadenia informačnej bezpečnosti v súlade s normou ISO/IEC 27001 a dodatočnými

[47] Bod 2 preambuly delegovaného nariadenia.

[48] Bod 15 preambuly delegovaného nariadenia.

[49] Čl. 23 delegovaného nariadenia.

požiadavkami uvedenými v bode 1.3.1 prílohy IV delegovaného nariadenia.[50]

V súvislosti so stanicami KIDS si je potrebné uvedomiť, že aj v prípade komunikácie V2I vždy pôjde o výmenu správ medzi jednotlivými stanicami KIDS. Preto, aby vozidlo mohlo komunikovať s inými stanicami KIDS je potrebné, aby takáto stanica bola na vozidle namontovaná.

## 4.3 KYBERNETICKÁ BEZPEČNOSŤ

Bezpečnosť inteligentných dopravných systémoch upravuje taktiež smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (ďalej len „smernica NIS“). V zmysle smernice sa kybernetická bezpečnosť týka ochrany sietí a informačných systémov, prostredníctvom ktorých sa poskytujú základné služby vo vybraných odvetviach (energetika, bankovníctvo, doprava, zdravotníctvo a pod.), ako aj digitálne služby (online trhovisko, internetový vyhľadávač a služby cloud computingu). V prípade základných služieb ide o služby, ktoré majú zásadný význam z pohľadu zachovania spoločenských a hospodárskych činností.

Prevádzkovatelia inteligentných dopravných systémov v postavení prevádzkovateľov základných služieb sú povinní plniť povinnosti týkajúce sa bezpečnostných opatrení a oznamovania incidentov v zmysle smernice NIS. Uplatňovanie smernice NIS a požiadaviek uložených podľa delegovaného nariadenia sa môže v určitých prípadoch navzájom dopĺňať.

Napriek skutočnosti, že výrobcovia autonómnych vozidiel nie sú v súčasnosti zaradení do jedného z odvetví v zmysle smernice NIS, je možné, že v budúcnosti môže byť v odvetví doprava pridané pododvetvie, ktoré sa bude týkať výrobcov vozidiel, ktoré disponujú systémami automatického riadenia alebo autonómnymi systémami, resp. dodávateľov takýchto systémov. Výrobcovia vozidiel, resp. dodávatelia systémov by v pozícii prevádzkovateľov základných služieb museli spĺňať povinnosti týkajúce sa bezpečnostných opatrení a oznamovania incidentov v zmysle smernice NIS.

[50] Čl. 27 delegovaného nariadenia.

Ďalším legislatívnym aktov z oblasti kybernetickej bezpečnosti, ktorý bol prijatý na úrovni Európskej únie je nariadenie Európskeho parlamentu a Rady o Agentúre EÚ pre kybernetickú bezpečnosť (ENISA), o zrušení nariadenia (EÚ) č. 526/2013 a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií (ďalej len „akt o kybernetickej bezpečnosti“), ktorý okrem iného vytvára systém certifikácie v oblasti kybernetickej bezpečnosti, ktorý by mal zabezpečiť dostatočnú úroveň kybernetickej bezpečnosti IKT produktov, postupov a služieb v Európskej únii.

Certifikácia IKT v oblasti kybernetickej bezpečnosti sa stáva veľmi dôležitou otázkou, a to najmä vo vzťahu k zvýšenému používaniu technológií, ktoré požadujú vysokú úroveň kybernetickej bezpečnosti. K odvetviam ako prepojené a autonómne vozidlá, elektronické zdravotnícke pomôcky, riadiace systémy priemyselnej automatizácie a inteligentné siete, kde sa bežne využíva certifikácia, by sa mali v blízkej budúcnosti pridať ďalšie odvetvia.[51]

Certifikát osvedčí, že výrobky a služby IKT, ktoré boli certifikované v súlade s takýmto systémom, spĺňajú stanovené požiadavky na kybernetickú bezpečnosť. Výsledný certifikát bude uznávaný vo všetkých členských štátoch, čo uľahčí podnikom cezhraničné obchodovanie a zákazníkom pochopiť bezpečnostné prvky produktu alebo služby.[52]

Využitie certifikácie kybernetickej bezpečnosti je dobrovoľné, pokiaľ sa to nestanovuje inak v právnych predpisoch Európskej únie alebo vnútroštátnych právnych predpisoch, ktorými sa stanovujú bezpečnostné požiadavky týkajúce sa produktov a služieb IKT. Postupy certifikácie kybernetickej bezpečnosti produktov a služieb IKT, na ktoré sa vzťahuje európsky systém certifikácie kybernetickej bezpečnosti, by mali stratiť účinky od dátumu, ktorý stanoví Komisia vo vykonávacom akte. Okrem toho by členské štáty nemali zavádzať nové vnútroštátne systémy certifikácie kybernetickej

[51] Bod 65 recitálu aktu o kybernetickej bezpečnosti.

[52] Bližšie k systému certifikácie v oblasti kybernetickej bezpečnosti pozri: VOSTOUPAL, J.: *Certifikace kyberbezpečnostních technologií. In* Revue pro právo a technologie. 2019, č. 20, s. 147-268. [on-line]. Dostupné z: https://journals.muni.cz/revue/article/view/12570 [citované 28.9.2020].

bezpečnosti v prípade produktov a služieb IKT, pre ktoré už existuje európsky systém certifikácie kybernetickej bezpečnosti.[53]

## 5. OCHRANA OSOBNÝCH ÚDAJOV

V tejto časti príspevku sa zameriame na klasifikáciu rôznych aktérov toku údajov na základe modelových situácií uvedených vyššie. V prvom rade považujeme za vhodné uviesť niekoľko poznámok ku osobnej pôsobnosti GDPR a distribúcií zodpovednosti za spracúvanie osobných údajov. Následne stručne charakterizujeme usmernenie Výboru na ochranu údajov (ďalej len „EDPB"), ktoré sa týka spracúvania osobných údajov aj v autonómnych vozidlách.[54]

V poslednej časti aplikujeme relevantný právny rámec na modelové situácie načrtnuté v predchádzajúcich častiach článku a poukážeme na možné aplikačné problémy v kontexte osobnej pôsobnosti GDPR.

### 5.1 GDPR A OSOBNÁ PÔSOBNOSŤ

Všeobecné nariadenia na ochranu údajov[55] (ďalej len „GDPR") síce neobsahuje výslovne vymedzené ustanovenie s názvom „osobná pôsobnosť," avšak v rámci právneho textu definuje a upravuje rôzne povinnosti súvisiace s aktérmi spracúvania osobných údajov. Ak určitá entita spĺňa požiadavky materiálnej[56] a teritoriálnej pôsobnosti[57] GDPR, je vhodné pristúpiť ku skúmaniu, v akej pozícií sa vlastne nachádza. V tomto kontexte GDPR definuje dvoch kľúčových aktérov spracúvania osobných údajov – prevádzkovateľa (*controller)* a sprostredkovateľa (*processor)* osobných údajov.

[53] Bod 69 recitálu aktu o kybernetickej bezpečnosti.

[54] European Data Protection Board Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications.[Online]. 2020. [cit. 29. 9. 2020] Dostupné z: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-12020-processing-personal-data-context_en.

[55] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov). In EUR-lex [právní informační system]. Úřad pro publikace Evropské unie. Dostupné z https://eur-lex.europa.eu/legal-content/SK/TXT/?qid=1584526623550&uri=CELEX%3A32016R0679

[56] Článok 2, GDPR.

[57] Článok 3, GDPR.

Správne definovanie entity je osobitne dôležité s ohľadom na distribúciu zodpovednosti za súlad s legislatívnymi požiadavkami na spracúvanie osobných údajov.

### 5.1.1 POJEM PREVÁDZKOVATEĽ

Prevádzkovateľ je v GDPR legálne definovaný ako *„fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý sám alebo spoločne s inými určí účely a prostriedky spracúvania osobných údajov.“*[58] EDPB vydal nedávno usmernenie[59] k pojmom prevádzkovateľ a sprostredkovateľ.[60] Dané usmernenie implicitne rešpektuje aj novšia judikatúra Súdneho dvora Európskej únie (ďalej len „SDEÚ“) k výkladu daného pojmu.[61]

EDPB vymedzuje päť osobitných prvkov definície prevádzkovateľa: (i) fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt; (ii) ktorý sám alebo spoločne s inými; (iii) určí; (iv) účely a prostriedky; (v) spracúvania osobných údajov.[62] Najdôležitejšie prvky danej definície analyzujeme nižšie.

Prvým aspektom definície je určenie entity, ktorá osobné údaje spracúva. WP29 zvýrazňuje, že v tomto kontexte je potrebné skúmať zaužívané inštitúty súkromného a verejného práva, ktoré by nás mali nasmerovať k fi-

---

[58] Článok 4 (7), GDPR.

[59] European Data Protection Board Guidelines 07/2020 on the concepts of controller and processor in the GDPR. [Online]. 2020. [cit. 29. 9. 2020]. Dostupné z: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en.

[60] Článok 2 d) obsahuje definíciu prevádzkovateľa v tomto znení: *"kontrolór" znamená fyzickú alebo právnickú osobu, verejný orgán, agentúru alebo akýkoľvek iný orgán, ktorý sám, alebo v spojení s inými, určí účely a prostriedky spracovania osobných údajov; tam, kde sú účely a prostriedky spracovania stanovené vnútroštátnymi zákonmi a nariadeniami, alebo zákonmi a nariadeniami spoločenstva, ten, kto spracovanie riadi, alebo konkrétne kritéria pre jeho menovanie, môžu byť navrhnuté na základe vnútroštátneho práva alebo práva spoločenstva“*

[61] Pozri napr. Rozsudok Súdneho dvora zo dňa 5. júna 2018 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein proti Wirtschaftsakademie Schleswig-Holstein GmbH. Vec č. C-210/16.

[62] European Data Protection Board Guidelines 07/2020 on the concepts of controller and processor in the GDPR. [Online]. 2020. [cit. 29. 9. 2020]. Dostupné z:https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en. S. 9.

nálnemu určeniu konkrétnej entity. Za prevádzkovateľa by mala byť považovaná spoločnosť alebo orgán, nie špecifická osoba v rámci ich štruktúr.[63] SDEÚ v prípade *Google Spain* uviedol, že *„založenie takejto inštitúcie na území členského štátu predpokladá účinné a skutočné vykonávanie činnosti prostredníctvom stabilných dohôd [prostredníctvom stálej prevádzkarne – neoficiálny preklad]“ a že „právna forma takejto inštitúcie, či je to pobočka, alebo dcérska spoločnosť s právnou subjektivitou, nie je určujúcim činiteľom.“*[64] Túto požiadavku v súčasnosti odzrkadľuje Recitál 22 GDPR.[65]

Druhý aspekt reflektuje, či subjektov, ktoré možno považovať za prevádzkovateľov je viacero alebo je len jeden. Tejto problematike sa osobitne venujeme v časti „spoloční prevádzkovatelia“ nižšie.

Najdôležitejším aspektom definície je určenie účelov a prostriedkov spracúvania osobných údajov. EDPB predmetný aspekt diferencuje na problematiku „určenia“ a „účelov a prostriedkov“ spracúvania osobných údajov.

Určenie účelov je potrebné vnímať v kontexte inštitútu prevádzkovateľa, ktorý je dynamický a funkčný, čo v praxi znamená posudzovanie faktických okolností a nie iba formálneho splnenie niekoľkých kritérií.[66] Požiadavka „určenia“ účelov a prostriedkov spracúvania osobných údajov môže vyplávať z troch legitímnych zdrojov. EDPB konkrétne uvádza (i) explicitnú požiadavku ustanovenú právom, (ii) implicitnú požiadavku ustanovenej právom alebo (iii) faktického vplyvu.[67] Pri explicitnej požiadavke upravenej

---

[63] Tamže, s. 10.

[64] Rozsudok Súdneho dvora zo dňa 13. mája 2014 Google Spain SL a Google Inc. proti Agencia Española de Protección de Datos (AEPD) a Mariovi Costejovi Gonzálezovi. Vec č. C-131/12.

[65] Recitál 22, GDPR: *„Každé spracúvanie osobných údajov v kontexte činností prevádzkarne prevádzkovateľa alebo sprostredkovateľa v Únii by sa malo vykonávať v súlade s týmto nariadením bez ohľadu na to, či sa samotné spracúvanie uskutočňuje v Únii. Prevádzkareň znamená efektívny a skutočný výkon činnosti prostredníctvom stálych dojednaní. Právna forma takýchto dojednaní, či už ide o pobočku alebo dcérsku spoločnosť s právnou subjektivitou, nie je v tomto ohľade určujúcim faktorom.“*

[66] European Data Protection Board Guidelines 07/2020 on the concepts of controller and processor in the GDPR. [Online]. 2020. [cit. 29. 9. 2020]. Dostupné z:https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en. S. 10 - 11.

[67] Tamže.

v právnom poriadku pôjde zväčša o situácie, keď právna norma obsahuje obligáciu zbierať a spracúvať osobné údaje.[68] Implicitná požiadavka na spracúvania osobných údajov spočíva v prirodzenom súvise medzi určitou entitou a spracúvaním osobných údajov, čo je osobitne dôležité v prípadoch, keď právny predpis priamu obligáciu neobsahuje, ale je nepriamo vyplýva zo znenia legislatívneho textu.[69] Tretím zdrojom postavenia prevádzkovateľa môžu byť faktický vplyv a okolnosti daného spracúvania osobných údajov. V tomto kontexte EDPB uvádza zmluvné podmienky ako faktor, ktorý je potrebné brať do úvahy, avšak nie absolútne, nakoľko rozhodujúci je reálny stav a nie ustanovenia v zmluve. Ďalšie faktory, ktoré je možné posudzovať sú stupeň kontroly v rámci spracovateľských operácii, „image" vytvorený voči dotknutým osobám či primerané očakávaní dotknutých subjektov.[70] Subjekt, ktorý má nulový faktický alebo právny vplyv na určenie účelov a prostriedkov spracovania osobných údajov nemôže byť považovaný za prevádzkovateľa.

Určenie účelu spracovania je výsadou prevádzkovateľa. Účel možno zjednodušene vymedziť ako cieľ spracovateľskej operácie. Určenie účelov a prostriedkov spracúvania teda reflektuje „prečo" a „ako" budú osobné údaje spracúvané. Esenciou pri analýze daného faktora je úroveň detailov pri predmetnom determinovaní.[71] Prostriedky spracúvania osobných údajov zahŕňajú technické a organizačné aspekty spracúvania osobných údajov. Môže ísť aj o určenie toho, aké údaje sa budú spracúvať, aké tretie strany

---

[68] Ako príklad zo slovenského právneho poriadku možno uviesť postavenie advokátov v zmysle § 18 ods. 6 zákona č. 586/2003 Z. z. o advokácii a o zmene a doplnení zákona č. 455/1991 Zb. o živnostenskom podnikaní (živnostenský zákon) v znení neskorších predpisov: *„Advokát spracúva osobné údaje klientov a iných fyzických osôb v rozsahu nevyhnutnom na účely výkonu advokácie v súlade s týmto zákonom a s osobitným predpisom. Advokát má pri spracúvaní osobných údajov v zmysle prvej vety tohto odseku postavenie prevádzkovateľa podľa osobitného predpisu."*

[69] Ako príklad možno uviesť spracúvanie osobných údajov zamestnávateľom v zmysle zákona č. 311/2001 Z. z. Zákonníka práce.

[70] European Data Protection Board Guidelines 07/2020 on the concepts of controller and processor in the GDPR. [Online]. 2020. [cit. 29. 9. 2020]. Dostupné z:https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en. S. 12.

[71] Tamže, s. 13.

budú mať k údajom prístup či určenie dôb uchovávania.[72] Prostriedky spracúvania osobných údajov a ich určenie môže byť delegované na sprostredkovateľov, ak hovoríme o organizačných a technických otázkach (software, hardware).

Problematiku (spoločného) vymedzenia účelu ilustruje známy prípad vo veci SWIFT. Spoločnosť SWIFT figurovala ako sprostredkovateľ pri spracúvaní osobných údajov európskych bankových inštitúcií. Zároveň ale bez príkazu európskych bánk sprístupňovala údaje o dotknutých osobách v Európe Ministerstvu financií v Spojených štátoch amerických.

WP29 (Article 29 Data Protection Working Party, predchodca EDPB) vo svojom názore[73] vyslovila záver, že spoločnosť SWIFT na seba delegovala právomoci prevádzkovateľa (poskytnutím údajov o dotknutých osobách) a stala sa tak spoločným prevádzkovateľom spolu s bankovými inštitúciami, ktoré na druhej strane značne zanedbali dohľad nad aktivitami svojho sprostredkovateľa.

### 5.1.2 POJEM SPOLOČNÍ PREVÁDZKOVATELIA

Ak dvaja alebo viacerí prevádzkovatelia spoločne určia účely a prostriedky spracúvania, sú spoločnými prevádzkovateľmi.[74] S inštitútom spoločných prevádzkovateľov rátala už síce Smernica 95/46/ES v intenciách usmernenia WP29, avšak výslovne zakotvenie daného inštitútu upravuje až GDPR. Nie je dôležitá úroveň prepojenia spoločných prevádzkovateľov (od spoločného zdieľania výkonu všetkých spracovateľských operácii až po zdieľanie výkonu len jednej spracovateľskej operácie).[75] Typickým príkladom spoločných prevádzkovateľov je vedenie databázy dlžníkov viacerými

---

[72] Tamže, s. 13 - 14.

[73] Article 29 Data Protection Working Party Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT). 2006. [cit. 29. 9. 2020]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp128_en.pdf.

[74] Článok 26 ods. 1, GDPR.

[75] European Data Protection Board Guidelines 07/2020 on the concepts of controller and processor in the GDPR. [Online]. 2020. [cit. 29. 9. 2020]. Dostupné z:https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en. S. 17 a nasl.

entitami napr. vo finančnom sektore. Na tomto mieste je ale potrebné upozorniť na rozdiel medzi spoločnými prevádzkovateľmi a prenosom osobných údajov (napr. cestovná agentúra, ktorá pošle dáta svojich zákazníkom leteckej spoločnosti a hotelovému zariadeniu). Iná by bola situácia, ak by cestovná agentúra, hotel a letecká spoločnosť založila spoločnú databázu manažmentu rezervácii. V takomto prípade by sa jednalo o spoločných prevádzkovateľov.[76]

Napriek výslovnému zakotveniu predmetného inštitútu v GDPR viacerí autori poukazujú na to, že špecifické otázky týkajúce sa alokácie zodpovednosti sú stále predmetom nejasností a diskusií.[77]

### 5.1.3 POJEM SPROSTREDKOVATEĽ

Sprostredkovateľ je v zmysle článku 4 bodu 8 GDPR *„fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý spracúva osobné údaje v mene prevádzkovateľa.“* Na kvalifikovanie entity ako sprostredkovateľa musia byť kumulatívne splnené dva atribúty. V prvom rade musí ísť o odlišnú entitu od prevádzkovateľa. Druhým kritériom je, že spracúvanie osobných údajov sa vykonáva v mene prevádzkovateľa.[78] Inštitút sprostredkovateľa reflektuje delegáciu resp. poverenie spracúvať osobné údaje na iné entity. Do spracúvania osobných údajov je zároveň možné zapojiť aj ďalších sprostredkovateľov (sub-sprostredkovateľov). Sprostredkovateľ to však môže urobiť iba so súhlasom prevádzkovateľa.[79]

### 5.1.4 INÉ ENTITY

Okrem kľúčových aktérov spracúvania osobných údajov v podobe prevádzkovateľa a sprostredkovateľ upravuje GDPR definíciu a postavenie ďalších troch entít.

---

[76] Tamže, s. 20 – 21.

[77] Pozri napr. VAN ALSENOY, Brendan: Liability under EU Data Protection Law. *In 7 (2016) JIPITEC 271*.

[78] European Data Protection Board Guidelines 07/2020 on the concepts of controller and processor in the GDPR. [Online]. 2020. [cit. 29. 9. 2020]. Dostupné z:https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en. S. 24.

[79] Článok 28 ods.4, GDPR.

V prvom rade GDPR na mnohých miestach v legislatívnom texte ustanovuje práva a povinnosti pre dotknuté osoby. GDPR dotknutú osobu definuje ako identifikovanú alebo identifikovateľnú fyzickú osobu, ktorej sa osobné údaje týkajú.[80] Inými slovami, dotknutá osoba je osoba, ktorej osobné údaje sú spracúvané ako napr. bežný užívateľ sociálnej siete, zamestnanec z pohľadu zamestnávateľa alebo zákazník alebo klient elektronického obchodu či služby.

Ďalším pojmom, ktorý GDPR upravuje je príjemca. V zmysle definície je príjemca *„fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorému sa osobné údaje poskytujú bez ohľadu na to, či je treťou stranou.“*[81] Zároveň GDPR obsahuje aj negatívnu definíciu príjemcu týkajúceho sa orgánu verejnej moci pri výkone svojich oprávnení a úloh.[82] Príjemcom tak napr. môže byť sprostredkovateľ alebo poverený zamestnanec prevádzkovateľa.

Posledným pojmom do mozaiky osobnej pôsobnosti GDPR je tretia strana. Tretia je strana je definovaná primárne prostredníctvom negatívnej enumerácie: *„Tretia strana...je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt než dotknutá osoba, prevádzkovateľ, sprostredkovateľ a osoby, ktoré sú na základe priameho poverenia prevádzkovateľa alebo sprostredkovateľa poverené spracúvaním osobných údajov.“*[83]

## 5.2 ZODPOVEDNOSŤ PRI SPRACÚVANÍ OSOBNÝCH ÚDAJOV

Ak porovnáme znenie Smernice 95/46/ES s GDPR v súvislosti s ustanoveniami týkajúcimi sa zodpovednosti, tie prešli určitými zmenami a na niektorých miestach boli výrazne doplnené. Niektorí autori konštatujú, že režim

[80] Viď článok 4 bod 1, GDPR.

[81] Článok 4 bod 9, GDPR.

[82] Článok 4 bod 8, GDPR: *„Orgány verejnej moci, ktoré môžu prijať osobné údaje v rámci konkrétneho zisťovania v súlade s právom Únie alebo právom členského štátu, sa však nepovažujú za príjemcov; spracúvanie uvedených údajov uvedenými orgánmi verejnej moci sa uskutočňuje v súlade s uplatniteľnými pravidlami ochrany údajov v závislosti od účelov spracúvania.“*

[83] Článok 4 bod 10, GDPR.

zodpovednosti podľa GDPR je veľmi blízko tradičnému ponímaniu opatrení v rámci *tort law* v zmysle angloamerickej právnej tradície.[84]

Článok 82 ods. 2 GDPR obsahuje všeobecnú klauzulu týkajúcu sa zodpovednosti za škodu: *„Každá osoba, ktorá utrpela majetkovú alebo nemajetkovú ujmu v dôsledku porušenia tohto nariadenia, má právo na náhradu utrpenej škody od prevádzkovateľa alebo sprostredkovateľa.“* Podobne ako pri predchádzajúcej právnej úprave, z tohto ustanovenia môžu byť derivované tri podmienky pre uplatnenie zodpovednosti: (i) protiprávnosť, (ii) vznik škody a (iii) príčinná súvislosť.[85] Podmienka protiprávnosti je splnená pri akomkoľvek porušení GDPR. V súvislosti so vznikom škody, GDPR explicitne ustanovuje, že môže ísť o materiálnu alebo nemateriálnu škodu. Príklady materiálnej škody môžu zahŕňať výpoveď z práce, nenaplnenie zmluvy či úpravu zmluvných podmienok v neprospech dotknutej osoby spôsobenú nezákonným spracúvaním osobných údajov. Nemajetkovú ujmu možno ilustrovať na príkladoch úzkosti, diskriminácie či negatívneho obrazu v očiach verejnosti.[86] Poslednou podmienkou pri právnom režime zodpovednosti je príčinná súvislosť medzi protiprávnym konaním a vznikom škody.[87] Pri otázke „kto“ si môže nárok na náhradu škody v zmysle GDPR existujú dve interpretácie, nakoľko legislatíva používa pojem „akákoľvek osoba“. Prvá interpretácia je reštriktívna a hovorí, že škodu si môže nárokovať iba dotknutá osoba v zmysle GDPR. Na strane druhej, existuje skupina autorov, ktorí presadzujú extenzívnejšie prístup v zmysle ktorého si škodu môže nárokovať aj akákoľvek tretia strana.[88] Prikláňame sa k reštriktívnej interpretácií nakoľko iná strana ako dotknutá osoba ťažko úspešne preukáže škodu pri spracúvaní osobných údajov. Je však potrebné zvýrazniť, že

---

[84] TRAKMAN, Leon – WALTERS, Robert – ZELLER, Bruno: Tort and Data Protection Law: Are There Any Lessons to Be Learnt? *In European Data Protection Law Review 4/2019*, s. 506.

[85] Tamže, s. 493 – 495.

[86] Pozri viac v CORDEIRO, A.B. Menezes: Civil Liability for Processing of Personal Data in the GDPR. *In European Data Protection Law Review 4/2019*, s. 495.

[87] Článok 82 ods. 2, GDPR: *„Každá osoba, ktorá utrpela majetkovú alebo nemajetkovú ujmu v dôsledku porušenia tohto nariadenia, má právo na náhradu utrpenej škody od prevádzkovateľa alebo sprostredkovateľa.“*

[88] Pozri viac CORDEIRO, A.B. Menezes: Civil Liability for Processing of Personal Data in the GDPR *In European Data Protection Law Review 4/2019,* s. 495 – 496.

SDEÚ presadzuje princíp kompletnej a účinnej ochrany (*full and effective protection)*[89] pri spracúvaní osobných údajov a v zmysle toho je potrebné akceptovať, že náhrada škody by nemala byť rezervovaná pre dotknuté osoby.

### 5.2.1 ZODPOVEDNOSŤ PREVÁDZKOVATEĽA

Režim objektívnej zodpovednosti podľa Smernice 95/48/ES ostal v GDPR nezmenený, čo je potvrdené v článku 82 ods. 2 GDPR: *„Každý prevádzkovateľ, ktorý sa zúčastnil na spracúvaní, je zodpovedný za škodu spôsobenú spracúvaním, ktoré bolo v rozpore s týmto nariadením."*

Na tomto mieste si však dovoľujeme zvýrazniť, že z hľadiska povinností prevádzkovateľov GDPR akcentuje princíp zodpovednosti (*accountability*).[90] Princíp zodpovednosti obsahuje dve roviny. V prvej rovine sú prevádzkovatelia povinní demonštrovať súlad s požiadavkami GDPR vo formálnej rovine napr. prostredníctvom vypracovania záznamov o spracovateľských operáciách, plnením informačnej povinnosti či prijatím interných predpisov a pravidiel pre narábanie s osobnými údajmi v rámci organizácie. Druhá rovina reflektuje implementáciu organizačných a technických opatrení do praxe ako napr. manažment identity v rámci automatizovaných počítačových systémov, proces pre nahlasovanie bezpečnostných incidentov v podobe porušení ochrany osobných údajov či kreovanie odlišného prístupu ku osobným údajom vzhľadom na pracovné zaradenie zamestnancov.[91] Tento princíp prakticky znamená, že ak dotknutá osoba poukáže na poru-

[89] Pozri napríklad Rozsudok Súdneho dvora zo dňa 13. mája 2014 Google Spain SL a Google Inc. proti Agencia Española de Protección de Datos (AEPD) a Mariovi Costejovi Gonzálezovi. Vec č. C-131/12; Rozsudok Súdneho dvora Európkej únie zo dňa 5. júna 2018 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein proti Wirtschaftsakademie Schleswig-Holstein GmbH. Vec č. C-210/16 alebo Rozsudok Súdneho dvora zo dňa 10. júla 2018 Tietosuojavaltuutettu za účasti Jehovan todistajat – uskonnollinen yhdyskunta. Vec č. C-25/17.

[90] Pozri článok 5 ods. 2, GDPR.

[91] Podrobnejšie pozri VAN ALSENOY, Brendan – DUMORTIER, Jos: The accountability principle in data protection regulation: origin, development and future directions. *In GUAGNIN, D. – HEMPEL, L. - ILTEN, C. (eds): Managing Privacy Through Accountability*. 2012, Palgrave Macmillian, s. 49 – 82.

šenie GDPR zo strany prevádzkovateľa, dôkazné bremeno sa presúva na stranu prevádzkovateľa, ktorý musí následne preukázať súlad s GDPR.[92]

Prevádzkovateľ sa zodpovednosti môže zbaviť iba v prípadoch udalostí mimo jeho kontrolu. Článok 82 ods. 3 GDPR ustanovuje, že *„prevádzkovateľ…je zbavený zodpovednosti podľa odseku 2, ak sa preukáže, že nenesie žiadnu zodpovednosť za udalosť, ktorá spôsobila škodu.“* Niektorí autori naznačujú, že táto možnosť liberácie by mala byť interpretovaná reštriktívne.[93] Vývoj zodpovedných vzťahov v GDPR odzrkadľuje aj výslovne uznanie výnimiek za cudzí obsah v rámci smernice o elektronickom obchode[94] v článku 2 ods. 4 GDPR.[95] Prakticky to znamená jednotnejší prístup ku otázkam zodpovednosti v rámci európskej legislatívy a posilnenie právnej istoty.[96]

### 5.2.2 ZODPOVEDNOSŤ SPOLOČNÝCH PREVÁDZKOVATEĽOV

Ako už bolo uvedené vyššie, GDPR výslovne upravuje inštitút spoločných prevádzkovateľov.[97] Spoloční prevádzkovatelia sú povinní vymedziť svoje vzájomné práva a povinnosti v zmysle GDPR transparentným spôsobom. Na tomto mieste si dovoľujeme zvýrazniť, že každý zo spoločných prevádzkovateľ môže byť zodpovedný za škodu v plnom rozsahu. Je však potrebné

---

[92] VAN ALSENOY, Brendan: Liability under EU Data Protection Law. *In 7 (2016) JIPITEC 271*, s. 283.

[93] LAROUCHE, Pierre – PEITZ, Martin – PURTOVA, Nadya: *Consumer Privacy in network industries* – A CERRE Policy Report, 2016, Centre on Regulation in Europe. [Online] 2016. [cit. 29. 9. 2020]. Dostupné z: https://cerre.eu/wp-content/uploads/2016/01/160125_CERRE_Privacy_Final.pdf. S. 58.

[94] Smernica 2000/31/ES Európskeho parlamentu a Rady z 8. júna 2000 o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu, najmä o elektronickom obchode (smernica o elektronickom obchode). In EUR-lex [právní informační system]. Úřad pro publikace Evropské unie. Dostupné z https://eur-lex.europa.eu/legal-content/AUTO/?uri=CELEX:32000L0031&qid=1585224374231&rid=1.

[95] *„Týmto nariadením preto nie je dotknuté uplatňovanie smernice 2000/31/ES, najmä pravidlá týkajúce sa zodpovednosti poskytovateľov služieb informačnej spoločnosti uvedené v článkoch 12 až 15 uvedenej smernice.“*

[96] Napr. CUNHA, A. Maria Viola – MARIN, Luisa – SARTOR, Giovanni: Peer-to-peer privacy violations and ISP liability: data protection in the user-generated web. *In International Data Privacy Law,* Volume 2, Issue 2, 2012, s. 57.

[97] Článok 26 ods. 1, GDPR: *„Ak dvaja alebo viacerí prevádzkovatelia spoločne určia účely a prostriedky spracúvania, sú spoločnými prevádzkovateľmi.“*

poznamenať, že článok 83 GDPR neupravuje špecificky alokáciu zodpovednosti medzi spoločnými prevádzkovateľmi v prípade porušenia GDPR. Dôvody pre zbavenie zodpovednosti a typy odškodnenia sa aplikujú analogicky ako pri prevádzkovateľoch a sprostredkovateľoch.

Inštitút spoločných prevádzkovateľoch a alokácia zodpovednosti boli predmetom viacerých rozhodnutí SDEÚ, najnovšie v prípadoch *Wirtschaftsakademie* a *Fashion ID*, ktoré nadviazali na premisy judikované v prípade *Google Spain*. V rozhodnutí *Google Spain*[98] Luxemburský súd rozhodoval v kontexte spracúvania osobných údajov populárneho internetového vyhľadávača a pôvodného zdroja žurnalistického textu. V tomto prípade uviedol: *„...činnosť vyhľadávača môže významne a vo vzťahu k činnosti editorov webových stránok doplňujúcim spôsobom ovplyvniť základné práva na súkromie a ochranu osobných údajov, poskytovateľ tohto vyhľadávača ako osoba, ktorá určuje ciele a prostriedky tejto činnosti, musí v rámci svojich zodpovedností, kompetencií a možností zaručiť, že táto činnosť spĺňa požiadavky smernice 95/46, aby záruky ňou stanovené mohli mať plný účinok a aby účinná a úplná ochrana dotknutých osôb, a najmä práva na rešpektovanie ich súkromia, mohla byť skutočne dosiahnutá.“*[99] SDEÚ tak diskutovanej kauze zvýraznil, že súlad s pravidlami pre spracúvanie osobných údajov musí byť posúdený prostredníctvom optiky „kompetencií a možností“ prevádzkovateľa. Napriek tomu, že predmetný judikát sa týka pomerne špecifického prevádzkovateľa – internetového vyhľadávača, SDEÚ umožnil interpretovať alokáciu zodpovednosti pomerne extenzívne a otvoril tým pandorinu skrinku pre potenciálne úniky prevádzkovateľov zo zodpovednostných vzťahov.

Prípad *Wirtschaftsakademie*[100] sa skutkovo týkal správneho určenia postavenia správcu fanúšikovskej stránky na sociálnej sieti Facebook (Wirtschaft-

[98] Rozsudok Súdneho dvora zo dňa 13. mája 2014 Google Spain SL a Google Inc. proti Agencia Española de Protección de Datos (AEPD) a Mariovi Costejovi Gonzálezovi. Vec č. C-131/12.

[99] Rozsudok Súdneho dvora zo dňa 13. mája 2014 Google Spain SL a Google Inc. proti Agencia Española de Protección de Datos (AEPD) a Mariovi Costejovi Gonzálezovi. Vec č. C-131/12., bod 38.

[100] Rozsudok Súdneho dvora Európkej únie zo dňa 5. júna 2018 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein proti Wirtschaftsakademie Schleswig-Holstein GmbH. Vec č. C-210/16.

sakademie) a prevádzkovateľa samotnej sociálnej siete (Facebook). Najdôležitejším aspektom rozhodnutia bolo určenie, nakoľko je správca fanúšikovskej stránky zapojený do rozhodovania o účeloch a prostriedkoch spracúvania osobných údajov spolu s Facebookom. Luxemburský súd v úvode rozhodnutia poznamenal, že nie každý užívateľ sociálnej siete bude považovaný za prevádzkovateľa, špecifické postavenie správcu fanúšikovskej stránky vyplýva z toho, že *„správca fanúšikovskej stránky umiestnenej na Facebooku vytvorením takej stránky umožňuje spoločnosti Facebook, aby umiestňoval súbory cookies na počítači alebo akomkoľvek inom zariadení osoby, ktorá jeho fanúšikovskú stránku navštívila, bez ohľadu na to, či táto osoba má alebo nemá účet na Facebooku.“*[101] SDEÚ taktiež poukázal na to, že správca takejto stránky má pomerne veľkú voľnosť pri nastavovaní filtrov na cielene (výber publika) a kritérií na kreovanie štatistík návštevnosti a dosahu stránky.[102] Vzhľadom na tieto okolnosti Luxemburský súd judikoval, že správca fanúšikovskej stránky a Facebook sú na tieto účely spoloční prevádzkovatelia. Zároveň však SDEÚ zvýraznil dôležitosť posúdenia stupňa zodpovednosti vzhľadom na konkrétne štádiá spracúvania osobných údajov: *„...existencia spoločnej zodpovednosti neznamená nevyhnutne rovnakú zodpovednosť rôznych subjektov, ktorých sa týka spracovanie osobných údajov. Tieto subjekty môžu byť naopak zapojené do tohto spracovania v rôznych fázach a stupňoch, takže mieru zodpovednosti každého z nich treba hodnotiť z hľadiska všetkých relevantných okolností prejednávanej veci.“*[103] Doktrína tento prístup a rozhodnutie charakterizovala ako posun z makroskopického pohľadu na mikroskopické nazeranie na spracúvanie osobných údajov.[104] SDEÚ však nechal viaceré otázky otvorené ako napríklad mechanizmus pre určenie zodpovednosti v rámci spoločných prevá-

[101] Tamže, bod 35.

[102] Tamže, bod 36.

[103] Tamže, bod 43.

[104] MAHIEU, René – HOBOKEN VAN, Joris - ASGHARI, Hadi: Responsibility for Data Protection in a Networked World. On the question of the Controller. „Effective and Complete Protection“ and its Application to Data Access Rights in Europe. *In JIPITEC 39, 10 (2019*), s. 48.

dzkovateľov či posudzovanie previazanosti určenia účelov *a* prostriedkov spracúvania.[105]

Podobné závery možno derivovať z prípadu *Fashion ID*.[106] Interpretačný spor sa skutkovo týkal situácie, v ktorej prevádzkovateľ webovej stránky (Fashion ID – online predajca oblečenia) integroval na svojej stránke tlačidlo „LIKE“ napojené na sociálnu sieť Facebook. V tomto kontexte bolo dôležité, že údaje o každom návštevníkovi stránky Fashion ID boli automaticky prenášané sociálnej sieti bez ohľadu na to, či tam daný návštevník mal registrovaný účet alebo nie. Otázka osobnej pôsobnosti legislatívy tak bola znova na stole. SDEÚ opätovne zdôraznil širokú interpretáciu pojmu prevádzkovateľ a nadviazal na rozhodnutie vo veci *Wirtschaftsakademie*. Spoločné určenie účelov a prostriedkov spracúvania osobných údajov bolo založené na počiatkoch spracovateľskej operácie (zbieranie a prenos).[107] Zároveň však súd judikoval, že v rozličných fázach spracúvania je možné viazať odlišný stupeň zodpovednosti aktérom spracúvania osobných údajov.[108]

### 5.2.3 ZODPOVEDNOSŤ SPROSTREDKOVATEĽA

V porovnaní so Smernicou 95/48/ES sa zákonodarca na úrovni EÚ rozhodol urobiť krok vpred a explicitne upravil povinnosti a súvisiacu zodpovednosť sprostredkovateľov v GDPR. Povinnosti týkajúce sa sprostredkovateľov môžu vyplývať z ustanovení GDPR[109] alebo sprostredkovateľskej zmluvy uzavretej medzi sprostredkovateľom a prevádzkovateľom v zmysle článku 28 ods. 3 GDPR. Z faktického hľadiska sprostredkovateľ vždy koná a spracúva osobné údaje na základe a v mene poverenia od prevádzkovateľa. V prípade deviácie od pokynov sprostredkovateľa prípadne sprostredkovateľskej zmluvy je potrebné riešiť otázky týkajúce sa zodpovednosti.

[105] Tamže, s. 49.

[106] Rozsudok Súdneho dvora Európskej únie zo dňa 29. júla 2019 Fashion ID GmbH & Co.KG proti Verbraucherzentrale NRW eV. Vec č. C-40/17.

[107] Tamže, body 79 – 81.

[108] Tamže, bod 71.

[109] Napríklad povinnosť vypracovať záznamy o spracovateľských operáciách v zmysle článku 30 GDPR, nahlasovať porušenia ochrany osobných údajov prevádzkovateľovi podľa článku 33 ods. 2 GDPR alebo dezignovať do funkcie zodpovednú osobu v zmysle článku 37 GDPR.

Ustanovenia regulujúce zodpovednosť sprostredkovateľov stoja na princípe pomernej zodpovednosti: *„Sprostredkovateľ zodpovedá za škodu spôsobenú spracúvaním, len ak neboli splnené povinnosti, ktoré sa týmto nariadením ukladajú výslovne sprostredkovateľom, alebo ak konal nad rámec alebo v rozpore s pokynmi prevádzkovateľa, ktoré boli v súlade so zákonom.“*[110] GDPR však ustanovuje aj možnosť plnej zodpovednosti sprostredkovateľa, ktorý *„zodpovedá za celú škodu, aby sa dotknutej osobe zabezpečila účinná náhrada.“*[111] Samotné zapojenie sprostredkovateľa do spracúvania osobných údajov však nemusí automaticky znamenať, že v prípade brania na zodpovednosť, tento sprostredkovateľ bude z časti alebo plne zodpovedať za spôsobenú škodu.[112] Vznik škody môže byť pripísaný sprostredkovateľovi iba v prípadoch, ak jeho konanie pri spracúvaní osobných údajov viedlo ku vzniknutej škode na základe porušení ustanovení GDPR alebo toto konanie bolo v rozpore s pokynmi prevádzkovateľa prípadne sprostredkovateľskou zmluvou. Na strane druhej však GDPR neupravuje stupeň a rozsah zodpovednosti a z teoretického hľadiska umožňuje pripísanie celej škody sprostredkovateľovi.[113] Dotknutá osoba má prakticky možnosť vybrať si entitu, u ktorej si škodu bude uplatňovať v prípade, že do spracúvania osobných údajov bol zapojený okrem prevádzkovateľa aj sprostredkovateľ.[114] Navyše, prevádzkovateľ má možnosť regresu (kompenzácií) voči sprostredkovateľovi ak preukáže porušenie GDPR, pokynu prevádzkovateľa či sprostredkovateľskej zmluvy u tohto sprostredkovateľa.[115]

V otázkach typu odškodnenia a liberácie platia rovnaké závery ako pri prevádzkovateľoch.

---

[110] Článok 82 ods. 2, GDPR.

[111] Článok 82 ods. 4, GDPR.

[112] Pozri diskusiu ku prijatiu článku 82 GDPR v VAN ALSENOY, Brendan : Liability under EU Data Protection Law. *In 7 (2016) JIPITEC 271* s. 285.

[113] Tamže, poznámka pod čiarou č. 108.

[114] Článok 82 ods. 4, GDPR: *„Ak sa na tom istom spracúvaní zúčastnil viac než jeden prevádzkovateľ alebo sprostredkovateľ alebo prevádzkovateľ aj sprostredkovateľ spoločne a sú podľa odsekov 2 a 3 zodpovední za škodu spôsobenú spracúvaním, každý z nich zodpovedá za celú škodu, aby sa dotknutej osobe zabezpečila účinná náhrada.“*

[115] Článok 82 ods. 5, GDPR.

## 5.3 OSOBNÁ PÔSOBNOSŤ GDPR A AUTONÓMNE VOZIDLÁ

Autonómne vozidlá či systémy sú pomerne široko akademicky diskutovanou témou.[116] Snahy o reguláciu autonómnych systémov v podobe technológií na báze umelej inteligencie naberajú na dôležitosti aj v rámci legislatívnych plánov na úrovní EÚ.[117] Svoje usmernenie k danej problematike vydal aj EDPB, ktorý je vedúcou interpretačnou autoritou v oblasti ochrany osobných údajov na úrovní EÚ.

### 5.3.1 USMERNENIE EDPB

28. januára 2020 vydal EDPB usmernenie o spracúvaní osobných údajov v kontexte prepojených vozidiel a aplikácií súvisiacich s mobilitou (ďalej len „Usmernenie").[118] Ide o verziu pre verejnú konzultáciu, čo znamená, že verejnosť môže k Usmerneniu zasielať pripomienky, ktoré sa môžu premietnuť do finálneho znenia textu. Na ilustráciu komplexu právnych aspektov spracúvania osobných údajov v autonómnych vozidlách je však táto verzia postačujúca.

Štruktúra Usmernenie reflektuje konkrétne aplikačné problémy pri spracúvaní osobných údajov v prepojených vozidlách. Usmernenie sa neza-

---

[116] Napr. POLČÁK, Radim : ODPOVĚDNOST UMĚLÉ INTELIGENCE A INFORMAČNÍ ÚTVARY BEZ PRÁVNÍ OSOBNOSTI. In: http://www.bulletin-advokacie.cz/. [online]. Datum publikování: 30.11.2018. Datum aktualizace [26.3.2020]. Dostupné z:http://www.bulletin-advokacie.cz/odpovednost-umele-inteligence-a-informacni-utvary-bez-pravni-osobnosti; CARP, Jeremy: Autonomous Vehicles: Problems and Principles for Future Regulation. In *University of Pennsylvania Journal of Law & Public Affairs*, Vol. 4, No. 1, 2018; YEEFEN Lim(ed) : *Autonomous Vehicles and the Law: Technology, Algorithms and Ethics*. Edward Elgar Pub. 2018.

[117] Pozri COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Coordinated Plan on Artificial Intelligence; 6.EU High-Level Expert Group on AI Ethics guidelines for trustworthy AI [online]. 2019. [cit. 29. 9. 2020] Dostupné z: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai alebo European Commission: White Paper on Artificial Intelligence: a European approach to excellence and trust. Brussels, 19.2.2020. COM(2020) 65 final. [online]. 2020. [cit. 29. 9. 2020]. Dostupné z: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

[118] European Data Protection Board Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications. [Online]. 2020. [cit. 29. 9. 2020] Dostupné z: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-12020-processing-personal-data-context_en.

meriava výslovne na autonómne vozidlá, ale jeho pôsobnosť možno z časti aplikovať aj na klasické formy vozidiel, ktoré využívajú nové technológie a sú určitým spôsobom pripojené na sieť (*connected vehicles*). Množstvo záverov však bude relevantných práve v súvislosti s autonómnymi vozidlami. Po úvodnej časti a definovaní základných problémov v kontexte ochrany súkromia a osobných údajov nasledujú dve ťažiskové časti. Prvá z nich predstavuje všeobecné odporúčania týkajúce sa kategórií spracúvaných údajov, účelov, zásady minimalizácie údajov, inštitútu špecificky navrhnutej a štandardnej ochrany osobných údajov, plnení informačnej povinnosti, práv dotknutých osôb, prenosu údajov a použití wi-fi technológií.[119] Druhá obsahová časť obsahuje konkrétne prípadové štúdie a konkrétne odporúčania pri spracúvaní osobných údajov v daných situáciách.[120] Z hľadiska zamerania predkladaného príspevku považujeme za vhodné charakterizovať základné postuláty, na ktorých Usmernenie stojí vrátane typov osobných údajov a aplikácií v rámci prepojených vozidiel a základných aktérov ich prevádzkovania.

Usmernenie vo svojom úvode veľmi pragmaticky uvádza, že už aj tradičné vozidlá bez autonómnych systémov sa stávajú „dátovými hubmi.“[121] Na strane druhej, prepojené vozidlá a spracúvanie osobných údajov predstavujú komplexný ekosystém. Tento ekosystém pridáva ku tradičnému poňatiu a účelu automobilu viaceré prvky. Ilustrovať to možno na príkladoch prehrávania hudby podľa nálady vodiča, aktuálne informácie o dopravnej situácií a počasí, systémy asistencie pri vedení vozidla resp. autopilot, meranie výšky poistenia na základe používania automobilu. Ďalej je možné akcentovať možnosti prepojiť vozidlo s ďalšími externými zdrojmi prostredníctvom siete ako prevádzkovateľmi dopravného značenia alebo telekomunikačnými operátormi.[122] Z hľadiska vodiča automobilu je tak

[119] Usmernenie, s. 12 – 21.

[120] Usmernenie, s. 21 – 30.

[121] Usmernenie, s. 3.

[122] Tamže.

možné na základe získaných údajov kreovať profil jeho štýlu vedenia vozidla či vodičských návykov.[123]

Usmernenie sa výslovne venuje spracúvaniu geo-lokalizačných údajov,[124] biometrických údajov[125] a údaje týkajúce sa uznania viny za trestné činy a priestupky.[126] Prirodzene, tieto údaje nie sú jedinými typmi spracúvanými pri prevádzkovaní autonómneho vozidla, avšak vzhľadom na ich osobitosť (citlivosť)[127] EDPB pragmaticky charakterizuje detaily ich spracúvania. Množstvo údajov, ktoré autonómne vozidlo spracúva možno klasifikovať ako osobné údaje v zmysle GDPR, či už ide o priame identifikátory v podobe identity vodiča alebo pasažiera alebo identifikátory nepriame ako štýl vedenia vozidla, prejazdená vzdialenosť či technické údaje týkajúce sa vozidla.[128] Už z vyššie uvedeného výpočtu jednoznačne vyplýva, že v rámci vozidla sú spracúvané osobitné kategórie osobných údajov v zmysle článku 9 ods. 1 GDPR.[129] Z toho priamo vyplýva požiadavka, aby prevádzkovateľ vozidla disponoval niektorou z výnimiek v zmysle článku 9 ods. 2 GDPR pre spracúvanie osobitných kategórií osobných údajov. Nájdenie a aplikácia potenciálne použiteľnej výnimky môže naraziť na pomerne reštriktívne koncipované ustanovenia diskutovaného článku. Vždy bude záležať na konkrétnom účele spracúvania osobných údajov, ale na prvý pohľad sa ako použiteľné výnimky javia životne dôležitý záujem (článok 9 ods. 2 písm. c) GDPR) pri spracúvaní údajov o zdraví vozidla alebo pasažierov a monitorovaní ich životných funkcií a alternatívne výslovný súhlas (článok 9 ods. 2 písm. a) GDPR).

---

[123] Tamže, s. 4.

[124] Tamže, s. 12 - 13

[125] Tamže, s. 13.

[126] Tamže, s. 13 – 14.

[127] K tomu pozri článok 9 GDPR a článok 10 GDPR.

[128] Pozri viac Usmernenie, s. 7 – 8.

[129] Článok 9 ods. 1 GDPR definuje tieto údaje ako také, ktoré *„odhaľujú rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách, a spracúvanie genetických údajov, biometrických údajov na individuálnu identifikáciu fyzickej osoby, údajov týkajúcich sa zdravia alebo údajov týkajúcich sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby.“*

Z hľadiska rôznych aplikácií a využitia údajov v rámci prepojených vozidiel EDPB demonštratívne spomína šesť oblastí. Prvou je manažment mobility a teda využitie údajov na efektívne vykonanie konkrétnej trasy prostredníctvom údajov o stave vozovky, počasia, hustoty premávky či uzáver. Druhá oblasť je manažment samotného vozidla a spracúvanie údajov, ktorí indikujú vodičom servisný stav vozidla či dáta o používaní vozidla a jeho konkrétnych komponentov. Treťou oblasťou je bezpečnosť na cestách a to v podobe upozornení na externé riziká pri vedení vozidla či automatické volania pri nehodách alebo ukladanie dát v rámci „čiernych skriniek." Štvrtá oblasť predstavuje všetky funkcie určené na „zábavu" v podobe prepojenia mobilných telefónov alebo hot-spotov na účely volania, počúvania hudby, generovania správ či prepojenia na smart-home alebo internet. Piatu oblasť predstavuje spracúvanie údajov na účely plnej alebo čiastočnej asistencie pri vedení vozidla. Napokon, šiesta oblasť sa týka zdravia vodiča ako meranie únavy alebo potreba lekárskej starostlivosti.[130] Vzhľadom na presah jednotlivých oblastí do konkrétnych účelov spracúvania bude nevyhnutné k ich vymedzeniu vždy pristupovať pragmaticky, nakoľko viaceré oblasti budú presahovať do jedného alebo viacerých účelov spracúvania osobných údajov. V zmysle zásady obmedzenia účelu podľa článku 5 ods. 1 písm. b) GDPR sa zdá ako najdôležitejšie precízne upraviť účel týkajúci sa samotného fungovania vozidla a subsumovanie relevantných spracovateľských operácií pod neho. Podľa nášho názoru nemožno všetky uvedené oblasti fungovania vozidla považovať za „nevyhnutné" a aj z hľadiska vymedzenia právneho základu bude preto nevyhnutné medzi rôznymi oblasťami a účelmi rozlišovať.

Už vyššie uvedených typov aplikácií a potenciálne spracúvaných údajov je možné zhrnúť, že pri prevádzke prepojeného vozidla sa k údajom môže dostať potenciálne pomerne veľké množstvo rôznych subjektov od tradičných výrobcov vozidiel až po firmy pôsobiace v digitálnom priemysle. EDPB demonštratívne vymenúva výrobcov vozidiel, výrobcov jednotlivých zariadení, komponentov a ich dodávateľov, autoservisy, predajne automobilov, spoločnosti zaoberajúce sa prenájmom a zdieľaním automobilov,

[130] Usmernenie, s. 7.

správcov vozového parku, poisťovne motorových vozidiel, poskytovateľov zábavy, telekomunikačných operátorov, správcov cestnej infraštruktúry a orgány verejnej moci, ako aj vodičov, majiteľov vozidiel, nájomcov vozidiel či pasažierov.[131] Prakticky sa tvorí pomerne robustný ekosystém entít s prístupom k osobným údajom z jedného vozidla. Tieto otázky sú z hľadiska spracúvania osobných údajov nesmierne dôležité, nakoľko determinujú rozdelenie zodpovednosti za súlad s GDPR a taktiež zodpovednosť za potenciálne porušenie regulácie ochrany osobných údajov.

Z hľadiska konkrétnych aktérov spracúvania osobných údajov EDPB exemplifikatívne určila postavenie v zmysle osobnej pôsobnosti GDPR, avšak prirodzene predmetné postavenie je potrebné vždy posudzovať v konkrétnej situácií a v špecifickom kontexte. Typickými dotknutými osobami by mali byť vodiči, pasažieri a majitelia vozidiel. Prevádzkovateľmi v súvislosti s spracúvaním osobných údajov v prepojených vozidlách môžu byť prevádzkovatelia služieb, ktorí spracúvajú údaje o vozidle za účelom poskytnutia rôznych informácií vodičovi (napr. najkratšia cesta do destinácie, dopravná situácia, servisné upozornenia). Ďalším prevádzkovateľom môže byť poisťovňa, u ktorej je vozidlo poistené či výrobca vozidla, ktoré využíva údaje na vylepšenie komponentov tvoriacich vozidlo. Sprostredkovateľmi môžu byť výrobcovia jednotlivých komponentov, ktorí údaje spracúvajú v mene výrobcov vozidiel. Ako typy príjemcov Usmernenie vymenúva obchodných partnerov poskytovateľov služieb uvedených vyššie, ktorí spracúvajú údaje generované vozidlom.[132] Pri poskytovateľoch externých služieb (ako napr. poisťovní alebo iných) EDPB zvýrazňuje, že jediným príjemcom osobných údajov by mali byť samotný prevádzkovatelia týchto služieb.[133] Totožný záver platí aj pri prenajímateľoch vozidiel a správcov parkovacích miest.[134] V prípade poskytovateľov zdravotnej starostlivosti v urgentných situáciách (tzv. účel 112) by tieto údaje taktiež ne-

[131] Tamže, s. 8.

[132] Tamže, s. 9

[133] Tamže, s. 24.

[134] Tamže.

mali spracúvať a byť prenesené iným subjektom.[135] Pri výskumných účeloch v zmysle článku 89 GDPR (napr. pri výskume nehodovosti) by príjemcom nemal byť žiadny iný subjekt s výnimkou prevádzkovateľa a sprostredkovateľa.[136]

EDPB výslovne spomína aj orgány verejnej moci a tretie strany, ktoré si údaje môžu vyžiadať pri plnení svojich úloh na základe zákonných zmocnení (napr. orgány činné v trestnom konaní prípadne v rámci priestupkového konania).[137]

Možno konštatovať, že diskutované Usmernenie sa konkrétnym aktérom nevenuje veľmi detailne a ponecháva priestor pre aplikačnú prax na vysporiadanie sa s touto otázkou.

### 5.3.2 APLIKAČNÉ PROBLÉMY (MODELOVÉ SITUÁCIE)

V úvodnej časti predkladaného článku boli definované tri rozmery komunikácie, ktoré sa týkajú autonómneho - prepojeného vozidla. V rámci tejto časti článku poskytneme naše úvahy v kontexte týchto modalít toku dát z hľadiska určenia zodpovednej entity v oblasti ochrany osobných údajov.

Prvou situáciou je pripojenie vozidla na internet, v rámci ktorého využíva rôzne služby (V2I – *Vehicle to Internet*). V tomto postavení je možné analyzovať dve modelové podstaty a to (i) pripojenie ku službe, ktorá je nevyhnutná na fungovanie autonómneho vozidla napr. ku GPS navádzaciemu satelitu a (ii) pripojenie ku aplikáciám, poskytujúcim užívateľom zábavné služby ako napríklad Spotify alebo Netflix. Pri prvej modelovej podstate (služba nevyhnutná na fungovanie autonómneho vozidla) pôjde pravdepodobne o vzťah dotknutá osoba (majiteľ alebo vodič vozidla) a prevádzkovateľ (prevádzkovateľ vozidla). Zaujímavý je však vzťah medzi prevádzkovateľom vozidla a poskytovateľom nevyhnutnej služby. Pri diskusií o tomto vzťahu pred niekoľkým rokmi by sa väčšina komentárov pravdepodobne priklonila ku vzťahu prevádzkovateľ – sprostredkovateľ, nakoľko poskytovateľ nevyhnutnej služby pre fungovanie vozidla by spracúval

[135] Tamže, s. 27.

[136] Tamže, s. 29.

[137] Tamže, s. 9.

osobné údaje v mene prevádzkovateľa vozidla. Tieto závery je však potrebné revidovať vo vzťahu ku rozhodnutia SDEÚ vo veciach *Wirtschaftsakademia* a *Fashion ID*. V spomínanej dvojici prípadov Luxemburský súd zvýraznil princíp plnej a efektívnej ochrany dotknutých osôb a analýzu spracovateľských operácií v mikroskopickom meradle.[138] Ak by sme sa teda v praxi mikroskopicky pozreli na spracovateľské operácie medzi vozidlom a poskytovateľom služby nevyhnutnej na fungovanie vozidla, v niektorých prípadoch môže ísť o spoločných prevádzkovateľoch v zmysle článku 26 GDPR, nakoľko do určitej miery vymedzujú účely a prostriedky spracúvania spoločne. Dopĺňame, že na aplikáciu inštitútu spoločných prevádzkovateľov nie je nevyhnutné výslovné spoločné určenie účelov alebo prostriedkov spracúvania, ale stačí, ak ide o dopĺňajúce (zbiehajúce – *converging decisions*) sa rozhodnutia v rámci spracúvania osobných údajov, ktoré majú hmatateľný vplyv.[139] Nie je preto vylúčené, že v prípade navádzania prepojeného vozidla poskytovateľom nevyhnutnej služby by došlo k naplneniu požiadavky zbiehajúcich sa rozhodnutí na určení účelov a prostriedkov spracúvania a aplikácií inštitútu spoločných prevádzkovateľov. Zodpovednosť by v danom prípade mala byť určená v konkrétnych prípadoch a za konkrétnych okolností.

Druhou modelovou podstatou je pripojenie ku službám, ktoré poskytujú v rámci vozidla zábavu. Sme toho názoru, že v takomto prípade ide o vzťah dotknutá osoba a prevádzkovateľ, pričom prevádzkovateľ autonómneho vozidla by nemal mať *stricto sensu* prístup k údajom získaným poskytovateľom zábavných služieb, nakoľko to nie je nevyhnutné pre fungovanie prepojeného vozidla.

Druhou situáciu je komunikácie vozidiel navzájom (V2V – *Vehicle to Vehicle*), za účelom vedenia vozidla a prevencie proti dopravným nehodám. Sme toho názoru, že v takomto prípade by sa malo pristúpiť ku dôslednej

[138] Rozsudok Súdneho dvora Európkej únie zo dňa 5. júna 2018 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein proti Wirtschaftsakademie Schleswig-Holstein GmbH. Vec č. C-210/16. Bod 43.

[139] European Data Protection Board Guidelines 07/2020 on the concepts of controller and processor in the GDPR. [Online]. 2020. [cit. 29. 9. 2020]. Dostupné z:https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en. S. 18.

anonymizácií údajov,[140] pričom kvalita dát v tomto nastavení by mala byť zameraná na iné ako osobné údaje (*non-personal data*) týkajúce sa vzdialenosti medzi vozidlami alebo inými technickými údajmi. Pri týchto údajoch by mala byť minimalizovaná možnosť spojenia údajov s konkrétnou dotknutou osobu. Predmetný prístup by prakticky znamenal „únik" z režimu GDPR a bol by v súlade s inštitútom špecificky navrhnutej a štandardnej ochrany údajov v zmysle článku 25 GDPR.[141]

Treťou situáciou je prepojenie vozidla s inými zariadeniami v rámci internetu vecí (V2IoT – *Vehicle to Internet of Things*). V tomto kontexte opätovne vidíme dve modality prepojenia a to medzi vozidlom a (i) inteligentnou cestnou infraštruktúrou a (ii) použitie týchto údajov v konaní o deliktoch orgánmi verejnej moci. Prvou modalitou je spracúvanie údajov vozidla a inteligentnej cestnej infraštruktúry v rámci tzv. kooperatívneho cestného systému (*cooperative – intelligent transportation system*), kde je zmyslom kooperácie prevádzkovateľa vozidla a cestnej infraštruktúry zamedzenie nehodovosti a dodržiavanie regulácie cestnej premávky. V tomto systéme nie je vylúčená ani komunikácia medzi prepojenými vozidlami navzájom.[142] Pri diskusií týkajúce sa pripojenia na inteligentnú cestnú infraštruktúru opätovne vzniká otázka postavenia a zodpovednosti v zmysle GDPR. Pôjde o spoločných prevádzkovateľov osobných údajov alebo samostatných prevádzkovateľov? Podľa nášho názoru je znova možné, že vo svetle nedávnej judikatúry SDEÚ bude musieť prax tento vzťah posudzovať ako spoločných prevádzkovateľov. Tento záver opierame o dva argumenty. Prvým argumentom je, že obaja prevádzkovatelia majú spoločný účel, ktorým je bezporuchový chod cestnej premávky. Tento účel je základnou úlo-

[140] Pozri viac Article 29 Data Protection Working Party: Opinion 05/2014 on Anonymisation Techniques. [online]. 2014. [cit. 29. 9. 2020]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

[141] Viac v European Data Protection Board: Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. [online]. 2020. [cit. 29. 9. 2020]. Dostupné z:https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en.

[142] Pozri vynikajúcu analýzu z pohľadu príčinnej súvislosti spôsobenej škody v ŽOLNERČÍKOVÁ, Veronika. Prokazování příčinné souvislosti u škod způsobených propojenými autonomními vozidly. *Revue pro právo a technologie*. [Online]. 2020, č. 21, s. 129-152. [cit. 2020-09-29]. Dostupné z: https://journals.muni.cz/revue/article/view/13048.

hou prevádzkovateľa inteligentnej infraštruktúry (štát alebo samospráva) a ekonomicky nevyhnutným pre prevádzkovateľa autonómneho vozidla, nakoľko bez rešpektovania diskutovaného aspektu je prakticky nemožné uviesť vozidlo na trh a používať ho. Zároveň prevádzkovatelia využívajú prepojenú infraštruktúru, ktorá navzájom komunikuje. Opätovne tak teda môže ísť o zbiehajúce sa rozhodnutia (*converging decisions*) o účeloch a prostriedkoch spracúvania osobných údajov. Druhým argumentom v prospech predmetnej klasifikácie je samotné rozhodnutie SDEÚ vo veci *Wirtschaftsakademie*. V tomto prípade išlo o to, že správca fanúšikovskej stránky na sociálnej sieti zasadil svoje aktivity do určitých mantinelov (napríklad v podobe špecifikácie cielenia reklamy alebo tvorby štatistík), ktoré mu vytvorila sociálna sieť, z čoho následne profitovali obe entity. Analogicky môže nastať podobná situácia, ak prevádzkovateľ autonómneho vozidla „zasadí“ svoje vozidlo do inteligentnej cestnej infraštruktúry.

Toto riešenie nie je z nášho pohľadu ideálne, nakoľko by vyžadovalo komplexnú revíziu vzťahov medzi prevádzkovateľmi vozidiel a prevádzkovateľmi infraštruktúry v zmysle požiadaviek článku 26 GDPR. Nemožno ale v tejto chvíli precízne prejudikovať, ako sa nastavením pôsobnosti a zodpovednosti v oblasti ochrany osobných údajov v danom nastavení vysporiada prax a judikatúra.

Druhou modalitou je využívanie údajov orgánmi verejnej moci na účely vedenia správnych alebo trestných konaní. V tomto smere figurujú orgány verejnej moci ako príjemcovia a následne v rámci konania samostatní prevádzkovatelia. V tejto súvislosti možno odkázať na nemeckú právnu úpravu, ktorá výslovne reguluje prístup a využitie údajov z tzv. čiernych skriniek autonómnych vozidiel.[143]

[143] § 63a English Translation of the German Road Traffic Act Amendment Regulating the Use of “Motor Vehicles with Highly or Fully Automated Driving Function” from July 17, 2017. CZARNECKI, Krzysztof. English Translation of the German Road Traffic Act Amendment Regulating the Use of “Motor Vehicles with Highly or Fully Automated Driving Function” from July 17, 2017. [Online]. [cit. 2020-09-29]. Dostupné z: https://www.researchgate.net/publication/320813344.

## 6. ZÁVER

Autonómne vozidlá pre maximálne využitie svojho potenciálu zbierajú, spracúvajú a zdieľajú častokrát aj osobné údaje s externými entitami. Legislatíva na úrovni práva EÚ umožňuje za určitých podmienok schválenie vozidiel s autonómnymi alebo automatizovanými systémami a čiastočne upravuje problematiku ochrany osobných údajov a kybernetickej bezpečnosti. Nariadenie o typovom schválení a najmä k nemu vydané usmernenie týkajúce sa výnimiek na schválenie automatizovaných vozidiel obsahuje usmernenia o inštalovaní nahrávacieho zariadenia, tak aby boli dodržané právne predpisy EÚ o ochrane údajov a boli chránené konkrétne informácie pred manipuláciou. Z pohľadu infraštruktúry, s ktorou môžu autonómne vozidlá komunikovať je legislatíva EÚ dosť špecifiká. V zmysle smernice o inteligentných dopravných systémoch a najmä delegovaného nariadenia musia prevádzkovatelia staníc kooperatívnych inteligentných dopravných systémov prevádzkovať systém riadenia informačnej bezpečnosti a taktiež by sa mali uplatniť bezpečnostné požiadavky na pseudonymizáciu údajov. Taktiež platí, že osobné údaje by sa mali spracúvať za prísneho dodržiavania zásady minimalizácie údajov, len na účely špecifikované v delegovanom nariadení. Legislatívne akty EÚ upravujúce problematiku kybernetickej bezpečnosti môžu zabezpečiť dostatočnú úroveň kybernetickej bezpečnosti budúcich technológií, ktoré sa budú používať v autonómnych vozidlách, a to najmä prostredníctvom systému certifikácie IKT produktov, postupov a služieb v EÚ, resp. prostredníctvom plnenia bezpečnostných opatrení v zmysle smernice NIS ak výrobcovia vozidiel alebo dodávatelia systémov budú v pozícii prevádzkovateľov základných služieb.

Z hľadiska postavenia rôznych aktérov spracúvania osobných údajov v autonómnom vozidle sme v prvom rade diskutovali súčasnú interpretáciu pojmov prevádzkovateľ, sprostredkovateľ a ich zodpovednosti v zmysle nedávnej judikatúry SDEÚ. Na základe vymedzenia a analýzy troch modelových situácií sme poukázali na to, že vo viacerých prípadoch spracúvania osobných údajov v rámci prepojeného autonómneho vozidla bude určenie zodpovednej entity nesmierne náročné a to vzhľadom na funkčný a pomerne široký výklad pojmu spoločných prevádzkovateľov z hľadiska

možnosti zbiehajúcich rozhodnutí o účeloch a prostriedkoch spracúvania v rámci diskutovaných vozidiel. Mikroskopický pohľad na spracovateľské operácie optikou SDEÚ nie je najvhodnejším riešením pri vymedzení daných vzťahov v súvislosti s prepojenými vozidlami. Je preto možné, že v budúcnosti dôjde ku veľmi komplikovaným právnym situáciám s nie jednoduchými a pozitívnymi praktickými dôsledkami z hľadiska spracúvania osobných údajov.

## 7. ZOZNAM LITERATÚRY

[1] MATTESON, S. *Autonomous versus automated: What each means and why it matters*. [online]. Dostupné z: https://www.techrepublic.com/article/autonomous-versus-automated-what-each-means-and-why-it-matters/ [citované 28.9.2020].

[2] TAEIHAGH, A. a SI MIN LIM, H. *Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks.* Transport Reviews, roč. 39. č. 1, 2019, s. 103-128.

[3] POLČÁK, R. *Odpovědnost umělé inteligence a informační útvary bez právní osobnosti.* In Bulletin Advokace 11/2018, s. 24. [on-line]. Dostupné z: http://www.bulletin-advokacie.cz/assets/zdroje/casopis/2018/BA_11_2018_web.pdf. [citované 28.9.2020].

[4] COLLINGWOOD, L. *Privacy implications and liability issues of autonomous vehicles*. In Information & Communications Technology Law, roč. 26. č. 1, 2017, s. 32-45.

[5] KOUROUTAKIS, A. E. *Autonomous Vehicles; Regulatory Challenges and the Response From UK and Germany*. 46 Mitchell Hamline Law Review forthcoming. 2019.

[6] YEEFEN LIM, H. *Autonomous Vehicles and the Law Technology, Algorithms and Ethics.* Edward Elgar Publishing, 2018, 147 s.

[7] SKEETE, JP. Level 5 autonomy: *The new face of disruption in road transport.* In Technological Forecasting and Social Change, Elsevier, roč. 134(C), 2018, s. 22-34.

[8] VOSTOUPAL, J.: *Certifikace kyberbezpečnostních technologií. In* Revue pro právo a technologie. 2019, č. 20, s. 147-268. [on-line]. Dostupné z: https://journals.muni.cz/revue/article/view/12570 [citované 28.9.2020].

[9] CZARNECKI, K. *English Translation of the German Road Traffic Act Amendment Regulating the Use of "Motor Vehicles with Highly or Fully Automated Driving Function" from July 17, 2017* [on-line]. Dostupné z: https://www.researchgate.net/profile/Krzysztof_Czarnecki3/publication/320813344_English_Translation_of_the_German_Road_Traffic_Act_Amendment_Regulating_the_Use_of_Motor_Vehicles_with_Highly_or_Fully_Automated_Driving_Function_from_July_17_2017/links/59fbbe680f7e9b9968bb5a0f/English-Translation-of-the-German-Road-Traffic-Act-Amendment-Regulating-the-Use-of-Motor-Vehicles-with-Highly-or-Fully-Automated-Driving-Function-from-July-17-2017.pdf

[10] International Transport Forum and Corporate Partnership Board: *Autonomous Driving: Regulatory Issues*. 2015. [on-line]. Dostupné z: https://www.itf-oecd.org/sites/default/files/docs/15cpb_autonomousdriving.pdf. [citované 28.9.2020].POLČÁK, R. *Informace a data v právu*. Revue pro právo a technologie 7, 2016, s. 67–91.

[11] Autonomous Vehicles. State of Nevada Register of Administrative Regulations. § 82A. [on-line]. Dostupné z: https://www.leg.state.nv.us/NRS/NRS-482A.html#NRS482ASec036. [citované 28.9.2020].

[12] Nariadene 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] Usmernenia týkajúce sa výnimky na schválenie automatizovaných vozidiel EÚ.

[14] Smernica Európskeho parlamentu a Rady 2010/40/EÚ o rámci na zavedenie inteligentných dopravných systémov v oblasti cestnej dopravy a na rozhrania s inými druhmi dopravy.

[15] Delegované nariadenie komisie ktorým sa dopĺňa smernica o inteligentných dopravných systémoch, pokiaľ ide o zavádzanie a prevádzkové využívanie kooperatívnych inteligentných dopravných systémov

[16] Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii

[17] Nariadenie Európskeho parlamentu a Rady o Agentúre EÚ pre kybernetickú bezpečnosť (ENISA), o zrušení nariadenia (EÚ) č. 526/2013 a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií

[18] SAE J3016:Sep 2016: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles

[19] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov). In EUR-lex [právní informační system]. Úřad pro publikace Evropské unie. Dostupné z https://eur-lex.europa.eu/legal-content/SK/TXT/?qid=1584526623550&uri=CELEX%3A32016R0679

[20] TRAKMAN, Leon – WALTERS, Robert – ZELLER, Bruno: Tort and Data Protection Law: Are There Any Lessons to Be Learnt? *In European Data Protection Law Review 4/2019*.

[21] CORDEIRO, A.B. Menezes: Civil Liability for Processing of Personal Data in the GDPR *In European Data Protection Law Review 4/2019.*

[22] VAN ALSENOY, Brendan – DUMORTIER, Jos: The accountability principle in data protection regulation: origin, development and future directions. *In GUAGNIN,*

[23] *D. – HEMPEL, L. - ILTEN, C. (eds): Managing Privacy Through Accountability*. 2012, Palgrave Macmillian, s. 49 – 82.

[24] VAN ALSENOY, Brendan: Liability under EU Data Protection Law. *In 7 (2016) JIPITEC 271*.

[25] LAROUCHE, Pierre – PEITZ, Martin – PURTOVA, Nadya: *Consumer Privacy in network industries* – A CERRE Policy Report, 2016, Centre on Regulation in Europe. [Online] 2016. [cit. 29. 9. 2020]. Dostupné z: https://cerre.eu/wp-content/uploads/2016/01/160125_CERRE_Privacy_Final.pdf.

[26] Smernica 2000/31/ES Európskeho parlamentu a Rady z 8. júna 2000 o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu, najmä o elektronickom obchode (smernica o elektronickom obchode). In EUR-lex [právní informační system]. Úřad pro publikace Evropské unie. Dostupné z https://eur-lex.europa.eu/legal-content/AUTO/?uri=CELEX:32000L0031&qid=1585224374231&rid=1.

[27] CUNHA, A. Maria Viola – MARIN, Luisa – SARTOR, Giovanni: Peer-to-peer privacy violations and ISP liability: data protection in the user-generated web. *In International Data Privacy Law,* Volume 2, Issue 2, 2012.

[28] Rozsudok Súdneho dvora zo dňa 13. mája 2014 Google Spain SL a Google Inc. proti Agencia Española de Protección de Datos (AEPD) a Mariovi Costejovi Gonzálezovi. Vec č. C-131/12.

[29] MAHIEU, René – HOBOKEN VAN, Joris - ASGHARI, Hadi: Responsibility for Data Protection in a Networked World. On the question of the Controller. „Effective and Complete Protection" and its Application to Data Access Rights in Europe. *In JIPITEC 39, 10 (2019*).

[30] Rozsudok Súdneho dvora Európskej únie zo dňa 29. júla 2019 Fashion ID GmbH & Co.KG proti Verbraucherzentrale NRW eV. Vec č. C-40/17.

[31] European Data Protection Board Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications. [Online]. 2020. [cit. 29. 9. 2020] Dostupné z: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-12020-processing-personal-data-context_en.

[32] Rozsudok Súdneho dvora Európkej únie zo dňa 5. júna 2018 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein proti Wirtschaftsakademie Schleswig-Holstein GmbH. Vec č. C-210/16.

[33] European Data Protection Board Guidelines 07/2020 on the concepts of controller and processor in the GDPR. [Online]. 2020. [cit. 29. 9. 2020]. Dostupné z: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en.

[34] Article 29 Data Protection Working Party: Opinion 05/2014 on Anonymisation Techniques. [online]. 2014. [cit. 29. 9. 2020]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

[35] European Data Protection Board: Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. [online]. 2020. [cit. 29. 9. 2020]. Dostupné z: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en.

[36] ŽOLNERČÍKOVÁ, Veronika. Prokazování příčinné souvislosti u škod způsobených propojenými autonomními vozidly. *Revue pro právo a technologie*. [Online]. 2020, č. 21, s. 129-152. [cit. 2020-09-29]. Dostupné z: https://journals.muni.cz/revue/article/view/13048.

[37] CZARNECKI, Krzysztof. English Translation of the German Road Traffic Act Amendment Regulating the Use of "Motor Vehicles with Highly or Fully Automated Driving Function" from July 17, 2017. [Online]. [cit. 2020-09-29]. Dostupné z: https://www.researchgate.net/publication/320813344.

---



---