https://doi.org/10.5817/RPT2021-2-1

OCHRANA OSOBNÍCH ÚDAJŮ V SYSTÉMECH AUTONOMNÍHO ŘÍZENÍ. CO JE NEZBYTNÉ PRO BEZPEČNÉ FUNGOVÁNÍ A JAK TOHO DOSÁHNOUT?[1]

ZDENĚK LOKAJ, MARTIN ŠROTÝŘ, MARTIN FLAŠKÁR, JAKUB JIROVSKÝ[2]

ABSTRAKT

Autoři se zabývají problematikou ochrany osobních údajů v systémech autonomního řízení představujících celé ekosystémy dílčích vzájemně komunikujících prvků a různorodých spolupracujících entit. Při provozu těchto systémů dochází k přenosu a zpracování obrovského množství dat, mezi kterými lze nalézt i řadu významných osobních údajů, které lze zpracovávat pouze v souladu s právními předpisy. V první části článku jsou tak obecně popsány systémy autonomního řízení, specifikace jejich prvků a představení klíčových hráčů, kteří se podílejí na vytváření nebo dalším zpracování těchto dat. Dále jsou rozpracovány jednotlivé kategorie osobních údajů, se kterými budou předmětné systémy autonomního

[1] Tento článek je zpracován jako výstup projektu TL03000691 s názvem „*Ochrana soukromí a osobních údajů v systémech autonomního řízení*“ v rámci Programu na podporu aplikovaného společenskovědního a humanitního výzkumu, experimentálního vývoje a inovací – ÉTA Technologické agentury České republiky.

[2] Doc. Ing. Zdeněk Lokaj, Ph.D., výzkumný pracovník Ústavu aplikované informatiky v dopravě Fakulty dopravní ČVUT v Praze, kontaktní e-mail: lokaj@fd.cvut.cz; Ing. Martin Šrotýř, Ph.D., výzkumný pracovník Ústavu aplikované informatiky v dopravě Fakulty dopravní ČVUT v Praze, kontaktní e-mail: srotyr@fd.cvut.cz; JUDr. Martin Flaškár, advokát trvale spolupracující s advokátní kancelář ROWAN LEGAL, advokátní kancelář s.r.o.; kontaktní e-mail: flaskar@rowan.legal; Mgr. Jakub Jirovský, advokát trvale spolupracující s advokátní kancelář ROWAN LEGAL, advokátní kancelář s.r.o., kontaktní e-mail: jirovsky@rowan.legal.

řízení pracovat nebo v nichž se budou nalézat. Stěžejní částí je pak návrh řešení přístupu k ochraně osobních údajů napříč celým ekosystémem s využitím principů privacy by design a privacy by default. V neposlední řadě se autoři zabývají dílčími právními oblastmi jako je kybernetická bezpečnost a ochrana soukromí v elektronických komunikacích, které v souvislosti s problematikou autonomního řízení nemohou být opomenuty.

KLÍČOVÁ SLOVA

Autonomní systémy; autonomní řízení; autonomní mobilita; samořiditelná vozidla; osobní údaje; ochrana soukromí; privacy by design; privacy by default; umělá inteligence; kybernetická bezpečnost

ABSTRACT

Authors address the issue of personal data protection in autonomous driving systems representing entire ecosystems of partial interacting elements and diverse cooperating entities. The operation of such systems involves the transmission and processing of a huge amount of data, among which can be found a number of important personal data that can only be processed in accordance with legal regulations. The first part of this paper therefore provides a general description of autonomous driving systems, a specification of their elements and an introduction to the key players involved in the generation or further processing of this data. Furthermore, the different categories of personal data with which the autonomous driving systems in question will operate or in which they will be found are elaborated. The central part is then a proposed solution for approaching data protection across the entire ecosystem using the principles of privacy by design and privacy by default. Finally, authors address specific legal areas such as cybersecurity and privacy in electronic communications, which cannot be ignored in the context of autonomous driving.

KEYWORDS

Autonomous Systems; Autonomous Driving; Autonomous Mobility; Self-driving Vehicles; Personal Data; Privacy by Design; Privacy by Default; Artificial Intelligence, Cybersecurity

1. ÚVOD

Autonomní mobilita je fenoménem dnešní doby. Všechny velké automobilky i výzkumné instituce se věnují výzkumu a vývoji komponent, které budou v samořiditelných vozidlech využitelné. Tomuto oboru se předpovídá obrovská budoucnost a rychlý rozvoj. I proto je nutné se kromě technického vývoje a zdokonalování algoritmů umělé inteligence detailně věnovat aspektům ochrany osobních údajů a ochrany soukromí v systémech autonomního řízení. Právě garance, že je s osobními údaji nakládáno právně konformním způsobem a nemůže dojít k jejich zneužití či úniku, bude jedním ze zásadních prvků akceptace moderních vozidel jejich uživateli a tím pádem i parametrem rychlosti jejich rozvoje.

Tento příspěvek je proto zaměřen v prvé řadě na identifikaci klíčových hráčů a datových toků mezi nimi při provozování samostatných, ale přesto vzájemně propojených systémů autonomního řízení vozidel, a to včetně těch systémů, které vykazují pouze nižší stupně takové autonomie. Následně je věnována pozornost principům *privacy by design* a *privacy by default*, které by měly sloužit jako základní stavební kámen při vývoji těchto systémů z hlediska zajištění řádné ochrany osobních údajů. Na závěr jsou pak shrnuty i přesahy do dalších oblastí, které s datovými toky v rámci autonomních systémů dopravy nepochybně souvisejí, jako je kybernetická bezpečnost a ochrana soukromí v elektronických komunikacích, nicméně nejsou hlavním těžištěm tohoto článku.

Oproti ostatním článkům,[3] vydaným v recenzovaných periodikách v České republice, má tento příspěvek za cíl zaměřit se zejména na samotné výrobce jednotlivých prvků v rámci automobilového průmyslu s cílem jim napomoci při postupném přechodu jejich výroby na prvky a zařízení pro systémy autonomního řízení a při způsobu aplikace ochrany soukromí v těchto systémech.

[3] ANDRAŠKO, Jozef a MESARČÍK, Matúš. *Čo vieš o mojom vozidle? Ochrana osobných údajov a kybernetická bezpečnosť v kontexte autonómnych vozidiel*. Revue pro právo a technologie. [Online]. 2020, č. 22, s. 3-50. [cit. 2021-11-19]. Dostupné z: https://journals.muni.cz/revue/article/view/13841.

2. AUTONOMNÍ MOBILITA A JEJÍ KLÍČOVÍ HRÁČI Z POHLEDU OSOBNÍCH ÚDAJŮ

Autonomní řízení, autonomní mobilita vozidel nebo samořiditelná vozidla jsou mezi laickou i odbornou veřejností obecná označení pro chování automobilů, které vykazují jisté prvky samostatného rozhodování, tj. samostatného řešení situací, ke kterým dochází v provozu na pozemních komunikacích. V tomto směru lze protnout jejich obecné vnímání s definicí autonomních systémů, které Watson a Scheidt označují jako *„systémy, které mohou změnit své chování v reakci na neočekávané události během jejich provozu“*.[4] Tato změna chování, resp. samostatné rozhodování samozřejmě může zahrnovat širokou škálu činností od pouhých asistenčních funkcí vozidla, které pomáhají řidiči v krizových situacích, až po zcela samostatné zajištění přepravy z místa A do místa B bez jakéhokoliv zásahu řidiče.

Právě výše zmíněná široká škála činností, které jsou nebo mohou být pod pojem autonomního řízení obecně zařazovány, byla jedním z důvodů, který vedl asociaci automobilového průmyslu SAE International v roce 2014 k tomu, že ve spolupráci s americkou organizací National Highway Traffic Safety Administration (NHTSA) definovala pět, resp. šest úrovní systémů autonomního řízení podle jejich technické vyspělosti a míry závislosti na lidském činiteli. Tato definice je součástí standardu SAE International J3016,[5] který byl od roku 2014 několikrát aktualizován (naposledy v dubnu 2021). Tento standard je uznáván i Evropskou radou pro výzkum silniční dopravy (ERTRAC).[6]

Stupeň nula označovaný jako *„No Driving Automation“* podle tohoto standardu SAE zahrnuje systémy, které řidiče jen varují, ale do řízení vozidla

[4] WATSON, David P.; SCHEIDT, David H. Autonomous systems. Johns Hopkins APL technical digest. [online]. 2005, 26.4: 368-376. [cit. 2021-11-12]. Dostupné z: https://www.jhuapl.edu/Content/techdigest/pdf/V26-N04/26-04-Watson.pdf.

[5] Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles J3016_202104 [online]. *SAE International* [cit. 2021-08-03]. Dostupné z: https://www.sae.org/standards/content/j3016_202104/.

[6] Connected Automated Driving Roadmap [online]. *ERTRAC* [cit. 2021-08-03]. Dostupné z: https://www.ertrac.org/uploads/images/ERTRAC2019-Connected-Automated-Driving-Roadmap%20-2019-04-04.pdf.

nezasahují. Stupeň jedna s názvem *„Driver Assistance“* pomáhá řidiči s ovládáním směru nebo rychlosti vozidla (např. adaptivní tempomat). Ve druhém stupni, *„Partial Driving Automation“*, je vozidlo schopno samo v některých specifických situacích převzít řízení, ale člověk musí být vždy připraven okamžitě zasáhnout (např. automatické parkování). Na třetí úrovni, *„Conditional Driving Automation“*, přebírá řízení v běžném provozu vozidlo, přičemž samo upozorní řidiče na potřebu jeho zásahu. Ve čtvrté úrovni označované jako *„High Driving Automation“* vozidlo řídí až na mimořádné situace samo, a i v těchto situacích je schopno bezpečně zareagovat, pokud řidič nepřevezme řízení ani po upozornění. *„Full Driving Automation“* je označení pro nejvyšší pátou úroveň v rámci které již člověk není potřeba pro řízení vůbec a vozidlo je samo schopno vyřešit všechny dopravní situace, a to včetně těch nepředvídatelných, a dopravit přepravované osoby z místa A do místa B.

Systémy autonomního řízení jsou založeny na fungování různých technických prostředků snímajících vlastní okolí a rovněž s tímto okolím komunikujících. Čím vyšší je stupeň autonomie vozidla, tím více dat a informací je vyžadováno pro jeho bezpečný provoz, a tím pádem bude takové vozidlo i disponovat větším množstvím technologií. Díky senzorům, čidlům a detektorům si autonomní vozidla utvářejí obraz o aktuální situaci ve svém okolí, následně jejich řídicí systém, případně i za pomoci dalších systémů, vyhodnocuje získané informace a reaguje na vzniklé podněty změnami v řízení.

Informace, na jejichž základě se autonomní vozidlo rozhoduje, však nemusejí pocházet pouze ze senzorů, kterými je vybaveno samo autonomní vozidlo. Vozidla totiž mohou zpracovávat i informace z vnějších zdrojů, ať se jedná o jiná vozidla nebo dopravní infrastrukturu. To vše primárně s cílem zajistit maximální bezpečnost provozu prostřednictvím sítě mezi sebou vzájemně komunikujících prvků, které si vyměňují relevantní informace. Abychom si tyto informační toky více přiblížili, budeme se dále věnovat tomu, jakými směry je taková komunikace vedena, a dále tomu, jaké informace jsou jejím obsahem.

Komunikace v rámci systémů autonomního řízení je tak dle francouzského CNIL[7] realizována jako:

a) Komunikace IN-IN.[8] Jde o komunikaci, která je využívaná v rámci mezi sebou vzájemně komunikujícími komponenty a aplikacemi v rámci jednoho vozidla. V tomto případě tak nedochází k jakémukoliv odesílání dat mimo vozidlo. Příkladem takovýchto aplikací je například „eco-driving“, kdy jízdní data zůstávají ve vozidle, vozidlo je samo vyhodnotí a následně řidiči poskytne zpětnou vazbu ve formě doporučení pro dosažení ekologické jízdy.

b) Komunikace IN-OUT.[9] V rámci této komunikace data opouštějí vozidlo a tato jsou odesílána třetí straně. Tato komunikace je tak jednosměrná a vozidlo na základě odeslaných informací nezískává žádné další informace nazpět. Příjemcem těchto informací může být široká škála subjektů, ať se jedná o některý z infrastrukturních prvků nebo jiný subjekt, který data využije pro poskytování dalších služeb. Takovým subjektem může být například poskytovatel služeb s přidanou hodnotou (např. pojišťovna) nebo výrobce vozidla, který má zájem získat informace z reálného provozu vozidla. Cílem této komunikace tak může být sběr dat pro tvorbu statistik o funkčních parametrech vozidla nebo o opotřebení částí vozidla na základě údajů o používání, zajištění dobrovolné účasti na nehodových studiích zaměřených na účinnější vyšetřování příčin dopravních nehod, naplnění uzavřené smlouvy s poskytovatelem služeb za účelem získání služeb s přidanou hodnotou vztahujících se k danému vozidlu (např. fleet management, tj. monitorování firemní flotily vozidel, výpočet pojistného v závislosti na způsobu jízdy, tzv. „Pay As You Drive“, asistenční služby při poruše vozidla atp.), zajištění bezpečnosti posádky díky automatickému systému tísňového volání eCall anebo ochrana proti krádeži, kdy v případě krádeže vozidla

[7] Commission Nationale Informatique & Libertés. *Compliance package – Connected vehicles and personal data* [online]. Internetové stránky cnil.fr. 2018. [cit. 2021-11-29]. Dostupné z: https://www.cnil.fr/sites/default/files/atoms/files/cnil_pack_vehicules_connectes_gb.pdf.

[8] Srov. str. 19 a násl. stanoviska CNIL.

[9] Srov. str. 23 a násl. stanoviska CNIL.

systém určí geografickou polohu vozidla a tyto údaje odešle poskytovateli služby vyhledávání vozidel.

c) Komunikace IN-OUT-IN.[10] Jak již z označení tohoto typu komunikace vyplývá, jedná se o případy, kdy jsou data z vozidla předávána mimo vozidlo a na základě těchto dat vozidlo obdrží zpět informaci, se kterou dále pracuje (např. na dálku spustí automatickou akci ve vozidle). Tato komunikace slouží zejména k zajištění vzdálené údržby, kdy má uživatel zpravidla uzavřenou smlouvu s poskytovatelem služeb za účelem přijímání zpráv nebo upozornění týkajících se funkcí vozidla (upozornění na stav opotřebení brzd nebo připomenutí data technické prohlídky vozidla) nebo aktualizací vozidlových systémů. Druhým případem je zvýšení jízdního komfortu (například získáváním dynamických dopravních informací) a zároveň poskytování vlastních polohových a stavových dat, zpráv včasného varování na nebezpečné situace či upozornění na ekologickou jízdu.

d) Komunikace OUT-IN, případně OUT-IN-OUT. Pro úplnost tohoto výčtu je třeba uvést i způsob komunikace, kdy na základě informace pocházející zvenčí vozidlo reaguje, a to bez toho, aniž by pro vznik informace poskytlo úvodní impuls. V tomto případě může jít například o ovládání některých součástí vozidla prostřednictvím mobilní aplikace (např. zapnutí vyhřívání sedaček apod.) nebo přijímání informací od jiných vozidel nebo infrastrukturních prvků. Pokud vozidlo na základě provedené reakce odesílá některá data zase zpět iniciátorovi požadavku, lze hovořit o komunikaci OUT-IN-OUT.

Není pochyb o tom, že prostřednictvím těchto komunikačních toků bude vyměňováno velké množství dat, která jsou nezbytná ke správnému fungování systémů autonomního řízení. Na základě informací z týmů vyvíjejících autonomní vozidla, jež mají údaje za tisíce hodin zkušebních jízd, lze dovodit, že za jednu hodinu může provoz autonomního vozidla vytvořit až 4 TB dat. Toto obrovské množství je aktuálně shromažďováno, přesunuto,

[10] Srov. str. 32 a násl. stanoviska CNIL.

uloženo a následně interpretováno pro zlepšování a trénink algoritmů autonomních vozidel.[11] Tato data v sobě nepochybně obsahují řadu osobních údajů, což je nutné zohlednit při návrhu a provozování těchto systémů. Právě s ohledem na to se nyní zaměříme na konkrétní data, která mohou být obsahem výše naznačených komunikačních toků.

Z pohledu architektury systémů autonomního řízení je možné identifikovat data, která potenciálně mohou obsahovat osobní údaje v následujících třech oblastech:

a) data uvnitř systému autonomního vozidla;
b) data v komunikačních sítích a aktivních prvcích;
c) data v koncových bodech.

2.1 DATA UVNITŘ SYSTÉMU AUTONOMNÍHO VOZIDLA

Na úrovni vlastního vozidla jsou data relevantní pro autonomní systémy řízení kombinována s různými senzory pro sledování okolí (např. radar, lidar, počítačové vidění, sonar, GNSS a další), které interpretují senzorické informace na identifikaci cesty, vyhnutí se překážkám, čtou a interpretují dopravní značení.[12] Takto získaná data lze třídit a kategorizovat podle různých hledisek. Níže uvádíme jedno z možných dělení, a to podle povahy sbíraných dat a účelu jejich možného následného použití.[13] Vozidlo tedy zpracovává a uchovává:

a) data podporující řízení motorového vozidla, tj. data ze senzorů (radarů, kamer, ABS, ESP a dalších) a elektronických řídících jednotek, které zpracovávají informace ze senzorů, provádějí diagnostiku, detekují chyby, vydávají povely (aktory) apod.;

---

[11] Addressing the autonomous vehicle data problem [online]. *Internetové stránky DXC.technology* [cit. 2021-08-03]. Dostupné z: https://dxc.com/us/en/insights/customer-stories/addressing-the-autonomous-vehicle-data-problem--.

[12] KOCIĆ, Jelena, JOVIČIĆ, Nenad and DRNDAREVIĆ, Vujo. *Sensors and Sensor Fusion in Autonomous Vehicles*, 26th Telecommunications Forum (TELFOR) [online], 2018, pp. 420-425, [cit. 2021-11-29]. Dostupné z: https://ieeexplore.ieee.org/document/8612054.

[13] Toto dělení autoři využívají na základě vlastní provedené analýzy reálného stavu pro účely metodiky, vznikající v rámci projektu, určené pro přijetí opatření stakeholdery v automotive průmyslu k dosažení privacy-by-design.

b) obrazová data, tj. data z kamer zachycující okolí vozidla a rovněž data z kamer uvnitř vozidla (např. pro účely sledování únavy řidiče);
c) data o řízení vozidla (i data o nehodách, tj. data z EDR jednotky) pro analýzu jízdy a forenzní analýzu v případě dopravní nehody či nestandardního stavu systému. U systémů autonomního řízení je možný sběr i dalších dat, než jen ze senzorů a řídících jednotek. Jedná se například o data o uživateli vozidla, počtu pasažérů či stylu jízdy;
d) lokalizační a polohová data, primárně z GNSS systémů a již běžných doplňkových systémů, jako například elektronický kompas, napojení na mobilní sítě apod. U systémů autonomního řízení se předpokládá potřeba většího rozlišení a také spojení s akcelerometry, laserovými gyroskopy, lidary a 4G/5G sítěmi. Polohu vozidla je možné zpřesňovat i s využitím komunikačních systémů krátkého dosahu. Jedná se především o V2I komunikaci, kde komunikační zařízení na infrastruktuře má svou pevnou polohu, která je známá a může poskytovat vypočtenou aktuální chybu určení geografické pozice;
e) data z biometrických, biologických nebo zdravotních senzorů pro účely jednoznačné identifikace osob, pro které se používají otisky prstu, dlaně, scan obličeje, oční duhovky, charakteristika hlasu aj. V systémech autonomního řízení je možné sledovat stav identifikovaného řidiče, jeho chování či reflexy a na základě toho upravovat parametry systému. Současně je možné personalizovat různé služby a funkce systémů ve vozidlech, které se spouštějí na základě identifikace osob;
f) audio data z vnitřních mikrofonů, která slouží pro hlasové ovládání systémů a funkcí, případně ve spojení s telefonem i pro hlasové volání či diktování krátkých zpráv. Autonomní vozidla používají také externí mikrofony jako dodatečné vstupy pro scanování svého okolí, čímž ale mohou detekovat i hovor náhodných kolemjdoucích;

g) personalizovaná data, uchovávaná ve vozidle, využívaná například pro tzv. infotainment, který může obsahovat řadu osobních údajů týkajících se subjektu údajů nebo například data z uživatelských zařízení a aplikací, získaná např. prostřednictvím propojení mobilních zařízení se systémem vozidla a využíváním specifických aplikací (jako je Apple CarPlay, Android Auto). Právě napojení na mobilní zařízení je zásadním rizikem, neboť obsahují velké množství dat spojených se subjektem údajů. Takovými jsou především seznamy realizovaných hovorů, telefonní seznamy, krátké textové zprávy (SMS, smart messaging aplikace), emaily atp.

2.2 DATA V KOMUNIKAČNÍCH SÍTÍCH A AKTIVNÍCH PRVCÍCH

Systémy autonomního řízení budou využívat nejen data z vnitřních senzorů, ale budou závislé i na datech z vnějších systémů. Stejně tak budou tyto systémy poskytovat senzorická data či zprávy jiným systémům v okolí. Z těchto důvodů je třeba zajistit kvalitní komunikační sítě, které budou poskytovat spolehlivé datové přenosové kapacity. Pro tyto účely se již mnoho let vyvíjejí vhodné technologie, které umožní digitální komunikaci mezi vozidly s cílem eliminace rizika dopravních nehod. Dle organizace NHTSA může tato komunikace mezi vozidlem a jakýmikoliv dalšími zdroji relevantních informací, ať již jde o jiná vozidla, dopravní infrastrukturu nebo jakákoliv jiná zařízení (např. mobilní zařízení chodců či cyklistů), která bývá označována jako V2X (Vehicle-to-everything) komunikace pomoci zabránit až 70 – 80 % dopravních nehod každý rok.[14] Předpokládáme však, že v nejbližších letech bude komunikace V2X sestávat zejména z V2V (Vehicle-2-Vehicle) a V2I (Vehicle-2-Infrastructure) komponent, tedy zařízení, která umožňují komunikaci mezi vozidly navzájem a komunikaci mezi vozidlem a prvky dopravní infrastruktury.

Současná vize implementace V2V komunikačních technologií předpokládá, že vozidla si budou vyměňovat zprávy, které budou mj. obsahovat

[14] BUTLER, Brandon. The future of auto safety is seat belts, airbags and network technology [online]. *Internetové stránky networkworld.com*. 2016 [cit. 13.1.2021]. Dostupné z: https://www.networkworld.com/article/3072486/the-future-of-auto-safety-is-seat-belts-airbags-and-network-technology.html

jejich geografickou pozici, rychlost či stav brzdového systému až desetkrát za vteřinu. Vozidlovým systémům tyto informace umožní vypočítat potenciální riziko srážky a předcházet vzniku nebezpečných dopravních situací. Vozidlo může buď upozornit řidiče, nebo v případě zčásti či plně autonomních systémů automaticky zahájit akci, která zabrání potenciální nehodě (např. snížení rychlosti jízdy, zastavení vozidla nebo provedení úhybného manévru).

Obdobné technologie se mohou využít pro komunikaci V2I (Vehicle-to-Infrastructure), kde z prvků infrastruktury mohou být šířeny dodatečné relevantní informace, jako například informace o signálním plánu nadcházející křižovatky nebo varování před rizikovým místem na vozovce (např. výskyt zpomalovacího pásu nebo nebezpečného výmolu).

Komunikace typu V2V může v podstatě rozšířit dosah senzorů vozidla, jež mají určité limity nebo za špatných klimatických podmínek nepracují tak spolehlivě. Tato komunikace v podstatě pomáhá vozidlům „vidět dále" pomocí využití dat ze senzorů jiných vozidel, a tím umožňuje lepší a včasnější vyhodnocení situace a případně i pohotovější reakci.

2.3 DATA V KONCOVÝCH BODECH

Poslední částí řetězce systémů autonomního řízení jsou koncové body, které mohou zpracovávat osobní údaje. V zásadě se dá konstatovat, že koncové body mohou zpracovávat jen taková data a osobní údaje, které jsou přeneseny prostřednictvím komunikačních sítí z vozidel, proto rozsah zpracovávaných údajů de facto odpovídá předešlé kapitole.

Tyto systémy dále mohou zpracovávat osobní údaje, které jsou poskytovány samotnými subjekty údajů v rámci akvizičního či registračního procesu, kde však lze nastavit již standardní opatření související s požadavky GDPR.[15]

[15] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

Z výše uvedeného je možné konstatovat, že v rámci systémů autonomního řízení jsou, resp. by v budoucnu mohly být zpracovávány následující osobní údaje:

a) základní osobní údaje – jméno a příjmení, telefonní číslo, unikátní identifikátor vozidlových komponent atp.;
b) behaviorální osobní údaje – způsob řízení, oblíbené trasy, denní časový rozvrh atp.

V rámci autonomních vozidel je možné mít díky propojení s mobilními zařízeními a jejich integrací s vozidlovým infotainmentem i teoretickou možnost přístupu k ekonomickým osobním údajům a citlivým údajům subjektu údajů.

Z hlediska zpracovávání osobních údajů vystupují v systémech autonomního řízení následující účastníci:

a) řidiči;
b) další pasažéři;
c) výrobci vozidel;
d) provozovatelé komunikačních sítí;
e) provozovatelé systémů, ve kterých jsou data zpracovávána (např. poskytovatelé služeb); a
f) případně i další zapojené osoby, které se nacházejí mimo vozidlo, včetně kolemjdoucích osob.[16]

Tito účastníci pak budou v návaznosti na jejich postavení a roli v systémech autonomního řízení:

a) subjekty osobních údajů;
b) správci osobních údajů, případně společní správci;
c) zpracovateli osobních údajů;
d) případně pouze dalšími osobami zpracovávajícími osobní údaje ve smyslu čl. 29 GDPR.

Právě nastavení transparentních pravidel mezi jednotlivými účastníky je základem pro právně konformní zpracování osobních údajů v systémech

[16] Autoři jsou si vědomi, že výčet účastníků není kompletní. Pro účely výzkumu však byli vybráni nejvýznamnější účastníci ekosystému autonomní mobility, kteří mohou mít vliv na zpracování a ochranu osobních údajů.

autonomního řízení. Dle názoru autorů tohoto článku jsou hlavními aktéry v celkovém budování systémů autonomního řízení a vymezování mantinelů jejich použitelnosti a použitelnosti shromažďovaných údajů výrobci vozidel, provozovatelé komunikačních sítí a provozovatelé systémů, ve kterých jsou data zpracována.

Právě tito aktéři by v rámci vývoje autonomních systémů řízení a stejně tak i při návrhu a vývoji jejich jednotlivých komponent měli zabezpečit to, že nebude docházet k neoprávněnému zpracování osobních údajů a nežádoucím zásahům do soukromí tak, aby nebyla ohrožena důvěra v moderní vozidlové technologie a reputace jich samotných. Vůdčími principy z hlediska zajištění ochrany osobních údajů jsou *privacy by default a privacy by design*, kterým bude věnována navazující kapitola tohoto článku.

3. PRIVACY BY DESIGN A PRIVACY BY DEFAULT JAKO KLÍČOVÁ VÝCHODISKA Z HLEDISKA OCHRANY A ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Při zpracování osobních údajů je ve smyslu čl. 25 GDPR nezbytné postupovat v souladu s koncepty záměrné a standardní ochrany osobních údajů. Oba koncepty ochrany osobních údajů zásadním způsobem dotvořily pokyny č. 4/2019 Evropského sboru pro ochranu osobních údajů[17] po jejich doplnění k 20. říjnu 2020 (dále jen „**Pokyny**“).

Privacy by design, neboli záměrná ochrana osobních údajů, je vůdčí koncept moderní ochrany osobních údajů, jehož zavedení je povinností všech správců osobních údajů, bez ohledu na jejich velikost či obor činnosti. Ve zkratce tento koncept odráží fakt, že samotnému vývoji a provozu produktu, služby či systému je ochrana osobních údajů natolik vlastní, že je jeho neoddělitelnou součástí. To mimo jiné znamená, že problematika související s ochranou osobních údajů je zvažována již při samotném návrhu, ale následně i v průběhu času tak, aby stále odpovídala *„aktuálnímu stavu tech-*

[17] Evropský sbor pro ochranu osobních údajů. *Pokyny č. 4/2019 k článku 25 - záměrná a standardní ochrana osobních údajů* [online] 2019. [cit. 2021-08-03]. Dostupné z: https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_cs.pdf.

niky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob.“[18]

Koncept standardní ochrany osobních údajů, v anglickém originále dle GDPR *privacy by default,* je postaven na východisku, že pokud již musí být některé osobní údaje zpracovávány, má k takovému zpracování docházet pouze v minimálním rozsahu, co do množství dat a jednotlivých činností zpracování, který je nezbytný pro dosažení vymezeného účelu jejich zpracování. Stejně tak by pouze na nezbytně nutnou měla být omezena i doba jejich zpracování a okruh osob, které mají nebo mohou mít k osobním údajům přístup.

Rozdíl mezi těmito koncepty shledává Bygrave[19] zejména v:

a) větší šíři možných opatření pro ochranu osobních údajů u *privacy by design* oproti zaměření na minimalizaci rozsahu zpracování a jeho důvěrnost u *privacy by default;* a
b) procesní orientaci *privacy by design* oproti zaměření na výsledky zpracování u *privacy by default*, které budou garantovat minimalizaci a důvěrnost údajů ve výchozím bodě.

Oba koncepty, které lze vnímat nicméně jako „*vzájemně se doplňující koncepty, které se synergeticky podporují,*“[20] je však potřeba vnímat a aplikovat ve fázích návrhu a vývoje produktu, tedy v době „*určení prostředků pro zpracování*“[21], tak i v rámci fáze zpracování, ačkoliv je tak výslovně uvedeno pouze u principu *privacy by design*.[22]

Oba koncepty, které jsou tak svou aktuálností i obecným záměrem neodmyslitelně provázané s prostředím autonomní dopravy a s poskytnutím vodítek pro jejich praktickou aplikaci při výrobě a provozu systémů autonomních řízení, jsou detailněji popsány níže.

---

[18] Viz čl. 25 GDPR

[19] BYGRAVE, L. A. *Data protection by design and by default: Deciphering the EU‘s legislative requirements*. Oslo Law Review. [online] 2017. 4(2), 105-122 [cit. 2021-11-12]. Dostupné z: https://heinonline.org/HOL/P?h=hein.journals/oslo4&i=106.

[20] Srov. Pokyny, odst. 5.

[21] Srov. čl. 25 odst. 1 GDPR.

[22] Srov. BYGRAVE, str. 116.

4. VÝVOJ SYSTÉMŮ AUTOMNÍHO ŘÍZENÍ V SOULADU S KONCEPTEM PRIVACY BY DESIGN

Literatura[23] řadí původ konceptu *privacy by design* do roku 1995, když se objevil v rámci reportu (zprávy)[24] společné výzkumné činnosti kanadského a nizozemského úřadu pro ochranu osobních údajů. Koncept, který představoval záměr ochrany osobních údajů pro nově vznikající informační systémy[25], se skládal ze tří kroků:

1) Analýza. V rámci analýzy má vývojář informačního systému posoudit, jaká data jsou nutná pro fungování systému a současně jaká data jsou sbírána a zaznamenávána s ohledem na zásadní princip minimalizace, jak bude rozveden dále;
2) Návrh. V návrhu by mělo být posouzeno, jaké údaje uživatele (subjekt údajů) budou využívány a přístupny v rámci informačního systému, jakož i jak bude subjekt údajů zpracování svých osobních údajů kontrolovat; a
3) Implementace. V rámci implementace by mělo být posouzeno, jaká opatření na ochranu osobních údajů jsou dostupná a mohou být při vzniku informačního systému využita.

Šlo tedy o strukturovaný postup pro vývojáře informačních systémů, jak uvažovat při záměru vybudovat nový informační systém a zahrnout do něj i ochranu osobních údajů způsobem, aby bylo respektováno soukromí jeho

[23] Srov. NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., KOVAŘÍKOVÁ, K. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář.* 2. vydání. Praha: Wolters Kluwer ČR, 2018, str. 281.

[24] HES, Ronald a BORKING, John. *Privacy-Enhancing Technologies: The Path to Anonymity*. [online]. 1995 [cit. 2021-08-03]. Dostupné z: https://www.researchgate.net/profile/John-Borking/publication/243777645_Privacy-Enhancing_Technologies_The_Path_to_Anonymity/links/56e6850708ae68afa1138167/Privacy-Enhancing-Technologies-The-Path-to-Anonymity.pdf.

[25] Srov. HES a BORKING, str. 41.

uživatelů. Do evropské směrnice o ochraně osobních údajů,[26] která byla přijata ve stejný rok, se však tento koncept neprosadil.

Zásadní krok pro další adopci konceptu *privacy by design* v unijním právu přinesly roky 2009 a 2010. Tehdy nejprve průkopnice Ann Cavoukian, kanadská komisařka pro informace a ochranu osobních údajů, která se podílela již na vzniku reportu, představila základní zásady pro koncept, který již dle samotného názvu *Privacy by Design* představoval posun od tehdejšího postupu technologií zvyšujících ochranu soukromí.[27] Představený koncept[28] stál na prvně holých sedmi základních zásadách:

a) proaktivní, ne reaktivní; preventivní, ne nápravný (*Proactive not Reactive; Preventative not Remedial*), kdy je výslovně uznána hodnota a přínosy včasného a důsledného proaktivního přijímání důsledných postupů v oblasti ochrany soukromí, aby se předešlo rizikům ohrožujícím soukromí;
b) soukromí je standardním nastavením (*Privacy as the Default Setting*): shromažďování osobních údajů musí být řádné, zákonné a omezené na rozsah nezbytný pro stanovené účely. Při navrhování programů, systémů a jiných ICT technologií by se mělo standardně vycházet z interakce a komunikace, která neumožňuje identifikaci;
c) soukromí je zakomponováno do návrhu (*Privacy Embedded into Design*), tzn. začleněno do návrhu obchodních procesů, technologií, provozu a informační architektury holistickým, integrujícím a kreativním způsobem;
d) plná funkčnost, nikoliv zbytečné kompromisy a falešné dichotomie (*Full Functionality — Positive-Sum, not Zero-Sum),* tzn. má být vy-

[26] Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. 1995. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=celex:31995L0046.

[27] Sdělení Komise ES o podpoře ochrany osobních údajů prostřednictvím technologií zvyšujících ochranu soukromí (PETs). 2007. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52007DC0228&from=EN.

[28] CAVOUKIAN, A. *Privacy by design: The 7 Foundation Principles*. [online] 2009 [cit. 2021-11-12]. Dostupné z: https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.

hověno všem legitimním zájmům "win-win" způsobem, aniž by byly přijaty falešné dichotomie v podobě soukromí vs. bezpečnost, když se ukáže, že je možné, a tedy i žádoucí splňovat obě tyto možnosti;

e) end-to-end zabezpečení (*End-to-End Security — Full Lifecycle Protection)*: soukromí musí být nepřetržitě chráněno po celou dobu životního cyklu osobních údajů. V ochraně ani v odpovědnosti za ochranu by tak neměly existovat žádné mezery, přičemž právě end-to-end zabezpečení má v tomto případě zvláštní význam, protože bez něj nemůže existovat žádné soukromí;

f) transparentnost a viditelnost (*Visibility and Transparency — Keep it Open*), které mají zajistit, aby všechny zúčastněné strany bez ohledu na to, o jakou obchodní praxi nebo technologii se jedná, skutečně zacházely se soukromím v souladu s uvedenými sliby a cíli, které podléhají nezávislému ověření: operace tudíž mají zůstat viditelné a transparentní jak uživatelům, tak poskytovatelům;

g) respekt k soukromí uživatele (*Respect for User Privacy — Keep it User-Centric*): které vyžaduje, aby systémoví architekti a poskytovatelé dbali především na zájmy jednotlivce a nabízeli možnosti silného výchozího nastavení ochrany soukromí, odpovídajících upozornění a uživatelsky-přívětivých možností.[29]

Tyto zásady byly následně v roce 2010 nejprve dále rozvedeny a doplněny[30] i s odkazem na tehdejší univerzální principy globálního standardu soukromí.[31] Následně je pak 32. mezinárodní konference komisařů pro ochranu osobních údajů v Jeruzalémě přijala rezolucí za nezbytnou součást základní ochrany soukromí a začala podporovat adopci sedmi základních principů při zajišťování soukromí ve společnostech jakožto jejich výchozí způsob

[29] Popisu jednotlivých principů se věnuje např. JEŽOVÁ, D. *Principle of Privacy by Design and Privacy by Default*. Regional Law Review [online]. 2020, 127-140. [cit. 2021-11-12]. Dostupné z: https://heinonline.org/HOL/P?h=hein.journals/rgllr2020&i=130.

[30] CAVOUKIAN, A. *Privacy by design: The 7 Foundation Principles. Implementation and Mapping of Fair Information Practices.* [online] 2010. [cit. 2021-11-12]. Dostupné z: https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf.

[31] International Data Protection Commissioners Conference. *Global Privacy Standards*. [online] 2005. [cit. 2021-11-12]. Dostupné z: https://thepublicvoice.org/2006/12/global-privacy-standard.html.

fungování.[32] Není bez zajímavosti, že ačkoliv i na základě samotné rezoluce[33] mělo být o rok později na konferenci zhodnoceno fungování tohoto konceptu,[34] přijaté rezoluce z roku 2011 nic bližšího k *privacy by design* neobsahují.[35]

Pod obsahově užším pojmem *data protection by design* se přijatý koncept promítl do prvního návrhu znění GDPR, jak bylo představeno v lednu 2012 Evropskou komisí.[36] Tehdy ještě v původním čl. 23 odst. 1 bylo stanoveno, že „s *ohledem na stav techniky a náklady provedení přijme správce při určování prostředků zpracování i při samotném zpracovávání vhodná technická a organizační opatření a postupy tak, aby dané zpracování splňovalo požadavky tohoto nařízení a zaručovalo ochranu práv subjektu údajů.“* Legislativní zakotvení konceptu doplnil bod 61 odůvodnění, který stanovil, že „*ochrana práv a svobod subjektů údajů v souvislosti se zpracováním osobních údajů vyžaduje, aby byla přijata příslušná technická a organizační opatření jak při přípravě zpracování, tak v průběhu vlastního zpracování, s cílem zajistit splnění požadavků tohoto nařízení. Aby správce zajistil a prokázal soulad s tímto nařízením, měl by stanovit interní politiky a přijmout vhodná opatření, která splňují zejména zásady ochrany údajů již od návrhu a standardního nastavení ochrany údajů*“.

O čtyři roky později přijaté konečné znění GDPR se od původní formulace *data protection by design* odlišilo, když začalo brát v úvahu nejen stav techniky a náklady na provedení, ale i další faktory v podobě „*povahy, rozsahu, kontextu a účelů zpracování, a různě pravděpodobných a různě závažných*

[32] International Conference of Data Protection and Privacy Commissioners. *Resolution on Privacy by Design*. [online] 2010. [cit. 2021-11-12]. Dostupné z: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf.

[33] Tamtéž.

[34] International Conference of Data Protection and Privacy Commissioners. *Agenda*. [online] 2011. [cit. 2021-11-12]. Dostupné z: http://www.privacyconference2011.org/htmls/adoptedResolutions/2011_Mexico/2011_EC_A_001_AGENDA_33_ICDPPC_ENG.pdf.

[35] Srov. International Conference of Data Protection and Privacy Commissioners. *Adopted Resolutions*. [online] 2011. [cit. 2021-11-12]. Dostupné z: http://www.privacyconference2011.org/index.php?lang=Eng.

[36] Návrh Nařízení evropského parlamentu a rady o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů). 2012. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52012PC0011&from=CS.

rizik pro práva a svobody fyzických osob." Zajímavým prvkem je explicitní doplnění pseudonymizace jakožto vhodného (technického) opatření. Současně byla přijata dikce s odkazem na provádění zásad ochrany údajů, s explicitní zmínkou zásady minimalizace údajů ve smyslu čl. 5 odst. 1 písm. c) GDPR.[37] Vedle této zásady musí tedy koncept *privacy by design* splňovat i zásady zákonnosti, korektnosti a transparentnosti, přesnosti, omezení uložení a integrity a důvěrnosti, pro které musí být zavedena vhodná technická a organizační opatření.[38]

S ohledem na výše uvedené by tak především výše popsaní hlavní aktéři v oblasti systémů autonomního řízení měli přistupovat k jejich vývoji a rozvoji vždy s vědomím toho, že součástí shromažďovaných dat budou s ohledem na jejich širokou definici i osobní údaje. Respekt k osobním údajům jako součásti soukromé sféry osob by měl být brán v úvahu již ve fázi návrhu systému jako takového, ale i jeho dílčích komponent. Současně by měly být brány v úvahu veškeré vnitřní a vnější hrozby a náklady na provedení. Současně je nepochybné, že s rozvojem techniky se budou měnit hrozby pro tyto systémy a stejně tak i náklady na zavedení odpovídajících opatření, hlavní aktéři tak budou muset neustále vyhodnocovat zranitelnosti systémů autonomního řízení a adekvátně na ně reagovat (např. formou bezpečnostních aktualizací apod).

5. VÝVOJ SYSTÉMŮ AUTOMNÍHO ŘÍZENÍ V SOULADU S KONCEPTEM PRIVACY BY DEFAULT

Koncept *privacy by default* lze popsat jako zavedení „*továrního režimu*"[39] u konfigurovatelných nastavení, aby bylo standardně prováděno pouze zpracování, které je nezbytně nutné k dosažení stanoveného zákonného

[37] Jak bude vysvětleno dále, právě tato zásada spolu se zásadou omezení uložení tvoří koncept *privacy by default*.

[38] Praktickým přístupem v souvislosti se zavedením potřebných opatření za zabývá i DAG WIESE SCHARTUM, *Making privacy by design operative*, International Journal of Law and Information Technology, Volume 24, Issue 2, Summer 2016, Pages 151–175. [cit. 2021-08-03]. Dostupné z: https://doi.org/10.1093/ijlit/eaw002.

[39] V rámci automobilového průmyslu lze z povahy výroby toto označení považovat za příléhavé, budeme ho proto využívat v kontextu standardního nastavení zařízení i dále v textu.

účelu. Jak popisují Pokyny, správci, resp. výrobci jednotlivých zařízení, která budou provádět zpracování osobních údajů, by se měli při zavádění tohoto továrního režimu spolehnout na „*své posouzení nezbytnosti zpracování s ohledem na právní důvody v čl. 6 odst. 1 GDPR*“.[40] To samozřejmě nebrání, aby konkrétní řidič nebo uživatel vozidla nastavil své preference z hlediska jeho zpracování jinak, ale pokud žádnou volbu neprovede, mělo by jeho soukromí být respektováno v maximální možné míře.

V první řadě tedy je třeba posoudit právní základ pro zpracování, na základě kterého lze tato standardní zpracování provádět, a to v kontextu zásad minimalizace a omezení uložení, aby „*správce standardně neshromažďoval více údajů, než je nezbytné, nezpracovával shromážděné údaje více, než je pro dané účely nezbytné, ani neuchovával údaje déle, než je nezbytné.*“[41] Pro řádné provedení těchto zásad je však ve smyslu *privacy by default* třeba explicitně přijmout konkrétní technická a organizační opatření.

S odkazem na dikci čl. 25 odst. 2 GDPR tak lze říct, že koncept *privacy by default a* tedy standardní zpracovávání osobních údajů je tvořeno následujícími čtyřmi složkami, které blíže rozvádíme níže.

5.1 OMEZENÍ ZPRACOVÁNÍ NA NEJMENŠÍ NEZBYTNĚ NUTNÉ MNOŽSTVÍ OSOBNÍCH ÚDAJŮ (ZÁSADA MINIMALIZACE)

V rámci omezení zpracování na nejmenší nezbytně nutné množství osobních údajů, které je současně jednou ze složek zásady minimalizace ve smyslu čl. 5 odst. 1 písm. c) GDPR, má být zvážen jak „*objem osobních údajů, tak i druhy, kategorie a míra podrobnosti osobních údajů, která je nutná pro účely zpracování*“.[42] Standardní zpracování v rámci „*továrního režimu*“ však nikdy nesmí zahrnovat údaje, které nejsou nezbytné pro konkrétní účel zpracování. Je proto třeba se omezit na co nejmenší množství a co nejmenší detail získávaných údajů. U tohoto projevu zásady minimalizace je třeba zavedenými opatřeními prověřovat jeho dodržování prostředky v reálném čase.

[40] Srov. Pokyny, odst. 42.

[41] Tamtéž.

[42] Srov. Pokyny, odst. 49.

5.2 OMEZENÍ ROZSAHU ZPRACOVÁNÍ, RESP. JEHO OPERACÍ, NA NEZBYTNĚ NUTNÉ (ZÁSADA MINIMALIZACE)

GDPR popisuje v čl. 4 odst. 2 demonstrativní výčet různých operací zpracování osobních údajů. S ohledem na účel zpracování by však měly být využity nezbytně jen takové operace a jen takový jejich počet, který povede ke splnění tohoto účelu. To však dle našeho názoru nutně nemusí znamenat, že musí být využito co nejmenšího počtu zpracování. V některých případech totiž bude správce/výrobce lépe provádět a zajišťovat dodržování „*zásad ochrany údajů*" včetně zásady minimalizace s ohledem na množství osobních údajů, lépe chránit práva subjektů údajů a bezpečněji dosahovat uvedeného cíle, pokud rozsah zpracování nebude naprosto minimalistický.[43] Tento přístup však musí být vždy vhodným způsobem popsán a odůvodněn.

5.3 OMEZENÍ DOBY ULOŽENÍ POUZE NA NEZBYTNĚ NUTNOU DOBU (ZÁSADA OMEZENÍ ULOŽENÍ)

Délka doby uchovávání osobních údajů závisí na účelu dotyčného zpracování. Pokud správce osobní údaje nadále nezbytně nepotřebuje pro jeho dosažení, musí být začleněným systematickým způsobem standardně vymazány nebo anonymizovány.[44] Podobně jako při omezení zpracování na nejmenší nezbytně nutné množství osobních údajů, i v tomto případě musí opatření prověřovat odůvodněnost zpracovávání v reálném čase.

5.4 OMEZENÍ PŘÍSTUPU K OSOBNÍM ÚDAJŮM POUZE NEJMENŠÍMU NEZBYTNĚ NUTNÉMU POČTU OSOB

Poslední, čtvrtá složka konceptu *privacy by default,* stojí relativně samostatně, když ze své podstaty není přímým projevem některé z obecných zá-

[43] Bude se tak dít například v případě, kdy namísto operací prostého shromáždění, uložení a použití osobních údajů jsou údaje napřed shromážděny, následně strukturovány a/nebo zkombinovány, potom je z nich část vymazána a teprve následně je jejich zlomek uložen a použit.

[44] Pracovní skupina pro ochranu údajů zřízená podle článku 29. *Stanovisko č. 5/2014 k technikám anonymizace* [online]. 2014 [cit. 2021-08-03]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_cs.pdf.

sad zpracování osobních údajů dle čl. 5 GDPR,[45] nýbrž se projevuje posouzením nezbytnosti okruhu osob, které budou mít ke zpracovávaným osobním údajům přístup, a současně také nastavením politiky přístupů včetně jejich kontrol.[46] Tato složka je naopak úzce provázána s cílem celého konceptu privacy by design, jak je uveden v poslední větě čl. 25 odst. 2 GDPR, tj. aby standardně nebyly údaje dostupné neomezenému počtu fyzických osob. Předtím, než by se tak stalo, musí mít subjekt údajů možnost zasáhnout. Tato možnost zásahu se potenciálně liší dle kontextu zpracování: v intenzivnějších případech by musel být udělen předchozí souhlas, v méně rizikových případech však může postačit i nabídka subjektu sám si ovlivnit přístup ke zpracovávaným osobním údajům.[47,48,49]

5.5 PŘÍSTUP EDPB K PRIVACY BY DEFAULT V AUTONOMNÍ DOPRAVĚ

Evropský sbor pro ochranu osobních údajů (EDPB) ve svých pokynech č. 1/2020 přímo uvádí, že „*konkrétní pokyny k tomu, jak mohou výrobci a poskytovatelé služeb dosáhnout souladu s předpisy ochranu údajů již od návrhu a ve standardním nastavení, by mohly být přínosné pro průmysl a třetí strany*.“[50]

Obecným závěrem a projevem jednotlivých složek konceptu *privacy by default* je, aby hlavní aktéři, tj. výrobci vozidel a vybavení, poskytovatelé

[45] Nejblíže má nejspíš k projevu zásady integrity a důvěrnosti dle čl. 5 odst. 1 písm. f) GDPR, když se omezením přístupu snaží správce zabezpečit údaje před protiprávním zpracováním neoprávněnou osobou.

[46] Srov. Pokyny, odst. 55.

[47] Srov. Pokyny, odst. 58.

[48] Dobrým praktickým příkladem může být nastavení sociálních sítí a veřejné zobrazování zpracovávaných údajů, které sociální sítě s ohledem na nezbytnost vzniku profilu subjektu údajů potřebují zpracovávat.

[49] Dopady aplikace konceptu privacy by design se zabývá mimo jiné i BERT-JAAP KOOPS & RONALD LEENES (2014) *Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law*, International Review of Law, Computers & Technology, 28:2, 159-171, [cit. 2021-11-18]. Dostupné zde: https://doi.org/10.1080/13600869.2013.801589.

[50] Evropský sbor pro ochranu osobních údajů. *Pokyny č. 01/2020 ke zpracování osobních údajů v souvislosti s propojenými vozidly a aplikacemi souvisejícími s mobilitou.* [online] 2021. [cit. 2021-08-03]. Dostupné z: https://edpb.europa.eu/system/files/2021-03/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_en.pdf

komunikačních sítí a služeb a další správci údajů obecně používali postupy, které:

a) nezahrnují osobní údaje,
b) omezí rozsah zpracování jednotlivých údajů pouze na nezbytně nutné,
c) omezí případné využívání osobních údajů na nezbytně nutnou dobu, a
d) minimalizují předávání osobních údajů mimo vozidlo na nezbytnou úroveň.[51]

S ohledem na výše uvedené lze považovat za klíčové, aby při implementaci tohoto konceptu v systémech autonomního řízení bylo vždy nejdříve zváženo, zda je účelné některé údaje sbírat a pokud ano, zda nepostačí k dosažení účelu, pokud budou ze shromážděných údajů například prostřednictvím technik anonymizace[52] učiněny údaje anonymní.

Pokud je již zpracování některých osobních údajů nezbytné, mělo by převládat lokální zpracování, které zaručuje výhradní a plnou kontrolu nad osobními údaji subjektu údajů, zejména tím, že zakazuje jakékoli zpracování údajů zúčastněnými stranami bez vědomí subjektu údajů. Současně se tím snižuje možnost útoků ze strany externích subjektů a riziko úniku lokalizačních či jiných údajů. Pro hlavní aktéry z toho vyplývá, že pokud je možné činnost zajistit lokálně v rámci vozidla, mělo by být této cesty maximálně využito v rámci továrního režimu s tím, že subjekt údajů může své preference nastavit jinak. Neopouštějí-li data vozidlo, může docházet i ke zpracování citlivých údajů, jako jsou biometrické údaje či podrobné údaje o poloze, které by jinak podléhalo přísnějším pravidlům.[53]

Lokální zpracování dat ve vozidle je však problematické vzhledem k tomu, že autonomní doprava stojí na principu předávání osobních údajů mimo vozidlo a vzájemné komunikaci připojených zařízení. Jako obecný

[51] Srov. odst. 74 Pokynů EDPB č. 01/2020.

[52] Pracovní skupina pro ochranu údajů zřízená podle článku 29. *Stanovisko č. 5/2014 k technikám anonymizace.* [online] 2014. [cit. 2021-08-03]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_cs.pdf.

[53] Viz čl. 9 GDPR.

princip autoři tohoto článku navrhují přistupovat k informacím z vozidla tak, že čím dále se data z vozidla dostávají, tím více agregovaná nebo anonymizovaná by měla být, aby jejich zpracování respektovalo výše uvedené principy na ochranu soukromí jednotlivce. Projev této zásady lze demonstrovat na reálném případu, kdy skutečně detailní informace o poloze vozidla jsou nejvíce relevantní pro vozidla v jeho bezprostředním okolí, aby bylo možné předejít potenciální srážce, ale pro jiné účely, například správu vozového parku nebo vedení knihy jízd, již postačí informace o poloze vozidla v menším detailu a současně mohou být odesílány z vozidla v časových intervalech v délce několika minut.

Tento postup také představuje menší rizika pro kybernetickou bezpečnost a vyhovuje i požadavkům na ochranu soukromí v elektronických komunikacích, které jsou podrobněji popsány v následující kapitole.

6. UMĚLÁ INTELIGENCE, KYBERNETICKÁ BEZPEČNOSTI A OCHRANA SOUKROMÍ V ELEKTRONICKÝCH KOMUNIKACÍCH

Jak již bylo uvedeno, systémy autonomního řízení pracují s enormními objemy dat, která je nutno chránit v souladu s výše uvedenými principy. Při vývoji a implementaci autonomních systémů však nemohou zůstat stranou ani další společenské a právní oblasti, které spoluvytvářejí mantinely vymezené pro jejich fungování.

S ohledem na výše uvedené se autoři tohoto článku v dalších částech tohoto článku věnují stručnému nastínění přesahů do oblasti regulace umělé inteligence, kybernetické bezpečnosti a ochrany soukromí.

6.1 UMĚLÁ INTELIGENCE

Pokud budeme chtít posoudit autonomní systémy a autonomní vozidla v kontextu legislativního rámce Evropské unie, začněme od, pro celou oblast regulace umělé inteligence klíčové, Bílé knihy o umělé inteligenci.[54] Ta byla představena v únoru 2020 jakožto právně nezávazná a představuje vizi

[54] Evropská Komise. *Bílá Kniha o umělé inteligenci – evropský přístup k excelenci a důvěře*. [online] COM(2020) 65 final. 2020. [cit. 2021-11-12]. Dostupné z: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_cs.pdf.

Evropské Komise pro regulatorní rámec oblasti umělé inteligence. Vize se následně zhmotnila 21. dubna 2021, kdy byl představen první návrh nařízení Evropského parlamentu a Rady, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci, tzv. Akt o umělé inteligenci.[55]

Návrh Aktu váže definici "*systémů umělé inteligence*" na software, který je vyvinut taxativně vymezenými přístupy, uvedenými Přílohou č. 1 k Aktu, jako je např. strojové učení, induktivní logické programování, statistické přístupy nebo Bayesovský odhad, a který je schopný generovat výstupy, jako je obsah, předpovědi, doporučení nebo rozhodnutí ovlivňující prostředí, se kterým software interaguje.[56] Právě v tomto směru lze tedy poukázat na provázanost s definicemi autonomních systémů a možné změny chování v návaznosti na přijetí rozhodnutí tohoto softwaru.[57]

Návrh Aktu rozlišuje mezi systémy umělé inteligence s nepřijatelným, vysokým, omezeným a minimálním rizikem; od výše rizika se následně odvíjí přístup a míra regulace. Sám je přitom zaměřen zejm. na regulaci vysoce rizikových systémů umělé inteligence.

Systém umělé inteligence bude považován za vysoce rizikový, pokud je určen k použití jako bezpečnostní součást výrobku nebo je sám výrobkem a na produkt nebo samotný systém umělé inteligence se vztahuje povinnost posouzení shody třetí stranou, oboje podle předpisů v příloze II návrhu. Jde o seznam 19 nařízení a směrnic regulujících oblasti jako strojní zařízení, diagnostické zdravotní prostředky in vitro a pro účely tohoto článku i některé dopravní prostředky, zejm. motorové vozidlo, kterým se ve smyslu Nařízení 2018/858 rozumí „*poháněné vozidlo, které je konstruováno a vyrobeno tak, aby se pohybovalo vlastními prostředky, má alespoň čtyři kola, je úplné, dokončené nebo neúplné a má nejvyšší konstrukční rychlost vyšší než 25 km/h*“.[58] Současně, jak stanoví rec. 34 Návrhu Aktu, jako vysoce rizikové lze klasifi-

---

[55] Evropská Komise. *Návrh Nařízení Evropského Parlamentu a Rady, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (Akt o umělé inteligenci) a mění určité legislativní akty Unie* [online] COM/2021/206 final. 2021. [cit. 2021-11-12]. Dostupné z: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0002.02/DOC_1&format=PDF.

[56] Srov. čl. 3 spolu s Přílohou č. 1 Aktu o umělé inteligenci.

[57] Srov. WATSON a SCHEIDT.

kovat i takové systémy umělé inteligence, které „(…) *jsou určeny k použití jako bezpečnostní součásti při řízení a provozu silniční dopravy (…).*[59]

U samořiditelných vozidel jakožto samostatných produktů systémů umělé inteligence, které podléhají povinnosti posouzení shody třetí stranou, tak bude ve vztahu k regulaci vysoce rizikových systémů návrh Aktu ukládat povinnosti poskytovateli, uživateli, dovozci a distributorovi systémů. Pokud přihlédneme k procesu zapracování konceptu *privacy by default,* bude i s ohledem na tento článek klíčovou osobou zejm. poskytovatel, kterým se dle návrhu Aktu rozumí osoba, která „*vyvinula systém umělé inteligence za účelem jeho uvedení na trh nebo do provozu pod svým jménem či ochrannou známkou.*“ Je tedy nezbytné se alespoň zběžně zabývat povinnostmi na tuto osobu kladenými.

Poskytovatel musí zajistit, aby byly dodrženy požadavky, které nařízení na systémy umělé inteligence klade. Patří mezi ně:

a) zavedení systému řízení rizik;
b) požadavky na data, jejich vysokou kvalitu, nezaujatost a reprezentativnost;
c) vypracovaná technická dokumentace;
d) možnost automatického zaznamenávání událostí během provozu systému umělé inteligence;
e) dostatečná transparentnost a možnost lidského dohledu nad fungováním systému umělé inteligence;
f) odpovídající úroveň přesnosti, robustnosti a kybernetické bezpečnosti systému.

Kromě povinnosti zajistit soulad systému umělé inteligence s výše zmíněnými požadavky, musí poskytovatel zavést systém řízení kvality, který bude zdokumentován ve formě písemných zásad, postupů a instrukcí,

[58] Srov. čl. 3 odst. 16 Nařízení Evropského parlamentu a Rady (EU) 2018/858 ze dne 30. května 2018 o schvalování motorových vozidel a jejich přípojných vozidel, jakož i systémů, konstrukčních částí a samostatných technických celků určených pro tato vozidla a o dozoru nad trhem s nimi, o změně nařízení (ES) č. 715/2007 a č. 595/2009 a o zrušení směrnice 2007/46/ES. Dostupné online z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32018R0858&from=CS.

[59] Srov. rec. 34 Návrhu Aktu o umělé inteligenci.

a současně technickou dokumentaci systému umělé inteligence, jehož minimální obsahové náležitosti popisuje Návrh Aktu v Příloze IV. Právě tuto technickou dokumentaci, která má obsahovat např. obecný i detailní popis systému umělé inteligence a procesu jeho vývoje, ale i informace o tréninkových datech a datasetech, může poskytovatel využít jako příležitost, aby byl schopen řádně a transparentně popsat zavedený koncept *privacy by default* v částech samořiditelného vozidla, když bude prokazovat, že při návrhu a konstrukci řešení bral v úvahu a zapracoval všechny čtyři prvky konceptu.

Autonomní systémy řízení a samořiditelná vozidla musí být dle našeho názoru před uvedením na trh nebo do provozu registrovány v evropské databázi pro samostatné vysoce rizikové systémy umělé inteligence. Těmi se totiž rozumí takové vysoce rizikové systémy umělé inteligence, které nejsou pouhými bezpečnostními součástmi výrobku, ale naopak jsou samy výrobky, a současně představují vysoké riziko poškození bezpečnosti.

6.2 KYBERNETICKÁ BEZPEČNOST

Zajištění kybernetické bezpečnosti bude i v autonomních vozidlech zcela zásadní oblastí, neboť případné kybernetické bezpečnostní incidenty můžou mít zcela fatální následky, a to jak v podobě škody na majetku, tak zejména újmy na zdraví a životě jak řidičů a pasažérů vozidla, tak i posádek okolních vozidel a kolemjdoucích.

Prvním zásadním počinem v oblasti kybernetické bezpečnosti systémů ve vozidlech je norma ISO/SAE 21434:2021 Road vehicles — Cybersecurity engineering, která byla publikována v srpnu 2021. Norma poskytuje výrobcům vozidel formalizované postupy pro dosažení odpovídající úrovně bezpečnosti: specifikuje technické požadavky na řízení rizik kybernetické bezpečnosti týkající se koncepce, vývoje produktu, výroby, provozu, údržby a vyřazování z provozu elektrických a elektronických systémů v sériově vyráběných silničních vozidlech, včetně jejich součástí a rozhraní. Součástí dokumentu jsou i požadavky na procesy kybernetické bezpečnosti a společný jazyk pro komunikaci a řízení rizik kybernetické bezpečnosti.

Přijetí normy do značné míry řeší nutnost nastavení sofistikovaných procesů posuzování shody a certifikace jednotlivých částí a komponent systémů autonomní mobility již v průběhu jejich vývoje a zejména před jejich uvolněním do reálného provozu. Nelze tím ovšem kybernetickou bezpečnost v systémech autonomního řízení řešit plošně. Bude pravděpodobně nutné upravit současný stav regulace schvalování vozidel a rovněž zahrnout do těchto procesů i systémy a komponenty, se kterými budou automatizovaná vozidla komunikovat.

Z prevenčního pohledu je pak třeba dbát a řešit detekci rizika kybernetického incidentu, když bude nutné zpracovávat velké množství dat, byť ve velké míře se bude jednat o údaje anonymizované. Osobní údaje pak budou zásadní v rámci ekosystému autonomní mobility pro účely identifikace zdroje kybernetického incidentu či události a jejich šíření, tedy komponent a systémů, které mohou být zasaženy či potenciálně ohroženy.

Zároveň však budou zásadní komponenty ekosystémů autonomního řízení (zejm. pak centrální prvky obsahující klíčová řídící a dopravní data) podléhat i zákonné regulaci kybernetické bezpečnosti, neboť tyto systémy mohou spadat do kategorie informačních systémů základní služby a jejich provozovatelé budou povinnými osobami dle zákona o kybernetické bezpečnosti.[60]

6.3 OCHRANA SOUKROMÍ V ELEKTRONICKÝCH KOMUNIKACÍCH

Ochrana soukromí v elektronických komunikacích vychází z evropské směrnice ePrivacy.[61] Ta mimo jiné zakazuje přístup k informacím uloženým v koncových zařízeních (*terminal equipment*) uživatelů a stejně tak i ukládání informací do těchto koncových zařízení. K těmto činnostem může do-

[60] Postupem dle § 23a zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

[61] Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích). Dostupná z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32002L0058&from=CS.

jít, až na ve směrnici vymezené a úzce aplikovatelné výjimky, pouze se souhlasem uživatele.[62]

Na výše uvedeném nic nemění ani to, zda jde o data, která jsou osobními údaji nebo nikoliv. Směrnice ePrivacy totiž nečiní rozdíl mezi osobními a neosobními údaji, jelikož chrání přístup ke koncovému zařízení uživatele jako takový, bez ohledu na charakter předmětných dat.

Podle Pokynů Evropského sboru pro ochranu osobních údajů č. 01/2020[63] je autonomní vozidlo kvůli svému (ať už přímému či nepřímému) připojení k rozhraní veřejné telekomunikační sítě nutné rovněž považovat za koncové zařízení. Takový přístup nicméně ve výsledku znamená, že data uložená v takovém vozidle jsou důvěrná a přístup k nim je možný pouze se souhlasem uživatele. Bez jeho udělení nelze data číst ani je do takového koncového zařízení ukládat.

Vzhledem ke vzájemné provázanosti směrnice ePrivacy a GDPR by takový souhlas měl splňovat požadavky stanovené v GDPR.[64] Jde zejména o jeho odvolatelnost, konkrétnost, informovanost a jednoznačnost projevu vůle, který směřuje k jeho udělení.[65] Dalším znakem souhlasu je jeho dobrovolnost, uživatel by měl mít tedy skutečnou možnost rozhodnout se, zda souhlas udělí nebo nikoliv. Není proto dovoleno udělení souhlasu vynucovat. Současně by udělení souhlasu mělo být stejně jednoduché jako jeho odvolání.[66]

Směrnice ePrivacy měla být podle původních plánů nahrazena nařízením ePrivacy a měla se stát použitelnou společně s GDPR. K tomu ovšem nedošlo, když datum přijetí nařízení ePrivacy byl již několikrát odložen. Na druhou stranu nelze očekávat významné rozvolnění výše popsaných principů na ochranu soukromí, spíše naopak. Lze předpokládat, že

---

[62] Viz čl. 5 směrnice ePrivacy.

[63] Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications [online]. *European Data Protection Board*. 2020 [cit. 2021-08-03]. Dostupné zde: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf.

[64] Viz čl. 2 písm. (f) směrnice ePrivacy ve spojení s čl. 94 odst. 2 GDPR.

[65] Viz čl. 4 bod 11) GDPR.

[66] Viz čl. 7 odst. 3 GDPR.

některá z výjimek ze získávání souhlasu by mohla být aplikovatelná i na systémy automatizovaného řízení vozidel, a to zejména v zájmu zajištění a zvýšení bezpečnosti, když výše popsaný souhlas musí být podle současných pravidel odvolatelný – nutnost souhlasu totiž může ohrozit celkové fungování systémů autonomního řízení.

7. ZÁVĚR

Z praktického pohledu je ochrana osobních údajů a soukromí všech účastníků v rámci ekosystému autonomní mobility téma, kterým se většina společností, podílejících se na vývoji systémů autonomního řízení (např. Valeo), prokazatelně zcela seriózně zabývá. Společnosti již nyní hledají cesty, jak implementovat opatření pro ochranu osobních údajů a ochranu soukromí již ve fázi vývoje,[67] a to způsobem, aby sériově vyráběná vozidla byla důvěryhodná a měla nastavena odpovídající opatření v souladu s přístupem *privacy by design*, resp. *privacy by default*.[68]

To v konečném důsledku znamená pro jednotlivé aktéry ekosystému autonomní mobility již ve fázi vývoje nutnost přemýšlet na několik kroků dopředu tak, aby dokázali regulatorní požadavky naplnit, což je v současné době, kdy existuje mnoho neznámých, značně komplikované.

Obecně se dá konstatovat, že všichni účastníci ekosystému autonomní mobility, kteří mohou potenciálně vystupovat v roli správců, resp. zpracovatelů osobních údajů, musí vědět, jaká data a na základě jakého právního titulu sbírají, k jakým účelům, v případě následné potřeby provést posouzení vlivu na ochranu osobních údajů ve smyslu čl. 35 GDPR. Zde je ze zkušenosti z provozu kooperativních systémů poskytujících aktuální dopravní informace prostřednictvím komunikace mezi vozidly a mezi vozidlem a dopravní infrastrukturou možné uvést, že souhlas subjektu údajů se

[67] Tento přístup je nutné volit i s ohledem různé právní regulace zpracování osobních údajů v zemích, kde je automobilový průmysl výrazně rozvinutý, např. v USA, Jižní Koreji či Japonsku již existují povinnosti i pro výrobce, jak mají s osobními údaji ve vozidlech (a to nejen autonomních) nakládat.

[68] Srov. ARAZ TAEIHAGH & HAZEL SI MIN LIM (2019) *Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks*, Transport Reviews, 39:1, 103-128, [cit. 2021-11-18]. Dostupné zde: https://doi.org/10.1080/01441647.2018.1494640.

zpracováním údajů[69] není zcela vhodným právním titulem, zejména s ohledem na možnost jeho odvolání ze strany subjektů údajů a vysokou procesní náročnost spojenou s použitím tohoto právního titulu, Proto bude nutné hledat jiné právní tituly, které by byly z pohledu provozního jednodušší.

Dále je nutné připomenout, že při návrhu nastavení adekvátní ochrany osobních údajů v rámci ekosystému autonomní mobility musí jednotliví aktéři respektovat aktuální stav techniky, předpokládané náklady a rovněž rizika plynoucí ze zpracování osobních údajů. Právě rychlý rozvoj autonomních vozidel klade na správce i zpracovatele osobních údajů značné nároky na pravidelný přezkum a zdokonalování použitých technických, procesních i organizačních opatření tak, aby vždy odpovídal aktuálním hrozbám a rizikům.

Řidiči i pasažéři vozidel s autonomními systémy řízení si rovněž musí uvědomit, že tato vozidla zpracovávají obrovské množství dat a informací, proto by měli věnovat zvýšenou pozornost udělování případných souhlasů, zajímat se o rozsah zpracovávaných dat a celkově více řešit ochranu svého soukromí, které může být v této souvislosti značně narušitelné.

Nelze ani opomenout zavádění nových postupů pro posuzování vlastností garantujících soukromí u jednotlivých komponent silničních vozidel s různými stupni autonomie. I proto bude nutné současné technické předpisy EHK/OSN, definující postupy pro schvalování vozidel,[70] revidovat a doplnit, aby i elektronická zařízení ve vozidlech podléhala posouzení či testování z pohledu zpracování dat a osobních údajů.

Před výrobci vozidel i provozovateli klíčových komponent autonomního řízení stojí velké výzvy, a to návrh a nastavení vozidlových systémů tak, aby tyto sbíraly jen minimální množství dat a maximálně chránily soukromí uživatele a současně mu umožnily tyto volby nastavit jinak (např. pomocí souhlasu se zpracováním osobních údajů). V rámci infotainmentu vozidla, případně v kombinaci s mobilními aplikacemi, je navíc nutné sub-

[69] Dle čl. 6 odst. 1 písm. a) GDPR.

[70] Předpis Evropské hospodářské komise Organizace spojených národů (EHK OSN) č. 107 – Jednotná ustanovení pro schvalování vozidel kategorie M2 nebo M3 z hlediska jejich celkové konstrukce [2015/922].

jekty údajů informovat o rozsahu jejich osobních údajů, která jsou v rámci vozidla a celého ekosystému zpracovávána a dát jim možnost se rozhodnout, jak budou tyto údaje využívány, komu budou předávány aj. Právě maximální transparentnost a zahrnutí řidičů i posádky do procesu rozhodování o rozsahu zpracování může významně přispět k akceptaci systémů autonomního řízení a zajištění potřebné míry důvěry. Je třeba upozornit, že zásadní výzvou bude zejména vytvořit takový model, který umožní vyhovět požadavkům vícero osob využívajících vozidlo, jejichž představy a požadavky na ochranu svého soukromí se mohou značně lišit.

Z pohledu provozovatelů sítí je nutné nastavit taková opatření, aby zpracovávali data a osobní údaje pouze pro definované účely, zajistili nastavení odpovídající úrovně kybernetické bezpečnosti, jelikož mohou mít přístup do aut a mohou potenciálně měnit jejich chování a případné kybernetické incidenty mohou mít fatální následky, a to jak na majetku, tak na zdraví a životě posádky autonomních vozidel.

V neposlední řadě stojí velká výzva i před zákonodárci, kteří se budou muset začít bavit o možnosti zavedení takového právního rámce, který by umožnil fungování autonomních systémů řízení v tzv. bezsouhlasovém režimu, alespoň v minimálním rozsahu pro zajištění bezpečnosti dopravy tak, aby právní regulace nebyla zásadní brzdou rozvoje a provozu vozidel s autonomními systémy řízení.

8. POUŽITÉ ZDROJE

[1] Addressing the autonomous vehicle data problem [online]. Internetové stránky DXC.technology [cit. 2021-08-03]. Dostupné z: https://dxc.com/us/en/insights/customer-stories/addressing-the-autonomous-vehicle-data-problem--.

[2] ANDRAŠKO, Jozef a MESARČÍK, Matúš. Čo vieš o mojom vozidle? Ochrana osobných údajov a kybernetická bezpečnosť v kontexte autonómnych vozidiel. Revue pro právo a technologie. [Online]. 2020, č. 22, s. 3-50. [cit. 2021-11-19]. Dostupné z: https://journals.muni.cz/revue/article/view/13841.

[3] ARAZ TAEIHAGH & HAZEL SI MIN LIM (2019) Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks, Transport Reviews, 39:1, 103-128, [cit. 2021-11-18]. Dostupné zde: https://doi.org/10.1080/01441647.2018.1494640

[4] BERT-JAAP KOOPS & RONALD LEENES (2014) Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law, International Review of Law, Computers & Technology, 28:2, 159-171, [cit. 2021-11-18]. Dostupné z: https://www.tandfonline.com/doi/abs/10.1080/13600869.2013.801589.

[5] BUTLER, Brandon. The future of auto safety is seat belts, airbags and network technology [online]. Internetové stránky networkworld.com. 2016 [cit. 13.1.2021]. Dostupné z: https://www.networkworld.com/article/3072486/the-future-of-auto-safety-is-seat-belts-airbags-and-network-technology.html

[6] BYGRAVE, L. A. Data protection by design and by default: Deciphering the EU's legislative requirements. Oslo Law Review. [online] 2017. 4(2), 105-122 [cit. 2021-11-12]. Dostupné z: https://heinonline.org/HOL/P?h=hein.journals/oslo4&i=106

[7] CAVOUKIAN, A. Privacy by design: The 7 Foundation Principles. [online] 2009 [cit. 2021-11-12]. Dostupné z: https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

[8] CAVOUKIAN, A. Privacy by design: The 7 Foundation Principles. Implementation and Mapping of Fair Information Practices. [online] 2010. [cit. 2021-11-12]. Dostupné z: https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf

[9] Commission Nationale Informatique & Libertés. Compliance package – Connected vehicles and personal data [online]. Internetové stránky cnil.fr. 2018. [cit. 2021-11-29]. Dostupné z: https://www.cnil.fr/sites/default/files/atoms/files/cnil_pack_vehicules_connectes_gb.pdf

[10] Connected Automated Driving Roadmap [online]. ERTRAC [cit. 2021-08-03]. Dostupné z: https://www.ertrac.org/uploads/images/ERTRAC2019-Connected-Automated-Driving-Roadmap%20-2019-04-04.pdf.

[11] DAG WIESE SCHARTUM, Making privacy by design operative, International Journal of Law and Information Technology, Volume 24, Issue 2, Summer 2016, Pages 151–175. [cit. 2021-08-03]. Dostupné z: https://doi.org/10.1093/ijlit/eaw002

[12] Evropská Komise. Bílá Kniha o umělé inteligenci – evropský přístup k excelenci a důvěře. [online] COM(2020) 65 final. 2020. [cit. 2021-11-12]. Dostupné z: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_cs.pdf

[13] Evropská Komise. Návrh Nařízení Evropského Parlamentu a Rady, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (Akt o umělé inteligenci) a mění určité legislativní akty Unie [online] COM/2021/206 final. 2021. [cit. 2021-11-12]. Dostupné z: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0002.02/DOC_1&format=PDF

[14] Evropský sbor pro ochranu osobních údajů. Pokyny č. 01/2020 ke zpracování osobních údajů v souvislosti s propojenými vozidly a aplikacemi souvisejícími s mobilitou. [online] 2021. [cit. 2021-08-03]. Dostupné z: https://edpb.europa.eu/system/files/2021-03/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_en.pdf

[15] Evropský sbor pro ochranu osobních údajů. Pokyny č. 4/2019 k článku 25 - záměrná a standardní ochrana osobních údajů [online] 2019. [cit. 2021-08-03]. Dostupné z: https://edpb.europa.eu/system/files/2021-04/
edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_cs.pdf

[16] Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications [online]. European Data Protection Board. 2020 [cit. 2021-08-03]. Dostupné z: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf.

[17] HES, Ronald a BORKING, John. Privacy-Enhancing Technologies: The Path to Anonymity. [online]. 1995 [cit. 2021-08-03]. Dostupné z: https://www.researchgate.net/profile/John-Borking/publication/243777645_Privacy-Enhancing_Technologies_The_Path_to_Anonymity/links/56e6850708ae68afa1138167/Privacy-Enhancing-Technologies-The-Path-to-Anonymity.pdf.

[18] International Conference of Data Protection and Privacy Commissioners. Agenda. [online] 2011. [cit. 2021-11-12]. Dostupné z: http://www.privacyconference2011.org/htmls/adoptedResolutions/2011_Mexico/2011_EC_A_001_AGENDA_33_ICDPPC_ENG.pdf

[19] International Conference of Data Protection and Privacy Commissioners. Adopted Resolutions. [online] 2011. [cit. 2021-11-12]. Dostupné z: http://www.privacyconference2011.org/index.php?lang=Eng

[20] International Conference of Data Protection and Privacy Commissioners. Resolution on Privacy by Design. [online] 2010. [cit. 2021-11-12]. Dostupné z: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf.

[21] International Data Protection Commissioners Conference. Global Privacy Standards. [online] 2005. [cit. 2021-11-12]. Dostupné z: https://thepublicvoice.org/2006/12/global-privacy-standard.html

[22] JEŽOVÁ, D. Principle of Privacy by Design and Privacy by Default. Regional Law Review [online]. 2020, 127-140. [cit. 2021-11-12]. Dostupné z: https://heinonline.org/HOL/P?h=hein.journals/rgllr2020&i=130

[23] KOCIĆ, Jelena, JOVIČIĆ, Nenad and DRNDAREVIĆ, Vujo. *Sensors and Sensor Fusion in Autonomous Vehicles*, 26th Telecommunications Forum (TELFOR) [online], 2018, pp. 420-425, [cit. 2021-11-29]. Dostupné z: https://ieeexplore.ieee.org/document/8612054

[24] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

[25] Nařízení Evropského parlamentu a Rady (EU) 2018/858 ze dne 30. května 2018 o schvalování motorových vozidel a jejich přípojných vozidel, jakož i systémů, konstrukčních částí a samostatných technických celků určených pro tato vozidla a o dozoru nad trhem s nimi, o změně nařízení (ES) č. 715/2007 a č. 595/2009 a o zrušení směrnice 2007/46/ES. Dostupné online z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32018R0858&from=CS

[26] Návrh Nařízení evropského parlamentu a rady o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů). 2012. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52012PC0011&from=CS.

[27] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., KOVAŘÍKOVÁ, K. GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář. 2. vydání. Praha: Wolters Kluwer ČR, 2018, str. 281.

[28] Pracovní skupina pro ochranu údajů zřízená podle článku 29. Stanovisko č. 5/2014 k technikám anonymizace [online]. 2014 [cit. 2021-08-03]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_cs.pdf.

[29] Předpis Evropské hospodářské komise Organizace spojených národů (EHK OSN) č. 107 – Jednotná ustanovení pro schvalování vozidel kategorie M2 nebo M3 z hlediska jejich celkové konstrukce [2015/922].

[30] Sdělení Komise ES o podpoře ochrany osobních údajů prostřednictvím technologií zvyšujících ochranu soukromí (PETs). 2007. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52007DC0228&from=EN

[31] Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. 1995. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=celex:31995L0046

[32] Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích). Dostupná z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32002L0058&from=CS

[33] Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles J3016_202104 [online]. SAE International [cit. 2021-08-03]. Dostupné z: https://www.sae.org/standards/content/j3016_202104/.

[34] WATSON, David P.; SCHEIDT, David H. Autonomous systems. Johns Hopkins APL technical digest. [online]. 2005, 26.4: 368-376. [cit. 2021-11-12]. Dostupné z: https://www.jhuapl.edu/Content/techdigest/pdf/V26-N04/26-04-Watson.pdf